

**Digital Ecosystems and Business Intelligence (DEBI) Institute  
Curtin Business School**

**An Architecture Framework for Enhanced Wireless Sensor Network Security**

**Pedram Radmand**

**This thesis is presented for the Degree of  
Doctor of Philosophy of  
Curtin University**

**April 2012**

## **Statement of Authorship**

Except where reference is made in the text of the thesis, this thesis contains no material published elsewhere or extracted in whole or in part from a thesis submitted for the award of any other degree or diploma.

No other person's work has been used without acknowledgment in the main text of the thesis.

This thesis has not been submitted for the award of any degree or diploma in any other tertiary institution.

Signed: \_\_\_\_\_

Mr Pedram Radmand

Date:

# Table of Contents

Statement of Authorship.....	I
1 Introduction.....	1
1.1 Introduction.....	1
1.2 Why Wireless Sensor Network?.....	1
1.2.1 Wireless Networks.....	2
1.2.2 Wireless Sensor Networks and Ad-hoc Networks.....	3
1.2.3 Wireless Sensor Network Architecture and Components.....	4
1.3 Applications of WSNs.....	6
1.4 WSN Security Challenges.....	8
1.4.1 Data Confidentiality.....	9
1.4.2 Data Authenticity.....	9
1.4.3 Data Integrity.....	10
1.4.4 Data Freshness.....	10
1.4.5 Availability.....	11
1.4.6 Access Control.....	11
1.4.7 Self-organisation.....	11
1.4.8 Time Synchronisation.....	12
1.4.9 Secure Localisation.....	12
1.4.10 Message-based, Node-based and Network-based Security Requirements.....	12
1.5 Wireless Network Vulnerabilities.....	13
1.6 Motivation of the Research.....	13
1.7 Objectives of the Research.....	14
1.8 Significance of the Research.....	14
1.9 Plan of The Thesis.....	16
1.10 Conclusion.....	17
2 Taxonomy of WSN Security and Attacks.....	18
2.1 Introduction.....	18
2.2 WSN Constraints and Issues.....	18
2.2.1 Wireless Communication.....	18
2.2.2 Wireless Network Issues.....	19
2.3 Wireless Sensor Network Environment.....	21
2.3.1 Device Limitations.....	22
2.3.2 Deployment Constraints.....	23
2.4 WSN Security Barriers and Challenges.....	24
2.5 WSN Security Overview.....	24
2.6 Wireless Network Attacks category.....	25
2.6.1 External and Internal Attacks.....	25
2.6.2 Applicable Passive Attacks.....	25
2.6.3 Applicable Active Attacks.....	26
2.7.1 Misbehaviour Attack.....	27
2.7.2 Replay Attack.....	27
2.7.3 Physical Tampering.....	28
2.7.4 Denial of Service (DoS).....	28
2.8 Message-based, Node-based, and Network-based Attacks.....	34
2.9 WSN Attack Strategies.....	35
2.10 Attack Outcomes.....	41
2.11 Advanced WSNs Elements.....	42
2.11.1 ZigBee.....	42
2.11.2 ZigBeePRO.....	42
2.11.3 WirelessHART.....	43
2.11.4 ISA100.11a.....	43
2.12 Conclusion.....	43
3 Literature Survey of State of The Art WSN Security.....	44
3.1 Introduction.....	44
3.2 State of The Art in WSN Security.....	44
3.2.1 Key Management.....	44
3.2.2 Symmetrical Key Management.....	44

3.2.3	Asymmetrical Key Management .....	45
3.2.4	Authentication .....	46
3.2.5	Secure Routing .....	46
3.2.6	Combating Traffic Analysis .....	47
3.2.7	Intrusion Detection .....	47
3.2.8	Secure Data Aggregation.....	48
3.2.9	Secure Localization of Sensor Node.....	48
3.2.10	Time Synchronization .....	48
3.3	Low-Rate Wireless Personal Area Network Technology - IEEE 802.15.4.....	49
3.3.1	Protocol Layers.....	49
3.3.2	Security Overview .....	51
3.3.3	Addressing.....	52
3.3.4	MAC Security.....	53
3.3.5	Keying Models .....	57
3.3.6	Data Payload.....	59
3.3.7	Access Control List .....	62
3.3.8	Security Issues .....	62
3.4	High Level Communication Protocols Technology - ZigBee .....	65
3.4.1	ZigBee .....	66
3.4.2	ZigBee Architecture .....	66
3.4.3	Protocol Layers.....	67
3.4.4	Protocol Devices.....	70
3.4.5	Network Topology.....	70
3.4.6	ZigBee Routing Protocols .....	71
3.4.7	ZigBee Installation and Configuration .....	72
3.4.8	Starting a Network.....	73
3.4.9	Joining a Network.....	73
3.4.10	Message Addressing.....	74
3.4.11	Establishing Communication between Two Nodes .....	74
3.4.12	Binding .....	75
3.4.13	Message Routing and Route Discovery.....	76
3.4.14	Co-existence and Interoperability.....	77
3.4.15	Profile .....	78
3.4.16	Attribute and Cluster .....	79
3.4.17	ZigBee Cluster Library.....	79
3.4.18	Discovery.....	79
3.4.19	Security.....	80
3.5	ZigBeePRO .....	82
3.5.1	Key Transport.....	84
3.5.2	Trust Centre.....	84
3.5.3	Security Issues.....	85
3.6	WirelessHART .....	86
3.6.1	Protocol Devices.....	86
3.6.2	Protocol Layers.....	88
3.6.3	Security Overview .....	89
3.6.4	Keying Models .....	90
3.6.5	Data Encryption.....	90
3.6.6	Security Issues.....	90
3.7	ISA 100 .....	90
3.7.1	Protocol Devices.....	92
3.7.2	Protocol Layers.....	92
3.7.3	Security Overview .....	94
3.7.4	Keying Model.....	95
3.7.5	Data Encryption.....	97
3.7.6	The Join Process .....	97
3.7.7	Key Update.....	97
3.7.8	Security Issues .....	97
3.8	Key Findings .....	98
3.8.1	State of The Art WSN Security Technology Compression Comparison.....	98



3.8.2	The Fundamentals of the Security Features.....	98
3.8.3	Strengths and Weaknesses of Security Techniques.....	99
3.9	Summary of the WSN Security Strengths and Weaknesses.....	102
3.10	Conclusion.....	103
4	Problem Definition.....	104
4.1	Introduction.....	104
4.2	Problems in WSN.....	104
4.3	Research Gap in ZigBee.....	105
4.4	Problem Definition in ZigBee.....	105
4.5	ZigBee Security Schema Vulnerability.....	105
4.5.1	ZigBee Threat Countermeasures.....	106
4.5.2	Defending Against Denial of Service (DoS) Attacks.....	115
4.6	Remaining Attacks.....	118
4.7	Research Issues.....	120
4.8	Research Approach.....	120
4.9	Research Question.....	121
4.10	Choice of Research Methodology.....	121
4.10.1	The Science and Engineering-based Research Method.....	121
4.11	Conclusion.....	123
5	Overview of the End-to-end WSN Security Architecture Framework.....	124
5.1	Introduction.....	124
5.2	The Conceptual Framework for Enhancing ZigBee WSN Security.....	124
5.3	Attack Execution Platform Component.....	127
5.3.1	Set-up of ZigBee Network.....	127
5.3.2	Applying Existing Security Schema.....	127
5.3.3	Executing Attack.....	127
5.3.4	Key Requirement.....	127
5.3.5	Behaviour Analysis.....	129
5.3.6	Record Vulnerability.....	129
5.4	Remaining Attacks and Solution Discovery Components.....	129
5.5	Recording Configurations and Design.....	131
5.6	Adding the New Solutions to the Countermeasure IList.....	131
5.7	Summary of the Framework Design.....	132
5.8	Conclusion.....	132
6	Design and Implementation of the Framework Architecture and Carrying Out Security Measures.....	134
6.1	Introduction.....	134
6.2	Hardware and Software Requirement for Development.....	135
6.3	Hardware and Software Set up and Configuration.....	138
6.3.1	Implementation the board with IAR.....	139
6.4	Software Application Development.....	140
6.5	Network Configuration.....	141
6.6	Configuring Destination Address and Performing Counter Attacks.....	144
6.7	Summary of Implementation.....	151
6.8	Conclusion.....	151
7	Evaluation of the Security Risk and Execution Counter Attack.....	152
7.1	Introduction.....	152
7.2	Manual-based Network Setup for Replay Counter Attack.....	152
7.3	Automated method through Network Set-up for Counter Replay Attack.....	153
7.4	Implementation of Counter Measure Against Attacks.....	157
7.4.1	Eavesdropping.....	157
7.4.2	Eavesdropping Solution.....	159
7.4.3	DoS Attack.....	159
7.4.4	DoS Solution.....	160
7.4.5	Replay Attack.....	162
7.4.6	Solutions for Replay Attack.....	169
7.4.7	Physical Attack.....	173
7.4.8	Physical Attack Solution.....	175
7.5	ZigBee Security Quality of Services.....	175
7.5.1	Design of the Network.....	175

7.5.2	Configuration of the Network.....	176
7.6	Summary of the Risk Evaluation and Counter Measures.....	177
7.7	Conclusion.....	178
8	Evaluation of the Proposed Architecture Framework in Statoil Remote Operation Environment.....	179
8.1	Introduction.....	179
8.2	The Case Study.....	179
8.3	Project Scope.....	179
8.4	Statoil WSN Lifecycle.....	180
8.5	Information Security in Integrated Operations.....	182
8.6	Security Requirements.....	182
8.7	Generic Attacks on Oil and Gas Wireless Network Installations.....	185
8.8	Taxonomy of Applicable Attacks on Oil and Gas WSN Installations.....	185
8.8.1	Active and Passive Attacks.....	185
8.8.2	The Security Architecture of Sensor Networks.....	187
8.9	Information Security Management System.....	188
8.9.1	ISO 27001.....	189
8.9.2	Information Security Requirements for Process Control, Safety and Support.....	189
8.10	Statoil WSN Networks.....	192
8.11	ICT Equipment in Technical Networks.....	192
8.11.1	Smart Wireless Gateway.....	193
8.11.2	SMARTMESH IA-510.....	194
8.12	Overview of WirelessHART Framework Experiment Set-up.....	194
8.12.1	WirelessHART Routing Protocols.....	195
8.12.2	Installation and Configuration of WirelessHART.....	196
8.12.3	Access@Plant.....	197
8.12.4	Access to the Wireless Gateway.....	198
8.13	Common Statoil Configurations.....	198
8.13.1	Set-up 1: Sensor Data to PCDA over Serial MODBUS.....	198
8.13.2	Set-up 2: Sensor Data via MODBUS over TCP 1.....	200
8.13.3	Set-up 3: Sensor Data to PCDA via MODBUS over TCP 2.....	200
8.14	Summary of the Case Study.....	201
8.15	Conclusion.....	203
9	Guidelines and Recommendations.....	204
9.1	Introduction.....	204
9.2	Guidelines and Recommendations.....	204
9.2.1	Jamming Recommendation.....	204
9.2.2	Physical Tampering Recommendation.....	205
9.2.3	Eavesdropping Recommendation.....	205
9.2.4	Flooding Attack Recommendation.....	207
9.2.5	Replay Attack Recommendation.....	207
9.3	Conclusion.....	208
10	Recapitulation and Future Work.....	209
10.1	Introduction.....	209
10.2	Recapitulation of Research Issues.....	210
10.3	Contribution of the Thesis.....	211
10.3.1	Contribution 1:.....	211
10.3.2	Contribution 2:.....	211
10.3.3	Contribution 3:.....	211
10.3.4	Contribution 4:.....	212
10.3.5	Contribution 5:.....	212
10.3.6	Contribution 6:.....	212
10.4	Contribution in Terms of Research Questions.....	213
10.5	Future Work.....	213
10.6	Conclusion.....	214
11	References.....	215
12	Appendix.....	223

## List of Figures

Figure 1-1: The typical WSN network.....	5
Figure 1-2: The components of a typical sensor node.....	6
Figure 1-3: WSN Security Concerns.....	13
Figure 2-1: ACK-MAC Layer Attack.....	28
Figure 2-2: Denial Service Attack.....	29
Figure 2-3: Physical Layer Attack.....	29
Figure 2-4: The Link Layer Attacks.....	30
Figure 2-5: The Network Layer Attacks.....	31
Figure 2-6: The Security Classification of Sensor Networks.....	35
Figure 3-1: Data Packet Format.....	52
Figure 3-2: Acknowledge Packet Format.....	52
Figure 3-3: IEEE 802.15.4 MAC frame.....	54
Figure 3-4: Security in the IEEE 802.15.4 MAC frame.....	55
Figure 3-5: Data Payload Encryption Mechanism.....	55
Figure 3-6: AES-CTR.....	59
Figure 3-7: AES-CTR Mechanism.....	59
Figure 3-8: AES-CBC-MIC counter block chaining mode.....	59
Figure 3-9: AES-CBC-MIC.....	60
Figure 3-10: AES-CCM.....	60
Figure 3-11: ACL Entry Format.....	61
Figure 3-12: Performing an XOR of two cipher-text.....	64
Figure 3-13: Basic Software Architecture.....	66
Figure 3-14: ZigBee functional layer architecture and protocol stack.....	69
Figure 3-15: Addressing.....	74
Figure 3-16: Indirect addressing.....	75
Figure 3-17: MAC association.....	81
Figure 3-18: Network re-join.....	81
Figure 3-19: Standard Security Mode.....	82
Figure 3-20: High Security Mode.....	83
Figure 3-21: WirelessHART Standard.....	87
Figure 3-22: Application protocols supported by ISA100.....	91
Figure 3-23: Overall Schema of Wireless Standards.....	98
Figure 4-1: The process of Attacks Filtering.....	118
Figure 4-2: Overview of science and engineering-based research method.....	123
Figure 5-1: The BESTSEC Model.....	127
Figure 5-2: ZigBee Attack Categories.....	128
Figure 6-1: SmartRF05EB with CC2530EM.....	136
Figure 6-2: IAR EW.....	139
Figure 6-3: Data on Coordinator LCD.....	140
Figure 6-4: Encrypted packet unicast coordinator and unicast End-device.....	146
Figure 6-5: Encrypted payload coordinator and end-devices broadcast.....	147
Figure 6-6: Encrypted payload coordinator unicast end-device broadcast.....	148
Figure 6-7: Packet captured no security with unicast address.....	149
Figure 6-8: Packet captured no security unicast coordinator broad cast end-device.....	150
Figure 7-1: Test-bed for Manual Attack.....	153
Figure 7-2: Programming RZ RAVEN USB by Atmel JTAGICE mkII.....	156
Figure 7-3: Test-bed for Automatic Attack.....	157
Figure 7-4: Grabbing the key by packet sniffer.....	158
Figure 7-5: KillerBee Tool for grabbing keys.....	159
Figure 7-6: Packet injection by Smart RF Studio.....	161
Figure 7-7: Intel 8051 Microcontroller.....	162
Figure 7-8: Program Status Word Register Flags.....	163
Figure 7-9: The procedure of executing Replay attack.....	164

Figure 7-10: Selecting packets from the packet sniffer .....	165
Figure 7-11: Packet injection by the Smart RF Studio packet.....	166
Figure 7-12: KillerBee tool for grabbing keys. ....	168
Figure 7-13: KillerBee tool for capturing packets.....	168
Figure 7-14: Wireshark packet captured with security schema .....	169
Figure 7-15: The procedure of executing Replay attack.....	169
Figure 7-16: Network Addressing .....	170
Figure 7-17: Attack Scenario .....	172
Figure 7-18: Replay Attack architecture .....	173
Figure 7-19: The Random Number Generator structure.....	175
Figure 7-20: The point-to-point communication .....	177
Figure 8-1: The life cycle of Oil and Gas.....	181
Figure 8-2: WSN Security Concerns .....	188
Figure 8-3: Taxonomy of WSN exposure attacks .....	189
Figure 8-4: WirelessHART Mesh Networking .....	196
Figure 8-5: Sensor data to PCDA over serial MODBUS. ....	200
Figure 8-6: WSN Dataflow through Firewall.....	200
Figure 8-7: Sensor data via MODBUS over TCP, wireless gateway and PCDA in the same LAN.....	201
Figure 8-8: Sensor data to PCDA via MODBUS over TCP, wireless gateway and PCDA in separate LAN's. ....	202

## List of Tables

Table 2:1 The list of Exposure Attack Outcomes .....	42
Table 3:1 IEEE 802.15.4 Standard Specs .....	50
Table 3:2 Cryptographic Protection By the Various Securities .....	61
Table 3:3 WSN Comparison .....	100
Table 4:1 List of ZigBee Threat Countermeasures .....	106
Table 4:2 Sensor Network Layers and DoS Attacks / Defenses .....	115
Table 6:1 Coordinator Authentication Configuration Options .....	143
Table 6:2 The Security Schema Configurations .....	144
Table 7:1 The average lost packet ratio in ZigBee with and without security schema.....	178

## THESIS SUMMARY

This thesis develops an architectural framework to enhance the security of Wireless Sensor Networks (WSNs) and provides the implementation proof through different security countermeasures, which can be used to establish secure WSNs, in a distributed and self-healing manner. Wireless Sensors are used to monitor and control environmental properties such as sound, acceleration, vibration, air pollutants, and temperature. Due to their limited resources in computation capability, memory and energy, their security schemes are susceptible to many kinds of security vulnerabilities. This thesis investigated all possible network attacks on WSNs and at the time of writing, 19 different types of attacks were identified, all of which are discussed including exposures to the attacks, and the impact of those attacks. The author then utilises this work to examine the ZigBee series, which are the new generation of wireless sensor network products with built-in layered security achieved by secure messaging using symmetric cryptography. However, the author was able to uniquely identify several security weaknesses in ZigBee by examining its protocol and launching the possible attacks. It was found that ZigBee is vulnerable to the following attacks, namely: eavesdropping, replay attack, physical tampering and Denial of Services (DoS). The author then provides solutions to improve the ZigBee security through its security schema, including an end-to-end WSN security framework, architecture design and sensor configuration, that can withstand all types of attacks on the WSN and mitigate ZigBee's WSN security vulnerabilities.

## ACKNOWLEDGEMENT

I would especially like to express my gratitude and heartfelt thanks to my supervisor, Professor Elizabeth Chang, for her excellent supervision and support in this research. She is a motivator, a challenger, and above all a helpful friend. Her constructive comments were invaluable for the completion of this thesis. Her encouragement has been an inspiration to me. I would like to express my sincere thanks to my co-supervisor Dr. Alex Talevski. His research expertise, his research community network, and his advice in setting up my research foundation have been a great help. I would also like to thank Statoil Company who provided me with an opportunity to investigate an oil and gas industrial project. I would also like to express deep gratitude to Zinaida Benenson at the University of Mannheim, Germany.

My thanks also extend to the staff and students at DEBII and University of Mannheim for providing such a friendly work environment. It has been an enjoyable experience interacting with these wonderful and talented people. Their advice and friendship have helped me to enjoy and learn a great deal from my PhD experience.

In short, without my supervisors' generous guidance and encouragement, it would have been difficult to achieve the goals and objectives of this research. The benefit of their guidance will not be limited to this research; I will also benefit from their knowledge, advice and wisdom in my future endeavors.

I would also like to thank my mother Maryam Behbahani, and my grandmother Farah Zohreh as well as my step-father, Homayoon Mohajer. I could never have reached my goal without their full support and continuous encouragement.

## List of Publications

1. Radmand, P., A. Talevski, et al. (2010). Taxonomy of Wireless Sensor Network Cyber Security Attacks in the Oil and Gas Industries. *Advanced Information Networking and Applications (AINA)*, 2010 24th IEEE International Conference on Perth Australia: 949-957.
2. Radmand, P., M. Domingo, et al. (2010). ZigBee/ZigBee PRO Security Assessment Based on Compromised Cryptographic Keys. *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, 2010 International Conference on Fukuoka Japan: 465 - 470
3. Radmand, P., A. Talevski, et al. (2010). Comparison of industrial WSN standards. *Digital Ecosystems and Technologies (DEST)*, 2010 4th IEEE International Conference on Dubai UAE: 632 - 637.
4. Radmand, P., J. Singh, et al. (2011). "The impact of security on voip call quality." *Journal of Mobile Multimedia* **7**(1): 113-128.



# 1 Introduction

## 1.1 Introduction

As organizations begin to implement the wireless network, they must ensure manageability, performance, and full security including authorization, authentication, confidentiality and integrity[1]. Wireless networks are susceptible to various security issues; hence, security should be assured in sensitive industries. Security processes, procedures, standards, risks, third-party agreements, change management, references, monitoring and maintenance, update, culture, including attitudes, knowledge and values, must be developed among all employees who are involved in this technology. An organisation has a significant job to do when it comes to increasing awareness related to information security. The challenges need to be faced at many levels since technical, human and organisational aspects must be taken into consideration [2]. Therefore, a framework is required to ensure security at all levels such as technical, human and organizational.

International standards such as the IEEE 802.11a/b/g/n for wireless local area networks and the IEEE 802.15.4 for low-rate wireless personal area networks, as well as numerous standards for Radio-Frequency Identification (RFID) enable application development such as wireless networking, sensing, monitoring, control, and asset tracking [3]. Wireless Sensor Networks (WSNs) are generating significant interest as industries move into the wireless domain. Such technology has the potential to be beneficial in many regards [4] such as remote operation in oil and gas industry or smart energy consumption monitoring.

## 1.2 Why Wireless Sensor Network?

Companies need to optimise their operations to effectively compete in today's global economy. Decreasing overhead costs is necessary to help companies stay ahead of the market competition. Wiring expenses are part of this overhead that a company must consider. In fact, one of the most attractive reasons for implementing a wireless network over the traditional wired network is the matter of cost savings [5].

There are several ways in which a wireless network can save costs for a company in terms of Total Cost of Ownership (TCO). This refers to a financial estimate designed to assess direct and indirect costs. 'Costs' involve more than a simple phone bill at the end of the month and include hardware requirements, training costs, and potential switch-over costs and loss of business during transition. There are several ways that wireless technology helps to

save the business money in terms of TCO such as lower cost of implementation, lower cost of maintenance and support, and reduced network infrastructure [6, 7].

Wireless technology is proving to be efficient and cost-effective in communications systems as a business solution for small and medium sized enterprises, which are looking for a means to improve their business and effectiveness in the most forward-looking manner possible. However, in order to appropriately achieve this, the implementation of security protocols in wireless networks is necessary because it reduces the risks associated with WSNs [1].

Wireless networks utilize radio waves and microwaves to maintain communication channels between devices. This wireless networking technology is a more modern alternative to wired networking. Wireless networks have both advantages and disadvantages in comparison with wired alternatives. Their advantages include: mobility, flexibility and elimination of cables as well as the provision of low-cost solutions to a variety of real-world challenges.

Recent advances in tiny microprocessors, low-power circuit designs, and radio technologies have made possible a new technological vision referred to as 'WSNs'. WSNs have attracted great attention not only in industry but also in academia because of their enormous application potential and unique security challenges. A typical sensor network can be considered as a combination of a number of low-cost sensor nodes along with very limited computation and communication capability, memory space, and energy supply.

### 1.2.1 Wireless Networks

There are many different standards that promote wireless communication in an enterprise setting. The following standards have produced promising results in wireless communication.

- **Wi-Fi** - International standards such as the IEEE Std 802.11a/b/g provide a solid foundation for personal and enterprise wireless local area networks[8]. WiFi is the popular name for the wireless Ethernet 802.11b standard for Wireless Local Area Network (WLAN). Wire line Local Area Networks (LANs) emerged in the early 1980s as a way to allow collections of computers, terminals, and other devices to share resources and peripherals such as printers, access servers, or storage devices. The Ethernet is one of the most popular LAN technologies. Over the years, the IEEE has succeeded in introducing a diverse array of media for Ethernet standards

to support higher capacity LAN. The 802.11x family of Ethernet standards has been introduced for wireless LANs [9]. A device working with WiFi, such as a personal computer, video game console, smartphone, tablet, or digital audio player, can connect to the Internet via a wireless network.

- **Bluetooth** – This is a proprietary open wireless technology standard to exchange data from fixed or mobile devices over short distances by creating personal area networks (PANs) . This technology applies short wavelength radio transmissions in the (industrial, scientific and medical) ISM band from 2400-2480 MHz [10].
- **LR-WPAN- IEEE Std 802.15.4**– This protocol addresses low-rate wireless personal area networks, presented as LR-WPAN, and focuses on enabling wireless sensor networks. This standard network is characterized by its high level simplicity and low cost and power consumption. It has a frequency similar to that of WiFi, which is 2.4 GHz, and includes ISM band [11].

### 1.2.2 Wireless Sensor Network and Ad-hoc network

A sensor is a device that reacts to changes in conditions and returns a value of a physical quantity or parameter. It converts the signal into value for visualization, processing, recording or automation. This information can be applied to monitor the operation of a factory, optimize production and improve factory performance. WSNs are comprised of a large number of spatially distributed autonomous devices that may collect data using a wireless medium. They may be used to cooperatively control and monitor physical or environmental conditions such as temperature, sound, vibration, pressure, motion or pollutants at different locations [12].

An ad-hoc network is defined as a local area network (LAN) that is built spontaneously once devices connect, rather than relying on a base station to coordinate the flow of messages to other nodes. It means that every single node forwards packets to and from each other [13].

WSNs are ad-hoc networks which are formed by autonomous nodes and communicate via radio without any additional backbone infrastructure. This means that if two nodes are not within transmission range, they communicate through intermediate nodes relaying their message [14].

WSNs demonstrate several unique properties in comparison with their wired counterparts such as large scale of deployment, mobility of nodes, temporary installations, redundancy, and dynamic network topologies. However, sensor nodes have constraints on the operational environment, energy, memory, computation speed and bandwidth [12].

WSNs consist of one or several base stations and perhaps hundreds or thousands of sensor nodes. The sensor nodes include low-cost sensing devices, a mini processor, and a battery-powered module. However, the price and size of sensors depend on applications, but generally it is less than US\$1.0, and the size is a few cubic millimetres. Sensor nodes report data or aggregated data to the base station and it makes decisions according to the aggregated data to assign tasks to sensors.

The specific application of WSNs, which is an important factor in determining the feasibility of the scheme, has been overlooked to a large extent in the existing literature.

A major benefit of sensor networks is that they perform in-network processing to reduce large streams of raw data to useful aggregated information. Sensors are self-organized into a network to sense environmental properties such as temperature, sound, vibration, humidity and so on from the surrounding environments as well as monitor surrounding information in an unattended environment.

### **1.2.3 Wireless Sensor Network Architecture and Components**

It should be mentioned that WSNs have to be capable of self-healing and self-configuring in order to provide a robust and reliable multi-hop network for rough RF environments. This can be achieved by the use of dynamic routing protocols. A routing protocol provides a mechanism for a wireless sensor to store and constantly update neighbour information, as well as handling network connection requests from other wireless sensors. Importantly, they must provide self-configurable, dynamic and adaptive application services [15].

A typical WSN network is illustrated in Figure 1.1. As can be seen, the network includes sensors, base station and control room to monitor data within the network. This data can include any environmental properties such as temperature, humidity, vibration and so on.

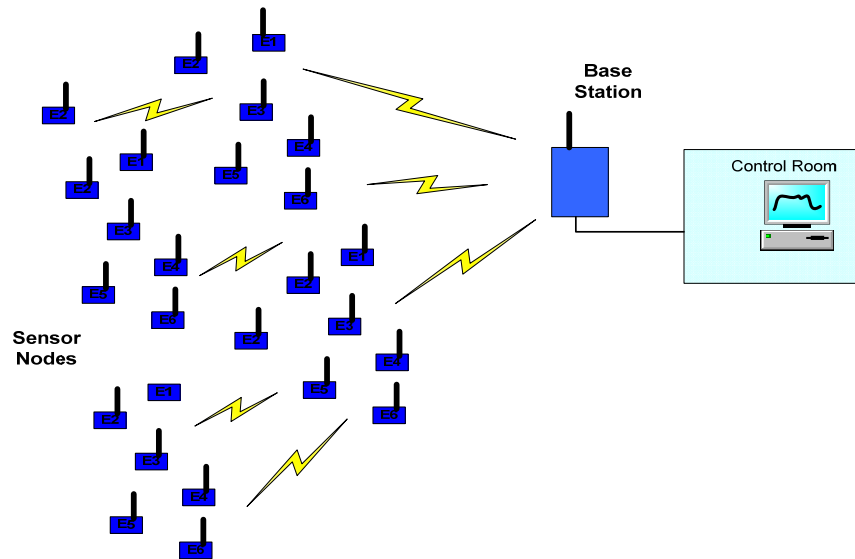


Figure1-1: The typical WSN network.

A typical sensor node has several components: a communication unit with an antenna which has the ability to send or receive packets, a processing unit, which is a microcontroller, to process data and schedule relative tasks, several kinds of sensing units to sense the environment data, and batteries providing energy supply, and a user interface.

A typical wireless sensor consists of the following components:

- **Sensing Unit** - A sensing unit measures information about a physical phenomenon and converts the measurements to a digital representation via an Analog/Digital-converter [3].
- **User Interface** - A user interface may display device information and interact with users in order to realize a certain required behaviour [3].
- **Processing Unit** - As a part of its processing unit, it has a processor, main board, memory (RAM) and storage (flash) components. This unit usually analyses and processes sensor data, as well as handling the network protocol, controls the local Radio Frequency (RF) transceiver and application software. Wireless sensors usually have very limited resources in terms of processing capacity, available memory and storage space due to strict low-power requirements. WSNs are required to execute software implementations of complex networking algorithms with real-time requirements [3].
- **Communication Unit** - The communication unit provides the wireless interface, and consists of an RF transceiver and an antenna [3].

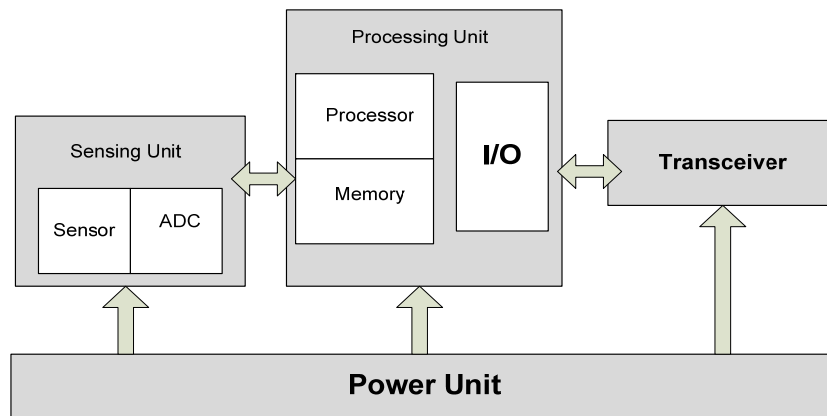


Figure1-2: The components of a typical sensor node

The components of a typical sensor node are illustrated in Figure 1-2 where a sensor network includes a power unit to supply energy, a processing unit to process data, a sensing unit to sense environmental properties, and at the end, a transceiver for data transmission.

### 1.3 Applications of WSNs

WSNs are event-driven networks widely applied for military and civilian operations. Sensors can be deployed to continuously monitor and report environmental properties. This is a very important improvement in comparison with human operators who had to move to the fields and take manual measurements periodically, resulting in less data, higher errors, higher costs and significant interference with life conditions of the observed species. The most important aspect of WSNs is that they reduce or eliminate the need for human involvement in information gathering in certain applications including oil and gas, agriculture, health, environment, the military and so on [16].

- **Oil and Gas** - The monitoring of oil and gas plants using sensors allows for greater insight into safety and operational performance. However, as a result of strict installation regulations of powered sensors near oil and gas fittings, the introduction of new sensors to optimize end-of-lifecycle plants has been expensive, complex and time consuming. Controlling oil and gas infrastructure is highly complex. It requires many sensors which monitor plant equipment. A delicate and accurate balance of flows, temperatures, pressures, and other parameters must be maintained to ensure safe and productive operation [3].
- **Agriculture** - In agricultural application, sensors are scattered over a farmland to monitor and measure any changes in water or chemicals. For instance, if the fertility points are below the requirement, the farmer can gain information from

sensors and as a result soil can be fertilized appropriately. In addition, sensors can also be applied to monitor the nutrition and health indexes of cattle on farms. WSNs can accurately report on animal species and collect data concerning their habits, population, or position to farmers. There are numerous examples of environment monitor applications of WSNs.

- **Seismic data** - Sensors can be installed on bridges or buildings to collect data about earthquake vibration patterns. Because wired facilities cannot research the deeply embedded points, wireless sensors are applied to detect marine ground floor erosion.
- **Pollution** - Pollution detection systems can also benefit from WSNs. Also, sensors are deployed to monitor the current levels of polluting substances in a town or a river to identify the source of anomalous situations, if there is any. Also, polluting substances in rain and water levels and forecast flooding can be monitored [17].
- **Military** - The military can also take advantage of this technology. For example, WSNs can be deployed behind enemy lines to monitor and observe movements/presence of troops and/or collect geographical information on the deployment area [18]. Due to the characteristics of WSN, which is wireless, low-cost and sustainable, it can be applied in many various areas.
- **CCTV Camera** - CCTV cameras and wireless IP telephones may be used to visualize and interact with the production floor staff. Such data is then used to make informed just-in-time decisions.

Furthermore, through the use of intelligent techniques and the monitoring of key historical operation properties, sensor data may be used to realize certain characteristics and patterns in typical operations to further promote a safe workplace and optimize production [3].

WSNs have several unique properties compared to their wired counterparts. However, each sensor node has constraints on operational environment, energy, memory, computation speed and bandwidth [12]. Many WSN applications require secure communications. Due to the absence of physical protection, the security of WSNs is extremely important [12].

Previous research investigations that deal with accessibility, availability and performance of WSNs have proven to be satisfactory and also recent advances in wireless technology have enabled low-cost wireless solutions capable of robust and reliable communication. However, WSN security issues have been poorly investigated in industry and academia [19]. Even though security for WSNs has been studied over the last years, the majority of the literature has focused on some assumed vulnerabilities along with corresponding countermeasures [3].

## 1.4 WSN Security Challenges

Availability, stability and reliability are the strict requirements of industrial networks. These requirements can be achieved by using self-organizing, self-healing and self-configuring multi-hop, ad-hoc networks. Time-varying network topology, power constraints, and the characteristics of the wireless channel cause some issues in network routing. If the network must have one hundred percent data reliability, it should be capable of dealing with temporary or permanent loss of any communication link. In wireless communication, the performance can be affected by any noise interference. Redundant paths are the solution to combat this problem so that alternate routes are available if one or more of the communication links fails [19].

Many WSN applications require secure communications. Due to the absence of physical protection, the security of WSNs is of paramount importance [12].

WSNs are additionally vulnerable to various security breaches because they are usually deployed in unattended environments and use unreliable radio communication. Due to various attacks, end users may lose or receive incorrect sensing data, and this may lead to making wrong decisions. This may be dangerous in environments requiring battlefield surveillance or environmental monitoring. Therefore, proper security mechanisms must be applied in order to keep networks secure.

A level of security risk must be accepted with WSNs. A productive WSN environment is one where addressable security issues are dealt with and others are managed and accepted. In industry specific configurations, this may mean that WSN devices are not ultimately relied on for critical tasks; they are used only as a form of redundancy, and appropriate contingency, management and mitigation plans exist if their function is interrupted or modified.

WSNs form a significant part of the picture as all industries move into the wireless domain. Unfortunately, WSNs are prone to cyber threats and some industries are an attractive target for such attacks. This raises some serious concerns about the implementation of this technology. So, in a commercial environment, such networks must operate in a secure manner. A security breach may cause significant issues in terms of safety, reliability, availability, privacy and leakage of information [15]. The following sections define the typical network security requirements in an industrial setting.



### 1.4.1 Data Confidentiality

Data confidentiality is one of the most basic security requirements. The standard approach to providing confidentiality is to encrypt the data with a secret key that can be decrypted only by the receiving node [20]. Encryption prevents message recovery and prevents adversaries from learning any information about the messages. This type of encryption is known as ‘semantic security’. The semantic security encrypts the same plaintext twice and generates two different cipher-texts. If the encryption process is identical for both invocations on the same message, then semantic security is clearly violated, and the resulting cipher-texts are identical [21]. The common way of achieving semantic security is to use a unique nonce for each invocation of the encryption algorithm. The main purpose of a nonce is to add variation to the encryption process when there is little variation in a set of messages. The security of most encryption schemes does not rely on nonces being secret because the receiver must use the nonce to decrypt messages. Nonces are usually sent unencrypted and are located in the same packet as the encrypted data.

There are two different schemes in packet encryption. The first one is encrypting only the data part of the packet, and in other, encrypting the packet header and data. In sensor networks, the confidentiality relates to the following [21]:

As a sensor may contain sensitive data, it should not leak sensor readings to its neighbours.

A sensor network requires a secure channel to transmit sensitive data, such as key distributions.

Public sensor information, such as sensor identities and public keys, should also be encrypted as this provides extra protection against traffic analysis attacks.

### 1.4.2 Data Authenticity

Another major security concern is the authenticity of the source providing the data received from the WSN. False information can be fed by masquerading as a legitimate sensor node and transmitting this data to the receiver by an attacker. Hence, the receiver needs to ensure that the data used originates from the correct source and has not been tampered with. Besides information processing, authentication is required for administrative tasks over the network. These tasks include network reprogramming and controlling the sensor node duty cycle [21]. Identifying the source of the communicated message is important for networked devices.

The most common method of providing packet authentication is through a Message Authentication Code (MAC). Once a sender and receiver share a secret key, the sender can compute the Message Authentication Code of the data to be sent and embed it in the packet. Once the destination node receives a packet with a correct Message Authentication Code, it knows the source of the packet and realizes that the packet has not been modified during the transition [20].

### 1.4.3 Data Integrity

The data, which is transmitted by a legitimate source, might be modified or corrupted during transition. For example, some interference by other wireless technologies such as WiFi, Bluetooth and Mobile can be introduced by attackers adding and deleting some bits. The integrity of data ensures that the received data is complete and correct. It ensures that any received data has not been altered in transit. Message authentication and integrity will be increased by including a Message Authentication Code in every packet. Only authorised senders and receivers will be able to view the message as they share a secret cryptographic key which computes the Message Authentication Code. Authentication methods like Message Authentication Code are applied in the receiver to know the packet has been tampered or corrupted. Due to the unreliable nature of the wireless medium, packet loss or damage can occur without the presence of a malicious node in the network [21].

### 1.4.4 Data Freshness

Legitimate messages between two nodes may be monitored at that time by unauthorised parties, which will later be replayed with a valid Message Authentication Code to deceive the recipient into believing that the sent message originated from an authorised sender. WSNs need to ensure the freshness of each message. This requirement is important for key management since shared keys need to be changed over time. However, it takes time for new shared keys to be propagated to the entire network. In this case, it is easy for an attacker to use a replay attack, which protects against using sequential numbering, to join the network with an older key. The use of a nonce, or another time-related counter, can be added into the packet to ensure data freshness. These counters are reset every time a new key is created [21].

Besides security, data freshness is important in certain situations, especially when using sensor nodes to monitor mission critical operations. Any disruption or delay to the data received can have a negative impact on the operations or safety of the personnel/equipment.

### **1.4.5 Availability**

Traditional encryption algorithms used in fixed wired networking must be adapted to low-powered sensor nodes to maximise the use of nodes in a WSN. Some adaptations modify the encryption/decryption code to reuse as much code as possible. Some adaptations in security force strict limitations on the data access, or propose an unsuitable scheme (such as a central point scheme) in order to simplify the algorithm. However, all these approaches weaken the availability of a sensor node and WSN for the following reasons [22]:

Additional computation consumes additional energy. Without energy, the data will no longer be available.

A single point failure will be introduced in the central point scheme. This greatly threatens the availability of the network. The security requirement affects the operation and the availability of the whole WSN.

### **1.4.6 Access Control**

Access control prevents the participation of unauthorised parties in the network. Legitimate nodes such as a nodes list in the Access Control List (ACL) are able to detect and reject messages from unauthorised nodes. In fact, network authorisation is achieved through an ACL to ensure that sensor nodes and members of the support network are authorised.

The ACL allows controlled access to devices providing a shared resource such as the process control service [23].

### **1.4.7 Self-Organisation**

A WSN is typically an ad hoc network which operates independently and is self-organising and self-healing according to different situations. A WSN does not have a fixed infrastructure available for the purpose of network management. This inherent feature poses a security challenge to the WSN. Upon deployment, the base station or coordinator of WSN self-organizes and learns the network topology. Knowledge of the topology is located at the base station or coordinator and it may be shared with the nodes of the WSN. This requires the use of more powerful sensors to serve as cluster heads for small coalitions within the WSN [24]. Due to its self-organising ability, a WSN is able to recover from an attack [21]. However, this same ability inhibits the same way that sensor networks must self-organize to support multi-hop routing; they must also self-organize to conduct key management and build a trust relationship among sensors [21]. Lack of self-organization may be devastating in case of an attack [25].

#### 1.4.8 Time Synchronisation

Some applications in WSNs rely on time synchronization. This is increasingly applied in WSN communication as sensor nodes may sleep for some period of time in order to conserve power. Furthermore, some sensor nodes may want to compute the end-to-end delay of a packet as it travels between two pairwise sensors. A WSN with many collaborating nodes may require group synchronization for tracking applications and so on [21].

#### 1.4.9 Secure Localisation

In some cases, the utility of a WSN relies on its ability to accurately locate each sensor node in the network. A sensor node that is placed in a particular location to monitor its environment will need to relay its readings along with the location data for it to be truly useful. Unfortunately, an attacker can easily manipulate non-secured location data by reporting false signal strengths or replaying signals [26].

Alongside the security requirements that were outlined in this section, there exist a number of threats to these concepts. WSNs need to employ strict security schemes to protect against the many WSN attacks that are documented in the following section [26].

#### 1.4.10 Message-based, Node-based and Network-based Security Requirements

The various security requirements of WSN networks are classified into three security levels that depend on those requirements. The security levels are as follows:

- **Message-based Level** - Similar to that in conventional networks, this level deals with data confidentiality, authentication, integrity and freshness. Symmetric key cryptography and message authentication codes are important to support information flow security. Also, data freshness is necessary to provide content-correlative information to transmit on a sensor network during a specific time.
- **Node-based Level** – On this level, situations such as node compromise or capture are investigated. When a node is compromised, loaded secret information might be applied by adversaries.
- **Network-based Level** - On this level, more network-related issues are addressed, as well as security itself. Protecting it is critical. The security issue is becoming more challenging in certain specific network environments. Firstly, securing a single sensor is completely different from securing the entire network; thus, the network-based security should be ascertained. Secondly, network parameters such

as routing, node's energy consumption, signal range, network density and so on should be considered correlatively. Moreover, the scalability issue is also important in the redeployment of node addition and revocation [27].

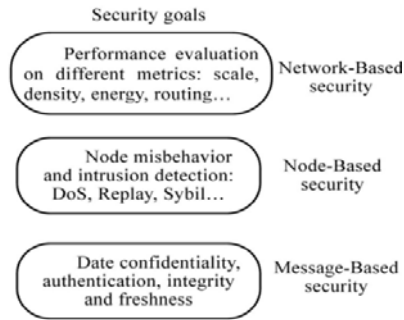


Figure1-3: WSN Security Concerns [27].

Figure 1-3 depicts the security architecture of sensor networks and gives a general view on security issues in sensor networks. There are three levels of security requirements that determine the principles of algorithm design for security mechanisms.

## 1.5 Wireless Network Vulnerabilities

With the use of wireless networks and devices, new privacy and security threats are more prevalent. A secure WSN must include strict encryption, transmitter authentication along with data consistency validation with constraints on energy, memory, computation and network bandwidth. These limitations of WSNs may potentially introduce many security issues and breaches to the security requirements outlined above.

In general, wireless networks are susceptible to various security issues and it is essential that security is assured from generic attacks. In a wireless network, there are several attacks which lead to a significant security breach in the proprietary network and may expose sensitive data. In the next chapter, all potential attacks possible in a wireless network will be described in detail.

## 1.6 Motivation of the Research

Due to wireless security challenges and wireless network vulnerabilities, there are security issues which pose significant challenges for industries. There may be several underlying factors that make such security implementation impossible. Hence, the primary issues that we have identified in the literature and intend to address in this research are:

- 1- There is a lack of proper sensor node configuration for security requirements in WSN technology that may result in serious consequences in terms of external security attack as well as implementation of such technology.
- 2- There is no architectural framework available that allows the testing of WSN security to identify the vulnerabilities and to allow evaluation or comparison with the alternative wireless systems.
- 3- There is no systematic approach to Risk and Impact Analysis when implementing WSNs. Hence, the issues identified are those which hinder industry and lead to potential money loss.

## **1.7 Objectives of the Research**

The objective of the thesis is to develop an architecture model to improve the security of the WSN which will protect it from and prevent security breaches. To achieve this aim, we define the following sub-objectives:

- 1- Identify the WSN security vulnerabilities of several keys wireless sensor network protocols in terms of WSN security requirements and provide recommendations regarding appropriate configuration for the implementation of WSNs.
- 2- Design and develop an end-to-end comprehensive architecture framework including the necessary software, hardware, process and procedures in order to test for vulnerabilities, and thereby mitigate the security risks associated with WSN systems.
- 3- Implement the security measures of the framework to address the susceptibilities to attack, including security devices, applications and network.
- 4- Evaluate the WSN security risks based on security requirements and identified threats.
- 5- Evaluate and validate the above framework and approach in a remote operation environment such as the oil and gas industry.

## **1.8 Significance of the Research**

The WSN security model that will be proposed in this research has the potential to be beneficial in many regards:

- 1- This research facilitates a security aware and attack resistive wireless environment for industries. Such an environment paves the way for many solutions that will improve industry operations [3].
- 2- This research will provide a method for companies to mitigate the risk of a wireless network being used to leak sensitive, commercially competitive information.

- 3- This research is significantly useful for industries that want to protect information against cyber terrorist threats, as information in such sensitive environments is of utmost importance.
- 4- In addition, mitigating risk in such a network is useful for industries to protect and maintain commercial privacy.
- 5- As data security over the Internet is one of the most talked about topics in the ICT area and the Internet community, this research can lead to important contributions in areas such as information security for technological networks. Moreover, it enables industries to secure a network's wireless connection as a whole as well as its components individually. This research can help to reveal the vulnerabilities of other wireless networks and may have important implications for investigations into solutions to counter cyber-attacks.
- 6- Through the use of intelligent techniques such as securing exchange keys to protect generated keys against attackers, and the monitoring of secure sensors, data may then be used to recognise certain characteristics and patterns in operations to further promote a safe workplace, optimize operations, and improve business.
- 7- A sensor network must be available and functional throughout its lifetime. For example, in a manufacturing monitoring application, loss of availability may cause failure to detect a potential accident and result in financial loss; in a battlefield surveillance application, loss of availability may open a back door for enemy invasion.
- 8- A security model for a WSN is extremely important for both controlled environments such as healthcare and automation in transportation, and uncontrolled and hostile environments such as environmental monitoring, military command and control, battlefield monitoring. The majority of the WSN applications should be able to run continuously and reliably without interruption.
- 9- The successful implementation of WSN security demands serious attention, unlike the neglected wireless sensor network. It is essential to have a WSN security scheme that maintains energy efficient data gathering and total protection. The future application of a WSN's mobile nodes, deployable in any environment including the oil and gas industries, where properly managed and implemented, can bring about a total significant change to the scope of WSNs and increase their usefulness in the oil and gas industry.

## 1.9 Plan of the Thesis

The thesis is organized as follows:

- **Chapter 1 - Introduction** - Provides a general overview of the goals of this project that investigates the security issues surrounding WSNs.
- **Chapter 2 – Taxonomy of WSN Security and Attacks** - Describes some constraints and vulnerabilities of WSNs and categorises and designs the taxonomy of attacks on wireless sensor networks in a systematic way.
- **Chapter 3 – Literature Review** - This chapter documents other research in WSN and describes the IEEE 802.15.4-2006, which is a standard that specifies the physical layer and media access control for Low-rate Wireless Personal Area Networks (LR-WPANs). Also, this provides an overview of the existing standards and compares the features of these standards.
- **Chapter 4 - Problem Definition** - This chapter explains the existing security issues in WSNs. All the barriers to and limitations of WSN technology are addressed. The network environment, which includes WSN and IP networks, is described and problems are addressed in this chapter.
- **Chapter 5 – Overview of the End-to-end WSN Security Architecture Framework** - The importance of security to counter exploitation of the WSN has been discussed in detail in the previous chapter. This chapter details the proposed WSN security framework to counter against security exploits.
- **Chapter 6 – The implementation of the Architecture and Security Measures** - This chapter presents several experiments using ZigBee WSN devices. The existing attacks to which ZigBee is still susceptible are described.
- **Chapter 7 – Evaluation of the Security Risk and Execution Counter Attack** - Describes how the researcher executes the remaining attacks such as Replay, DoS and physical tempering attack within the ZigBee network and how the researcher controls the risk of those attacks.
- **Chapter 8 – Evaluation of the Proposed Architecture Framework in an Oil and Gas Industry**- This chapter presents a case study which explores the cyber security issues surrounding WSNs in the oil and gas industry and specific Statoil installations. This chapter presents the WSN system's development lifecycle in the oil and gas industry and the goal of the TAIL Integrated Operation project. In addition, the overall information security of the offshore industry was considered in order to improve the safety and regularity of Statoil operations.



- **Chapter 9 – Guidelines and Recommendations** – Provides risk analysis guidelines, recommendations and impact studies for WSN implementation.
- **Chapter 10 – Future work and Conclusions** - This chapter discusses future work and concludes the thesis.

A number of assumptions have to be made in conducting this research, including:

It is assumed that access to the wireless sensors and their configurations/set-up is restricted to authorized persons who will not intentionally or otherwise introduce specific configurations which obviously introduce vulnerabilities clearly outside of regular secure operation and/or maintenance processes.

The physical security of the devices is considered and it is assumed that the device readings can be physically manipulated.

It is assumed that the devices perform as specified by their standard and manufacturer. Any faults or operation outside of standard and manufacturer specification will not be considered.

## **1.10 Conclusion**

The proliferation of WSNs has driven the research into sensor network security. In this chapter, several unique properties of WSNs were discussed and compared to their wired counterparts. A comprehensive overview of WSN security, including the architecture, device components and applications was presented. This overview facilitates an understanding of the characteristics of WSNs and the importance of security in WSNs since they are particularly susceptible to physical and network-based security attacks, accidents, and failure. This chapter outlines the WSN challenges and typical security requirements which exist when wireless devices are employed. This chapter explains why WSNs are prone to cyber threat and why industries are an attractive target for such attacks. This raises some serious concerns about the use of WSN technology in this domain.

## 2 Taxonomy of WSN Security and Attacks

### 2.1 Introduction

Since wireless sensor networks are being utilized in practical applications, the design of optimum security mechanisms for WSNs has become a big challenge within this area. Hence, it is necessary to propose a taxonomy of attacks on wireless sensor networks, since a good security mechanism should address such attacks. This chapter describes some constraints and vulnerabilities of WSNs, then categorises and designs the taxonomy of attacks on wireless sensor networks in a systematic manner. This will help the researcher in the area of wireless sensor networks to better understand the security issues and design more effective security countermeasures for wireless sensor networks.

Eliminating the need for cables can contribute to reduced installation and operating costs; it enables installations in remote areas, and allows for cost-efficient, temporary and mobile systems and also introduce some issues and security challenges for this technology [28]. A big factor in the adoption of WSNs is that these technologies can be used where the installation of wires is prohibitive, impractical and/or dangerous. However, the self-organization characteristic makes the networks susceptible to various attacks.

### 2.2 WSN Constraints and Issues

WSNs, like traditional wireless channels, have several communication issues as well as some restrictions on WSN devices that raise security concerns. These issues include several disadvantages of wireless systems, namely, the potential for radio interference due to weather, other wireless devices, or obstructions like walls, and more security issues [29].

#### 2.2.1 Wireless Communication

A wireless channel is an open communication medium that can be accessed by everyone within its signal range. This openness is of great advantage since it reduces infrastructure costs, although communication is heavily dependent on the environmental conditions. The very openness of wireless communication raises the very important issue of security, because access to the communication channel is available to every user through a wireless network device [19].

Some problems regarding wireless communication are explained in the following:

- **Unreliable Transfer** - the wireless channel, unlike fixed wired network channels, is inherently unreliable. A wireless channel is susceptible to interference, channel

error, congestion and devices moving out of range. These conditions which could be either permanent or temporary, lead to damaged or dropped packets on the wireless network. If a wireless protocol does not provide error handling, it can lead to incoherent communication or loss of critical security packets, or insecure communication [19].

- **Conflicts** - WSN is susceptible to packet collision in the wireless channel. Collision occurs when two or more sensor nodes transmit packets to each other at the same time. This is a major problem in a highly dense WSN. An effective mechanism for handling traffic collision/conflicts is required because the retransmission of packets will exhaust the sensor node resources [30].
- **Latency** - The nature of WSN communication which includes multi-hop routing, network congestion and node processing, can lead to greater latency in the network. This latency can cause synchronization issues among sensor nodes and impacts on the security of WSN in cases of event reporting and cryptographic key distribution [31].

### 2.2.2 Wireless Network Issues

Due to these restrictions in wireless networks, several issues and attacks have been introduced.

- **Accidental Association** – This is an unintentional access to wireless networks where outsider computers or devices try inadvertently to connect to an overlapping neighbouring wireless network without being aware of this access. This represents a significant security breach in a proprietary network and may expose sensitive data [22].
- **Malicious Association** – This attack is typically performed as a result of weak security measures and protocol loopholes allowing access to the network. It may also be possible to lure computers to log in to networks that impersonate the real thing by exploiting faults in the wireless protocol. By temporarily disrupting the response of the network and granting access to the fake device in the network, it is possible to capture all communications through a central hacker point. This also makes it possible to capture valid users, steal passwords and data, launch other attacks and install Trojans [32].
- **Identity Theft** - Identity theft occurs when a hacker is able to listen in to key user credential traffic and is able to use this information to impersonate an authorized computer or user [22].

- **Man-in-the-Middle** – Man-in-the-Middle Attacks use the Malicious Association techniques to gain access to a network and its users and transparently monitor passing traffic. If data is unencrypted or is easy to decipher, then a hacker is given access to sensitive company information. A hacker is able to provide false information by transparently listening , removing and replacing key network packets with others [33].
- **Denial of Service** – This attack occurs when a targeted access point or device is flooded with bogus protocol messages and data in an attempt to reduce or even suspend its responsiveness and ability to perform its regular functions. This is a very serious problem when wireless devices may be required to deliver time critical data. Jamming the wireless communication link utilizing dedicated jamming devices also falls into the Denial-of-Service category [34].
- **Network Injection** – A network injection attack makes use of access points that are exposed to non-filtered or broadcast network traffic, by introducing bogus network configuration commands that may affect routers, switches, and intelligent hubs. The network devices may crash, shut down, restart or even require reprogramming [22].
- **Radio Interference** – The coexistence of the different systems and technologies is of greatest importance, as more and more wireless communication devices utilize the license free portions of the frequency spectrum, in particular the ISM bands [35].
- **Environment Tampering** – The adversary in principle can compromise the integrity of the sensor readings by tampering with the deployment area. For example, the adversary can place a magnet on top of a magnetometer, or tamper with the temperature of the environment around temperature sensors. This is an effective attack on service integrity. The main drawback of this attack is the high risk of apprehension if the network is under some kind of surveillance [36].
- **Byzantine Attack**– Wireless sensor networks are vulnerable to Byzantine attacks in which a fraction of the sensors are tampered with. In this attack, the intruder can reprogram the compromised sensors and authenticate them, and compromised sensors collaboratively send fictitious observations to the centre. This attack eventually results in severe consequences as the network operation may seem to be operating as normal to the other nodes [37].

WSNs, like traditional wireless channels, are open and unreliable and the transmission of data packets may be delayed and manipulated. Also, due to some constraints in WSNs devices, some security challenges in WSNs stem from such constraints.

- **Node Compromise** - One of the most fruitful attacks that can be launched against a sensor node is node compromise. As nodes have to be physically near the event for monitoring, they are very easy to access. In fact, by accessing a node in the network, the attacker is able to gain access to internal information, and use it for malicious purposes by launching complex or stealthy attacks [20].
- **Replay Attack** - This is the intercepting of data packets and replaying them where decryption of the data or payload is not required. This attack is used to facilitate other attacks. Imagine a scenario in which a node sends an encrypted user name and password to a server to log in, so if a hacker intercepts the packet with a sniffer and replays the packet, the attacker will obtain the same rights as the original user [38].
- **Node Replication Attacks** – Conceptually, this attack is quite simple. An attacker tries to add a node to an existing sensor network by replicating the node ID of an existing sensor node. A node replicated in this method can disrupt a sensor network's performance by corrupting or misrouting packets, which leads to a disconnected network and false sensor readings. If an attacker can gain physical access to the entire network, the cryptographic keys can be obtained by copying from an existing one and inserting it at strategic points in the network. This allows the attacker to manipulate a specific segment of the network, perhaps by disconnecting it altogether [21]. The centralized approach will fail if the adversary can compromise the base station or interfere with its communications [39].
- **Misbehaviour** - This is unauthorized behaviour of an internal node that may unintentionally cause damage to other nodes. For example, the aim of a node may be to obtain an unfair advantage over the other nodes rather than launching an attack [39].

### 2.3 Wireless Sensor Network Environment

A typical Wireless Sensor Network (WSN) is built of several hundreds or even thousands of “sensor nodes”. As mentioned, the topology of WSNs can vary and include star network, tree network, and mesh network. Each node has the ability to communicate with every other node wirelessly. Hence, the network includes nodes, which have the responsibility to sense

the environmental properties, and base stations. This device is responsible for gathering all the data within a network and sending them to the control room for monitoring.

Due to the device limitations and wireless characteristics, which do not have physical protection, as well as some issues related to the wireless communication and WSN deployment, several exposure attacks in a WSN network are introduced.

### 2.3.1 Device Limitations

WSNs have additional constraints that prevent the application of traditional network security features. Current WSN sensor nodes are low-powered devices with very limited resources. Therefore, current sensor nodes cannot support complicated and computationally heavy applications such as the security algorithms used in Internet Protocol (IP) networks. Strong security algorithms require a trade-off between security and performance. The following device limitations require careful consideration [15].

Even though wireless devices usually have very limited resources, they are still required to execute software implementations of complex networking algorithms with real-time requirements.

- **Processing Performance** - Sensor nodes have restriction in limited processors. The restrictions include the complexity of the functions data processing, encoding and encryption.
- **Memory and Storage Space** - A sensor node has limited memory and storage space, so communication packets need to be small and simple. Most sensor nodes have 8-16 bit CPUs with 10-64K of program memory and 512K-4MB of flash storage [40]. Recently, new devices have 250 kbps wireless transfer rate with very limited range, which is around 150 metres. Thus, any security and communication algorithms have to be very small. For example, the total code space of TinyOS is 4K and the core scheduler needs 178 bytes [40].
- **Power** - Energy usage is another major constraint in WSNs. The power source of sensor nodes is usually a battery, as they are physically small and autonomous. The replacement of batteries of many such sensors in a vast network would be very difficult and increase the operational costs. Also, the use of rechargeable batteries would be very expensive in such a network. Therefore, the battery installed in these sensor nodes will have to last for a long time, like a few years instead of days or hours. This ensures that the devices do not need to be maintained constantly. It should be mentioned that, due to this limitation, the energy impact of a security

algorithm in WSN must be considered because the complicated security algorithms require more processing overheads, which increases energy usage and may decrease the performance of sensors [10].

### 2.3.2 Deployment Constraints

One of the main benefits of WSNs is their ability to collect information from public, even potentially hostile, environments without supervision. Just as a coin has two sides, the unattended deployment environments render WSNs susceptible to various types of attacks and make some physical protection measures, such as infrastructure support and tamper-proof components, infeasible.

- **Resource Management** - For industrial sensor networks to be a viable option for sensing, monitoring and control, it is important to keep the power consumption as low as possible. The communication layer RF transceiver, when transmitting and receiving data, is a major source of power consumption in a wireless sensor. To save the power of sensors, it is recommended that the transceiver be shut down when it is not in use. This is also beneficial for the power consumption of processing unit. In fact, the microprocessor can enter low-power sleep modes when there is no need for communication [41].
- **Unattended Operation** - One of the major benefits of WSNs is that sensor nodes can be placed in an environment without requiring any supervision. This can produce some security issues to the network and backend system. For example, the sensor nodes which are located in harsh environments or in an unsecured manner, are readily accessible to people.
- **Exposure to Environment/Physical Attacks** - Sensor nodes may be installed in an environment open to physical attacks and bad weather. For example, sensor nodes in the ocean might be eaten by fish or washed away during storms. Since these nodes are in the open, they can also be attacked or stolen by malicious users to compromise the security of the WSN. Such sensor devices are usually not secured against theft or unauthorised physical access [22].

- **Remote Management** - One benefit of a WSN is its ability to be managed remotely. This enables sensor nodes to be placed in hazardous or inaccessible environments. This requires physical security to protect the WSN devices and their information, which is relayed to the control centre [22].
- **Dynamic Infrastructure** - WSNs are able to self-organise and form a distributed network without a central management point. This provides a robust and dynamic communication network for information to be passed from the sensor nodes to the backend servers. In fact, poor design and implementation of WSN network makes the network organization difficult, inefficient, and fragile [22].
- **Application-specific property** - WSNs are application-specific networks and there is no single security mechanism that is ideal for all WSN implementation scenarios. It is impossible to design a “one-size-fits-all” solution for every different type of application [22].

## 2.4 WSN Security Barriers and Challenges

Due to the constraints mentioned above, it is not easy to implement security defences in WSNs. One of the major obstacles in deploying security on WSNs is that the current WSNs have limited computation and communication capabilities and it is impossible to manually replace the battery due to the unattended nature and hazardous sensing of environments. The constraints make the provision of adequate security countermeasures even more difficult and present some security challenges since the WSNs are made susceptible to several exposure attacks, and are therefore more vulnerable. Some of these exposure attacks have been inherited from traditional wireless technology and some of them are specific only to WSN technology. In the following section, each of the possible attacks which can threaten the security of WSNs, is described.

## 2.5 WSN Security Overview

Sensor nodes are low-cost and have very limited resources. These nodes are usually scattered randomly in a designated field and self-organized into a network after their deployment. The scale of WSNs varies from hundreds to thousands of sensor nodes. Due to the mobility of nodes in some applications, the topology of WSNs may frequently change. Wireless channels are open and unreliable and the transmission of data packets may be delayed and manipulated. In fact, security challenges in WSNs stem from these constraints.



In this section, we analyse the current capabilities of the WSN network, in order to assess the security level currently provided by this platform. The existing vulnerabilities are categorized according to the following factors: constraints on performing a successful attack and the kind of disruption an attack may cause to the network. The existing vulnerabilities can further be divided into those which require knowledge of the WSN cryptographic keys, and those which do not. Depending on this fact, the set of sub-scenarios varies.

## **2.6 Wireless Network Attacks category**

Wireless network attacks can be classified according to their origin or their nature. An origin-based attack may be either external or internal; whereas a nature-based attack may be either a passive attack or an active attack.

### **2.6.1 External and Internal Attacks**

Usually, a wireless network is deployed and managed by one authority. External attacks are those launched by a node that does not belong to the logical network. This attack is launched only from outside of the scope of the network and has limited impact.

If an attacker can obtain authorization to access the network, it becomes an internal attacker. In this case, the attacker can cause more severe damage because it is seen as a legitimate entity. In an internal attack, the attacker can become an internal one by compromising and deploying malicious nodes [42].

### **2.6.2 Applicable Passive Attacks**

Passive attacks should be examined as the first step because through these, active attacks are launched. Eavesdropping and traffic analysis are examples of a passive attack. Thus, examining the occurrence of these two attacks would be extremely important.

The goal of passive attack is to obtain information without being detected. In this attack, the attacker eavesdrops on passing traffic. A passive attack is a continuous collection of information from one or multiple targets that might be used in the future to launch an active attack. By passively participating in the network, the attacker collects a large volume of traffic data and analyses it in order to extract some secret information which can be used for various purposes. Usually, the passive attack is very difficult to detect.

Due to the nature of the wireless communication medium which is widely shared, it is easier for an attacker to passively eavesdrop in this environment than in traditional wired

environments. So, information confidentiality must be one of the security features in a wireless environment.

- **Eavesdropping** - Since an adversary by having the appropriate equipment may eavesdrop on the communication, the confidentiality objective is required in a sensors environment to protect information travelling between the sensor nodes of the network. For example, the adversary could overhear critical information such as sensing data and routing information by eavesdropping. Based on the sensitivity of the stolen data, an adversary may cause severe damage by using this data for many illegal purposes. By listening to the data, the adversary could easily discover the communication contents [21].
- **Traffic Analysis** - Traffic analysis attacks allow an adversary to obtain information about the network topology and the location of the base station by monitoring traffic transmission patterns. Once the topology of the network is known, the attacker is able to target a node to attack [21].

### 2.6.3 Applicable Active Attacks

In an active attack, the attackers try to bypass or break into secured systems. This attack attempts to circumvent or destroy protection features in order to introduce a malicious code and steal or modify information. Disclosure or dissemination of data files, DoS, or modification of data are the result of active attack [43].

In an active attack, the attacker exploits the security holes in the network protocol stack to launch various attacks such as packet modification, injection, or replaying. The impact of active attacks is more severe than that of passive attacks [28].

Active attacks include almost all attacks launched by actively interacting with victims such as sleep deprivation, which targets to exhaust the battery; hijacking, which is control of a communication between two entities, one of which is masquerading as authentic; jamming, which causes channel unavailability, routing protocol attacks, and so on.

**Note:** Both passive and active attacks can be executed through a packet sniffer, which is computer software and/or hardware that can intercept and log network traffic [43]. Running a packet sniffer, an attacker may intercept 802.15.4 network traffic and employ passive attacks, whether internal or external.

## 2.7 Wireless Sensor Network Attacks Exposure

WSN attacks are relatively recent phenomena. They are described as operations to disrupt, deny, degrade or destroy data within nodes and network. Specific WSN attacks include any action that intentionally or unintentionally manipulates the WSN performance. Due to the nature of the WSN, which has been inherited from the traditional wireless network medium which is widely shared, it is easier for an attacker to passively eavesdrop in this environment than in traditional wired environments. So, a WSN is still vulnerable to passive attacks such as eavesdropping and traffic analysis. Below, all the existing types of active attacks on WSNs are explained.

### 2.7.1 Misbehaviour Attack

Because attacks deviate from normal behaviours, it is possible to identify attackers by observing the pattern of the network and ascertain what has happened. Various data and actions can be deployed for this purpose. The misbehaviour can take different forms: packet dropping, modification of data structures important for routing, modification of packets, skewing of the network's topology or creation of bogus nodes [44].

### 2.7.2 Replay Attack

This is an attack against the message which is repeated or delayed. It could be using duplicated authentication or malicious data. In WSN, replay attack can use for creating a new session or to bypass authentication [38]. The scenario is shown in Figure 2-1. There are three devices: the sensor (sender), the router (receiver) and an external device (attacker). (1) While the sensor is sending a message to the network, the attacker interferes and corrupts the transmitted data, so the receiver does not receive the complete message. (2) To ensure that the sensor does not resend the message, the attacker generates an ACK message and sends it back to the sensor (sender). Due to not checking the authentication, the sensor assumes that the message has been sent to the router. Corrupted ACK messages usually lead to costly exponential back-off in some MAC protocols. For example, in a server room where the temperature is controlled by a ZigBee sensor and the data changes by +1 or -1 degrees, by executing replay attack, the temperature can be changed by an adversary. This means that if the attacker who implemented the replay attack sniffs the sent packet from the ZigBee device to the air conditioning and replays it n-times, the temperature is added or decreased by n-degrees. This incorrect temperature can cause damage to servers.

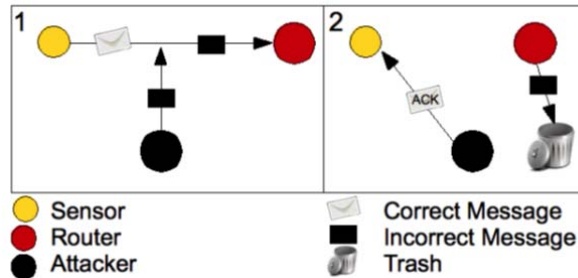


Figure2-1: ACK-MAC Layer Attack

### 2.7.3 Physical Tampering

Locating the sensor nodes in a large WSN in an unrestricted environment is very vulnerable to physical tampering and allows an attacker to remove or destroy these nodes. These nodes can be easily destroyed or tampered with by disrupting their communications in the WSN. It is always very difficult to distinguish between the natural failure of sensor nodes and the malicious destruction of sensor nodes. Other security exploitations such as insertion of malicious nodes into the WSN and extraction of information such as cryptographic keys from legitimate sensor nodes are the result of tampering [45].

### 2.7.4 Denial of Service (DoS)

A Denial-of-Service attack (DoS) is an active attack that occurs when a targeted access point or device is flooded with false protocol messages and data in an attempt to reduce its responsiveness and the performance of its regular functions. This can be a very serious problem if a wireless device is required to deliver time-critical data. A DoS attack is generally defined as an event that can diminish or eliminate a network's capacity in terms of performance. Most of the attacks resulting in a Denial of Service halt the communication between nodes.

Sensor networks are usually structured as a layered architecture, which makes WSNs vulnerable to DoS attacks as these may occur in any layer of a sensor network [46]. Lists of these attacks are identified below:

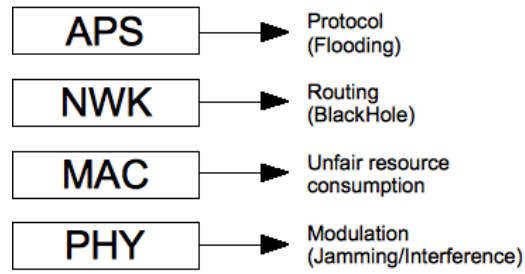


Figure2-2: Denial Service Attack

Figure 2-2 classifies all possible DoS attacks according to each layer. The possibility of launching the DoS attack at several layers is important because more complex attacks will be more difficult to detect, as an attacker always intends to be invisible.

- **Physical Layer** – Nodes in a sensor network apply wireless communication because the network’s ad hoc, large-scale deployment makes anything else impractical [47].

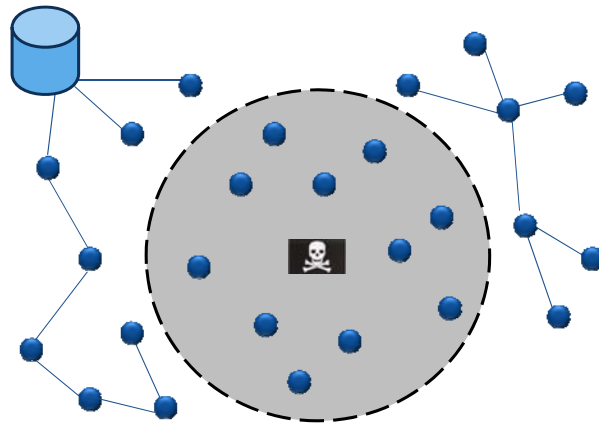


Figure2-3: Physical Layer Attack

Figure 2-3 shows the physical layer attack that interferes with the radio frequencies that a network's nodes are using. As can be seen, some nodes were influenced by the interference of radio frequencies and halt the communication between nodes.

- **Jamming** – This type of attack interferes with the radio frequencies being used by a WSN. A typical jamming attack can disrupt the entire WSN. This type of attack is simple to implement and is very effective against single frequency networks. There are two types of jamming, constant jamming and sporadic jamming. Both these

attacks can disrupt the network, particularly if the communication is sensitive or time-critical. Jamming from other natural causes of communication disruption can be easily distinguished by sensor nodes. This can be detected by determining that constant energy, not lack of response, is impeding communication. If a sensor node does not know it is being jammed, it will increase its transmitter power, thus depleting its resources faster [45].

- **Link Layer Attacks** – This is responsible for medium access, error control, multiplexing of data streams and data frame detection. It ensures reliable connections in the network [47].

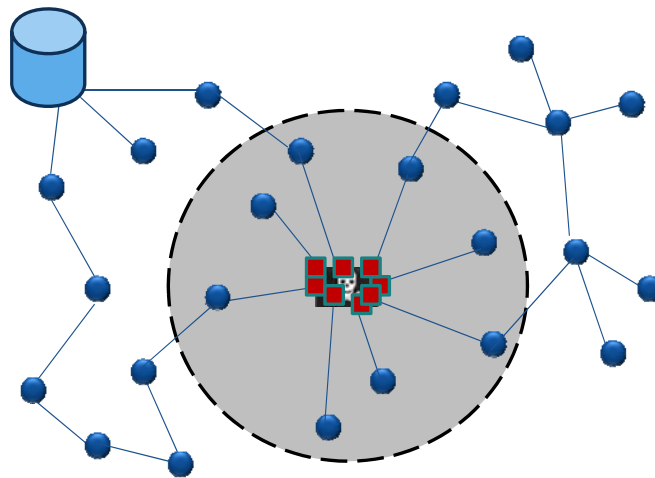


Figure2-4: The Link Layer Attacks

Figure 2-4 shows the link layer attack to alter transmission so as to disrupt the packets like checksum mismatch. As can be seen, the MAC layer provides channel arbitration for neighbour-to-neighbour communication and cooperative schemes to rely on carrier sense, which let nodes detect communication. They are particularly vulnerable to DoS if other nodes are transmitting.

- **Collision** – This attack is introduced by an attacker in the WSN to create a costly exponential back-off in some MAC protocols. The energy expended by an attacker is minute, while the energy which is expended within the WSN is significant. A malicious node in the network can cause more collisions to occur than the error-correcting codes can handle in a WSN. Collision errors are minimised by using

error-correcting codes. [48]. For example, if an attacker can manipulate an octet of transmission like a checksum mismatch, then the entire packet can be disrupted.

- **Resource Exhaustion** – Due to collision, a simple link-layer protocol may attempt to repeat the retransmissions. This will lead to exhaustion of battery resources in sensor nodes in the WSN as well as delays in transmissions. Random back-offs only decrease the probability of inadvertent collision and would be ineffective at preventing this kind of attack. Time-division multiplexing distributes a specific time slot to each node for transmission without requiring arbitration for each frame. A malicious node could constantly request channel access or elicit a response from sensor nodes in the WSN. Constant transmission would exhaust the energy resources of both malicious nodes and targeted sensor nodes [48]. For example, exhaustion of battery resources may occur when a node attempts to repeat retransmission.
  - **Unfairness** – Abusing a cooperative MAC-layer priority scheme can cause unfairness, a weaker form of DoS. This threat may not entirely prevent legitimate access to the channel, but it could degrade service. For example, it may cause users of a real-time MAC protocol to miss their deadlines [48]. In fact, unfairness is a weaker form of DoS that abuses MAC priority [49].
- **Network Layer Attacks** - This layer provides a critical service nonetheless. In a large-scale deployment, messages may traverse many hops before reaching their destination. A variety of attacks targeting the network layer have been identified [47].

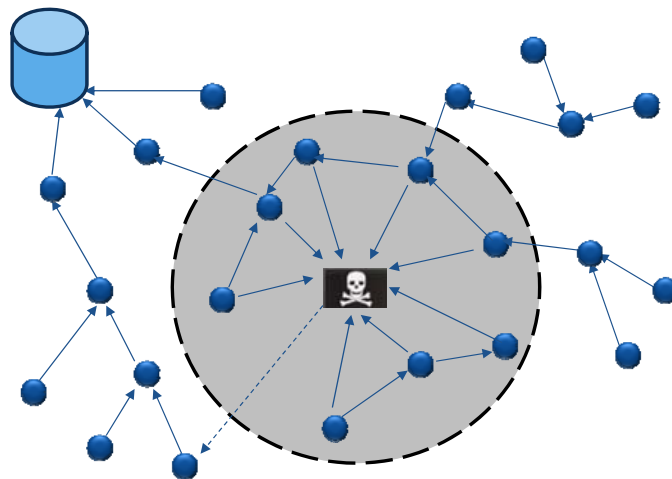


Figure2-5: The Network Layer Attacks

Figure 2-5 shows the network layer attack whereby an adversary attracts the surrounding nodes with unfaithful routing information. By attacking the routing protocols, it is possible to absorb network traffic, and inject packets into the path between the source and destination in order to control the network traffic flow.

- **Wormhole Attack** – A wormhole is a low latency link between two portions of the network over which an attacker replays network messages. This link is a single node forwarding messages between two adjacent nodes or a pair of nodes in different parts of the network which are able to communicate with each other. The latter of these cases is closely related to the sinkhole attack because an attacking node near to the base station can provide a one hop link to that base station through the other attacking node in a distant part of the network[46]. A wormhole attack is a malicious node that eavesdrops on a packet and tunnels it through the sensor network to another malicious node, and then replays the packets. It also can disrupt the routing protocol by misleading the neighbour discovery process [50]. For example, in wormhole attack, the adversary tunnels the traffic received in one part of the network to another.
- **Selective Forwarding** – A large assumption made in multi-hop networks is that all nodes in the network will accurately forward the received messages. In this attack, an attacker may create malicious nodes to forward only certain messages and simply drop others. Black hole is a specific form of this attack in which a node drops all messages it receives [51]. For example, in such an attack the adversary places himself/herself in the path of data, choosing not to forward certain packets and dropping them [49].
- **Rushing Attack** – Most on-demand routing protocols rely on broadcast route-requests to find routes. In a rushing attack, an attacker is able to forward route-requests more quickly than legitimate nodes. This makes it possible for the route to choose and include the adversary. If not overcome, the rushing attack is able to prevent secure on-demand routing protocols from finding routes longer than two-hops. The rushing attack is made possible by the widely-used duplicate suppression technique, when a node considers only the first copy of a given control packet and drops other copies [52].
- **Acknowledgment Spoofing**– Acknowledgment is sometimes required in the routing algorithms. An attacking node can spoof the acknowledgments of



overheard packets destined for neighbouring nodes in order to provide false information to those nodes. An example of such false information is claiming that a node is alive when in fact it is dead [46]. For example, the attacker spoofs the acknowledgement to convince the sender that a weak link is strong or a dead node is alive.

- **Hello Flood Attack** –An attacker sends or replays a routing protocol’s Hello packets from one node to another with more energy. In this attack, an adversary uses HELLO packets as a weapon to deceive the sensors in WSN. This can be done by high radio transmission range and processing power that sends HELLO packets to a number of sensor nodes which are isolated in a large area within a WSN. As a result, the victim nodes, which are spoofed by the attacker, go through the attacker as they know that it is their neighbour. This can be done by sending the information to the base station [53].
- **Sybil Attack** – The Sybil attack is defined as a “malicious device illegitimately taking on multiple identities” [54]. This is an attack that defeats the redundancy mechanisms of distributed data storage systems in peer-to-peer networks. The Sybil attack is also effective against routing algorithms, data aggregation, voting, fair resource allocation and foiling misbehaviour detection. In Sybil attack, all of the techniques involve utilizing multiple identities. The Sybil attack, like the routing protocol attack, relies on a malicious node taking on the identity of multiple nodes, and thus routing multiple paths through a single malicious node [21]. For example, in Sybil attack a single node presents multiple identities to other nodes.
- **Sink/Black Hole Attack** – In this attack, a malicious node advertises very attractive routes to data sinks (sources). The neighbouring nodes will select the malicious node as the next hop for message forwarding since it is considered a high quality route and will propagate this route to other nodes in the WSN. In fact, all traffic in the WSN is sent through the malicious node (man-in-the-middle) to manipulate the data packet such as dropping the packet, selectively forwarding the packet and changing the content of the messages before relaying the packet. The sink hole is characterized by limiting bandwidth and channel access to intense resource contention among neighbouring nodes of the malicious node. As a result, it increases congestion and energy consumption of the nodes involved [55]. For example, in Sink Hole attack, the adversary attracts the surrounding nodes with unfaithful routing information.

- **Spoofed, Altered, or Replayed Routing Information**– Most of the direct attacks against a routing protocol in any network target the routing information, when information is being exchanged between two nodes. In fact, an attacker tries to spoof, alter, or replay routing information to disrupt the traffic in the network. These disruptions include the creation of routing loops, attracting or repelling network traffic from select nodes, extending and shortening source routes, generating fake error messages, partitioning the network, and increasing end-to-end latency. The addition of a MAC to the message is a countermeasure against spoofing and alteration because the receivers can verify whether the messages have been spoofed or altered [46].
- **Transport Layer Attacks** - This explicitly targets the connection between identifiable nodes in order to block off the connections [47].
  - **Flooding** – In this attack, an adversary sends many connection establishment requests to the victim. This causes the victim to allocate resources that maintain the state of that connection. It should be mentioned that the connectionless or stateless protocols can naturally resist this type of attack somewhat, but adequate transport-level services for the network cannot be properly provided [48]. For example, the attacker tries to exhaust memory resources of a victim system by sending numerous packets and forcing the victim to allocate memory in order to maintain the state of each connection [56].
  - **De-synchronization** – This attack can disrupt an existing connection between two end points. In this attack, the adversary repeatedly forges messages, which carry sequence numbers or control flags, to one or both end-pints. Forged messages can cause the end points to request retransmission of missed frames. The end points can be prevented from exchanging any useful information that causes them to waste energy in an endless synchronization-recovery protocol, if proper timing is maintained by the adversary [48]. For example, the attacker forges messages between nodes to take over flags and modify sequence numbers [56].

## 2.8 Message-Based, Node-based, and Network-Based Attacks

As mentioned earlier, there are three levels of security requirements: message-based level, node-based level, and network-based level. Message-based attacks try to break data confidentiality, integrity and freshness. Node-based attacks target the valid nodes to obtain secret information stored by the nodes and make further attacks using the obtained

information. Node compromise, node replication, resource exhaustion, and node misbehaviour are categorised as the node-based attacks. Network-based attacks attempt to reduce network connectivity or availability such as routing attack and time synchronization attack. This attack can be launched both locally and globally [57]. It should be mentioned that these three types of attacks are not isolated from each other and some message-based and node-based attacks may result in Denial of Service that affects the network performance.

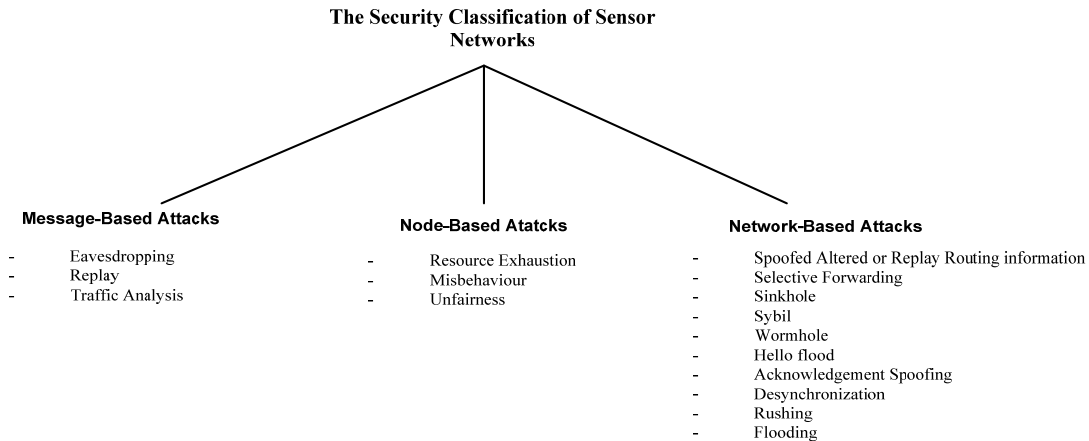


Figure2-6: The Security Classification of Sensor Networks

Figure 2-6 illustrates the security classification of a sensor network into three overarching attacks: message-based, node-based and network-based attacks. Note that most of the attacks are network-based attacks, such as routing attack and time synchronization attack, which attempt to reduce network connectivity or availability.

## 2.9 WSN Attack Strategies

This section explains the strategies of attacks on WSN, how these attacks can be executed, and how it is possible to exploit the WSN network through these attacks. Strategic attack is an offensive action that is specifically selected to execute attacks. All strategy attacks are explained below:

- **Eavesdropping** - Eavesdropping is the most common attack on privacy where the attacker intercepts or sniffs transmitted packets. Because packets contain the control information about the sensor network configuration, such an attack can be effectively executed against privacy protection schemes [58]. If the packets are encrypted, the attacker will only see the encrypted data using basic eavesdropping techniques. However, there are tools available for cracking certain encryption

techniques. These types of tools enable the contents of the packets to be decrypted and read.

- **Traffic Analysis** - Traffic analysis can be performed even when the messages are encrypted and cannot be decrypted. It includes intercepting and analyzing messages in order to find useful information such as communication patterns and even the location of the base station. Since the base station is a central point of failure, once its location has been exposed, an attacker tries its best to destroy the base station, and furthermore disable the data-gathering capability of the entire sensor network. In general, the greater the number of messages observed, the greater the number of messages inferred from the traffic [59].
- **Jamming** - The most effective approach would be to send random unauthenticated packets to every wireless station in the network. This can be easily achieved by purchasing hardware off the shelf from an electronics retailer and downloading free software from the Internet [60]. Since radio frequency is essentially an open medium, jamming can be a huge problem for wireless networks. Jamming is one of the many strategies used to compromise the wireless environment. If the knowledgeable attacker has a powerful transmitter, an overwhelming frequency can be generated that will jam the 2.4 GHz frequency and disrupt communications. The most common types of this form of signal jamming are random noise and pulse. In addition, jamming attacks can be mounted from a location remote to the target networks [60]. Jamming is made more complex by the fact that it may not be caused intentionally, as other forms of wireless technology are relying on the 2.4 GHz frequency as well. Some widely-used consumer products are capable of disrupting the signal of a wireless network and faltering traffic [60].
- **Spoofed, Altered, or Replayed Information** - The most direct attack against a routing protocol is to target the routing information exchanged between nodes. By spoofing, modifying, or replaying routing information, adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency and so on [61].
- Spoofing is a process of impersonating another node in the network. In routing, the attacker can impersonate a node by changing the source address of the routing message. The spoofing of a routing message enables the malicious node to attack the network routing functions in a wide range of possibilities. Spoofing can create fake neighbor nodes and emulates supporting information to the malicious routing

information, which is spread by the malicious node. The goal of spoofing includes route invasion, routing disruption, network partitioning, and DoS [62]. Once an attacker changes other contents in the routing message such as declaration of neighbors, sequence number, instead of the source address, it is usually referred to as a simple modification attack. Modification of routing message contents affects the network functions significantly and the objective of modification is similar to spoofing. However, the modification of a routing message, unlike spoofing, is confined to neighborhood nodes only [62].

- **Hello Flood Attack** - Many routing protocols need to broadcast HELLO packets to inform their neighbours of their presence. Hence, the sensors are self-organized into a network. An attacker does not necessarily need to be able to compromise encryption or construct legitimate traffic in order to use the HELLO flood attack. An attacker mounts a hello flood by recording hello packets with data extraction tools (such as Smart RF Studio protocol packet sniffer and WiSens [63]), and broadcasting them from a laptop-class node with high transmission power. These replayed HELLO packets could convince the node which receives the packet that the adversary is its neighbour [64].
- **Wormhole Attack** - In this attack, the attacker can use laptops or other wireless devices to send the packets on a low latency channel. If the attacker is able to distinguish the types of the packets, such as data, acknowledgement, or time update, in transmission with traffic analysis tools, the attacker can tunnel the control packet and cause more damage to the underlying protocols. Wormhole attacks would likely be applied in combination with eavesdropping or selective forwarding [51].
- **Replay** - Replay attacks involve intercepting data packets and replaying them. Attackers do not need to decrypt the packet. Replay attack is used to facilitate other attacks [137]. Imagine a scenario in which a node sends an encrypted user name and password to a server to log in. If a hacker intercepts the packet with a sniffer and replays the packet, the attacker will obtain the same rights as the user. For example, in the oil and gas industry, the attacker may delay or replay the collected data, so the control room is receiving outdated data. The objective of replay attack is to disrupt routing functions and cause DoS. Replay attacks are less severe, but can thwart intrusion prevention mechanisms such as encryption and digital signatures [62].

- **De-synchronization** - In a de-synchronization attack, an attacker interrupts an active connection between two nodes by transmitting forged packets with incorrect sequence numbers or control flags to desynchronize end points [65]. There are several ways that the external attacker can influence time synchronization. “Supposed pair-wise sender-receiver synchronization is performed by a handshake protocol between node A and B. T1, T4 represent the time measured by local clock of node A. Similarly, T2, T3 represent the time measured by local clock of node B. At time T1, A sends a synchronization packet to B. Node B receives this packet at T2. At time T3, B sends back an acknowledgment packet. Node A receives the packet at T4. An attack can be launched by the following three ways: (1) by modifying the values of T2 and T3 in transmission with sniffer tools (such as WiSens [66]), (2) by assuming the identity of one of the network nodes, and (3) by delaying the transmission of the messages between the nodes and thus increasing the value of T2 (or T4) with the Fabric for Sensor Network Management and Data Transfer” [67].
- **Collision** - In a collision attack, the attacker uses a radio to listen to the frequency on which a WSN is transmitting. When it hears the start of a message, it sends out its own signal, thereby interfering with the message. In fact, only one byte is enough to create a CRC error and cripple the message [68].
- **Unfairness** - Intermittently using the above link-layer attacks by an attacker may cause unfairness in a network. Instead of preventing access to a service outright, an attacker can degrade it in order to gain an advantage such as causing other nodes in a real-time MAC protocol to miss their transmission deadline [46]. Repeated application of these exhaustion- or collision-based MAC layer attacks or an abusive use of cooperative MAC layer priority mechanisms, can also lead to unfairness. In addition, an attack can exploit unfairness attack via traffic-flooding to deliberately starve some node of bandwidth.
- **Resource Exhaustion** - Resource exhaustion attacks can be easily performed by transmitting numerous packets from one or multiple attackers. The batteries of all nodes can be intentionally exhausted to disable further packet handling. Due to the characteristic of an ad-hoc network whereby each node handles all received packets naturally, the resource exhaustion attacks are more effective and severe than DoS attacks because in resource exhaustion attacks, more nodes will become unavailable at the same time [69].

- **Acknowledge Spoofing** - An attacker jams the packets from nodes which send packets to their intended target and sends acknowledgments (ACKs) back to the sender. Hence, the data would never reach the intended target, and the sender would have no idea whether or not the data has been received since it would see the ACKs [70].
- **Misbehaviour** - Misbehavior in wireless sensor networks can occur in different ways such as: packet dropping, modification of data structures important for routing, modification of packets, skewing of the network's topology or creating fictitious nodes. An attacker obtains full control of sensors in order to engage in any form of misbehavior ranging from a desire to save battery power to making a given wireless sensor network non-functional. Misbehavior can take place at all layers. At the Physical layer, a misbehaving node can increase its transmitting power, which can affect the network performance. At the MAC layer, a node may be chosen to prevent it accessing the medium in its turn; thereby unfair advantage is taken of the shared medium [71]. At the Network layer, the basic threat is non-cooperative behavior where packet forwarding is concerned. In fact, the proper execution of a routing protocol demands that intermediate nodes correctly forward the packets to the intended receiver nodes in a path; these packets are not forwarded in a misbehavior attack [71].
- **Rushing** - Rushing is a protocol-dependent attack. It targets all multicast routing protocols that use the duplicate suppression technique. Many demand-driven protocols such as ODMRP, MAODV, and ADMR, which use the duplicate suppression mechanism in their operations, are vulnerable to rushing attacks [72]. According to the duplicate suppression technique, a node forwards a message only once and discards the message if it receives it again. In a rushing attack, when a source node floods the network with routing discovery packets in order to find routes to destinations, two colluded attackers use the tunnel procedure to form a wormhole and quickly forward the tunneled routing discovery packets by skipping some processing or routing steps [72]. Due to duplicate suppression, each intermediate node processes only the first non-duplicate packet and discards any duplicate packets that arrive at a later time. Hence, the rushing attackers gain priority to be selected for the routing path.
- **Flooding** - In this attack, an adversary sends many connection establishment requests to the victim. This causes the victim to allocate resources that maintain the state for that connection. Limiting the number of connections prevents complete

resource exhaustion, which interferes with all other processes. It should be mentioned that the connectionless or stateless protocols can naturally somewhat resist this type of attack, but adequate transport-level services for the network cannot be provided properly by such protocols [48].

- **Sink/Black Hole** – The attacker nodes act like a black hole, where the attacker node listens to the route request packets from its neighbours and replies to them by sending fake information about routing protocols such as the shortest route to a sink node. Hence, every single node sets a next node for data forwarding toward the sink. Any node which intends to send data to a base station will be forwarded to the attacker. This provides an opportunity for the adversary to analyse these packets and extract important information [73].
- **Sybil Attack** - Wireless sensor networks are more susceptible to Sybil attack. In this attack, an attacker node tries to change its ID node continuously by using multiple identities of the legitimate sensor nodes at the same time. The main purpose of this attack is to increase the resource utilization and decrease data integrity. Sybil attacks occur mostly in distributed systems on network servers for data aggregation. It is very difficult to detect the nodes that launch Sybil attacks. The lack of a centralized controller increases the chance of Sybil attack. Therefore, in wireless sensor networks, having a centralized base station helps to prevent such attacks [73].
- **Physical Tampering** – An attacker is able to execute this attack by: (1) gaining complete read/write access to the microcontroller; (2) reading whole or part of the RAM or flash memory; (3) influencing sensor readings; and (4) manipulating radio communications [74].
- **Selective Forwarding** – Multi-hop networks, such as sensor networks, rely on the fact that neighbouring nodes forward packets to the base station. However, a malicious node located in the path of the data flow is able to refuse to forward certain messages. This attack is known as a selective forwarding attack and occurs when the adversary drops packets coming from specific sources in the network. This attack can cripple the network performance and isolate certain nodes from the base station. “In a selective forwarding attack, malicious nodes behave like black hole and may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further” [75]. However, sometimes neighbouring nodes decide to seek another route. This attack can be trickier, if an adversary selectively forwards packets. In fact, an adversary is interested in suppressing or



modifying packets originating from a few selected nodes and reliably forwards the rest of the traffic in order to deflect suspicion from its operation [75].

## 2.10 Attack Outcomes,

In this section, the consequences of actions are explained. It describes a set of strategies used by the attackers, which results from the actions or strategies taken by all attackers.

The table below lists existing attacks and briefly explains their outcomes and consequences for every single attack.

Table 2:1: The list of Exposure Attack Outcomes

<b>Exposure Attacks</b>	<b>Outcomes</b>
<b>Eavesdropping</b>	The transmitted packets are exposed to the attacker. Unencrypted traffic can be clearly seen [57].
<b>Traffic Analysis</b>	The communication pattern of the network, or the topology of the network, and even the location of the base station is exposed to the attacker [58].
<b>Jamming</b>	Radio signals can be jammed or interfered with, which causes communication to be corrupted or lost [60].
<b>Spoofed, Altered</b>	The outcome of this attack is to create fake neighbour nodes and emulates supporting information to the malicious routing information, which is spread by the malicious node. The goal of spoofing includes route invasion, routing disruption, network partitioning, and DoS [60]. Spoofing of a routing message enables the malicious node to attack the network routing functions in a wide range of possibilities.
<b>Hello Flood</b>	The outcome of this attack is that the node which receives the packet is convinced that the adversary is its neighbour [61].
<b>Wormhole</b>	The purpose of this attack is to disrupt routing by creating a well-placed wormhole [62]. Nodes are convinced that the wormhole provides a better route through an artificially high quality route to the base station. This attack also can disrupt the routing protocol by misleading the neighbour discovery process [62].
<b>Replay</b>	The purpose of this attack is to disrupt routing functions and cause DoS attack. Replay attacks are less severe, but can thwart intrusion prevention mechanisms such as encryption and digital signatures [60].
<b>De-synchronization</b>	An attacker interrupts an active connection between two nodes by transmitting forged packets with incorrect sequence numbers or control flags to de-synchronize end points [63].
<b>Collision</b>	The purpose of this attack is to create a CRC error and cripple the message [64].
<b>Unfairness</b>	Through this attack, the attacker is able to gain an advantage over other nodes in a real-time MAC protocol so that they miss their transmission deadline [45].
<b>Resource Exhaustion</b>	Batteries of all nodes can be intentionally exhausted to disable further packet handling [65].
<b>Acknowledge Spoofing</b>	An attacking node can spoof the acknowledgments of overheard packets destined for neighbouring nodes in order to provide false information to those neighbouring nodes [45].

<b>Misbehaviour</b>	Misbehaviour in wireless sensor networks can occur in different ways such as: packet dropping, modification of data structures important for routing, modification of packets, skewing of the network's topology or creating fictitious nodes [66].
<b>Rushing</b>	The outcome of this attack is that a source node floods the network with routing discovery packets in order to find routes to destinations. Two colluding attackers use the tunnel procedure to form a wormhole and quickly forward the tunnelled routing discovery packets by skipping some processing or routing steps [67].
<b>Flooding</b>	The outcome of this attack causes the victim to allocate resources that maintain the state of that connection. Limiting the number of connections prevents complete resource exhaustion, which interferes with all other processes [47].
<b>Sink Black Hole</b>	This attack provides an opportunity for the adversary to analyse packets and extract important information [68].
<b>Sybil Attack</b>	The outcome of this attack is an increase of resource utilization and decrease of data integrity [68].
<b>Physical Tampering</b>	(1) gaining complete read/write access to the microcontroller; (2) reading whole or part of the RAM or flash memory (3) influencing sensor readings; and (4) manipulating radio communications [69].
<b>Select Forwarding</b>	This attack is able to cripple the network performance and isolates certain nodes from the base station [70].

## 2.11 Advanced WSNs Elements

In this section, the advanced WSN elements, which will be used and focused on in this thesis, are briefly described. We intend to experiment with the actual devices to measure the security in WSNs. Therefore, one of the WSN standards based on IEEE 802.15.4 will be chosen as the proxy of a WSN to set up the test-bed in our Lab to measure the security of WSN technology.

### 2.11.1 ZigBee

ZigBee is a specification for a suite of communications that uses small, low-power digital radios based on an IEEE 802 standard protocol for personal area networks (PAN). For example, applications include wireless light switches, smart home application, and other equipment that requires low-power radio and short-range wireless transfer of data [76].

### 2.11.2 ZigBeePRO

This standard is the mature version of ZigBee and was standardised by the ZigBee Alliance in 2007. In fact, this standard has been re-innovated due to ZigBee's susceptibility to noise, as ZigBee always operates on the same static channel. Hence, ZigBee is not regarded as a proper standard in industrial environments and applications [76].

### **2.11.3 WirelessHART**

WirelessHART is a wireless sensor networking technology based on the Highway Addressable Remote Transducer Protocol (HART) to define the processing requirements of field device networks. This protocol supports operations in the 2.4 GHz ISM band by applying IEEE 802.15.4 standard radios. It was developed as a multi-vendor, interoperable wireless standard [77].

### **2.11.4 ISA100.11a**

ISA100.11a is an open wireless networking technology standard developed by the International Society of Automation (ISA). This protocol is a wireless standard for industrial automation and process control and supports operations in the 2.4 GHz ISM band by applying IEEE 802.15.4 standard radios [78].

## **2.12 Conclusion**

In this chapter, the vulnerabilities of WSNs were examined, as were all the possible attacks to which WSNs are susceptible. A DoS attack taxonomy was presented to identify the attacker in different layers. A wide variety of possible security attacks on WSNs were described together with security mechanisms, attack strategies and the consequences of those attacks. These concepts will be used consistently throughout this thesis.

The following chapters will discuss the typical security requirements that exist when wireless devices are employed and will outline the theoretical security risks of applying WSNs in industry from both specification and research literature perspectives. IEEE 802.15.4, ZigBeePRO, WirelessHART and ISA100 are considered in detail.

## **3 Literature Survey of State of Art WSN Security**

### **3.1 Introduction**

Nowadays, data security over the Internet is a much-discussed topic among the Information and Communication Technologies (ICT) and the Internet communities. The security mechanism, which ensures data security over the Internet, uses encryption to protect data and helps users to protect and conceal their data from unauthorized access [79]. However, the implementation of security mechanisms impacts on the quality of service in real-time communication.

The technical requirements for the deployment of wireless technology in commercial and resources industries have been identified [28]. This chapter documents the WSN state-of-the-art when it comes to secure transmission and operation and the typical attack countermeasures that can be effectively employed. There are several fundamental operations that must be addressed in order for a WSN to function properly.

### **3.2 State of The Art in WSN Security**

The importance of security to counter attacks on WSNs has been discussed in detail in the previous chapters. The WSN nodes are required to provide secure and confidential data to the data collector/control server and the control server must be able to securely control the function of the sensor nodes remotely. The user(s) of a WSN must ensure that the network is protected against unauthorised access to its local or corporate networks. Some of the security countermeasures used in WSNs might be able to successfully address one or more security issues, but in doing so might decrease protection against another security issue. This chapter describes the architecture model which mitigates the risk of WSN implementation.

#### **3.2.1 Key Management**

Key management is an important aspect of WSNs as it is crucial for providing data authentication, confidentiality and integrity. However, due to the limited memory and processing power constraints, as well as the dynamic nature of sensor nodes, new key management/establishment protocols must be developed [80].

#### **3.2.2 Symmetrical Key Management**

Symmetric cryptography is the least computationally complex cipher and is frequently used in ZigBee. Symmetric schemes utilize a single shared key known only between the two communicating sensor nodes. This shared key is used for both encrypting and decrypting

data. The example of symmetric cryptography in fixed wired networks is DES, 3DES (Triple DES), RC5, AES, and so on [81].

While symmetric cryptography can be easily run on ZigBee, the establishment of keys is the biggest problem since a mechanism is required for securely providing secret keys to all legitimate sensor nodes. Key management issues are not unique to ZigBee and have been studied in depth outside of the wireless net [21]. However, most of the traditional techniques for key management are not suited to ZigBee. Some are not applicable as they involve a Trusted Third Party (TTP) and others are insecure, too costly or not robust. Therefore, the most suitable key management mechanism in large sensor networks may be a key pre-distribution scheme, where key information is installed in each sensor node prior to deployment [21].

### 3.2.3 Asymmetrical Key Management

Asymmetric cryptography, also called public key cryptography, is generally unsuitable for use in low power devices such as sensor nodes because asymmetric cryptography is computationally intensive. In this type of scheme, the sensor node needs to maintain two mathematically related keys, one of which is made public while the other is kept private. This allows data to be encrypted with the public key and decrypted only with the private key [21].

The two best-known asymmetric cryptographic techniques in fixed networks use RSA and Elliptic Curve Cryptography (ECC) [82]. However, several researchers have successfully implemented asymmetrical cryptography in WSN. The ECC scheme has been successfully used in 8-bit CPUs with 160 bit keys resulting in shorter messages during transmission [83]. The ECC private key operation is many times faster than RSA, while the public key operation is slower. The portions of the RSA cryptosystem on the UC Berkeley MICA2 actual devices has been successfully implemented [84]. The public key operations were implemented on the sensors, while private key operations were performed on more computationally intensive devices [85].

The Diffie-Hellman ECC key exchange algorithm performs the public key operations on the Berkeley MICA2 nodes [86]. This asymmetrical cryptography technique is adequate for infrequent use in generating keys in WSNs. In fact, in some applications, validating the identity of a node is more critical and important than other security concerns.

### 3.2.4 Authentication

Authentication techniques can be used in packet routing to exclude attackers and unauthorized nodes from participating in the routing within the WSN. These techniques modify existing routing protocols to build authentication-based solutions [50, 52, 82, 87, 88]. Most of these solutions use asymmetrical keys such as digital signatures which require the use of a centralised trusted certificate server whose public key is a priori known to all valid nodes. While these solutions are not flexible, they exclude external unauthorised nodes from participating in the routing, thereby preventing external attacks. They also provide protection against spoofing attacks within the network, unauthorised modification to the route table by malicious nodes, and rushing attacks by external nodes.

### 3.2.5 Secure Routing

Routing in wireless sensor networks has, to some extent, been reasonably well studied [89]. However, most current research primarily focuses on providing the most energy-efficient scheme. The in-network processing characteristic of sensor networks requiring intermediate nodes to have access to the data complicates the design of routing protocols. Once one of these intermediate nodes is compromised, it can eavesdrop and even modify the data, thus threatening the entire network. So, the routing protocols in sensor networks should provide not only reliable delivery, but also security services [90].

The routing security problem in WSNs summarizes attacks against the current proposed routing protocols and discusses countermeasures and design considerations for secure routing protocols. The attacks can be classified into two categories: (1) trying to manipulate user data directly or (2) trying to affect the underlying routing topology. Both kinds of attacks can consume valuable resources to cause a Denial-of-Service attack. The author claimed that it is unlikely to find effective countermeasures against those attacks after the design of a protocol has been completed. So, it is crucial to consider security issues at the beginning of routing protocol design [61].

It is easy for a malicious node to disrupt the entire routing protocol in a WSN by disrupting the route discovery process. A secure route discovery protocol needs to guarantee that correct topological information will be obtained. A protocol proposed in [91] uses a Message Authentication Code (MAC) to authenticate the sensor nodes between the source and destination nodes. The message will append the node identity to this trusted path. In order to ensure that the message has not been tampered with, a Message Authentication Code is

constructed and is verified both at the destination and the source (for the return message from the destination).

### **3.2.6 Combating Traffic Analysis**

This attack can be prevented by using a random walk forwarding technique that occasionally forwards a packet to a node other than the sensor's parent node [82]. This method makes it difficult to distinguish a path from the sensor node to the base station and it helps to mitigate the rate monitoring attack, but is susceptible to a time correlation attack. A fractal propagation strategy [82] is proposed to defend against the time correlation attack. In this technique, a sensor node will generate a fake packet when its neighbour is forwarding a packet to the base station. The fake packet is sent randomly to another neighbour to force them to generate a fake packet, which essentially uses a time-to-live (TTL) method to decide when forwarding should stop.

### **3.2.7 Intrusion Detection**

Intrusion detection is based on two methods: Anomaly-based Intrusion Detection (AID) and Misuse Intrusion Detection (MID) [124]. AID examines abnormal behaviour compared to that of the legitimate nodes. This is done by first developing a profile of the system in normal and then evaluating the system for intruders. WSN benefits from this technique, since any unusual network behaviour is an indication of an attack. However, anomaly-based intrusion detection incurs costs for the network. Because it is difficult to distinguish normal system behaviour and also legitimate use that is not normal, it is susceptible to error. Anomaly-based intrusion detection has high computational cost to the base profile in comparison with the current system activity.

MID techniques maintain a database of intrusion signatures and the system can easily detect intrusions on the network. This approach is less likely to return false positives but is unable to detect unknown attacks. WSN benefits from this approach, and it requires less computation to identify intruders in comparison with network events [124].

In order to detect an intrusion, either approach can be applied in a WSN. Once a node detects an intrusion, it should communicate this intrusion to other nodes on the network. "Possible responses include forcing the potential intruder to re-authenticate or ignore the suspicious node, when performing cooperative actions" [145].

### 3.2.8 Secure Data Aggregation

This data is collected by individual sensor nodes within the network, but the sensors have limited storage and sensing capabilities. Hence, to gather meaningful information from this data, the raw stream of data must be securely processed first. This is typically done by using a series of aggregators, which are responsible for collecting the raw data from a subset of nodes, and processing and aggregating them from the nodes into more usable data. However, these aggregators are a single point of failure. For example, in a case where an aggregation node is compromised, then all of the data delivered by the sensors can be forged. This type of security problem is called a ‘stealth attack’ whereby the attacker seeks to provide incorrect aggregation results to the user without the user knowing that the results are incorrect.

In order to counteract forged data, a statistical en-route filtering mechanism is proposed to utilise multiple MACs along with the path from the aggregator to the base station. Any packet that fails the MAC test will be disregarded [145]. A mathematical framework, which evaluates the security of aggregation, has been developed to quantify the robustness of an aggregation operator against malicious data [146].

### 3.2.9 Secure Localization of Sensor Node

The location of a wireless sensor node is usually difficult to specify, particularly if nodes are randomly distributed. A technique called Verifiable Multilateration (VM) is applied to accurately compute the location of sensor node [92]. It uses authenticated ranging and distance bounding to ensure the accurate location of a node. This method will easily discover whether or not node location information has been manipulated, as a node is bounded to a reference point. The SPINE (Secure Positioning for Sensor Networks) algorithm, which is based on VM, is applied in the large sensor networks to discover the node location information. In addition, the SerLoc (Secure Range-Independent Localization) technique uses special locators to transmit beacons that are used by sensor nodes to calculate their position. These locators are assumed to be trusted and not compromised and also have their own location [92].

### 3.2.10 Time Synchronization

The Time Synchronization includes a set of secure synchronization protocols for sender-receiver (pairwise), multi-hop sender-receiver, when the pair of nodes is not within single-hop range, and group synchronization [93].



### 3.3 Low-Rate Wireless Personal Area Network Technology - IEEE 802.15.4

IEEE 802.15.4 is a protocol which has been applied as the communication technology in WSNs. Due to the optimization of networks for different applications, the Medium Access Control (MAC) layer requirement in WSNs is varied. So, one particular standard is unlikely to suit all possible applications. The IEEE 802.15.4 protocol is a standard which specifies the physical layer and media access control for low-rate wireless personal area networks (LR-WPANs) and is maintained by the IEEE 802.15 working group. It is the basis for different standards such as ZigBee, WirelessHART and ISA100.11a. The upper layers, which are not defined by 802.15.4, have been developed by each standard. In the following section, the IEEE 802.15.4 protocol along with all three different standards are described and compared to each other.

This section outlines the IEEE 802.15.4-2006 as a physical layer and media access control for Low-Rate Wireless Personal Area Networks (LR-WPANs) standard. The IEEE 802.15.4-2006 is a standard which specifies the physical layer and media access control for Low-Rate Wireless Personal Area Networks (LR-WPANs). It is maintained by the IEEE 802.15 working group.

#### 3.3.1 Protocol Layers

The 802.15.4 offers lower network layers which focus on ubiquitous low-power and low-cost communication between devices with little to no underlying infrastructure where interaction is performed over a conceptually simple wireless network [94]. The following layers are considered:

- **Physical Layer (PHY)** – This layer provides the data transmission service along with the interface to the physical layer management entity. It offers access to every layer management function and maintains the personal area network database. The PHY layer manages the RF transceiver and performs channel selection, energy and signal management functions [94].
- **MAC Layer (MAC)** – This layer allows the transmission of MAC through the PHY layer. The MAC layer manages the interface as well as access to the physical channel and network beaconing. In addition, it handles network association and dissociation functions and applies unique 64-bit MAC hardware addresses assigned by the manufacturer. The MAC layer provides optional security services including frame encryption, integrity, and access control. The unit of transmission at this

layer is the MAC frame. The standard DLL layer in the IEEE model normally consists of two sub-layers such as a MAC sub-layer and a Logical Link Control (LLC) sub-layer, which is the IEEE 802.2 standard. It should be mentioned that both the wired Ethernet network standard (802.3) and the wireless Ethernet standard (802.11) utilize the standard 802.2 sub-layer [94].

- **Higher Layers** – This layer and interoperability sub-layers are not defined in the standard. There exist specifications such as ZigBeePRO, WirelessHART and ISA100, which build on this standard [94].

There are four fundamental frame types including data, acknowledgment, beacon and MAC command frames. They provide a reasonable trade-off between simplicity and robustness. In IEEE 15.4, a super-frame structure which is defined by the coordinator, may provide synchronization to other devices and configuration information. A super-frame consists of sixteen equal-length slots, which can be further divided into an active part and an inactive part and may be used to enter power saving mode [94].

Table 3.1: The IEEE 802.15.4 Standard Specs [94].

Band	Frequency	Channels	Data Rate	Availability and Usage
868 MHz	868-868.6 MHz	1	20 Kbps	Most European countries
915 MHz	902-923 MHz	10	40 Kbps	Americas, Australia and NZ
2.4 GHz	2.4-2.4835 GHz	16	250 Kbps	Most countries worldwide

Table 3.1 shows the IEEE 802.15.4 standards spec for different countries. It shows the different frequencies, bands, channels and data rates being utilized by different countries as their standard.

The IEEE Std 802.15.4 defines a total of 27 channels, numbered 0 to 26. Channel 0 is in the 868 MHz band with a centre frequency of 868.3 MHz. Channels 1 through 10 are in the 915 MHz band, with a channel spacing of 2 MHz, and channel 1 having a centre frequency of 906 MHz. Channels 11 through 26 are in the 2.4 GHz band, the channel spacing is 5 MHz, and the centre frequency of channel 11 is 2.405 GHz [95].

Note: For the purposes of the 802.15.4 standard, the IEEE considers the 868 MHz and 915 MHz bands to be a single, contiguous band and vendors that choose to support either band must support both [94].

### 3.3.2 Security Overview

LR-WPANs are vulnerable to passive eavesdropping attacks and, due to the wireless communication, active tampering attacks. Therefore, LR-WPANs are no different from any other wireless network from a security perspective. LR-WPAN devices are low-cost and have limited capabilities in terms of computing power, memory, available storage, and limited battery life [96]. They cannot be considered as a trusted computing base or a high-quality random number generator.

These constraints influence the design of the security architecture and the choice of cryptography algorithms as well as protocols. Design of the security architecture requires the establishment and maintenance of trust relationships between devices, which need to be addressed with special consideration and compliance with the devices' inherent limitations. Also, battery lifetime and cost constraints limit the availability of processor time and bandwidth [96].

It should be mentioned that most architectural elements of security can be implemented at higher layers and may be considered to be outside the scope of IEEE 802.15.4. The communications in WPAN cannot rely on the online availability of a fixed infrastructure. Moreover, it may involve short-term ad-hoc relationships between temporarily installed or available devices that may never have communicated previously [96].

Due to the constraints of WPANs and their cost objectives, these are amongst the most difficult environments to secure. The cryptographic mechanism in this standard is based on symmetric-key cryptography, and uses keys which are provided by higher layer processes [97]. The IEEE 802.15.4 standard provides a secure implementation of cryptographic operations and authentic storage of keying material for the cryptographic mechanism and particular combinations of the following security services:

- **Data Confidentiality** - Assures the transition of information to the intended parties
- **Data Authenticity** - Assures the source of transmitted information.
- **Replay Protection** - Assures the prevention of duplicate information [97].

The actual frame protection provided can be adapted on a frame-by-frame basis. It allows for varying levels of data authenticity and for optional data confidentiality. The actual frame protection minimizes the security overhead in transmitted frames where required. Cryptographic frame protection may use a key shared between two peer devices (link key) or a key shared among a group of devices (network key) [96]. If a network key is used for peer-

to-peer communication, protection is provided only against outsider devices and not against potential malicious devices [96].

The actual frame protection provided can be adapted on a frame-by-frame basis and allows for varying levels of data authenticity and for optional data confidentiality. In fact, replay protection is always provided. Cryptographic frame protection may use a key shared between two peer devices, which is called a ‘link key’, or a key shared among a group of devices, which is called a ‘group key’. Therefore, allowing some flexibility and application-specific trade-offs between key storage and key maintenance costs versus the cryptographic protection provided [98].

### 3.3.3 Addressing

Addressing in the 802.15.4 is accomplished through a 64-bit node identifier and a 16-bit network identifier. The 802.15.4 supports a few different addressing modes [99].

**Data packet** – This has variable length that is used by a node to send a message to a single node or to broadcast a message to multiple nodes. Each data packet has a flags field that indicates the packet type, and whether or not it includes security. A 1-byte sequence number serves to identify the packet number for acknowledgments and the packet optionally includes source and destination addresses. The data payload field comes after the addressing fields. A 2-byte Cyclic Redundancy Check (CRC) checksum field protects the packet against transmission errors [99].

1 byte	2 bytes	1 byte	0/2/4/10 bytes	0/2/4/10 bytes	variable	2 bytes
Len.	Flags	Seq. No	Dest. Address	Source Address	Data payload	CRC

Figure 3.1: Data Packet Format[100].

Figure 3-1 illustrates the data packet format along with flags. As can be seen, Dest.Address and Source Address flags vary in terms of size from 0 to 10 bytes.

**Acknowledgment packet** – This is sent by the recipient only if the corresponding data packet was not sent to a broadcast address and the sender requested an acknowledgment. An acknowledge packet format includes: a 2-byte flags field similar to the one in the data packet and the 1-byte sequence number from the packet for the acknowledging, and a 2-byte CRC. There is no addressing information in the acknowledgment packet [99].

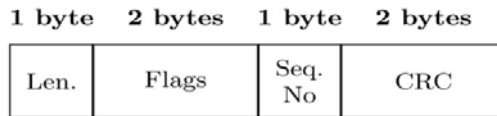


Figure 3.2: Acknowledge Packet Format [100].

As shown in Figure 3-2, the acknowledgement packet format includes Len, Flags, Seq. No. and CRC flags. The total size of the acknowledgement packet format is 6 bytes.

The destination address of an outgoing packet is matched with the address field in an Access Control List (ACL) entry. An indicated security suite processes the packet with the key in the ACL entry. The address field in the ACL entry should match the source address field [99].

Cryptographic operations use the key from the ACL entry. If replay detection is enabled, the replay counter can recognize the data payload as duplicate information. The longer the MAC decreases the chance of guessing an appropriate code and the larger packet size increases the protection against authenticity attacks. For instance, with a 6-byte MAC, an adversary has a  $2^{36}$  chance of guessing the MAC [99].

Based on source and destination addresses, the application indicates its choice of security suite. The 802.15.4 radio chips have an Access Control List (ACL) to control the security suite and keying information. Compliant devices may support up to 255 ACL entries, which all the flags of ACL Entry have mentioned in Figure 3-11. The security material is necessary to execute the security suite. It consists of the cryptographic key and suites that provide encryption [99].

The nonce state should be preserved across different packet encryption invocations. The security material receives a packet's identifier when replay protection is invoked. As a part of the interface for sending packets, the application must specify a Boolean indicating whether security is enabled [99].

### 3.3.4 MAC Security

The 802.15.4 MAC sub-layer provides the desired level of security by adding this sub-layer to the stack. Higher-layer processes may specify keys to perform symmetric cryptography, which protects the payload and restricts it to a group of devices. These groups of devices can be specified in access control lists. Furthermore, MAC computes the freshness of successive receptions to ensure that presumably old frames or data do not ascend to higher layers. The MAC sub-layer provides two services that interface to the MAC Layer Management Entity (MLME) and Service Access Point (SAP) (known as MLME-SAP)[101].

- MAC Data Service
- MAC Management Service

The MAC data service provides the transmission and reception of MAC Protocol Data Units (MPDUs) in the PHY data service. The features of the MAC sub-layer include beacon management, channel access, GTS (Guaranteed Time Slots) management, frame validation, acknowledged frame delivery, association, and disassociation [98].

The following security attributes for MAC PAN Information Base (MAC PIB) specify the security constants and attributes required by the MAC layer:

- **Key Table** – This table provides security processing of outgoing and incoming frames [102].
- **Device Table** – This table provides device descriptors, which maintains device-specific addressing information and security-related information [102].
- **Minimum Security Level Table** – This table maintains the minimum security level information that a device expects [102].
- **Frame Counter** – This is applied for secure outgoing frames to provide replay protection and semantic security of the cryptographic building blocks [102].
- **Automatic Request Attributes** – This table holds all the information needed to secure outgoing frames generated automatically [102].
- **Default Key Source** - This is the shared information between originator and recipient of a secured frame. This frame is combined with additional information explicitly contained in the requesting primitive or in the received frame. Required key for the purpose of security in an originator or a recipient is done by default key source [102].
- **PAN Coordinator Address** - The address of the Personal Area Network (PAN) coordinator is information commonly shared between all devices in a PAN. This is also combined with additional information explicitly contained in the requesting primitive or in the received frame. The key and security-related information required for securing a frame is determined in the PAN Coordinator Address [102].



Figure 3.3: IEEE 802.15.4 MAC frame[103].

The IEEE 802.15.4 MAC frame is shown in Figure 3.3. As illustrated, this frame includes three overarching parts: MAC Header, MAC Payload, and MAC Footer. The MAC Header includes flags to handle addressing and security schemas.

The encryption algorithm used is the Advanced Encryption Standard (AES) with a 128b key length (16 Bytes). The AES algorithm is used not only to encrypt information but also to validate the data which is sent. This concept is called Data Integrity and it is achieved by using a Message Integrity Code (MIC) also named Message Authentication Code (MAC) which is appended to the message. This code ensures the integrity of the MAC header and payload data attached. It creates encrypting parts of the IEEE MAC frame using the key of the network. Hence, if a message is received from a non-trusted node, it will see that the MAC generated for the sent message does not correspond to the one what would be generated using the message with the current secret key, so this message can be discarded. The size is just the bits length which is attached to the frame [103].

The 802.15.4 MAC layer implements security features which are used by the higher-level protocols in the network and application layers [103]. There are three fields in the IEEE 802.15.4 MAC frame which are related to security issues:

- Frame Control (located in the MAC Header)
- Auxiliary Security Control (in the MAC Header)
- Data Payload (in the MAC Payload field)

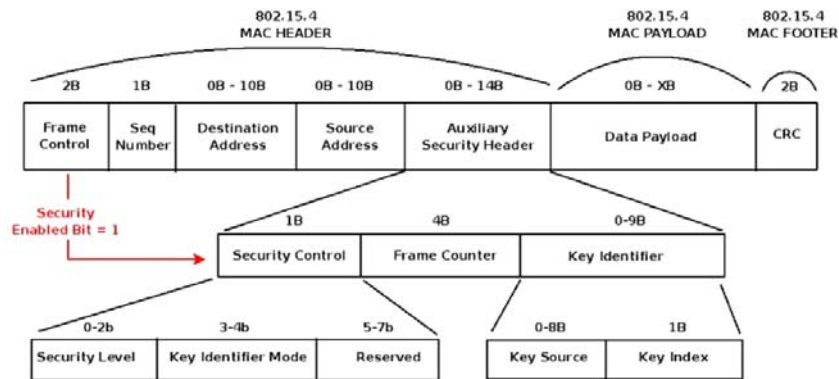


Figure 3.4: Security in the IEEE 802.15.4 MAC frame[103].

Figure 3.4 shows in detail the security schema in the IEEE 802.15.4 MAC frame. It indicates that once the security schema is enabled in IEEE 802.15.4, the three security

schemas which are included in Security header, are activated. This means that through these flags, the security level and key identifier are checked to secure the MAC frame.

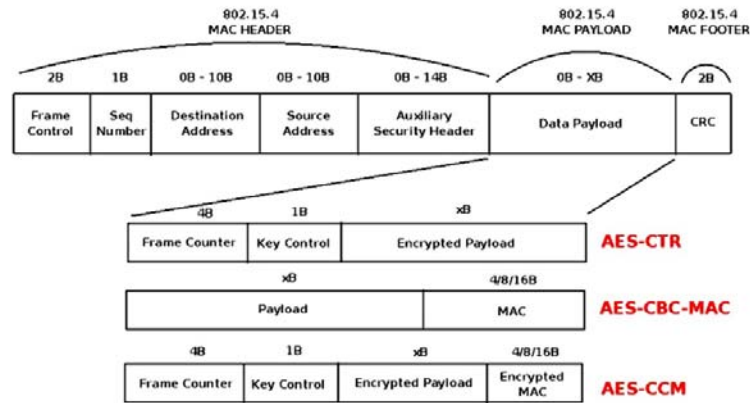


Figure 3.5: Data Payload Encryption Mechanism [103].

Figure 3-5 shows in detail the Data Payload Encryption Mechanism in the IEEE 802.15.4 MAC frame. It outlines the application of three different security algorithms to the Data Payload. These three algorithms will be explained later.

The encryption algorithm ensures the integrity of the MAC header and payload data attached. AES encrypts parts of the IEEE MAC frame using the key of the network. However, the MAC can have different sizes: 32, 64, 128 bits, but security is always created using the 128b AES algorithm. Data Security is performed by also encrypting the data payload field with the 128b key. The greater length is more secure. Data security is performed by encrypting the data payload field through the 128b key length [99].

The Auxiliary Security Header field is variable in length and contains information required for security processing. It is enabled only when the Security Enabled sub-field of the Frame Control Frame is activated [99]. This special header has 3 fields:

**Security Control (1B)** - Specifies the protection scheme that is used.

**Frame Counter (4B)** - Represents the macFrameCounter attribute of the protected originator frame. It is used to provide semantic security of the cryptographic mechanism to protect a frame against replay.

**Key Identifier (0-9B)** - Specifies the required information about key for using and communicating with the nodes [103].

The security control field is 1 octet in length and sets the global security policy. The security level sub-field is 3 bits in length and indicates the specific protection that is provided.



This value can be adapted on a frame-by-frame basis. It allows for varying levels of data authenticity and data confidentiality. Replay protection is always provided, when significant protection is required [103].

**Key Identifier Mode** - The Key Identifier Mode sub-field is 2 bits in length and indicates whether a key is used to protect the frame. It can be derived implicitly or explicitly. In fact, if subfield has a value that is not equal to 0x00, the Key Identifier field of the auxiliary security header can be present [103]. The Key Identifier Mode sub-field can be set to one of the values listed in the following:

- [0]: The key id is known implicitly by the sender and the receiver
  - [1]: The key id is determined explicitly by the 1Byte Key Index from the Key Identifier Field and the macDefaultKeySource.
  - [2]: The key id is determined explicitly by the 1-Byte Key Index and the 4-Byte Key Source both sub-fields from the Key Identifier Field.
  - [3]: The key id is determined explicitly by the 1-Byte Key Index and the 8-Byte Key Source both sub-fields from the Key Identifier Field [103].
- 
- **Key Identifier** - This is set when the Key Identifier Mode sub-field is not zero. It has a variable length and identifies the key that is used for cryptographic protection of outgoing frames, either explicitly or implicitly defined side information [103].
  - **Key Source** - The *Key Source* is either 4 octets or 8 octets in length, according to the value specified by the *Key Identifier Mode* subfield of the Security Control field to specify the group Key originator [103].
  - **Key Index** - The *Key Index* is 1 octet in length that allows unique identification of different keys along with the same originator [103].

### 3.3.5 Keying Models

Symmetric cryptography relies on both endpoints by employing the same key. In a group of nodes, the keying model manages the key of every single node to communicate with another node. The keying model is the most appropriate technique for an application. It should be noted that the keying model depends on the threat model and types of resources which can be expended for key management [100].

The 802.15.4 provides many different ways to generate cryptographic keys, which gives the opportunity to choose a keying model that reflects the threat level an application faces; hence, non-critical applications may use a simpler and less complex keying model. Critical

applications such as control and alarm systems, which deal with sensitive data, should use more complex keying models. However, such models are more costly in terms of processing power and more extensive management [100]. In the following, some common keying models for sensor networks are presented:

- **Network Shared Keying** - Network shared keying is the simplest keying model, which is also the easiest to manage. All nodes in the system share the same key. Every node can communicate with all other nodes. As the memory requirements are small, applications can use network share keying with little effort. However, the cost of simplifying network shared keying is a threat to security, in terms of insider attacks. A single node contains the common key for the entire network. An adversary can use a compromised node to undermine the security guarantees for the whole network [100].
- **Pairwise Keying** - Pairwise keying limits the scope of each key. Each pair of nodes shares a different key. In case of a node compromise, only past and future messages sent from the particular node are affected. Other network traffic is unaffected. Pairwise keying is more secure than network shared keying. On the other hand, the price is the need for more extensive key management. In general, memory requirements increase as one node must store several keys. There also must be controlled logic in selecting which key to use with which node. On resource limited devices, pairwise keying can be a challenge in terms of storage space [100]. The IEEE 802.15.4 allows radio chips to have up to 255 ACL entries. On the other hand, the specification does not have a lower limit regarding the number of ACL entries. For example, the Chipcon CC2420 covers only two keys. Thus, ACL entries cannot be safely shared among a group of nodes. In principle, for a network with  $n$  nodes, there is need for ACL entries to maintain security. In other words, pairwise keying requires the possibility to store a large number of ACL entries on the radio chip [100].
- **Group Keying** - Group keying represents a compromise between networks shared keying and pairwise keying. The network is divided into groups. A group can be a collection of nodes performing the same function, connected to the same segment of the network and so on. Each group has a common key which is shared between all nodes in that group. Different keys are used for communication between nodes from different groups. Group keying provides partial resistance to node

compromise. The cost in terms of processing and memory requirements is lower than for pairwise keying [100].

- **Hybrid Keying Models** - It is possible to simultaneously combine several keying models in an application. An application that uses a combination of different keying models is often said to use a hybrid keying model [100].

### 3.3.6 Data Payload

The Data Payload field can have four different configurations depending on the previously defined security fields. The configuration based on different encryption algorithms such as AES-CTR mode, AES-CBC-MIC-*n* mode and AES-CCM-*n* mode.

- **Null (No Security):** Only provides a simple checksum with no security implementation. The null scheme is implemented as a default feature by chip manufacturers of IEEE 802.15.4 spec radios.
- **AES-CTR Mode:** Data is encrypted by using the defined 128b key and the AES algorithm. The Frame Counter sets the unique message ID, and the Key Counter (Key Control sub-field) is used by the application layer if the Frame Counter max value is reached [103].

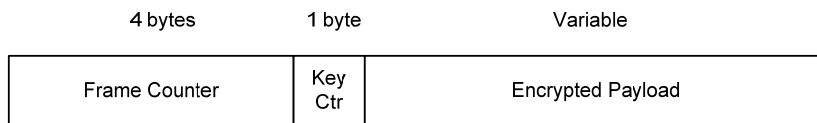


Figure 3.6: AES-CTR[103].

The clear-text data packet is broken into 16-byte blocks  $P_1, \dots, P_n$ . Each 16-byte block uses its own variable counter  $x_i$ . The sender encrypts the data by performing a logical XOR operation:  $c_i = p_i \oplus E_k(x_i)$ , where  $c_i$  = encrypted data payload,  $p_i$  = data block (16 bytes),  $x_i$  = individual counter (IV or nonce). On the receiver side, the clear-text data packet is reconstructed by XOR-ing the encrypted payload with  $E_k(x_i)$ :  $p_i = c_i \oplus E_k(x_i)$

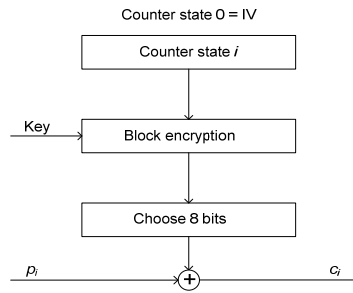


Figure 3.7: AES-CTR Mechanism [103].

- **AES-CBC-MIC:** CBC (*Counter Block Chaining*) is the most common mode to preserve data integrity. One whole block at a time is processed. There is a feedback loop from the previous cipher block. If a one-bit transmission error occurs the whole block is destroyed, plus one more bit.

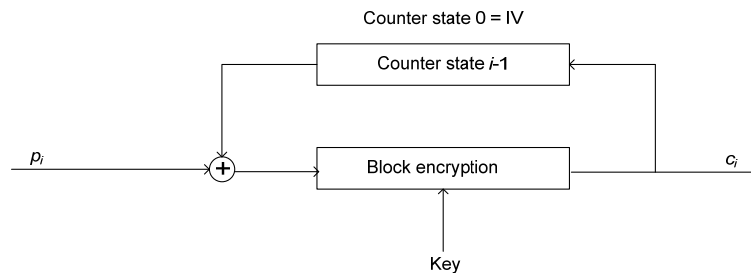


Figure 3.8: AES-CBC-MIC counter block chaining mode [103].

The MIC can only be computed by parties with the symmetric key. The packet headers and data payload are protected by the MIC. The sender adds the MIC to the clear-text data. At the receiver side the MIC is verified by computing the MIC and it compares it to the value included in the packet[100].

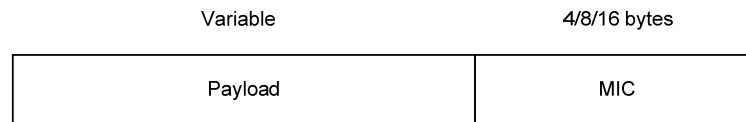


Figure 3.9: AES-CBC-MIC[103].

- **AES-CCM Mode:** CCM mode (Counter with CBC-MAC) is a mode of operation for cryptographic block ciphers. It is an authenticated encryption algorithm designed to provide both authentication and privacy. CCM mode is defined only for block ciphers with 128b lengths. This algorithm is the combination of counter mode of encryption and CBC-MAC mode of authentication. The key in AES-CCM Mode is the same for encryption and authentication [50]. AES-CCM is a mix of the previously defined methods. The subfields correspond with the AES-CTR mode along with AES-CBC-

MAC mode. The AES-CCM mode applies integrity protection over the header and data payload using CBC-MAC and then encrypts the data payload and MAC by using AES-CTR mode. The AES-CCM includes a MAC, and the frame and key counters. In this algorithm, a receiver can optionally enable replay protection by the security suite, which provides confidentiality protection. This includes AES-CTR and all of the AES-CCM variants. The recipients use the frame and key counter as a 5-byte value and the replay counter, with the key counter occupying the most significant byte of this value. The recipient then compares the replay counter from the incoming packet to the highest value it has seen. The packet is rejected if the value is out of sequence [103].

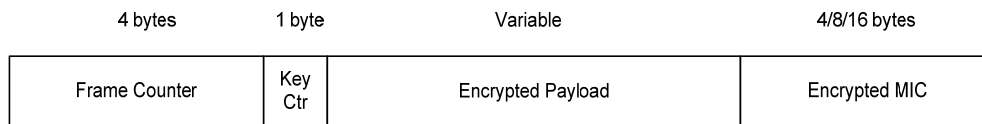


Figure 3.10: AES-CCM [103].

The Table 3.2 illustrates the summary of security schema in three different encryption algorithms which are applied in the IEEE 802.15.4 protocol.

Table 3.2: Cryptographic Protection By the Various Security[103].

Sec. Level	Security Scheme	Attributes	Encrypted	Authenticity
0x00	No security	No security	×	×
AES-CBC				
0x01	AES-CBC-MAC-32	MIC-32	×	√
0x02	AES-CBC-MAC-64	MIC-64	×	√
0x03	AES-CBC-MAC-128	MIC-128	×	√
AES-CTR				
0x04	AES-CTR	ENC	√	×
AES-CCM				

0x05	AES-CCM-32	AES-CCM-32	√	√
0x06	AES-CCM-64	AES-CCM-64	√	√
0x07	AES-CCM-128	AES-CCM-128	√	√

### 3.3.7 Access Control List

Each 802.15.4 transceiver has to manage a list of trusted nodes along with the security policy. For this reason, each node has to control its own Access Control List (ACL) which stores the following fields [103]:

Address	Security Suit	Key	Last IV	Replay Counter
---------	---------------	-----	---------	----------------

Figure 3.11: ACL Entry Format [51].

- **Address:** This is the address of the nodes that want to communicate to each other.
- **Security Suite:** This is the security policy which is being used.
- **Key:** 128b key using the AES algorithm.
- **Last Initial Vector (IV) and Replay Counter:** The Last IV is used to avoid reply attack by the source and the Replay Counter by the destination as a message ID.

### 3.3.8 Security Issues

There are many security issues in the 802.15.4 standard, which can be generally divided into the following categories:

#### 3.3.8.1 Power Loss and Low-Power Operation

Since many of the 802.15.4 devices most likely will be battery-operated, potential security vulnerabilities will occur in the case of power-loss. The main security hole is the potential loss of the ACL table due to power interruption. This causes the node to come up again with a cleared ACL table. It is likely that the application will repopulate the ACL table with the appropriate keys. However, it is not clear what will happen with the nonce state. If all nonces are just reset to an initial value such as 0, nonces will be reused, thereby comprising security [100].

It is possible to avoid reuse of the nonce if the application is designed in such a way that it is able to detect a power failure. It is very important that application developers are aware of the pitfalls that power disruption represents [100].

Similar problems may occur if the device goes into low-power operation. If a device emerges from a low-powered state with a cleared ACL, security problems similar to those of power loss will occur. A possible solution would be to store the ACL state in some memory before entering low-power mode. The current IEEE 802.15.4 lacks a specification for handling this scenario [100].

#### 3.3.8.2 Lack of support for safe group keying

The 802.15.4 does not have appropriate support for group keying. As an example, suppose that a group  $g_1$  of nodes  $n_1 \dots n_5$  wish to communicate with each other using key  $k_1$ . Then there is another group  $g_2$  of nodes  $n_6 \dots n_9$  that uses key  $k_2$ . According to IEEE 802.15.4, each ACL entry can only be associated with a single destination address. Several workarounds can be done to achieve group keying support, but they are not considered safe. There is no simple way to support group keying safely in 802.15.4 networks [100].

#### 3.3.8.3 Replay Protection

When there are more than a few nodes in a network, in practice it is not possible to sustain replay protection. When a sender  $s_1$  communicates with a specific recipient, the recipient increments its replay counter for each data packet received. Now, if another sender  $s_2$  wants to communicate with that same recipient using the same key, the recipient will reject the packet because its replay counter is out of sync with the replay counter received in the packet from  $s_2$ . To avoid such a scenario, application developers must maintain some kind of network-wide coordination regarding the use of replay counter space [100].

#### 3.3.8.4 Integrity Protection

In AES-CTR mode, the device operates in counter mode without MAC. This means that the communication channel is set up using encryption, but not authentication. The encryption is thus protected only by a CRC. This is not secure, as the methods for undermining these security mechanisms are well known. By modifying the cipher-texts, it is possible for an adversary to construct certain modifications to the CRC so that the receiver accepts the packet [100].

### 3.3.8.5 DoS Attacks with AES-CTR

When using AES-CTR with replay protection, it is quite easy for an adversary to block the communication between a sender and the recipient. The receiver keeps count of received packages by means of a “high water mark” register. The recipient does not accept packets with counter values lower than the high water mark. Now, if an adversary sends a packet with source address, key counter 0xFF and frame counter 0xFFFFFFFF, the recipient will set its high water mark to the maximum value. The actual data payload of the fake packet is irrelevant. As the high water mark is now set to 0xFFFFFFFF, the recipient will not accept any further packets [100].

### 3.3.8.6 ACK Packets without Integrity Protection

The current IEEE 802.15.4 specification does not require integrity or confidentiality protection for acknowledgment (ACK) packets. The sender has the option to ask for an acknowledgment packet for each data packet it transmits. Suppose an adversary forges an acknowledgment packet. This is relatively easy, as the acknowledge packet consists of a sequence number. The sequence number corresponds to the sequence number in the senders’ packet, and this number is sent in clear text. In this way, an adversary can fool the sender by letting it know that the packet has arrived safely. This, combined with targeted jamming, can prevent delivery of selected packets. This opens up a potential security risk. An intruder can prevent certain packages from reaching the legitimate recipient by interfering with the radio channel at the time of transmission (to prevent the packet from reaching the recipient), and then sending an acknowledgment packet to fool the sender into thinking that the packet has arrived safely [100].

### 3.3.8.7 Initial Vector Management

There is a risk that two separate recipients can end up with the same key in two separate ACL entries. Up to 255 ACL entries are used to store different keys together with their associated nonce. There is a possibility that an application will set up the same key in two different ACL entries. Although integrity is preserved, there is a chance that confidentiality will be breached if the application programmer is not paying attention to the nonce state. In that case, an adversary can breach the confidentiality by performing an XOR of the two cipher-texts, that is XOR’ing cipher-text to receiver A with cipher-text to receiver B [100].



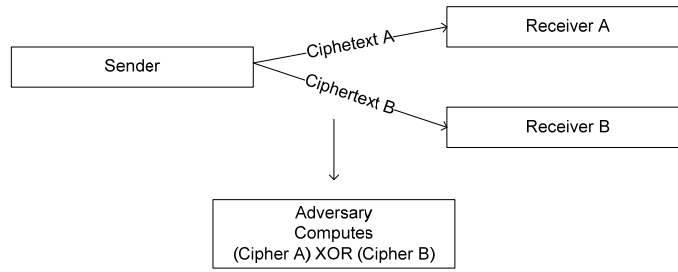


Figure 3.12: Performing an XOR of two cipher-texts [100].

Figure 3-12 depicts that if the sender transmits a message to A, and then a message to B, the sender will use the same nonce. An adversary can easily compute the XOR of the plain texts by XOR'ing the two cipher-texts. To avoid using the same nonce for a different receiver, the application programmer must pay special attention to this issue [100].

### 3.3.8.8 ACL Entries

There are up to 255 ACL entries in the IEEE 802.15.4 specification to store different keys and an associated nonce. The sender chooses the appropriate ACL entry based on the destination address. But there are a number of ways that two separate recipients end up with the same key in two separate ACL entries. This means that confidentiality has been violated.

Also, in the case of power failure, the ACL state will be lost resulting in loss of all nonce states which are used for replay protection.

In addition, there is no support for group keying under the current 802.15.4 specifications; moreover, support for pair-wise keying is also inadequate. Also, unauthenticated encryption supported by AES-CTR mode introduces significant risk of protocol level vulnerabilities [100].

This section outlined the IEEE 802.15.4-2006 as a physical layer and media access control for Low-Rate Wireless Personal Area Networks (LR-WPANs) standard. ZigBee defines the network, security, and application framework layers for an IEEE 802.15.4-based system.

## 3.4 High Level Communication Protocols Technology - ZigBee

In order to satisfy the requirements of industrial WSN installations, a number of groups have provided standards, systems and devices to meet such requirements. International standards for wireless devices and networks such as Bluetooth, Wi-Fi, ZigBeePRO, WirelessHART and ISA100.11a use stacks to provide a layered and abstract description of the network protocol design. Each layer in the stack is a collection of related functions, and each layer is responsible for providing services to the layer above it, while receiving services from the layer below it [3].

### 3.4.1 ZigBee

The ZigBee Alliance is a group of companies that develop and maintain the ZigBee standard. ZigBee is a specification for a suite of high level communication protocols built over IEEE 802.15.4. One important characteristic of ZigBee is that tries to be simpler and less expensive than other Wireless Personal Area Networks (WPAN) standards such as Bluetooth and IrDA. The main focus of the ZigBee standard is on applications that require low data rate, have long battery life and security.

The ZigBee specification defines network and application layers on top of the IEEE Std 802.15.4 PHY and MAC, enabling a low-rate, low-power WSN. The technology defined by the ZigBee specification is intended to be simpler and less expensive than other consumer WPANs such as Bluetooth. ZigBee is targeted at radio-frequency applications that require a low data rate, long battery life, and secure networking. The low cost allows the technology to be widely deployed in wireless control and monitoring applications [76].

ZigBee can operate in both beacons and non-beacons modes. In the beacons mode, the nodes are synchronized and the super-frame is divided into 16 slots using CSMA/CD within the frame. There is an option to use up to seven of these as dedicated slots to specific nodes to increase determinism, which is called Guaranteed Slot Time (GTS) [104].

#### 3.4.1.1 ZigBee Versions

There are two versions of the ZigBee standards. The public revision of the specification is ZigBee 1. It includes the network layer, the application layer, and the 'Home Controls, Lighting' (HCL) application profile. Due to only tree addressing in ZigBee 1.0, it does not include any commissioning recommendations; nor does it specify any particular stack profile.

The other public revision of ZigBee is 1.1 which includes advanced features imposed by tree addressing and centralized binding. New application profiles, along with corresponding commissioning frameworks are also included [105].

### 3.4.2 ZigBee Architecture

The software architecture of ZigBee is built on top of IEEE 802.15.4, along with established and proven standards for wireless communication. The ZigBee network comprises three basic levels: Physical/Data Link level, ZigBee Stack level and Application level. The Physical/Data Link level is the lowest level and the Application level is the highest level [76].

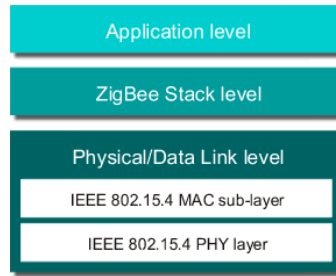


Figure 3.13: Basic Software Architecture [76].

These basic levels are described below:

The Physical/Data Link level is provided by the IEEE 802.15.4 standard. This level includes two separate layers: Physical and Link layers.

- The Physical layer is responsible for handling the interface to the physical transmission medium (radio, in this case), exchanging data bits in this layer and to the above layer Data Link layer [106].
- The Data Link layer is responsible for addressing, assembling data packets, and determining where data is going, and where data is coming from. It is also responsible for the transmission of frames. The Data Link layer is referred to as IEEE 802.15.4 MAC (Media Access Control) and the frames used are MAC frames [106].

The ZigBee Stack level provides the ZigBee functionality, and it is a kind of interface layer between the applications and the IEEE 802.15.4 layer. The ZigBee stack layer includes network structure, routing and security schemas such as encryption, key management and authentication[106]. ZigBee Stack will be explained in detail in the Protocol Layers section.

The Application layer contains the applications that run on the network node and give functionalities to the devices such as converting input into digital data or converting digital data into output. It is possible to run several applications on a single node. For example, a sensor may contain separate applications to measure temperature, humidity and air pollutants [106].

### 3.4.3 Protocol Layers

The ZigBee stack architecture is made up of a set of blocks (layers). Each layer performs a specific set of services for the layer above. A data entity provides a data transmission service and a management entity provides all other services. Each service entity exposes an interface to the upper layer through a Service Access Point (SAP), and each SAP supports a number of service primitives to achieve the required functionality [107].

The following layers are implemented:

- **Application Layer (APL)** - The Application layer framework consists of the Application Support Sub-layer (APS) and the ZigBee Device Objects (ZDO). Manufacturer-defined application objects use the framework and share APS and security services with the ZDO [107].
- **Application Framework (AF)** - Provides a description of how to build a profile onto the ZigBee stack (to help ensure that profiles can be generated in a consistent manner). It also specifies a range of standard data types for profiles, descriptors to assist in service discovery, frame formats for transporting data, and a key value pair constructs to rapidly develop simple attribute-based profiles [107].
- **Application Objects** - Software at an endpoint that controls the ZigBee device. A single ZigBee node supports up to 240 application objects. Each application object supports end points numbered between 1 and 240 (with end point 0 reserved for the ZigBee Device Object [ZDO]) [107].
- **ZigBee Device Object (ZDO)** - Defines the role of a device within the network (coordinator, router or end device), initiates and/or responds to binding and discovery requests, and establishes a secure relationship between network devices. It also provides a rich set of management commands defined in the ZigBee Device Profile (used in ZigBee commissioning). The ZDO is always endpoint zero. The ZigBee Device Object (ZDO) manages the security policies and the security configuration of a device [107].
- **ZDO Management Plane** - Facilitates communication between the APS and Network Layers (NWK) with the ZDO. This allows the ZDO to deal with requests from applications for network access and security using ZDP (ZigBee Device Profile) messages [107].
- **Application Support (APS) Sub-Layer** – this provides a data service to the application and ZigBee device profiles. It also provides a management service to maintain binding links and the storage of the binding table itself. The APS sub-layer provides services for the establishment and maintenance of security relationships [107].
- **Security Service Provider (SSP)** – this provides security mechanisms for layers that use encryption (NWK and APS). Initialized and configured through the ZDO [107].

- Network Layer (NWK)** - Handles network address and routing by invoking actions in the MAC layer. Its tasks include starting the network (coordinator), assigning network addresses, adding and removing network devices, routing messages, applying security, and implementing route discovery. The ZigBee Alliance builds on the 802.15.4 foundation by providing the Network Layer (NWK) and the framework for the application layer. The NWK is responsible for the secure transport of frames. The NWK supports star, tree, and mesh topologies [103].
- Medium Access Control Layer (MAC)** - The IEEE 802.15.4 standard defines the MAC sub-layer. The IEEE 802.15.4 MAC sub-layer controls access to the radio channel using a CSMA-CA mechanism. Its responsibilities may also include transmitting beacon frames, synchronization, and providing a reliable transmission mechanism [103]. ZigBee, through the 802.15.4 MAC layer, provides guaranteed time slots in a scheme that is similar to TDMA and is more complex and less power-efficient than TDMA [103].
- Physical Layer (PHY)** - The IEEE 802.15.4 standard defines the physical layer. The IEEE 802.15.4 has two PHY layers that operate in two separate frequency ranges: 868/915 MHz and 2.4 GHz. The lower frequency PHY layer covers both the 868 MHz European band and the 915 MHz band, used in countries such as the United States and Australia. The higher frequency PHY layer is used virtually worldwide [103].

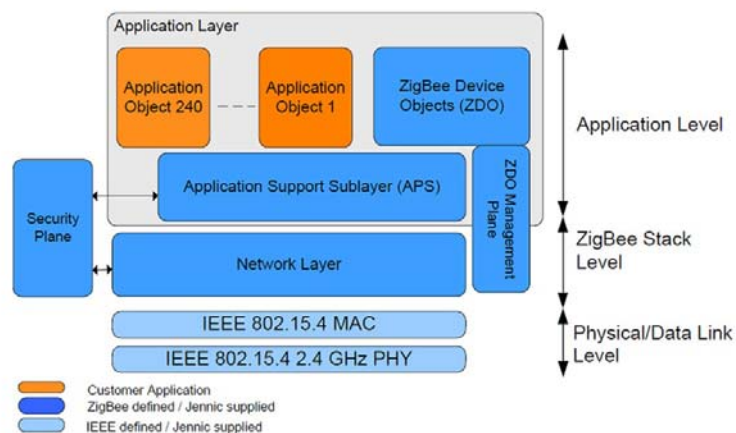


Figure 3-14: ZigBee functional layer architecture and protocol stack[106].

Figure 3-14 shows the ZigBee functional layer architecture and protocol stack. As mentioned earlier, ZigBee added an application layer on top of the IEEE 802.15.4 protocol. This layer includes ZigBee Device Objects and an Application Support Sub-layer. The security schema in ZigBee is defined in both network and sub-layer application. As can be seen, up to 240 objects are supported in the application layer in ZigBee.

#### 3.4.4 Protocol Devices

In a ZigBee network, all nodes share the same channel and there is no frequency hopping and a channel with the least amount of interference is used. There are two classes of network devices in ZigBee: Full-Function Devices (FFD) and Reduced-Function Devices (RFD) that communicate in a star network set-up. The following node roles are possible:

- **Coordinator** - This device starts and controls the network. The coordinator stores information about the network, which includes acting as the Trust Centre and being the repository for security keys [108].
- **Router** - These devices extend network area coverage, dynamically route around obstacles, and provide backup routes in case of network congestion or device failure. They can connect to the coordinator and other routers, and also support child devices [108].
- **End Devices** - These devices can transmit or receive a message, but cannot perform any routing operations. They must be connected to either the coordinator or a router, and do not support child devices [108].

The main difference between ZigBee and other WPAN definitions is the kind of devices that can be deployed in the network, namely: Full Function Devices (FFD) and Reduced Function Device (RFD). An FFD can receive and send messages over the 802.15.4, whereas an RFD is usually a sensor which sleeps most of the time and wakes up only in order to send messages.

#### 3.4.5 Network Topology

Network topology is the layout pattern of interconnections of nodes. A ZigBee network can have one of three topologies:

- **Star Topology** - In a star topology, the network is controlled by one single device called the ZigBee coordinator which is responsible for initiating and maintaining the devices on the network. All other devices, known as end devices, directly communicate with the ZigBee coordinator [76].

- **Mesh Topology** – In mesh topology, the ZigBee coordinator is responsible for starting the network and for choosing certain key network parameters, but the network may be extended through the use of ZigBee routers. Mesh networks allow full peer-to-peer communication. ZigBee routers in mesh networks do not currently emit regular IEEE 802.15.4 beacons. This specification describes only intra-PAN networks, that is, networks in which communications begin and terminate within the same network [76]. Mesh topology consists of a mesh of interconnected routers and end devices. Two pathways are connected to the router and enable the router to relay messages for its neighbours. Mesh networks includes a coordinator and multiple routers and end devices. In mesh topology, once a direct or indirect message is sent to a destination address, which has not yet been discovered, the coordinator or router should start a route discovery before sending message [76].
- **Tree Topology** - In tree networks, routers move data and control messages through the network using a hierarchical routing strategy. Tree networks may employ beacon-oriented communication as described in the IEEE 802.15.4 specification [76].

#### 3.4.6 ZigBee Routing Protocols

ZigBee networks are well organized by distributed address allocation mechanisms. In this network, any node that wants to join in the network must scan the network and choose a parent node. Then the parent node assigns it an address. The node, which is a router, is able to permit other nodes to join and construct a parent-child [109].

Considering the well-organized characteristics, ZigBee combines the Tree-based Hierarchical Routing (THR) and the well-known on Ad-hoc On Demand Distance Vector (AODV) routing protocol in order to meet certain cost-effectiveness and path robustness objectives [109].

THR directly gets the next hop node for a given destination address without routing discovery. This algorithm depends on the topology and a distributed addressing scheme of ZigBee networks.

AODV performs a route discovery process when the destination node address is new. However, route discovery is achieved by flooding the whole network, which may cause serious redundancy, contention, and collision.

The ZigBee Tree-based routing considers neighbour nodes and chooses the local node with the shortest path to the destination as next hop node. There are three steps to navigate nodes in the ZigBee standard [110].

- Step 1: if the destination node is in its neighbour table, directly transmit to corresponding node.
- Step 2: if the destination node is its descendant node, choose one of its children nodes as the next hop node.
- Step 3: if the above conditions are not satisfied, then choose the node with minimum hop to the destination node.

When a node wants to transmit data to another, it first checks that there is an entry in the route table for the destination. If it is there, it directly obtains the next hop address from the routing table. Otherwise, it performs a routing discovery process by broadcasting RREQ before sending the data in order to build a routing path [110].

When receiving the RREQ, the destination node responds by unicasting RREP along the reverse path. The routing discovery process is finished when RREP reaches the source node. Then the built path is added into the routing table and the source node starts to transmit data along the path [110].

For broadcasting RREQ, a straightforward approach is blind flooding which requires no knowledge of network topology, and packets are broadcast to all destinations. Therefore, it generates an excessive amount of traffic in large networks and suffers from a broadcast storm problem, which refers to the fact that flooding may result in excessive redundancy, contention collision. So if the flooding packets are limited to certain sets of nodes and avoids redundantly broadcasting to the whole network, the control overhead can be significantly decreased [110].

### 3.4.7 ZigBee Installation and Configuration

One of the great advantages of a ZigBee network is the ease with which it can be installed and configured. As already mentioned, the installation is simplified and streamlined by the use of certain battery-powered devices, with no need for power cabling. In addition, since the whole system is radio-based, there is no need for control wiring to any of the network devices. Therefore, ZigBee avoids much of the wiring and associated construction work required when installing cable-based networks [111].

The configuration of the network depends on how the installed system has been developed. There are three system possibilities for configuration: pre-configured, self-configuring and custom.

- **Pre-configured System** - A system in which all parameters are configured by the manufacturer. The system is used as delivered and cannot readily be modified or extended. Examples: vending machine, patient monitoring unit.



- **Self-configuring System** - A system that is installed and configured by the end-user. The network is initially configured by sending “discovery” messages between devices. Some initial user intervention is required to set up the devices; for example, by setting switches on the devices. Once installed, the system can be easily modified or extended without any re-configuration by the user; the system detects when a device has been added, removed or simply moved, and automatically adjusts the system settings.
- **Custom System** - A system that is tailored for a specific application/location. It is designed and installed by a system integrator using custom network devices. The system is usually configured using a software tool [111].

The size of the network and configuration are defined by the coordinator. The number of nodes, routers and children in the network are determined by the coordinator. In fact, these concepts include Depth, Number of Children and Network Address Allocation.

- Depth: This is the depth of devices from the root of the network.
- Number of Children: The number of children that are assigned to a router within a network.
- Network Address Allocation: The coordinator allocates a block of sequential addresses to each router for its children. The block address of the router can be subdivided to the child routers and other nodes in the network [76].

### 3.4.8 Starting a Network

The coordinator initializes a scan of all channels and searches for the best radio channel to avoid interfering with other frequencies such as LAN Wireless. Then it starts to define the PAN ID (Personnel Network Identification) and prepares to hear from the nodes which want to join the network [76].

### 3.4.9 Joining a Network

Routers and end devices can be joined to the available coordinator. Both routers and coordinator are able to allow nodes to join the network. These steps show the sequence of a node joining the network:

- 1- The node wants to join the network; firstly scan the channel and try to find a suitable channel for communicating; sometimes multiple networks may operate in the same channel and are differentiated by PAN ID.
- 2- The node may be able to see multiple coordinators and routers. In this case, it usually communicates with the router or coordinator which has the best signal.

- 3- The node sends a message to the router asking to join the network.
- 4- The router gives permission to the node to join the network. This decision is made by permit list or address space available in the router [76].

#### 3.4.10 Message Addressing

In the ZigBee network, every single node should have unique identification. This identification can be achieved by IEEE MAC address and Network Address. There are two types of addressing in the ZigBee network; one is global identification and the other one is local..

- IEEE MAC Address: This is a 64-bit address which uniquely identifies the device in the network. This address is unique in the world and there are no two devices with the same MAC address.
- Network Address: This 16-bit address identifies the node in the network. Network address is allocated by the parent node once it joins the network [76].

#### 3.4.11 Establishing Communication between Two Nodes

Establishing communication between two devices is the process that allows the devices to exchange information and perform the appropriate functions. A device in the network should be able to discover other devices to use their information needed by the device to perform its own functions according to its profile. Hence, two nodes should be compatible in order to generate data which can be accepted and interpreted by other nodes in a meaningful way [76].

Compatible nodes can be established by service discovery, and communication between two compatible nodes can be implemented through a binding process.

In service discovery, a node is able to find and select other nodes with which it will communicate. This means that the node has requested services from other nodes by broadcasting a message to the network [76].

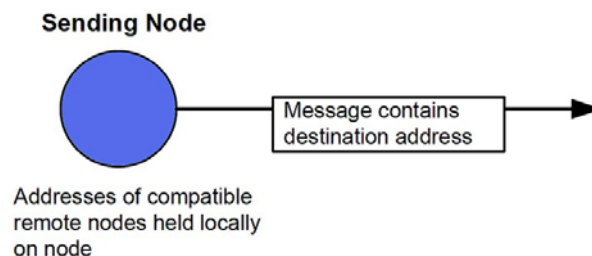


Figure 3-15: Addressing[76].

Figure 3-15 shows any node that has the requested information responds by the unicast. In this process, the requesting node may receive more than one response. This response includes the network address of the remote node with the requested services. The node stores this information and the application is able to use this information for future communications.

#### 3.4.12 Binding

Binding occurs when one node automatically routes data to the paired node. The two nodes must be compatible in order to submit a binding request to the coordinator [76]. Binding occurs in the application level using clustering. So, the binding of two application nodes produces a compatible cluster. For instance, for binding two temperature applications on two different nodes, one application must generate an output cluster related to temperature and the other one consumes an input cluster.

The binding between two applications is specified by:

- End point of the application, where the cluster is generated, and the source network address.
- End point of the receiving application and destination network address.
- The cluster ID, which has been sent between two applications.

It should be noted that bindings are stored in a binding table. By multiple entries for the cluster in the binding table, it is possible to develop complex binding.

The binding between two applications is specified by:

- One-to-one: This means that one node binds to only one other.
- Many-to-one: This means that any node in the network can route data to a coordinator by a single routing table entry in every device.
- One to-many: This means that one node binds to more than one destination end point [76].

Binding tables are stored in the coordinator of the network and the transmission of the cluster information is located in the coordinator. Thus, the message must be sent through the coordinator.

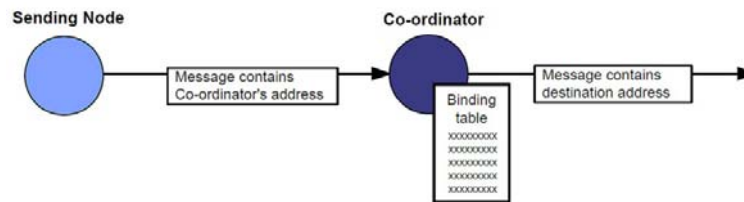


Figure 3-16: Indirect addressing[76].

Figure 3-16 shows the steps when the output cluster information changes on the source code:

- The coordinator receives the new information and the source application address, which includes network address and end point.
- The coordinator generates a message replicating cluster information and finds all binding tables which contain source cluster and application address.
- The destination address information from the table entry to the appropriate destination application is inserted in every single message by the coordinator and the sending node does not need the network address of the destination [76].

Therefore, the node that wants to send the network address of the destination node does not need to have the address of the destination node, as it has been already inserted by the coordinator. This process of addressing is called 'indirect message'.

### 3.4.13 Message Routing and Route Discovery

Routing allows remote devices to be joined to the network by connecting to the router and also allows the network to be extended beyond the distance supported by direct radio communication.

Route discovery is a facility in the ZigBee stack which helps the network to find the best available route to the destination during message sending. There are three options for route discovery:

- 1- Super Route Discovery: The message is routed throughout the whole of the tree.
- 2- Enable Route Discovery: The message is routed along the discovered mesh route; if there is already a discovered route, the router initiates another route. This depends on whether there is enough space in the router to store the new route; if there is no enough space, the router directs the message along the tree.
- 3- Force Route Discovery: In this route discovery, the router should have enough space for the route capacity to initiate the route discovery. After finishing the route discovery,

the router will send the message along the calculated route. Otherwise, the router will route the message along the tree. It should be noted that this latter process generates a great deal of traffic in the network [76].

The mechanism for the route discovery between two end-devices:

A route discovery is sent by the parent router of the source end device, which contains the network address of target destination address of the end-device. Then, all the routers in the network receive the broadcast address. The parent router of the destination node returns the address to the parent router of the source. During this travel, all the hop counts and signal quality are measured and recorded. Hence, every single router in the network builds a routing table entry along with the best path, which usually has the least number of hops. However, if a hop on the direct route has poor signal quality, a path with more hops and better signal quality may be selected. Finally, every router in the path has the routing table entry from source to destination of the end-device [76].

#### **3.4.14 Co-existence and Interoperability**

All devices which are used in a ZigBee network must comply with the ZigBee Standard to ensure co-existence and interoperability between ZigBee devices.

- Co-existence: This means no interference between devices which exist in the same network [76].
- Interoperability: The ability of a device to operate in conjunction and function with other devices.

It should be noted that interoperability implies co-existence, but co-existence does not imply interoperability.

### 3.4.15 Profile

The profile which has been designed by ZigBee Alliance for the purpose of interoperability contains the essential properties of a device for a particular application. There are two classes of the profile: Stack Profile and Application Profile [76].

- a) Stack Profile: Stack Profiles determine resources which are provided by the ZigBee stack the configuration of the network, such as the network type and shape, and the features that are available to applications, such as the types of security[76].
- b) Application Profile: An Application Profile addresses the needs of a specific application and it is associated with a particular Stack Profile.

ZigBee targets simpler, smaller networks that typically operate in a residential environment. Addressing is done in a tree fashion, security implementation is simple, and application bindings are done by the coordinator in a centralized manner. ZigBee Pro formerly targets larger and more sophisticated networks for any Commercial, Industrial and Institutional application. Also, addressing such as multicast is included, routing is more scalable, and security is more robust [105].

ZigBee 1.0 includes the Home Controls, Lighting (HCL) application profile, which provides basic definitions for simple residential lighting applications. This application is used for devices such as switches, dimmers, occupancy sensors and load controllers [76].

ZigBee 1.1 includes additional application profiles:

- Home Automation Profile (HA) which replaced HCL. It relies on the ZigBee stack profile and applies to a set of devices for use in home environments: switches, thermostats, window shades, radiators, and so on [112].
- Commercial Building Automation (CBA) targets large building systems and relies on the ZigBeePRO stack profile. The specification includes device descriptions for lighting and HVAC management [112].
- Industrial Plant Monitoring (IPM) includes device definitions for sensors and actuators and it is used in industrial control for temperature, pressure, infrared, and so on [112].
- Smart Energy profile relies on the ZigBeePRO stack profile and provides an approach to the clever use of energy encompassing measures ranging from keeping consumers informed about their power consumption to the automated rescheduling of power-hungry activities to off-peak/low-price periods [113].

c) Application Profile Security: All communications in the ZigBee profiles network are secured to protect them against both intentional and unintentional interference. To do this, ZigBee PRO incorporates a number of security features. In addition, the ZigBee profiles provide security enhancements concerned with establishing the security keys used in network communications[114].

#### **3.4.16 Attribute and Cluster**

The type of data, which a device with a profile can exchange with other ZigBee devices, is defined by attributes and clusters.

- Attribute is a data item which passes between two ZigBee devices. Every attribute has the unique identifier [76].
- A cluster is a group of attributes. Every cluster also has a unique identifier [76]. In fact, cluster is a related collection of commands and attributes which define the interface to specify functionalities[115].

For instance, a switch device has the attribute with identifier of OnOff, which has the value of On (0xFF), Off (0x00), and Toggle (0x0F) and the OnOffSRC identifier contains the attribute OnOFF in a cluster [76].

#### **3.4.17 ZigBee Cluster Library**

The ZigBee Cluster Library is a repository for cluster functionality working as a library with regular updates if a new function is added. When developing a new application profile, the ZCL should be applied to find the relevant cluster functionality to incorporate into the new profile. Also, this means that the ZigBee Profile is developed in an object-oriented manner. The optional or mandatory clusters are defined by an application profile. For example, two devices which operate together for temperature monitoring and control are concerned with temperature cluster. The sensor must have an output cluster containing the monitored temperature, and the controller must have an input cluster that uses temperature to control a decision [115].

#### **3.4.18 Discovery**

Discovery is used when a node is being introduced into a user-configured network. The ZigBee enables devices to find out about the capabilities of other nodes in the network such as addressing, power source and sleep behaviour. This information is stored on each node, which then tailors its behaviour to the requirements of the network. To integrate the device

into the network, it is necessary to determine whether there is any other appropriate device with which it can communicate. [115].

Device discovery returns the address of the network node, which can be the MAC (IEEE) address of the node along with network address or vice versa. In fact, if the node being identified is a router or coordinator, it may supply its own address as well as the addresses of all devices which are associated with this node. Hence, if other queries need to be launched, it is possible to discover all devices in a network through the coordinator [116].

### 3.4.19 Security

ZigBee provides a standardized toolbox of security specifications and software. Security services for ZigBee include methods for key establishment, key transport, frame protection, and device management. In fact, all these services constitute the security policies within a ZigBee device.

#### a) Keying Models

ZigBee uses three types of keys to manage security: Master, Network and Link.

- Master Keys - These optional keys are not used to encrypt frames. Instead, they are used as an initial shared secret between two devices when they perform the Symmetric-Key Key Establishment (SKKE) to generate Link Keys. Keys that originate from the Trust Center are called Trust Center Master Keys, while all other keys are called Application Layer Master Keys [117].
- Network Keys - These keys are used by the Network Layer. All devices on a ZigBee network share the same key. High Security Network Keys must always be sent encrypted over the air, while Standard Security Network Keys can be sent either encrypted or unencrypted [117].
- Link Keys - These optional keys secure unicast messages between two devices at the Application Layer. Keys that originate from the Trust Center are called Trust Center Link Keys, while all other keys are called Application Layer Link Keys [117].



## b) Key Transport

The transport-key service provides secured and unsecured transport key commands to transfer a key to other devices.

The secured transport-key command provides a means to transport a master, link, or network key from a key source to other devices.

The unsecured transport-key command provides a means for loading a device with an initial key. This command does not cryptographically protect the key being loaded. In this case, the security of the transported key must be realized by non-cryptographic means [118].

### 3.4.20 Joining a ZigBee Network

There are two ways to join a ZigBee network: MAC association and NWK re-join.

- **MAC Association:** In this case, a ZigBee router or coordinator that intends to allow other devices to join to the network must issue a request, which is called NLME-PERMIT-JOINING. The joining device, must issue a NLME-JOIN.request, which kicks off the request, with the re-join flag set to FALSE to discover the network to join a specific device to that network. Therefore, the joining device makes a request to join the network and the receiving device issues a response. This response includes an address for the device to use while associated with that network. As the MAC association is an unsecured protocol and is sent openly, this association is not recommended [108].

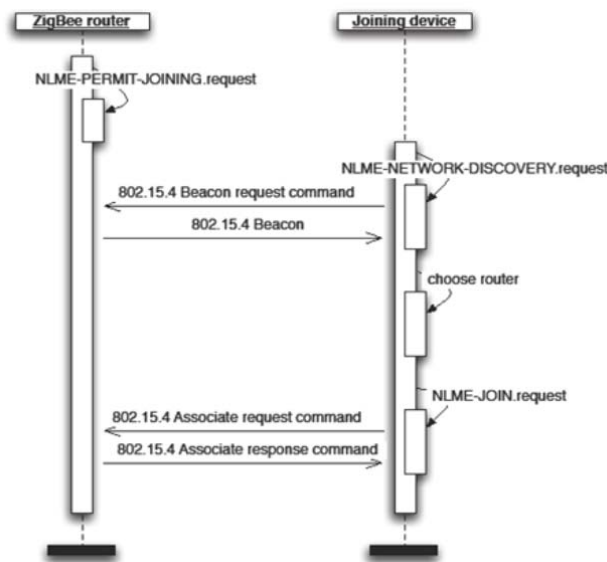


Figure 3-17: MAC association [108].

Figure 3-17 shows that the joining device makes a request to join the network and the receiving device issues a response, which includes an address for the device to use while associated with that network. It is shown that a ZigBee router or coordinator that intends to allow other devices to join must issue a NLME-PERMIT-JOINING.request. During the joining, after a device has discovered which network and device to join, a request should be made to issue a NLME-JOIN.request with the re-join flag set to FALSE.

- **Network Re-join:** The network re-join process takes place in the Network layer protocol and it is not subjected to the MAC address, which is already built into the devices. It means that the transaction may be secured by a joining device which knows the current NWK key. This occurs even if the device obtains the NWK via an out-of-band mechanism to join the network [108].

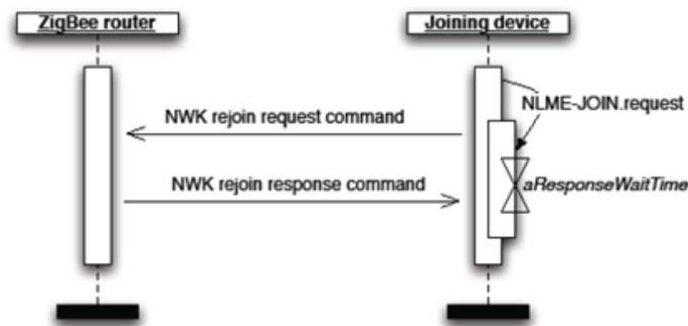


Figure 3-18: Network re-join[108].

Figure 3-18 shows the optional network discovery steps and mechanism for permitting devices to join the network and can be used whether or not the ZigBee router has issued a NLME-PERMIT-JOINING.request.

### 3.5 ZigBeePRO

The ZigBee Alliance has created the ZigBee PRO specification which is targeted at the industrial market. ZigBee PRO offers both enhanced security features and the ability to change the channel when faced with large amounts of noise.

ZigBeePRO offers significant advantages in many areas of operation such as scalability of large networks, security, network resilience and ease of commissioning. ZigBee PRO offers two Standard and High security modes:

Standard Security Mode - The list of devices, master keys, link keys and network keys can be maintained by either the Trust Centre or by the devices themselves. The Trust Centre is still responsible for maintaining a standard network key and it controls policies of network admittance. In this mode, the memory requirements for the Trust Centre are far less than they are for High Security mode [119].

Key Exchange in ZigBeePRO is Symmetric-key Key Exchange (SKKE), which is a new security mechanism in ZigBee PRO and is applied to periodically update the Link Key. SKKE employs the Master Key to initialize a secure exchange, thereby increasing the system's security.

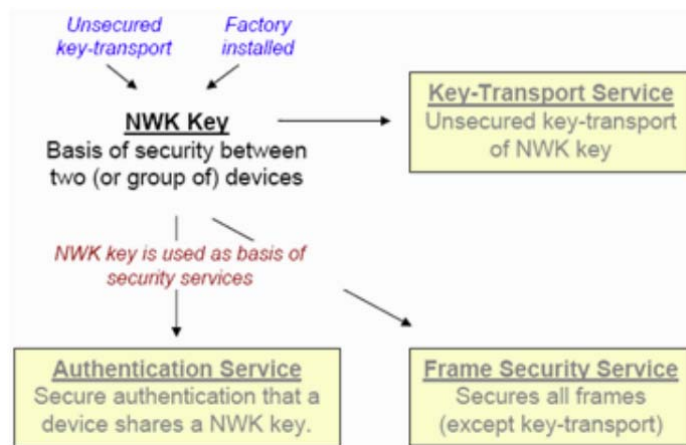


Figure 3-19: Standard Security Mode [119].

Figure 3-19 illustrates the Trust Center that is still responsible for maintaining a standard network key and it controls policies of network admittance. In this mode, the memory requirements are far less than those of the High Security mode.

In High Security mode, the additional security capabilities are used to control the infrastructure of critical systems, whether in a commercial building, utility grid, industrial plant, or a home security system.

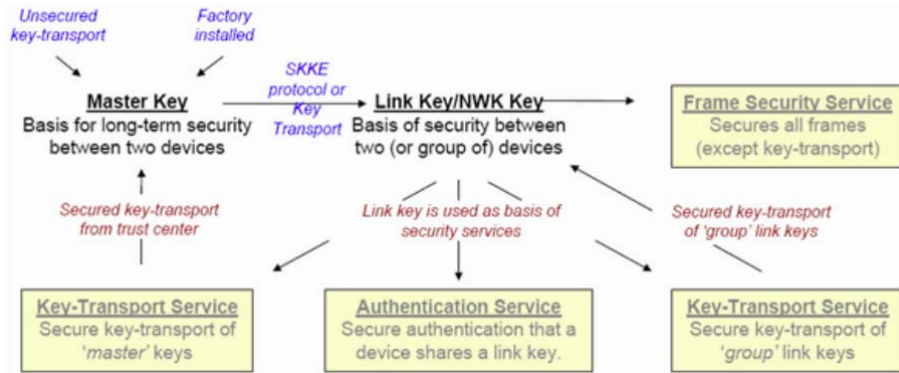


Figure 3-20: High Security Mode [119].

Figure 3-20 shows High Security Mode in the Trust Centre that maintains a list of devices, master keys, link keys and network keys for which it needs to control and enforce the policies of network key updates and network admittance. As the number of devices in the network increases, so too does the memory required for the Trust Centre [119].

### 3.5.1 Key Transport

The network establishes secure communications between nodes through a secure network. This is done by establishing routing and exchanging security information including a key. This key is then used to encrypt the data and make it available to nodes that hold the correct key. The integrity of communications is ensured so that the messages have not been altered or corrupted.

ZigBee/ZigBeePRO has a transport-key service which provides secured and unsecured transport key commands to transfer a key to other devices [113].

- The secured transport-key command provides a means to transport a master, link, or network key from a key source to other devices.
- The unsecured transport-key command provides a means for initializing a device with an initial key. This command does not cryptographically protect and a key is sent in plain text. It means the security of the transported key must be realized by non-cryptographic means [113].

### 3.5.2 Trust Centre

The Trust Centre decides whether to allow or disallow new devices into its network. It is responsible for the following security roles:

- Trust Manager: authenticates devices that request to join the network.
- Network Manager: maintains and distribute network keys.
- Configuration Manager: enables end-to-end security between devices.

The Trust Centre or coordinator can be any other dedicated device on the network [119].

### 3.5.3 Security Issues

This section reveals several security concerns regarding the ZigBee standard. There are several issues that make the ZigBee standard insecure and allow an adversary to execute attacks. However, an attempt was made to address these issues with ZigBeePRO. The issues are briefly explained below:

- Same Key on Multiple ACL Entries: ZigBee has a bug when the same key with two different ACL entries exists [120].
- Power Failures: If ACL provides the same nonce and the same security key for two messages, an eavesdropper is able to recover partial information regarding the plain text. This is known as the same-nonce-attack. Same-nonce-attack can happen after power failure, which results in a clear ACL. In fact, if the last nonce states are unknown after the power failure, the system resets the nonce state to a default value [121].
- No Support for Group Keys: The same key on different ACL entries causes nonce utilization. Only one ACL entry and change address according to destination on every frame and causes a problem that the receiver must know the “the Next Sender” to set up the ACL address [122].
- Sequential Freshness vs. Single ACL Entry: The same frames should not be transmitted more than once and security service is used by the receiving device [123].
- Weak AES-CTR Integrity Protection: The use of integrity protection based on a simple CRC calculation is not strong. It is possible to change the payload and generate a new CRC. It is then possible to forge a message and execute a confidentiality attack [123].
- Fast AES-CTR Denial-of-Service Attack: With replay protection enabled, when an adversary sends a forged packet with key counter 0xFF, frame counter 0xFFFFFFFF, and any payload any subsequent packet will be replayed and rejected [100].
- Acknowledgement Forgery: An adversary can forge the sequence number in acknowledgement packets. In this scenario, targeted jamming fools the sender into thinking that the packet has been received; hence acknowledgement could be legitimated or forged [100].

**Note:** For the next sections and chapters in this thesis, the author will use the term ‘ZigBee’ when referring to ZigBee PRO.

### 3.6 WirelessHART

WirelessHART is a mesh networking technology operating in the 2.4GHz ISM radio band that utilizes IEEE 802.15.4 compatible DSSS radios with channel hopping on a packet by packet basis. WirelessHART is backward compatible with core HART technology [77].

WirelessHART communication uses Time Division Multiple Access (TDMA) technology for communications between coordinate and network devices. The TDMA Data Link Layer establishes links specifying the timeslot and frequency for communication of devices. These links are organized into super frames to support periodically both cyclic and acyclic communication traffic. A link also is dedicated to decrease data processing latency [75].

Starting the transceiver consumes more power than when it is in use. In industrial sensor networks, there is a method to minimize network collision, contention and reduce the power consumption of devices. This method involves Time-Division Multiple Access (TDMA) algorithms. With this algorithm, all network communication is divided into distinct timeslots of equal length. A timeslot gives enough time for a device to transmit one packet and receive an acknowledgement from the recipient [124]. Every communication has its own unique timeslot. Therefore, the ability of each device to enter a low-power sleep mode as well as enabling contention-free communication throughout the network is not reserved for its own link. Inability to scale in an efficient manner is the weakness of this algorithm. To combat this problem, a hybrid TDMA algorithm can be used. This algorithm assigns a certain number of timeslots in the frame, which is not dedicated to a given communication link, along with open, free contention between the devices in the network [15].

#### 3.6.1 Protocol Devices

The following are key components of WirelessHART:

- **Gateway** - Provides the connection to the host network. WirelessHART and the main host are interfaced using Modbus, Profibus and Ethernet. The Gateway also provides the network and security manager [77]. HART devices deploy the Process Variable (PV) which is connected to a control or asset management system via a WirelessHART Gateway, and is read at the control system via the 4-20mA loop.
- **Network Manager** - Builds and maintains the mesh network to identify the best paths and manages distribution of slot time access, which depends upon the

required process value refresh rate and other access. In WirelessHART, each second is divided into 10msec slots. [77].

- **Security Manager** – This component distributes security encryption keys and holds the list of authorized devices in the network [77].
- **Repeater** - Routes WirelessHART messages and is used to extend the range of a WirelessHART network. All instruments in a WirelessHART network have routing capability [125].
- **Adapter** - Plugs into an existing HART-enabled instrument to pass the instrument data through a WirelessHART network to the host. This component could be located anywhere along the instrument 4-20mA cable. It could be battery powered or obtain its power through 4-20ma cable [125].
- **Terminal** - This component is used to join a new instrument to an existing WirelessHART network and has a connection to the gateway. It can be used for diagnostics [125].
- **Asset Management System** – This can utilize WirelessHART without the need for software upgrades [125].

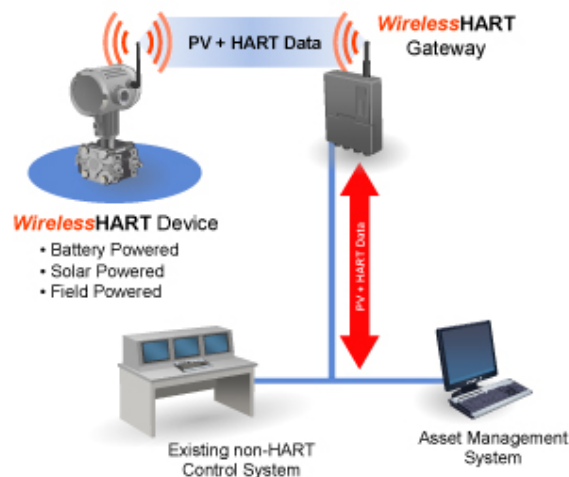


Figure 3-21: WirelessHART Standard [77].

Figure 3-21 shows WirelessHART devices which are free-standing devices in the control system. The devices can be installed anywhere in the plant without the cost of wires. As seen, the Adapter and HART data are connected to a control or asset management system via a WirelessHART Gateway.

### 3.6.2 Protocol Layers

The HART Protocol implements layers 1, 2, 3, 4 and 7 of the Open System Interconnection (OSI) protocol model:

- **Physical Layer** – This is based on the Bell 202 standard, using Frequency Shift Keying (FSK) to communicate at 1200 bps. The signal frequencies representing bit values of 0 and 1 are 2200 and 1200Hz respectively. The signal, without causing any interference with the analogue signal, is superimposed at a low level on the 4-to-20mA analogue measurement [126].
- **Data Link Layer** – This layer ensures that communications are successfully propagated from one device to another. It follows a master-slave protocol. There can be two masters such as control system and a HART communicator as a primary and secondary master. When each master initiates a communication transaction, timing rules are established [126].
- **Network Layer** - Provides routing, end-to-end security, and transport services. It manages sessions for end-to-end communication with correspondent devices [126]. Various keys to provide confidentiality and data integrity for end-to-end connections are employed in this layer. Four types of keys are defined in the security architecture:
  - **Public Key** - This is used to generate MICs on the MAC layer by the joining devices.
  - **Network Key** - This is shared by all network devices and is used by existing devices in the network to generate MAC MIC's.
  - **Join Key** – This key is unique in every network device and is applied during the joining process to authenticate the joining device.
  - **Session Key** – This key is generated by the network manager and is unique for each end-to-end connection between two network devices. End-to-end confidentiality and data integrity are provided by this key [127].
- **Transport Layer** – This layer can be used to ensure that end-to-end communication is successful [126].
- **Application Layer** – Defines the commands, responses, data types and status reporting supported by the protocol. The public commands of the protocol are divided into four major groups [126]:



- **Universal Commands** – They provide the necessary functions which must be implemented in all field devices.
- **Common Practice Commands** – They provide functions common to some devices not all field devices.
- **Device Specific Commands** – They provide functions that are specified by the device manufacturer and are unique to a particular field device.
- **Device Family Commands** – They allow full generic access without using device-specific commands and provide a set of standardized functions for instruments for the purpose of particular measurement types.

### 3.6.3 Security Overview

Both ZigBee and WirelessHART use the IEEE 802.15.4 standard protocol for communication in the WSN. However, WirelessHART uses the Physical layer specified in the IEEE 802.15.4-2006 standard, but specifies new Data-link (including MAC), Network, Transport, and Application layers.

Security is mandatory in WirelessHART. It is not possible to turn it completely off. Considering that security schemes consume additional processor time, memory and bandwidth this mandatory feature may be something that needs to be carefully considered for devices that may not require such security features but need to achieve extended battery life.

WirelessHART provides end-to-end and hop-to-hop security measures through payload encryption and message authentication on the Network and Data-link layers. However, the security measures are transparent to the Application layer. WirelessHART uses CCM 2 mode in conjunction with AES-128 block cipher using symmetric keys for message authentication and encryption [128].

Security mechanisms in WirelessHART aim to provide security through the following features:

- AES-128 block ciphers with symmetric keys.
- Separate join key per device.
- Network key to authenticate Data-Link PDUs.
- Session keys encipher network payloads between end-point devices.
- Point-point and broadcast sessions supported.

### **3.6.4 Keying Models**

A set of different security keys is used to ensure secure communications. A new device should be provisioned with a Join Key if it wants to join the wireless network. The Join Key is applied to authenticate the device for a specific WirelessHART network. Once the device has successfully joined the network, the Network Manager will provide it with proper Session and Network Keys for further communication. Security Manager handles the actual key generation and communication. Keys are distributed to the network devices by the Network Manager [128].

Two devices such as Field device and the Gateway use a Session Key in the Network Layer to authenticate the end-to-end communication. Different Session Keys are applied for each pairwise communication between Field device to Gateway and Network Manager. The Data Link Layer uses a Network Key to authenticate messages on a one-hop basis. This key is applied in devices to join to the network. In this process, only trusted devices are allowed to join the network. Trusted devices are identified by the Join Key and standard HART identity data. This standard includes Manufacturer ID, Device Type, Device ID and Tag [128].

### **3.6.5 Data Encryption**

The AES-128-bit security features provide privacy and are intended to prevent eavesdropping by unauthorized devices, whether inside or outside of the network. A WirelessHART sensor network provides end-to-end CCM mode AES-128-bit. This is based on a real-time unique timestamp which is a unique encryption key for each message [129].

### **3.6.6 Security Issues**

WirelessHART is a relatively secure protocol, but it relies on a Security Manager for the management of the Security Keys and the authentication of new devices. This means that any Security Manager failure causes a loss of security in the standard. In fact, the lack of Security Manager Design and unclear security specifications impede the implementation of this standard. In addition, the WirelessHART standard does not provide specifications and design of the Security Manager and the security specifications in the standard are not well organized [130].

## **3.7 ISA 100**

The ISA is a non-profit technical society that focuses on industrial automation. The ISA100 is the brainchild of the Instrumentation, Systems, and Automation Society (ISA). It has been the most trusted source for standards among industries, and is supported by industry

experts worldwide. ISA100 brings together experts in wireless technology, instrumentation, security, and a wide range of industrial end-user applications. This standard is intended to enable a single, integrated wireless infrastructure platform for plants and delivers a family of standards defining wireless systems for industrial automation and control applications. The ISA100.11.a standard adheres to a comprehensive coexistence strategy, which provides “the ability of wireless networks to perform their tasks in an environment where there are other wireless networks that may or may not be based on the same standard” [78].

The ISA100.11a standard is based on the IEEE Std 802.15.4 PHY and MAC, operating only in the 2.4 GHz band. It concerns frequency hopping, multi-hop mesh networks, inter-network routing. Like WirelessHART, ISA100 uses TDMA along with network self-configuring and self-healing algorithms [78].

ISA100.11a also provides a tunnelling protocol which enables the network to carry existing protocol such as HART, Fieldbus, Modbus, Profibus, Common Industrial Protocol (CIP), and so on. The ISA100 wireless network is able to send all these protocols wirelessly, preserving existing protocol investments and protecting future protocol need [78].

Recently, the ISA100.12 subcommittee was established by ISA 100 to investigate options for the convergence of WirelessHART and ISA100.11a. The goal of this committee is to integrate these key standards [78].

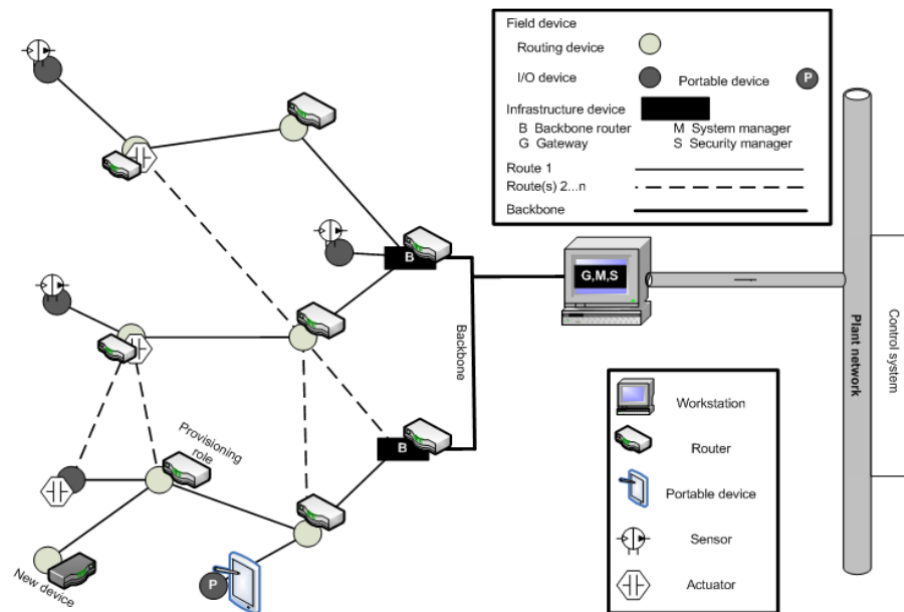


Figure 3-22: Application protocols supported by ISA100 [78].

Figure 3-22 shows application protocols supported by ISA100 and a complete network compliant with this standard. As depicted, there are several types of devices including sensors, actuators, routers, a hand held computer, and a workstation.

### 3.7.1 Protocol Devices

The primary components of the management service includes a device management application process that resides in every ISA100.11a device and the system applications manager that may exist on a small subset of devices [78].

- Workstation - has the roles of gateway, system manager, and security manager.
- Backbone routers – it is the role of routers.
- Sensors – they are the singular role of an I/O device.
- Router – has assumed a provisioning role.
- Actuator - has both the router and I/O roles.

### 3.7.2 Protocol Layers

ISA100 uses the OSI layer description methodology to define protocol suite specifications in terms of security, management, gateway, and provisioning for an industrial wireless sensor network [78]. ISA100 provides reliable and secure operation for non-critical monitoring, alerting, supervisory control, open loop control, and closed loop control applications. It defines the specifications for low data rate wireless connectivity along with very limited power consumption requirements[131]. The object-oriented modelling concepts support both ISA100.11a and non-ISA100.11a protocol tunnelling applications. The object model is protocol, platform, and language neutrality [78].

- **Physical Layer** - The physical layer converts the digital data information into the radio frequency energy emitted, which is captured by a devices antenna. The PhL provides two services, the PhL Data Service and the PhL Management service. These services are collectively known as the PhSAP. The PhL data service enables the transmission and reception of actual user data (PhPDUs) through the physical radio channel. The PhL management service is used to control the operating functions of the radio such as frequency selection and transmission power [131].
- **Data Link Layer** - The data link (DL) layer in this standard is designed to constrain the range of building options for a field device and enables flexible system solutions. The DL specification provides a set of capabilities and is verifiable for each field device. The DL can be conceptualized as a table-driven state machine that operates independently on each field device.

- **Network Layer** - The network layer is responsible for translation between the various types of addresses, when a Protocol Data Unit (PDU) moves from a DL subnet to a backbone network. PDU is a specific format that implements the features and requirements of protocol. The network layer in this standard performs the following functions:
  - **Addressing** - The network layer determines the appropriate address information for a PDU.
  - **Address Translation** - This standard uses two types of addresses: short (16-bit), and long (128-bit). The short address is used within a DL subnet to conserve energy and bandwidth and application end points and backbone networks use long addresses.
  - **PDU Formats** - In this standard, the network layer selects an appropriate format for the PDU based on such considerations as addressing, routing and level of service.
  - **Fragmentation and Reassembly** - This is handled by the network layer in this standard.
  - **Routing** - ISA100 11a performs routing at two levels: the backbone level and the mesh level. The network layer is responsible for routing PDUs at the backbone level and routing at the mesh level is performed by the DL [131].
  
- **Transport Layer** - The Transport Layer (TL) responds to service requests from the application layer at a Transport Layer Service Access Point (TSAP) and issues service requests to the Network Layer (NL) at a Network Layer Service Access Point (NDSAP). The TL is responsible for end-to-end communication and operates in the communication end points [131]. It has the responsibility to transfer data between end systems and end-to-end error recovery [78].
  
- **Application Sub-Layer** - ISA 100 provides some capabilities and services to enable an open interoperable ISA100.11a application environment. This standard provides support for wireless field devices to integrate a gateway to an ISA 100a wireless network with a host control system. The Application Sub-Layer determines how all the applications are plugged together [80]. Every ISA100.11a device contains an application process called the Device Management Application Process (DMAP), which manages the local communication aspects of the device.

More advanced devices in ISA100a have DMAP along with an additional User Application Process (UAP) [131].

### 3.7.3 Security Overview

The security services in ISA100 are selected by policy. The policy is distributed with each cryptographic material, permitting focused policy application. Since a single key is used at a time at the DL, except for a brief period of the key handover, the entire sub-network is subject to the same policies as the DL. The Security Manager controls the policies for all the cryptographic materials it generates [131].

One of the most important aims of the ISA100 standard is to provide security mechanisms for Single Security System Management for the automation industry. ISA100 provides simple, flexible, and scalable security that addresses major industrial threats by leveraging 802.15.4-2006 security [131].

Security is a major design facet of ISA100.11a that considers the entire WSN life cycle including configuration, operation and maintenance. Security is considered throughout the whole system, not only at the PHY layer or MAC sub-layer. This standard reduces costs and allows quicker implementations [131].

Security specifications provide authentication, encryption, and authorization services through the following security mechanisms:

- The communications security functionality is primarily transmission security with authorization based primarily on device identity and configured plant communication.
- Transmission security is provided for the MAC sub-layer and for the transport layer.
- Medium access control security protects the system against attackers who are outside the system (out-of-band) and do not share the system.
- Transport security protects the system against attackers who are already inside the system (in-band) and have co-opted some devices [132].

The security services in this standard are selected by policy. The policy is distributed with each cryptographic material, permitting focused policy application. Since a single key is used at a time at the DL, the entire sub-network is subject to the same policies as the DL [131]. The primary security components of the provided services include [131]:

- Authorization of secure communications relationships between entities.
- Message authenticity, ensuring that messages originate from an authorized member of a communications relationship and that they have not been modified by an entity outside of the relationship between the sender and the receiver.
- Assurance that delivery timing and order does not exceed anticipated bounds.
- Data confidentiality that conceals the contents of payloads.
- Protection against malicious replay attack.

Various combinations of these services are provided at both the DL and the TL. Additionally, various cryptographic services are available for use by the Device Security Management Objects (DSMO) for the join process, session establishment and key update [131].

### 3.7.4 Keying Model

The types of keys used in ISA100 are both symmetrical and asymmetrical key variants [132]. Session keys have a limited lifetime and are updated periodically, which is initiated by a device, to ensure that the session is kept alive. The key update process may be initiated by a device, although it should be pushed from the Security Manager between the soft and hard lifetime of a session key.

- **Proxy Security Management Object (PSMO)** - This object acts as a proxy for the Security Manager.
- **Device Security Management Object (DSMO)** - This object facilitates the management of the security functions of the device.
- **Security Manager** - Application software that supervises various operational security aspects of a multi-device network, usually through interaction with device security management objects (DSMO) in the supervised device(s) [131].

Symmetric keys are used for data encryption and authentication. Each key is limited in time and can be updated. All WSN symmetric keys are 128 bits. The symmetric keys used include:

- **Global Key** - A well-known key that is not used to guarantee any security properties.
- **Join Key** - A key received at the conclusion of the symmetric key provisioning step. It is used to join a network.
- **Master Key** - A key first derived at the conclusion of the key agreement scheme. This key is used for communication between the Security Manager and the device. The key expires and needs to be periodically updated.

- **DL Key** - A key used to compute the MIC at the DL. That key expires and needs to be periodically updated.
- **Session Key** - An optional key used to encrypt and/or authenticate Protocol Data Unit (PDU) at the transport layer. This key expires and needs to be periodically updated [131].

#### 3.7.4.1 Asymmetric keys and certificates

All WSN asymmetric keys have a cryptographic bit strength of 128 bits. The asymmetric keys used include:

- o **CA\_root** - The public key of a certificate authority that signed a device's asymmetric-key certificate. This key is commonly referred to as a root key and is used to assist in verifying the true identity of the device communicating the certificate, as well as some related keying information.
- o **Cert\_A** - The asymmetric-key certificate of device A, used to evidence the true identity of the device, as well as related keying information, during execution of an authenticated asymmetric-key key establishment protocol [131].

#### 3.7.4.2 Data link layer frame security

The degree to which a device is permitted to participate in a DL network or subnet is determined by system policy applied to credentials supplied by the device. Devices without credentials are permitted full, limited, or no participation beyond join attempts, as determined by system policy for such devices [131].

The AES security processing engine is always on at the DL. In non-secure mode, the key distributed might have travelled over an insecure channel. When a properly secured secret DL key is used, the following security services are always provided [131]:

- Media access control sub-layer Protocol Data Unit (MPDU) authentication.
- MPDU integrity.
- Proof that the MPDU was received at the intended time, providing rejection of MPDUs.
- Data is not sourced by a device within the network that shares an appropriate data key.
- Data is not received at a time for which their reception was intended.
- Encryption of the Data link layer Service Data Unit (DSDU).



### 3.7.5 Data Encryption

This standard uses AES-128 as a symmetric encryption algorithm and asymmetric encryption standard for this standard is based on elliptic curves defined over binary finite field. There is a public key encryption scheme for wireless sensor networks, which combines codes and encryption [131, 133].

### 3.7.6 The Join Process

The join process follows the provisioning step, during which cryptographic information and non-cryptographic configuration parameters may be provided to the new device. A new device obtains such necessary provisioning information from the provisioning device [131]. A joining device joins the target network with one of the following security options:

- Symmetric keys
- Public keys
- No security

The no security option does not apply security key for transfer of join keys. The MIC then is the equivalent of a strong CRC with no security guarantees, but with a very high probability of detection of random errors. Additionally, no end-to-end secure sessions are allowed.

A device implementing the symmetric key join process option has the following security-related information:

- A 128-bit join key.
- The 64-bit unique ID of the security manager that shares the join key.

A device implementing the asymmetric-key join process option has a certificate signed by a certificate authority trusted by the target network. A device implementing the no security join process option has the well-known, published, non-secret 128-bit key common to all standard-compliant networks [131].

### 3.7.7 Key Update

Session keys have a limited lifetime and are updated periodically to ensure that the session is kept alive. The key update process may be initiated by a device, although it should be pushed from the Security Manager between the soft and hard lifetime of a Session Key [131].

### 3.7.8 Security Issues

The details of the security issues of ISA100 are yet to be formally documented. The following issues require further consideration:

- Data privacy
- The keying architecture
- The encryption architecture

### 3.8 Key Findings

Through the above literature review, the State of the Art review of WSN discussed. According to that, a comparison table was designed to compare all existing features in three WSN standards such as ZigBeePRO, WirelessHART and ISA100. The table, along with explanation, is presented in the next section.

#### 3.8.1 State of the Art WSN Security Technology Compression Comparison

ZigBeePRO and WirelessHART represent proven industry WSN technologies. However, ISA100 is an emerging technology which promises many new features. This section presents a comparison of these standards from the perspective of basic features and security.

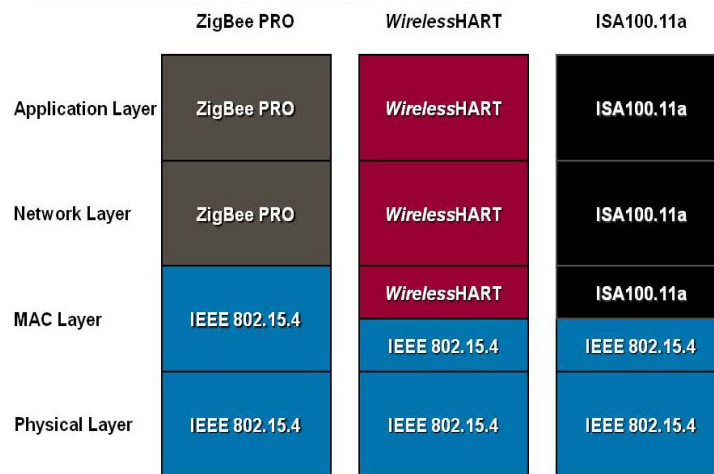


Figure 3-23: Overall Schema of Wireless Standards [94].

Figure 3-23 illustrates the overall schema of Wireless Sensor network in three standards. As can be seen, a two-layer network and the top application of the IEEE 802.15.4 have been added in ZigBee standard, whereas the MAC layer in both standard WirelessHART and ISA100 have been changed and modified and a two-layer network and application have been added.

#### 3.8.2 The Fundamental of the Security Features

ZigBee is a specification for the higher protocol layers of a WSN built upon the Physical (PHY) and Medium-Access Control (MAC) Layers in the 802.15.4 specification [98]. The

basic channel access mode is CSMA/CA. There are two classes of network devices in ZigBee: Full-Function Devices (FFD) and Reduced-Function Devices (RFD). In the FFD, coordinator, router, and end device nodes roles are possible. For RFD, only end device roles are possible. ZigBee supports star, tree, and mesh topologies.

WirelessHART is based on the PHY layer specified in the IEEE 802.15.4-2006 standard [98], but specifies new Data-link (including MAC), Network, Transport, and Application layers. WirelessHART is a TDMA-based network. The devices in the WirelessHART network include network manager, router, adapter, gateway, and handheld devices. WirelessHART forms mesh topology networks (star networks are also possible, but not recommended), providing redundant paths which allows messages to be routed around physical obstacles, broken links, and interference.

Like WirelessHART, ISA100 is based on the PHY layer specified in IEEE 802.15.4 but it specifies new Data-link (including MAC), Network, Transport, and Application layers, whereas ZigBee is a specification for the higher protocol layers only. It builds upon the Physical (PHY) and Medium-Access Control (MAC) layers in the 802.15.4 specification [88]. The Application Sub-Layer in ISA100a is necessary. This promotes interoperability and is a unique feature of the ISA100 specification that provides a set of common functions available to all applications. The Application Sub-Layer in ISA100a allows different applications in the Application Layer to communicate with each other in different stack layers through a common interface [131].

In the industrial market, the International Society of Automation's new ISA100a wireless standard is going to be a threat to the future of ZigBee. The ISA100a standard uses the 2.4 GHz band with Direct-Sequence Spread-Spectrum (DSSS) wireless technology, which is similar to ZigBee. Also, ISA100 is able to communicate simultaneously with most popular wired protocols while ZigBee does not support wired protocols. Furthermore, like WirelessHART, the ISA100 standard incorporates several strategies that are used simultaneously to optimize coexistence with other users of the 2.4 GHz radio spectrum [134].

### **3.8.3 Strength and Weakness of Security Techniques**

Security in ZigBee is not mandatory. However, there is support for encryption, authentication and integrity. ZigBee uses the security mechanisms in 802.15.4 which consists of a counter with CBC-MAC (CCM) and AES-128 encryption. Three keys are used in ZigBee: Master key, Link key and Network key. The Master key is used to join the network. The Link key is used for end-to-end encryption. The Network key is shared between all the

devices. All keys can be set at the factory, be given from the trust centre over the air, or through a physical interface [135].

Security in WirelessHART is mandatory. Like ZigBee, a counter with CBC-MAC (CCM) and AES-128 is also used. Three keys are used in WirelessHART: Join Key, Network Key and Session Key. The Join Key is similar to Master Key in ZigBee and is used to authenticate a device for a specific WirelessHART network. After the device has successfully joined the network, the Network manager supplies Network and Session Keys for further communication. The actual key generation and management are handled by a Security Manager, which is not specified by WirelessHART, but the keys are distributed by the Network Manager. The Session Key is used for authentication of end-to-end communications between two devices. That means different session keys are used for each pairwise communication. For example, in a WSN with two nodes, a sensor node and a gateway node, a Session Key is required. The Data Link Layer uses the Network Key to authenticate messages on a one-hop basis [135].

Like WirelessHART, ISA100 is based on the PHY layer specified in IEEE 802.15.4 but it specifies new Data-link (including MAC), Network, Transport, and Application layers, whereas ZigBee is a specification for the higher protocol layers only. It builds upon the Physical (PHY) and Medium-Access Control (MAC) layers in the 802.15.4 specification [135].

The Application Sub-Layer in ISA100a is necessary. This promotes interoperability and it is a unique feature of the ISA100 specification that provides a set of common functions available to all applications. The Application Sub-Layer in ISA100a allows different applications in the Application Layer to communicate with each other in different stack layers through a common interface [131]. Table 3-3: summarises the features of ZigBee, WirelessHART and ISA100 standards:

Table 3-3: WSN Comparison

	<b>ZigBeePRO</b>	<b>WirelessHART</b>	<b>ISA 100a</b>
<b>Frequency</b>	2.4 GHz	2.4 GHz	2.4 GHz
<b>Transceiver</b>	IEEE 802.15.4	IEEE 802.15.4	IEEE 802.15.4
<b>Radio Channel</b>	CSMA-CA	TDMA	TDMA/CSMA
<b>Node Roles</b>	Coordinator which is the trust centre; router; and end devices	Gateway, repeater; adapter; and handheld terminal, and network manager	System manager, Security Manager, gateway, backbone router, system time source, provisioning, and I/O devices.
<b>Topology</b>	Mesh, Star, Tree	Mesh, Star, Combined Star and mesh	Mesh, Star, Combined Star and mesh
<b>Security</b>	Optional	Mandatory	Optional
<b>Keys</b>	Symmetric/Asymmetric keys	Symmetric keys	Symmetric/Asymmetric Keys

	Master, network and link keys		Join key, network key, and Session Key which equals to link key		Symmetric keys include global key, join key, master key, DL key, and session key; Asymmetric keys include CA_root and Cert-A.	
<b>Keying Modes</b>	Standard security mode High security mode		Rotating keys which can prevent unauthorised devices from joining or communicating on the network		The security services are applied at each layer. Security services also are used within devices and for special cases the join process when lower layer security services are not available	
<b>Key Establishment and Transport</b>	Handled by the trust centre		Handled by a Security Manager and network manager		The Security Manager controls the policies for all cryptographic materials it generates	
	Master key	Factory pre-loaded, in-band delivery, or out-of-band delivery [94]	Join key	Provisioned before the device joins the network.	Global key	This key is static and published.
					Join key	Symmetric key provisioning step
					Master key	Derived at the conclusion of the key agreement scheme
	Network key	Factory pre-configured, or sent via in-band unsecured key transport [136]	Network key	Network manager provides it	DL key	In non-secure mode, the key distributed might have travelled over an insecure channel [98]
					Session Key	Key centre uses KEKs (masters) to distribute sessions. Session keys needs to be periodically updated
	Link key	Key agreement based on the master key	Session key	Network manager provides it	CA-root	Root key
Cert-A					During execution of an authenticated public-key key establishment protocol	
<b>Key Updating</b>	No		No		Each key is limited in time and can be updated. Key update process may be initiated by a device	
<b>Encryption</b>	AES-128 CCM*		AES-128 CCM*		AES-128 CCM*	
	Network level	The common network key	It provides end-to-end and hop-to-hop security measures through payload encryption and message authentication on the Network and Data-link layers. Based on real (unique) timestamps, the ciphers of messages are different		Encryption protection is possible at the bottom and the top of protocol stack.	
	Device level	Link keys between pairs of devices [136]				
<b>Integrity</b>	AES-CCM*		AES-CCM*		AES-CCM* HMAC, digital signature	
	ZigBee specifications provide options of providing 0.32, 64, or 128 bit data integrity for the		Message integrity codes verify each packet			

	transmitted messages. The default is 64 bit integrity [136].					
<b>Authentication</b>	AES-CBC-MAC		AES-CBC-MAC		HMAC, Asymmetric keys	
	Network level	The common network key	End-to-end	Session keys	Message authentication	Keyed hash function
	Device level	Link keys	The Data Link layer	Network key	Device authentication	Symmetric keys and unique device IDs, with an option for asymmetric keys
<b>Robustness</b>	Low		High		High	
<b>Priority Management</b>	No		Yes		Yes	
<b>Co-Existence</b>	Low		Low		High	
<b>Energy Consumption</b>	High		Low		Low	
<b>Reliability Determinism</b>	Yes		Yes		Yes	
<b>Implementation</b>	Easy		Challenging		Effective implementation through: - Compliance testing programs - Associated market awareness - Technical support	
<b>Latency Determinism</b>	No		Yes		Yes	

As shown in Table 3-3, all the discussed features in the ISA100 have been dramatically improved. The ISA100 standard was an attempt to remove the existing weaknesses of ZigBeePRO and WirelessHART. Some parts of the ISA100 derive from the Wireless-HART system. In comparison with ZigBeePRO and Wireless HART, the ISA100.11 is intended to provide more reliable and secure operation for non-critical monitoring, alerting, and control applications specifically focused on meeting all security requirements.

### 3.9 Summary of the WSN Security Strength and Weaknesses

This chapter outlined the unique strengths and weaknesses of WSN technology. An overview of WSN and a survey of existing literature were carried out. Also, existing literature was critically examined with a view to analysing and assessing each category. The constraints of WSN in terms of communication, device limitation and deployment have been explained. Stemming from these constraints, the vulnerabilities and challenges of WSNs were introduced.

- 1- There is a lack of proper sensor node configuration as a security requirement in WSN technology that may result in serious consequences in terms of external security attack as well as implementation of such technology.

- 2- There is no architectural framework available that allows the testing of WSN security to identify the vulnerabilities and to allow evaluation or comparison of the alternative wireless systems.
- 3- There is no systematic approach to Risk and Impact Analysis when implementing WSNs. The absence of such an approach means that the issues identified are those which hinder in industry and lead to potential money loss.
- 4- Disadvantages of wireless include the potential for radio interference due to weather, other wireless devices, or obstructions like walls, and more security issues [29].
- 5- Due to lack of specific guidelines in wireless stack development, the creation of software stacks for international wireless standards has become a major challenge.

To find out how secure WSN technology is, in this thesis an experiment was conducted on actual devices from one of the mentioned WSN standards - ZigBee, WirelessHART and ISA100. Due to several restrictions and limitations which will be explained in the next chapter, the ZigBee standard was chosen for the test-bed network.

### **3.10 Conclusion**

This chapter outlines the current, state-of-the-art features of WSN security. The importance of security to counter exploits in WSN has been discussed in detail. Also, it documents the WSN state-of-the-art when it comes to secure transmission and operation and the typical attack countermeasures that can be effectively employed. The IEEE 802.15.4 protocol, which is employed as the communication backbone in WSNs, was considered and the typical WSN standards such as ZigBee, WirelessHART and ISA100 were described. This chapter ended with a comparison of the features of ZigBee, WirelessHART and ISA100 technologies. The following chapter will propose problem definitions.

## **4 Problem Definition**

### **4.1 Introduction**

A survey of the literature was presented in Chapter 3 and a series of weaknesses in current WSN approaches and existing standards were identified. Despite significant contributions made in recent years, and that many practical solutions and approaches regarding the security aspects of WSN have been proposed, due to the emerging attacks, there is a need for the ongoing development of solutions to counter these attacks.

Following the previous chapter, and especially the later part of literature review, we choose the advanced ZigBee technology and evaluate its security. Several research issues that address the problems of ZigBee were identified in the previous chapter. To address the shortcomings discerned in the literature, in this chapter, the problems that are addressed later in this thesis are outlined. Then the research methodology and solutions are proposed.

In Section 4.2 of this chapter, the research gap in the ZigBee security area is described. In Section 4.3, the research issues are presented and in Sections 4.4 and 4.5 the research objectives and the significance of this thesis are explained. The hypothesis of this thesis, based on the research question, is stated in Section 4.6. Section 3.8 contains the problem definition in terms of ZigBee security vulnerabilities. In Section 4.7, the research method to be adopted in this thesis is introduced, and the definitions that will be used throughout the thesis, are outlined. In Section 4.6, the main problems to be addressed by this thesis are described. In Section 4.7, the main problem is broken down into research issues in order to better propose the solution. Section 4.8 concludes the chapter.

### **4.2 Problems in WSN**

Although the ZigBee, WirelessHART and ISA100 standards are advertised as being open and public, there were serious issues with the supply of WirelessHART and ISA100 technical resources, development equipment, and software. WirelessHART cannot be purchased by non-OEM customers and promised documents outlining third-party security tests have never surfaced. Also, ISA100 specification is only ratified well into the project and no development kits are currently available. Therefore, the only available choice was to conduct experiments using the Texas Instruments ZigBeePRO development kit.

It is hypothesized that the ZigBee protocol security schema is secured when its security schema is activated. To prove this, we set up a ZigBee network and executed every attack one-by-one when the ZigBee security schema was activated, in order to validate the hypothesis.



### 4.3 Research Gap in ZigBee

The following aspects are yet to be thoroughly investigated in the area of ZigBee security:

- An exploration of ZigBee security vulnerabilities in terms of encryption, integrity and authentication and the associated vulnerabilities in each overarching security concept.
- An examination of the current security schema such as encryption, access control list, and authentication and authorization in ZigBee technology.
- Identification security risks in the implementation of ZigBee technology.
- Development of a proper framework that mitigates the security issues associated with ZigBee systems.

### 4.4 Problem Definition in ZigBee

After an in-depth review of the security model of ZigBee, we found several vulnerabilities in the security model of the ZigBee network. These vulnerabilities make it susceptible to the intrusion of a number of threats at all different layers including the physical, data link, the routing networking, transport and the application layers.

### 4.5 ZigBee Security Schema Vulnerability

To determine the effectiveness of current measures to deal with attack, firstly, every exposure attack is explained briefly along with existing countermeasures. Then, those attacks which are still not protected by the existing security schema in the ZigBee network, are discovered, specified and explained. In fact, to answer research questions, we examine all current countermeasures in the ZigBee network. It is proposed that all existing countermeasure are covered by ZigBee security schemas. This means that once the ZigBee security schemas are applied, all existing countermeasures come into force. Table 4.1 below describes the typical countermeasures taken against ZigBee exposure attacks and explains how ZigBee security schemas are applied to employ these countermeasures.

After examining ZigBee's countermeasures against threat, it was found that the ZigBee security schema is still susceptible to several types of attack. Table 4.1 gives a list of ZigBee Threat Countermeasures for nineteen attacks which are considered in this research.

Table 4.1: List of ZigBee Threat Countermeasures

	Exposure Attacks	Existing Countermeasures
1	Eavesdropping	Yes
2	Jamming	<b>No</b>
3	Traffic Analysis	Yes
4	Spoofed, Altered	Yes
5	Hello Flood	Yes
6	Wormhole	Yes
7	Replay	<b>No</b>
7	De-Synchronization	Yes
9	Collision	Yes
10	Unfairness	Yes
11	Resource Exhaustion	Yes
12	Acknowledge Spoofing	Yes
13	Misbehavior	Yes
14	Rushing	Yes
15	Flooding	<b>No</b>
16	Sink Black Hole	Yes
17	Sybil Attack	Yes
18	Physical Tampering	<b>No</b>
19	Select Forwarding	Yes

#### 4.5.1 ZigBee Threat Countermeasures

Many countermeasures are discussed in this section. In fact, detecting attacks and defending the network by taking the necessary countermeasures against the existing attacks would help to improve the performance of the application.

- 1) **Defending Against Eavesdropping** – Encryption and authentication using cryptographic techniques makes a system significantly more secure against eavesdropping and other attacks. Encryption can be used to keep data secure from the adversary, and authentication can be used to safeguard against spurious data. In essence, these techniques attempt to ensure system-level confidentiality by protecting all links. Non-cryptographic techniques include data filtering and attribute-value correlation. Data filtering techniques deliberately send spurious data (or data with spurious offsets) from the sensors to filter the noise at the aggregating

point, while attribute-value correlation uses correlations between different attributes [137].

- **ZigBee Security Schema Against Eavesdropping** – By adding the ZigBee security schema, the AES-128 CCM is applied and all messages are encrypted. However, there is an issue in terms of key distribution. This issue is discussed and examined in later chapters.

**2) Defending against Traffic Analysis** – There are countermeasures against traffic analysis attacks that seek to locate the base station, particularly the rate monitoring attack and the time correlation attacks [138]. Four anti-traffic analysis techniques are proposed to generate randomness. Firstly, introducing a multiple parent routing scheme, which allows a node to forward a packet to one of multiple parents. Second, introducing a controlled random walk which is into the multi-hop path. This traversed by a packet through the node to the base station. Third, introducing random fake paths to confuse an adversary from tracking a packet, this travels toward the base station. Fourth, creating multiple, random areas of high communication activity, which deceives an adversary as to the true location of the base station. “These four techniques can withstand against traffic analysis attacks as well by virtues of providing increased randomness in communication patterns and increased deceptive mechanism to confuse an adversary” [138].

- **ZigBee Security Schema against Traffic Analysis** – By adding ZigBee security schema and implementing the mentioned countermeasures, this attack is controlled.

**3) Defending Against Misbehaviour** – There is a mechanism to detect and handle MAC layer selfish misbehaviour in WSN. This countermeasure is a preliminary solution for handling receiver misbehaviour and collusion between senders and receivers [139].

- **ZigBee Security Schema against Misbehavior** – The behavior of the network may be monitored by using “watchdog” on every node to monitor whether or not the neighbours of a node forward the packets sent out by this particular node. A neighbour not forwarding packets will be identified by the watchdog as a misbehaving node. Therefore, an Intrusion Detection System (IDS) is required on each node as a solution against this attack [56].

**Note:** As this attack is very general and embraces various attacks such as packet dropping, modification of data structures important for routing, modification of packets, skewing of the network's topology or creating bogus nodes, this research does not focus on such an attack.

**4) Defending against Replay Attack** – The best solution here is for the defence functionality to be applied at the application layer because only the application layer can fully and accurately detect the replay of data packets and a secure routing protocol provides no defence against this attack [61]. A  $\mu$ TESLA is a broadcast authentication mechanism which can prevent replay attack. With this technique, messages are authenticated along with previously disclosed ignored keys [140].

- **ZigBee Security Schema Against Replay Attack** – However, although the algorithm mentioned above has been applied in the ZigBee security schema, ZigBee is still vulnerable to replay attack.

**5) Defending Against Physical Tampering** – A sensor network is susceptible to being attacked physically. Destruction of sensor nodes will decrease the performance of the WSN network. Thus, the sensor nodes should be equipped with physical tamper-resistant hardware to improve the protection against various physical attacks.

These issues should be taken into three considerations: “(a) possible physical attack consideration while designing sensor node; (b) resources available for design, construction and testing of sensor nodes; and (c) the ingenuity and determination of the attacker”.

One method which incorporates a two-phase defence algorithm on sensors is used to protect against search-based physical attack. In this case, an attacker walks through the sensor network and tries to use signal detecting equipment to locate active sensors and destroy them [92]. In the first phase, the attacker is detected and attack notification messages are sent out to other sensors. In the second phase, other sensors receive the notification and schedule their states to switch.

Another method is to make the actual data and memory contents on the sensor chip inaccessible to attackers. This can be done by self-terminating the data during an attack so that a sensor destroys itself, all data and all keys. This is feasible in large scale WSNs, which have enough sensors to provide a redundancy of information, and the cost of a sensor is less expensive than the loss suffered after an attack. However, self-termination might produce a DoS effect in some WSN deployments [141].

- **ZigBee Security Schema against Physical Tampering** – Both mentioned countermeasures protect the ZigBee network against this attack.

#### 4.5.2 Defending Against Denial of Service (DoS) Attacks

As mentioned previously, ZigBee is vulnerable to many different types of DoS attacks. A summary of different types of DoS attacks and defences is presented in Table 4.2 below. The details of these methods are available at [48].

##### - **Physical Layer Defence**

- 6) Defending against Jamming** – The best practice to defend against this attack is various forms of spread-spectrum communication. Unfortunately, these defence mechanisms cannot be applied in WSNs, as it requires greater complexity and power, thus making it unsuitable [142]. In a dense, large scale WSN, the sensor nodes are able to map a region being jammed and route traffic around this region. A more costly strategy is to use an alternative mode of communication available to the sensor node, such as infrared to communicate through the jammed network. This functionality will increase the cost and complexity of a node.

- **ZigBee Security Schema against Jamming** – The ZigBee security schema is not able to protect the ZigBee network from this attack.

##### - **Link Layer Defence**

- 7) Defending against Collision** – A typical defence against collisions is the use of error-correcting codes. However, low levels of collisions are used in most codes, but these codes introduce some additional processing and communication overhead such as those caused by environmental or probabilistic errors. It is reasonable to assume that an attacker will always be able to corrupt more than what can be corrected [46]. The network collision detector can be used in the network to identify these malicious collisions, which create a kind of link-layer jamming.

- **ZigBee Security Schema against Collision** – By adding the ZigBee security schema, the MAC (Message Authentication Code) and CRC (Cyclic Redundancy Check) are employed to create error-correcting codes, so that the reception of incorrect messages is minimised.

- 8) Defending against Resource Exhaustion** – The sensor nodes might use a rate-limiting MAC admission control. This helps the network resources to resist flooding by malicious nodes. However, rate-limiting MAC admission control may not be applicable for sensor networks that transmit high volumes of large data [92].

There is a possibility that an attacker can monopolize the network even with this defence. The use of small frames, can be an effective countermeasure against this attack. It reduces the amount of time available to an attacker who is intending to capture the communication channel. This technique often reduces efficiency and is susceptible to further unfairness [46].

- **ZigBee Security Schema against Resource Exhaustion** – This can be controlled through the rate-limiting MAC admission control. By adding the ZigBee security schema, this attack is controlled.

**9) Defending against Unfairness** – A possible solution is to apply rate limits to the MAC admission control to ignore excessive requests and prevent the energy drain which is caused by repeated transmissions. However, this solution prevents legitimate clients from connecting to the victim because its queues and tables fill with abandoned connections. Another solution is to use Time-Division Multiplexing Access (TDMA), where each node is chosen for a time slot to transmit data. This method is applied in WirelessHART. This method eliminates the need of arbitration for each frame and solves the indefinite postponement problem in a back-off algorithm [46].

- **ZigBee Security Schema against Unfairness** – This attack is controlled by adding the ZigBee security schema, as small frames are used to capture data for a small amount of time.

- **Network Layer Defence**

**10) Defending against Selective Forwarding** – The simplest strategy to overcome a DoS attack is to identify the affected part of the sensor network and route around the unavailable portion. Two approaches are proposed for routing around an attacked node [48]. First, the perimeter nodes and the denied region report their status to their neighbouring nodes, which will change their routing table around this region. Second, attack packets from the sensor network can be filtered filtering out. In addition, another method is to apply multi-path routing to provide facility for redundant messages, which are sent on different routes to the receiver node [46].

- **ZigBee Security Schema against Selective Forwarding** – By adding the ZigBee security schema and implementing an Access Control List on the Coordinator, this attack is controlled.

**11) Defending against Sybil** – To defend against the Sybil attack, the WSN needs to validate a particular identity, which is being held by a given physical node. There are two methods to validate identities: direct validation and indirect validation. In direct validation, a trusted node directly tests the validity of the joining node's identity. In indirect validation, another trusted node is allowed to confirm the validity of a joining node [92]. Validation techniques include a radio resource test and a random key pre-distribution test. In the radio resource test, a sensor node assigns each of its neighbours to a different channel to communicate, so a channel randomly is chosen in a node. If the node detects a transmission on the channel, it is assumed that the node transmitting on the channel is a physical node and if a node does not detect a transmission on the specified channel, it is assumed that the node transmitting on the channel is not a physical node. In the random key pre-distribution technique, there are a limited number of keys on a key ring. A malicious node, which randomly generates identities, is not able to possess enough keys to take on multiple identities and is therefore unable to exchange messages on the network. This is due to the fact that the invalid identity will be unable to encrypt or decrypt messages [92].

- **ZigBee Security Schema against Sybil** – This can be done by applying a unique key between each node shared with the base station. This means that two neighboring nodes then communicate with each other by using a shared key to encrypt and verify the link between them. This can be done by adding the ZigBee security schema and Link key, which is a unique key for each link in the network.

**12) Defending against Wormhole Attack** – As a wormhole is caused by a malicious node, so probes can be applied to monitor the routing path and detect the routing path in the ZigBee network. In a network, where probes that take longer to reach a destination than the maximum routing time, it is an indication of a problem in the ZigBee network. There is no current method to solve this except through recreating the routing table by authenticated nodes. This will not allow a malicious node to change the routing table. However, this approach assumes that the malicious node is an external attacker and currently there is no protection if the attacker is inside the network [43].

- **ZigBee Security Schema against Wormhole Attack** – by adding ZigBee security schema and implementing Access Control List on the Coordinator, this attack is controlled.

**13) Defending against Spoofed Altered** – A countermeasure against spoofing and alteration is to append a MAC (Message Authentication Code) after the message. The receivers can verify whether the messages have been spoofed or altered by adding a MAC to the message [140].

- **ZigBee Security Schema against Spoofed Altered**– By adding ZigBee security schema, the Message Authentication Code is employed and this attack is controlled.

**14) Defending against Acknowledgement Spoofing** – The best way to control this attack is authentication via encryption of all sent packets and also packet headers. Since base stations are trustworthy, attackers cannot spoof broadcast or flooded messages from any base station. In order to establish a trustworthy base station, some level of asymmetry is required so that no node should be able to spoof messages from a base station. Authenticated broadcast is also applied for localizing node interactions [143].

- **ZigBee Security Schema against Acknowledgement Spoofing** – By adding ZigBee security schema and implementing Access Control List on the Coordinator, this attack is controlled.

**15) Defending against Sink / Black Hole Attack** – The use of authentication and link layer encryption are countermeasures against the sink hole attacks [61]. This will prevent malicious nodes from participating in the route discovery process and injecting incorrect routing information in the ZigBee network. This method cannot be used to protect against wormhole attacks. Four possible defences against the sink holes have been identified [46].



- Authorization solution – Only authorized nodes can exchange routing information with each other. This solution is not scalable due to high computation and communication overhead.
- Monitoring solution – Nodes become watchdogs to verify the next hop to transmit the message. This scheme will fail if an attacker simply modifies the contents of the message and forwards it.
- Redundancy solution – Multi-path routing is used to send duplicate messages from the source to the destination. This will ensure that at least one message will get through the network to the receiver.
- Probing solution – Location-based protocols are used to detect the presence of sink holes. The nodes can periodically send probes across the network diameter to check the routes.
- **ZigBee Security Schema against Sink / Black Hole Attack** – By adding ZigBee security schema and implementing Access Control List on the Coordinator, this attack is controlled.

**16) Defending against Rushing** – The Rushing Attack Prevention (RAP) [52] is used to counter a rushing attack for on-demand protocols. As long as no underlying protocol fails to find a working route, RAP incurs no cost and provides provable security properties even against the strongest rushing attacks. Both cached route requests and the node lists embedded in the route requests can be applied to check the rushing attack [28].

- **ZigBee Security Schema against Rushing** – By adding ZigBee security schema and implementing Access Control List on the Coordinator, this attack is controlled.

**17) Defending against Hello Flood Attack** – A countermeasure against Hello flood attack is to utilize bidirectional verification and multipath routing that can be done by applying shared secret between sensors[144]. A probabilistic key assignment among sensor nodes is done and every single node calculates a pairwise key by sharing secrets during communication. This improves the network resilience against Hello flood attack. The Hello flood attack can be encountered by verifying the bi-directionality of a link between two nodes[61]. By applying encryption and authentication in Link Layer, sensor nodes can be protected against Hello Flood attacks[145].

- **ZigBee Security Schema against Hello Flood Attack**– By adding ZigBee security schema and implementing Access Control List on the Coordinator, this attack is controlled.

- **Transport Layer Defend**

**18) Defending against Flooding Attack** – One method of defending against this type of attack is to ensure that the sender commits its own resources to each connection by solving client puzzles [43]. While clients are solving the puzzle, the server can create and verify the puzzles easily, and storage of client-specific information is not required. The puzzle is distributed by the servers to clients wishing to connect the puzzle to the server before receiving a connection. Therefore, an adversary must commit more computational resources per unit time to flood the server with valid connections. Under a heavy load, the server could scale the puzzles to require more work by potential clients. This technique is the most appropriate means for combating adversaries that possess the same limitations as the sensor nodes. However, this technique has the disadvantage of requiring more computational energy for legitimate sensor nodes, but it is less costly than wasting radio transmissions by flooding. This strategy is not effective in a low-powered ZigBee since sensor nodes have very limited resources [48].

- **ZigBee Security Schema against Flooding Attack** – the ZigBee security schema is susceptible to this attack because the adversary is still able to stop the communication between ZigBee Coordinator and end-devices.

**19) Defending against De-synchronization Attack** - The authentication of all packets exchanged, including all control fields in the transport header packet will prevent this attack. The end points of the communication can detect any malicious tampering and ignore the attack packet. By applying an authentication method, which is itself secure, an attacker will be unable to send the spoofed messages to the end hosts [46].

- **ZigBee Security Schema against De-synchronization Attack** – By adding ZigBee security schema and implementing Access Control List on the Coordinator, this attack is controlled.

Table 4.2 summarises DoS-type attacks and countermeasures against them.

Table 4:2 Sensor Network Layers and DoS Attacks / Defences.

<b>WSN Layers</b>	<b>Attacks</b>	<b>Defences</b>
<b>Physical</b>	<b>Jamming</b>	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change, proper control mechanism [107].
<b>Data Link</b>	<b>Collision</b>	Error correcting code or ignores excessive requests without sending expensive radio transmission [35].
	<b>Resource Exhaustion</b>	Rate limitation [35].
	<b>Unfairness</b>	Small frames [35].
<b>Network</b>	<b>Wormhole</b>	Authentication, packet leashes by using geographic and temporal information [109].
	<b>Acknowledgement Spoofing</b>	Authentication [111].
	<b>Hello Flood</b>	Verify the bidirectional link [105, 106], Authentication [90].
	<b>Selective Forwarding</b>	
	<b>Rushing</b>	Rushing attack prevention technique in [2, 39].
	<b>Spoofed Altered</b>	Egress filtering, authentication, monitoring [104].
	<b>Sybil</b>	
	<b>Sink Hole / Black</b>	
<b>Transport</b>	<b>Flooding</b>	Authentication mechanism [35].
	<b>De-synchronization</b>	Authentication mechanism [35].

Table 4.2 shows the possible types of DoS attacks and countermeasures against them at the four different layers. Some attacks are protected by similar countermeasures and defences.

Figure 4.1 below indicates the remaining attacks after applying the ZigBee security schema. It is proposed that by applying the security requirement through the ZigBee security schema, all the existing countermeasures are employed and the ZigBee network is secure against those exposure attacks. However, a few exposure attacks such as eavesdropping, physical tampering, relay, jamming and flooding are still possible and the ZigBee security schema is unable to protect the ZigBee network against them. In this thesis, we will execute those exposure attacks and recommend solutions to ensure that they are controlled.

Note: It is supposed that the ZigBee security issues, which are mentioned in Section 3.7.8, are successfully addressed by the ZigBeePRO security schema. Thus, we focus only on the remaining attacks which have been ascertained through the process below.



Figure 4-1: The process of Attacks Filtering

## 4.6 Remaining Attacks

In this step, we will find those attacks which are not protected by the ZigBee security schema.

An attacker can obtain the Network Key through different methods such as remote attack or a physical attack [146]. In the former case, this feat may be achieved by intercepting the key during the out-of-band transmission or capturing plain text traffic sent from a ZigBee Coordinator. In the latter case, the physical device is stolen, extracting the information directly from its hardware.

Remote attacks rely on message interception and exploiting the out-of-band exchange key mechanisms, which may be executed through a social engineering attack. There are two methods of grabbing the key: eavesdropping and physical tampering.

- **Eavesdropping:** In ZigBee, broadcast messages are encrypted using the Network key, which is shared by all the devices in the network. Unfortunately, it is only necessary to compromise a single device in the network for the attacker to be able to compromise the entire network. By using this key, the attacker is able to capture the content of broadcast messages in the network; hence, this is one of the most critical vulnerabilities in the ZigBee technology. This attack is feasible since an adversary may obtain the cryptographic keys remotely or physically [147].
- **Physical Tampering:** Physical attacks are feasible by dumping device firmware using existing available hardware to steal keys by using unprotected data memory and exploiting flash memory. This means that if a network device is compromised by physical attack, an attacker is able to capture the contents of all the direct unicast communications of the device.

One of the security flaws, discovered during this research, is that the ZigBee network is susceptible to replay attack even when the security schema is enabled.

- **Replay Attack:** This is the intercepting of data packets and replaying them where decryption of the data or payload is not required. This attack is used to facilitate other attacks [148]. Imagine a scenario in which a node sends an encrypted user name and password to a server to log in, so if a hacker intercepts the packet with a sniffer and replays the packet, the attacker will obtain the same rights as the original user. This kind of attack can apply to many applications.

ZigBee technology provides one mechanism to prevent replay attacks [149], called the Frame Counter, which has been added to the frame header at the Network layer. It consists of a counter that is employed in each transmission and is supposed to detect replicated data. However, it was found that this security schema (Frame Counter) does not work properly and ZigBee network is susceptible to replay attack.

In addition, the execution of a replay attack has been claimed as an effective attack by Joshua Wright, a senior security analyst from In Guardian [150]. He states: "802.15.4 has no replay protection and ZigBee has meagre replay protection so Attacker can replay any previously observed traffic until key rotation "[150].

DoS attack is another type of ZigBee attack that is sometimes very difficult to detect. This attack can be performed at several layers and depends on whether the attacker has joined the network, is part of it (an insider) or not (an outsider) [151], [152]. The DoS can be either internal attack or external attack. If the attacker is an insider, the DoS attack may be conducted at the PHY/MAC/NWK/APS layers, whereas if the attacker is an outsider, DoS may be conducted only at the PHY/MAC layers[152].

- **Denial of Service:** A great deal of effort has been expended by the ZigBee Alliance to be able to perform authentication and provide confidentiality to transmitted data. However, limited attention has been given to the avoidance of DoS attacks.

The possibility of DoS attacks at several layers is important because more complex attacks will be more difficult to detect, as an attacker always strives to be invisible. A DoS attack occurs if a device starts consuming bandwidth unfairly. For example, if the attacker starts continuously sending data over the communication channel, other devices cannot communicate with each other.

- **Jamming:** At the PHY layer, the DoS attack is performed by direct jamming of the channel. This attack can be launched by an outsider device which disrupts the signal of other devices by changing the Power Spectral Density (PSD) [152]. In fact, a jammer can never reproduce a signal; nor can it pretend to be a receiver node. There are some parameters such as signal strength of a jammer as well as the location and its type which may influence the performance of the network.
- **Flooding:** ZigBee is susceptible to flooding attack. This attack attempts to bring down the network's critical components such as the Coordinator by

overwhelming it with excessive traffic. So, it is important that the ZigBee coordinator be protected against high amounts of certain types of traffic.

#### **4.7 Research Issues**

ZigBee security issues pose significant challenges for industries. However, there may be several underlying factors that make such implementation impossible. So the primary issues that we have identified in the literature and intend to address in this research are:

1. There is a lack of proper configuration and process in ZigBee technology that may result in serious consequences in terms of external security attack as well as implementation of such technology.
2. No framework has been proposed to help test ZigBee security and find the vulnerabilities of such existing and newly proposed / alternative wireless systems.
3. There does not exist any risk analysis approach to the implementation of ZigBee in critical applications such as the oil and gas industry and the military. This may have serious consequences in terms of stakeholder health and safety, and plant performance.

#### **4.8 Research Approach**

The objective of the thesis is to develop an architecture framework to enhance security for protecting and maintaining confidentiality of ZigBee while preventing security breaches. To achieve this objective, the sub-objectives to be addressed are as follows:

1. Identify WSN security vulnerabilities of several keys wireless sensor network protocols including ZigBee, WirelessHART and ISA100 security vulnerabilities of several keys wireless sensor network protocols in terms of all existing WSN standards security requirements (achieved in Chapter 3).
2. Identify all existing WSN attacks and all existing ZigBee attacks (achieved in Chapter 4)
3. Design and develop an architecture framework for enhanced security that mitigates the security issues associated with the ZigBee standard. This model will include the necessary software, hardware, process and procedures (Chapter 5).
4. Recommend the proper configuration for implementation of secure ZigBee networks (Chapter 6).
5. Implement security measures to respond effectively to vulnerabilities, including security devices, applications and network (Chapter 7).



6. Evaluate and validate the developed end-to end security model through a case study (Chapter 8).
7. Present an architecture framework for enhanced security in ZigBee network to industries and companies, which intend to implement this technology, to improve security design and configuration (Chapter 9).

## 4.9 Research Question

Section 4.2 identified the shortcomings of the ZigBee security system. Firstly, it is necessary to determine the potential attacks which pose threats to the ZigBee standard; and secondly, to discover the level of security provided by the ZigBee when the ZigBee security schema is activated.

The following questions have been formulated for the research:

- 1- How secure is the ZigBee security schema?
- 2- Does the ZigBee security schema cover all security requirements?
- 3- How many existing exposure attacks can be removed by adding ZigBee security schema?
- 4- Is the ZigBee standard secured against all existing exposure attacks by activating the ZigBee security schema?

In order to test the hypothesis defined in the section 4.2, we need to execute, in a laboratory environment, all types of attacks on the actual devices within the ZigBee network. The results will enable us to validate the above hypothesis, and provide solutions to the research issue.

## 4.10 Choice of Research Methodology

“Research method literatures often contain inconsistent, overlapping or contradictory definitions for terms such as paradigm and research method, which tends towards the practical” [153].

### 4.10.1 The Science and Engineering Based Research Method

In addressing the stated technical problem, this thesis focuses on the development of an architecture model to enhance the security in a ZigBee network. In order to propose a solution for the research issues, a systematic scientific approach must be followed to ensure that the methodology development is scientifically-based. A science and engineering-based research approach is adopted in this research project. Science and engineering research leads to the development of new techniques, architecture, methodologies, devices or a set of concepts,

which can be combined together to form a new theoretical framework [154, 155]. This research approach commonly identifies problems and proposes solutions to these problems. Particularly in the engineering field, the spirit of “making something work” is essential.

Science and engineering-based research is concerned with confirming theoretical predictions. It states that in the engineering field, the spirit of ‘making something work’ is essential and has three levels [154, 155]: conceptual level, perceptual level and the practical level, as explained below:

- Conceptual level (level one): creating new ideas and new concepts through analysis.
- Perceptual level (level two): formulating new methods and approaches through designing and building the tools or environment or system through implementation.
- Practical level (level three): carrying out testing and validation through experimentation with real world examples. The process of testing and validating a working system provides unique insights into the benefits of the proposed concepts, frameworks and alternatives. An overview of this research method is depicted in Figure 4-2.

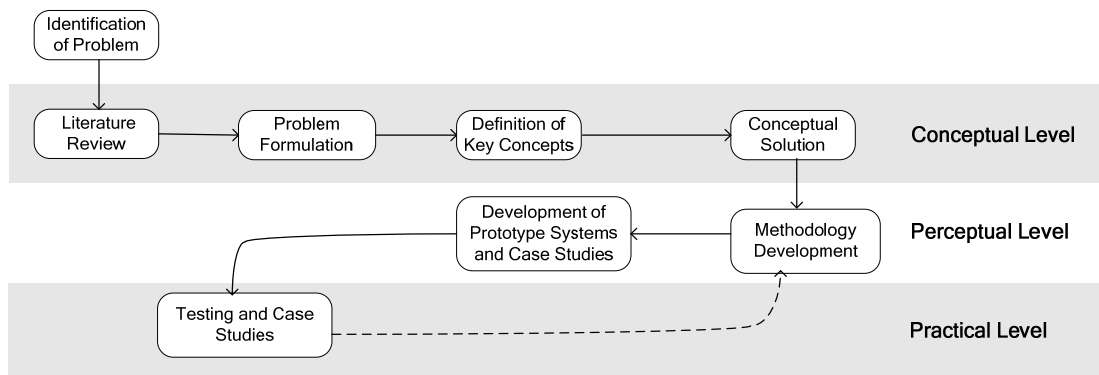


Figure 4-2: Overview of science and engineering-based research method.

As can be seen from Figure 4-2, this research method begins with an identification of the research problem(s). Extensive literature on topics related to the study are collected and analysed. Based on an extensive review of the existing literature, the problem that needs to be addressed is formulated and then some key concepts for addressing the problem, taking into account the characteristics of the interaction, are defined. These definitions are applied when developing the conceptual solution. Subsequently, the conceptual solution for the problem being addressed is formulated. All processes from the literature review to the conceptual solution are included in the conceptual level. Finally, in the conceptual level, the methodology for development an architecture framework for WSN security is developed.

At the perceptual level, the proposed end-to-end WSN security framework will be implemented by applying all the security measures, developing prototype systems and carrying out counter-attacks.

At the practical level, a case study will be used to test the concepts; we will evaluate and validate our proposed security framework in a real-world remote operation environment, namely Statoil. Based on the evaluation and validation, we then fine-tune our proposed framework. We then provide guidelines and a risk analysis approach for WSN deployment.

#### **4.11 Conclusion**

In this chapter, it was explained why the ZigBee Kit development was chosen to conduct the experiment. The research issues and research gap were described. The objective of the thesis, which is to develop an architecture model for protecting and maintaining confidentiality in WSNs while preventing security breaches, along with the significance of this research, were explained. Further, a science and engineering-based research approach, which will be utilized in this thesis for the proposed solution development, was discussed. Also, it was hypothesized that the ZigBee protocol security schema provides adequate security when activated. Based on this hypothesis, the research questions were introduced. The four issues were introduced which this research intends to address. The technical problems arising from the literature review in terms of current exposure attacks were addressed. In this thesis, four exposure attacks – eavesdropping, replay attack, physical tampering and DoS attack in two different layers – were discussed in detail. The reasons for choosing these particular exposure attacks, are explained. In the next chapter, an overview of the solution for these issues is presented.

## **5 Overview of the End-to-end WSN Security Architecture Framework**

### **5.1 Introduction**

In this chapter, we present a framework for enhanced security for ZigBee networks. The provided framework (Figure 5.1) helps us to design and configure the ZigBee network in a secure way. Through this framework, an appropriate Network Design and Network Configuration of the ZigBee network for implementation will be achieved.

In this chapter, the solution to each of research issue is identified and discussed. In Section 5.2, a model for mitigating the current attacks is introduced. The model includes many different steps and procedures, all of which are abstractly explained. In section, those attacks which can still occur after employing the ZigBee security schema are identified, and proposed solutions to prevent or mitigate such attacks are recommended. The conclusion recaps the main points of the chapter.

### **5.2 The Conceptual Framework for Enhancing ZigBee WSN Security**

In order to improve the ZigBee security schema, a model known as the BESTSEC Model, is designed to mitigate the risk of current attacks to which ZigBee is exposed. This model allows the researcher to better control and mitigates the risk of attacks in the ZigBee network. For this purpose, we set up the network and execute the existing countermeasures. This ensures that these countermeasures are applied and the risk of current exposure attacks is mitigated. Therefore, it is necessary to launch all known attacks and use the currently available countermeasure on the actual devices, whether these are ZigBee, WirelessHART or ISA100.

As explained earlier, ZigBee was the only choice available to the researcher for the purpose of conducting experiments by using the Texas Instruments ZigBeePRO development kit.

As explained in Chapter 2, the ZigBee standard dictates that by activating the security schemas on their technology, the ZigBee security requirements are provided. This means that by activating only the security option on the ZigBee standard, all the security requirements will be applied to protect the ZigBee network. To prove this claim, after setting up the network, the security schema was activated and then each attack was launched in turn. This process allows us to discover the extent to which the current security schemas and countermeasures are effective against the various attacks.

The BESTSEC model includes a few steps intended to identify which exposure attacks are removed by the current ZigBee security schema and which one not. This can be achieved by activating the security schema, executing all exposure attacks, and then recording those attacks to which ZigBee is still susceptible. After determining these attacks, the process of finding a solution to prevent or mitigate them, begins. The recommended solutions, which include network configuration or network design along with additional software or hardware, are recorded and added to the current countermeasures list. Figure 5.1 illustrates this process.

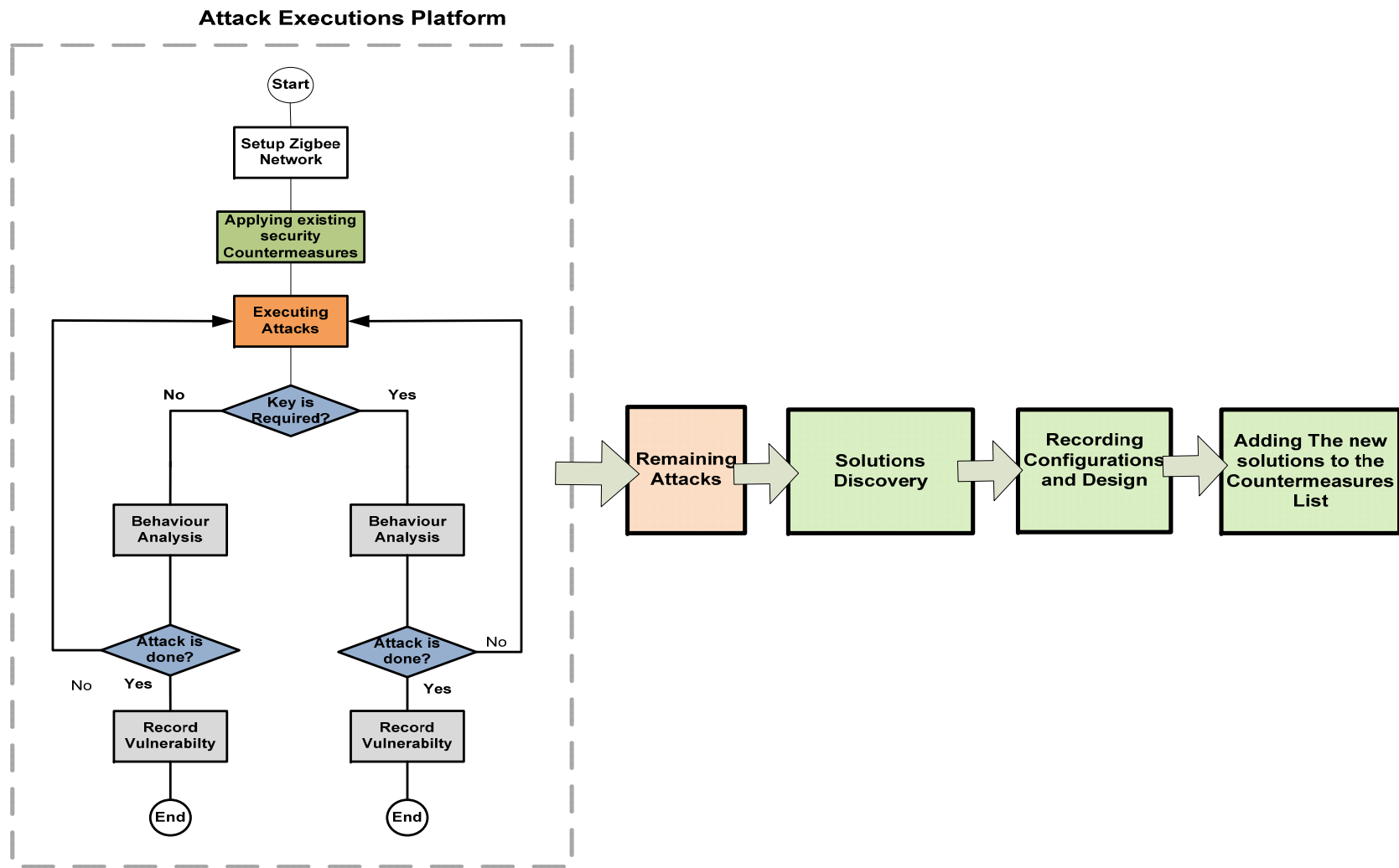


Figure 5-1: The BESTSEC Model.

### 5.3 Attack Execution Platform Component

A cyber-attack is one that is intended to make a device or network resource behave abnormally or become unavailable to its intended users. “The goal of attack is to attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of resources” [156]. In this step, all exposure attacks described in Chapter 2 are executed and the effects of these attacks are examined.

#### 5.3.1 Set up ZigBee Network

This step requires the setting up of a ZigBee network using actual devices. This network allows the researcher to conduct experiments in order to launch exposure attacks.

#### 5.3.2 Applying Existing Security Schema

In ZigBeePRO, the development key includes the security schema feature. By adding the security, which is located in the ZigBee Stack code, full security measures come into force.

#### 5.3.3 Executing Attack

After the security schema in the ZigBeePRO development kit is activated, all exposure attacks are launched in order to determine which exposure attacks are dealt with effectively, and which one not. Due to the different objective of each attack, the attack strategy for every single attack is different. For example, in a few cases, some attacks depend on others which are a prerequisite for subsequent attacks. Hence, by removing these preliminary attacks, the risk of certain other further attacks is removed.

#### 5.3.4 Key Requirement

In this section, the current capabilities of the ZigBee are analysed in order to assess the security level. The existing vulnerabilities are categorised according to the following factors: constraints on performing a successful attack and the kind of disruption that an attack may cause to the network. Previous analysis indicates that the existing vulnerabilities are one of two types: those which require knowledge of the ZigBee cryptographic keys (Link, Master or Network), and those which do not.

- Attacks Requiring Key Compromise – All unicast communications between ZigBee nodes are secured using a 128-bit Link key shared between two devices at the APS layer. All broadcast communications are secured by a 128-bit Network Key shared by all devices in the network layer [157]. Therefore, a compromised key is a very important issue as far as security is concerned. Once an attacker gets hold of a key, it will be able to act at leisure within the network.

- Attacks with Unrequired Key Compromise – Attacks which do not require an attacker to gain access to the cryptographic keys stored in a ZigBee device are a bigger concern, since they can be performed remotely from the wireless space. It is not necessary to manipulate physical devices. The two existing main attacks which follow this condition are replay and DoS.

a) Internal Attacks: At the APS layer, DoS is performed by sending a great deal of messages to the device (flooding) to interrupt message processing. In addition, this action exhausts the device resources such as battery. This attack can be easily detected, since all the messages are sent from a specific device. At the NWK layer, DoS is executed by modifying the default routing protocol. If the attacker, which is placed within the network, is a compromised router, it can stop forwarding messages between nodes, which leads to changes in the routing protocol. Fortunately, this DoS attack may be directly detected and avoided by the default routing protocol. The sensor can just start sending messages via another router, if possible [152].

b) External Attacks: At the MAC layer, ZigBee uses CSMA/CA [146] if it is running in non-beacon mode to guarantee that all the devices can communicate through the same communication channel. Once a device intends to transmit data, the communication channel should be listened to during the specific time. If the channel is sensed as idle, then the node is permitted to begin the transmission. However, if the channel is sensed as busy, the node defers its transmission for a random period of time [149]. Figure 5.2 shows this category.

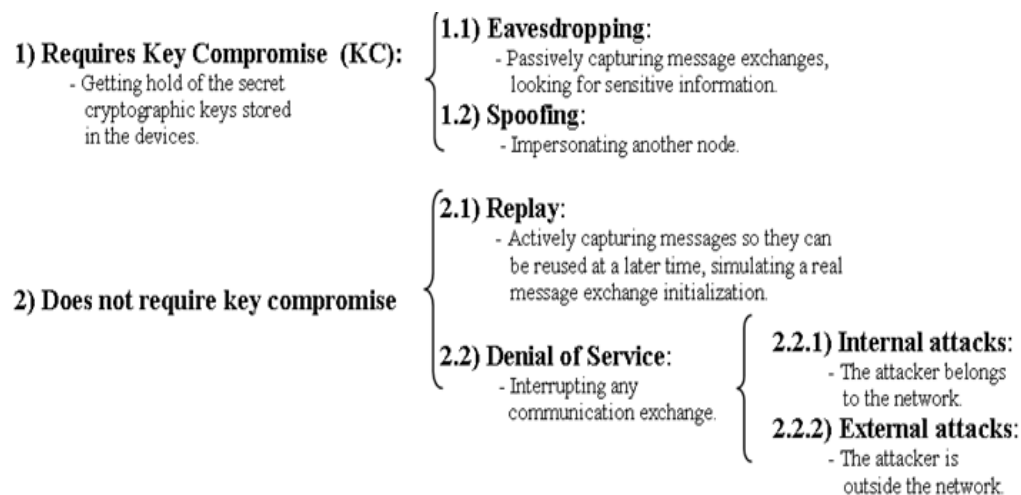


Figure 5-2: ZigBee Attack Categories



### 5.3.5 Behaviour Analysis

Behaviour Analysis collects and analyses exposure attacks and traffic of the entire network and nodes and examines the reconnaissance attacks.

### 5.3.6 Record Vulnerability

Once the behaviour of the attack has been recognised, the vulnerability should be recorded in order to arrive at a solution. The vulnerability may lie in node configurations or network design. By recording them, the researcher has a better chance of working on the solution to remove these vulnerabilities.

## 5.4 Remaining Attacks and Solution Discovery Components

As mentioned in Chapter 4, there are several types of attack that are still possible even when the ZigBee security schema is enabled. Having identified such attacks, the researcher attempts to provide solutions to prevent or mitigate them.

An attacker can obtain the Network Key by different methods such as remote attack or a physical attack [146]. The remote attack can be done through eavesdropping and physical attack can be done through physical tampering.

The recommended solutions for each attack are described in the following:

- 1) **Eavesdropping:** A key can be obtained through eavesdropping by capturing plain text traffic sent from a ZigBee Coordinator. Remote attacks rely on message interception and exploiting the out-of-band exchange key mechanisms, which may be executed through a social engineering attack.
  - **Eavesdropping Solution:** This problem can be solved by using a key which has been pre-installed at the factory, added by the final user in an out-of-band manner, instead of the coordinator trustingly distributing the security keys to other devices.
- 2) **Physical Tampering:** As mentioned, a key can be obtained by dumping device firmware using existing available hardware to steal keys by using unprotected data memory and exploiting flash memory.
  - **Physical Tempering Solution:** Physical security is the solution to a physical tampering attack. This countermeasure involves having a secure facility for the location of devices which provides a barrier against an intruder. It prevents intruders from gaining physical access to the devices [158]. The defence against

a physical attack on the ZigBee MCU may be provided by programmed JTAG or a serial bootstrap loader (BSL) which resides in a masked ROM along with appropriate physical security [159].

One of the security flaws discovered by this research is that the ZigBee network is susceptible to replay attack, even when the security schema is enabled.

- 3) **Replay Attack:** When a forged packet with key counter 0xFFFF is sent by an adversary, the coordinator generates several broadcast packets, whether encrypted packets or unencrypted. Through these broadcast packets, an adversary is able to execute the replay attack and insert the broadcast packet into the network again.

However, ZigBee technology provides one mechanism to prevent replay attacks [149], called the Frame Counter, but this security schema (Frame Counter) is not totally effective, so the ZigBee network is still open to replay attack. Joshua Wright, a senior security analyst from *In Guardian* comments on the effectiveness of a reply attack by stating: "802.15.4 has no replay protection and ZigBee has meagre replay protection so Attacker can replay any previously observed traffic until key rotation " [150].

- **Replay Attack Solution:** By appropriately addressing the destination address of network devices, the Coordinator can be prevented from generating the broadcast packet in order to protect the ZigBee network from such attack. Also, the KillerBee framework will be set up to evaluate Joshua Wright's claim.

- 4) **Denial of Service:** As mentioned earlier, the DoS attack may be conducted at the PHY/MAC/NWK/APS layers. Because it is possible to launch the DoS attack at several layers, this type of attack is more significant because more complex attacks will be more difficult to detect, as an attacker always intends to be invisible.

- a. **Jamming:** To perform jamming, the attacker should be near to the device or use an adequate level of transmission power [152], [60] because the transmitted signal loses energy as the distance increases.
  - **Jamming Solution:** When considering jamming as a security aspect, there is no currently available and practical commercial solution to secure a ZigBee network against this attack. It is obvious that ZigBee security cannot deal effectively with this issue, particularly if powerful jamming equipment is used.
- b. **Flooding:** ZigBee is susceptible to flooding attack. This attack attempts to bring down the network or critical components such as the Coordinator by overwhelming it with excessive traffic. So, it is important for the ZigBee coordinator to be protected against high amounts of certain types of traffic. The Coordinator and all the critical nodes should protect themselves by limiting the number of specific management frames per time unit in order to not fall prey to such attacks.
  - **Flooding Solution:** Limiting the number of connections prevents complete resource exhaustion which interferes with all other processes at the victim end. By properly addressing the destination address of nodes, this attack can be controlled better. The destination address of the coordinator and end-devices should be addressed properly to control this attack. This means that by assigning a unicast address to the destination address of the coordinator, the coordinator processor does not overflow because of the large numerical operation which cannot be stored in one register.

## 5.5 Recording Configurations and Design

The solution might be done in several ways such as having a code on the Stack code, changing the network configurations or changing the network design or some regulation practice or external hardware or software application. Any of these practices which are effective against exposure attacks, are documented as the solution to each exposure attack.

## 5.6 Adding the New Solutions to the Countermeasure list

As can be seen, in the last stage of this framework, solutions which were recommended by the researcher are added to the countermeasures list to find the best practice for implementing WSNs to achieve the proper network configuration and design for WSN security.

Network configuration plays a very important role in mitigating the risk of attacks and describes a broad range of activities associated with establishing and maintaining a WSN network [158].

Network design reflects the architecture of the network to ensure that all nodes are accessible and communicating within their own base stations in a secure way [158]. Network design and network configuration are inherent elements of the proposed architecture model.

By adding the new solutions to the existing countermeasure lists, we are able to mitigate the risk of all exposure attacks which have been discussed in this thesis. In fact, by achieving the new solutions for those remaining attacks, the proper design and configuration of the network to prevent those attacks will be provided.

## **5.7 Summary of the Framework Design**

As indicated by the title, the goal of this research is to present an architecture framework to enhance security in a ZigBee network. This architecture framework has been introduced in this chapter. This framework outlines solutions for attacks to which a ZigBee network is still susceptible and which are not adequately addressed by the ZigBee security schema. In this chapter, the BESTSEC framework was introduced. This framework contributes significantly to finding an appropriate configuration and design for the ZigBee network. Using this framework, we are able to discover which attacks can be eliminated by the current countermeasures and which ones cannot; this is a first step in finding a solution to prevent or mitigate these attacks. In this chapter, the solution to the eavesdropping issue in ZigBee was briefly introduced. The replay attack issue in ZigBee was discussed as was the issue of how this can be better controlled. As mentioned earlier, DoS attacks can be launched at different layers. Solutions for the two DoS attacks of jamming and flooding, which still threaten a ZigBee network, were discussed. However, there is no currently available commercial solution that is practical and effective in securing a ZigBee network against jamming. The solution for a flooding attack was suggested to better control this type of attack. Finally, the solution for physical tampering was explained.

## **5.8 Conclusion**

In this chapter, solutions for those attacks which remain to be addressed (introduced in the last chapter), are identified through an architecture framework (The BESTSEC Model). Also, all the steps taken to establish the framework have been described in detail. In fact, the deployment of an effective, scalable and secure ZigBee network requires proper design and configuration. Therefore, the network design and network configuration which play a very

important role in enhancing the security of a ZigBee network will be achieved through our framework.

## 6 Design and Implementation of the Framework Architecture and Carrying Out Security Measures

### 6.1 Introduction

In this chapter, there is a description of the software and hardware required to set up the test-bed and to configure the network to measure and examine the security in ZigBee network. The three standards in the WSN area have been explained in detail in Chapter 3. However, all of these standards are advertised as open and public, but there are serious issues concerning the supply of WirelessHART and ISA100 development equipment and software. Also, the ISA100 specification is only ratified well into the project and no development kits are currently available. So, the only choice was to conduct experiments using the Texas Instruments ZigBeePRO development kit.

In vast contrast to WirelessHART and ISA100, it was found that a number of OEM module manufacturers' products incorporate ZigBee-compliant chipsets. The Texas Instruments ZigBeePRO kits are widely available, quickly sourced, well-documented, supported and tooled, enabling the experiment to be conducted. After the ZigBeePRO configuration and custom software updated to a single node, it was obvious that a number of the vulnerabilities outlined in this research could be tested.

However, although the ZigBee development kit and source code are available from Texas Instruments, this source code is not open to the public in all its layers. In fact, security schemas in the ZigBee standard have been defined in the layers whose code is not available to us. Therefore, we have to deal with only the Application layer and NWK layer to find the vulnerabilities in the ZigBee standard in terms of security. However, the security schemas are defined in the Sub-Application layer, which is not an open source, in the ZigBee standard.

As mentioned in Chapter 3, ZigBeePRO provides a security model and a set of security services in order to provide a comprehensive network security infrastructure. The security model in ZigBeePRO standards provides some security services such as trust infrastructure, encryption, authentication, and admission control for nodes joining the network. As the ZigBee applications are widely used, the security of ZigBee should be given full consideration.

Executing attacks on ZigBee network requires a test-bed which includes hardware and software along with design the network, code developments and node configurations.

To launch attacks on ZigBee Standard, the CC2530ZDK development kit from Texas Instrument has been chosen to work on it. The CC2530ZDK is designed to deliver the most

powerful elements for ZigBee and ZigBee PRO development. The kit is based on 2.4GHz IEEE 802.15.4 compliant System-on-Chip, the CC2530. The CC2530ZDK includes CC2530-based evaluation modules, SmartRF05EB and SmartRFBB development boards, a USB interface dongle, cables, antennas and documentation. The CC2530EM evaluation modules can be plugged into SmartRF05EB and SmartRF05BB boards, which are included in the Development Kit. The CC2530ZDK comes with TI's ZigBee compliant Z-Stack supporting ZigBee, ZigBee PRO, and the Smart Energy and Home Automation application profiles. The CC2530ZDK includes CC2530-based evaluation modules, SmartRF05EB and SmartRFBB development boards, a USB interface dongle, cables, antennas and documentation to get you up and running with the Z-Stack on the CC2530 [105].

In this section, there was a description of the software for the CC2530 System-on-Chip solution for IEEE 802.15.4/ZigBee.

## **6.2 Hardware and Software Requirement for Development**

This section describes the necessary hardware and software, and how we get started with the ZigBee Sample application for CC2530. We describe the necessary hardware and software download and an explanation of the way to set up the network, program the board, and run software examples from the IAR debugger. The hardware includes:

- 2 x SmartRF05 EB
- 2 x CC2530EM boards with appropriate antennas
- CC2430DB
- IAR Embedded Workbench for 8051
- Z-Stack Sample Application
- Texas Instrument Packet Sniffer
- Smart RF Studio



Figure 6-1: SmartRF05EB with CC2530EM

Figure 6-1 shows the typical configuration of SmartRF05EB with CC2530EM. As can be seen, this device has been configured as the Coordinator and Network ID 9C36, which is shown on the LCD of the Coordinator in the above diagram.

- **SmartRF05 EB:** This is a flexible test and development platform that works together with RF Evaluation Modules from Texas Instruments. An Evaluation Module is a small RF module with the RF chip, matching filter, SMA antenna connector and IO connectors. The modules can be plugged into the SmartRF05EB, which lets the PC take direct control of the RF device on the EM over the USB interface [160].
- **CC2530EM:** The CC2530EM includes the RF IC (Integrated circuit) and necessary external components and matching filters for getting the most out of the radio. This module can be mounted on the SmartRF05EB [161].
- **CC2430DB:** The CC2430DB includes a USB interface that can be used as an emulator interface for the CC2530. It can be powered over the USB interface as the listener and injector. In our network, we use the CC2430DB which can be powered over the USB interface as the listener and injector.
- **IAR Embedded Workbench for 8051:** The IAR Embedded Workbench is a set of development tools for building and debugging embedded applications using assembler, C and C++[162].
- **Z-Stack:** The Z-Stack is TI's ZigBee compliant protocol stack for IEEE 802.15.4 products and platforms. The Z-Stack complies with ZigBee and ZigBee PRO and supports both ZigBee and ZigBee PRO feature sets on the CC2530 System-on-Chip



(SoC), MSP430+CC2520. Z-Stack supports the Smart Energy and Home Automation profiles.

The Z-Stack is a fully compliant ZigBee PRO feature set on the CC2530 and MSP+CC2520 platforms and compliant ZigBee feature set on the CC2530 family of SoCs and MSP430 microcontrollers [163]. The Z-stack is freely available, but it is not an open source project and it is delivered in the form of libraries. In the Z-stack, there are some source files in the name of MAC.

As mentioned earlier, the software examples are designed to run on the CC2530EM mounted on SmartRF05EB. We also describe how to run each of the software on the CC2530 kit. The Hex files for the Sample Applications along with software library are explained. IAR EW8051 full version is needed for building the source code.

- **Z-Stack Sample Application:** The Z-Stack Sample Application is a simple head-start to using the TI distribution of the ZigBee Stack in order to implement a specific Application Object. A range of Sample Applications including support for the ZigBee Smart Energy and ZigBee Home Automation Profiles [163].

The Sample Application uses the minimal subset of ZDO to make a device reasonably viable in a ZigBee network. Also, for inter- and intra-task communication, the Sample Application applies the essential Operate System Abstract Layer (OSAL) API functionality by sending and receiving messages, setting and receiving task events, setting and receiving timer call-backs and using dynamic memory. The Z-Stack Sample Application implements a Private Profile and it is chosen for the development of the test-bed in this research [161].

OSAL is designed and distributed as a source and the entire OSAL functionality can be changed by the Z-Stack user. The OSAL implements a cooperative, round robin scheduling task servicing loop and each major sub-system of the Z-Stack runs as an OSAL Task. The user must create at least one OSAL Task in which their application will run. This is accomplished in the implementation of the `osalAddTasks()` function. The sample applications clearly show how the user must add an invocation to `osalTaskAdd()` for at least one user task after all of the Z-Stack tasks [161].

The round-robin scheduling algorithm is one of the simplest scheduling algorithms to design, especially for time-sharing systems. This algorithm assigns a time slice for every single process in the queue in order, so it is possible to handle all processes without priority. If the remaining request is less than a time slice, only the remaining request time is allocated [160].

The software application framework is built upon the operating system which provides services for task management, power management, non-volatile memory, dynamic memory management, software timers, event generation, inter- and intra-task messaging, and a seamless interface to the Hardware Abstraction Layer (HAL). Each layer of the application framework is designed as a task within OSAL, and the HAL task [164].

The sample application instantiates only one application object and supports the one corresponding profile. Only two or more application objects may be instantiated in the same device. In fact, each application object must implement a unique profile ID on a unique end point number. The sample applications meet the unique ID's and end point numbers requirement and could be merged into one device with minimum changes [161].

- **TI Packet Sniffer:** The Packet Sniffer is a PC software application that displays and stores RF packets captured with a listening device, which is connected to the PC via USB. The Packet Sniffer filters and decodes packets and displays them. It has the options to filter data and storage data in binary format [165].
- **Smart RF Studio:** This is a Windows application that can be applied to evaluate and configure low-power RF-ICs from Texas Instruments. The application is especially useful for practical testing of the RF system and for optimizing external component values. Smart RF Studio supports all the Low Power RF-ICs from TI [166].

### 6.3 Hardware and Software Set-up and Configuration

The hardware and software is configured as follows:

1. Install IAR Embedded Workbench for 8051 and the patch to enable support for CC2530.
2. Download the CC2530 software examples file from TI website.
3. Mount the CC2530EM board to the SmartRF05EB.
4. Connect the SmartRF05EB to the PC with a USB cable.
5. Make sure the EM selection switch (P19 on SmartRF05EB) is placed in position *SoC/TRX*.

The CC2530ZDK is supported by the IAR EW8051 C-compiler, which is the Z-Stack compiler. The C-SPY debugger is used as an emulator interface.

### 6.3.1 Implementing the board with IAR

1. Open IAR Embedded Workbench.
2. Open the workspace file SampleApp.eww with IAR.
3. Each application has its own project tab in the IAR workspace viewer. Select the project to be compiled in the workspace viewer of IAR.
4. Select Project->Rebuild All. This will perform a full rebuild on the selected project.
5. Select Project->Debug. IAR will now establish a connection with the CC2530 and program the application. The debugger will be started, halting the target at main().
6. Start the application by selecting Debug -> Go.
7. The board can be reset by selecting Debug -> Reset.
8. The debugger can be stopped by selecting Debug -> Stop Debugging.
9. The unit can now be operated independently from the debugger by disconnecting the USB cable and using the AA batteries as power source. Cycle power with the power switch on the SmartRF05EB.

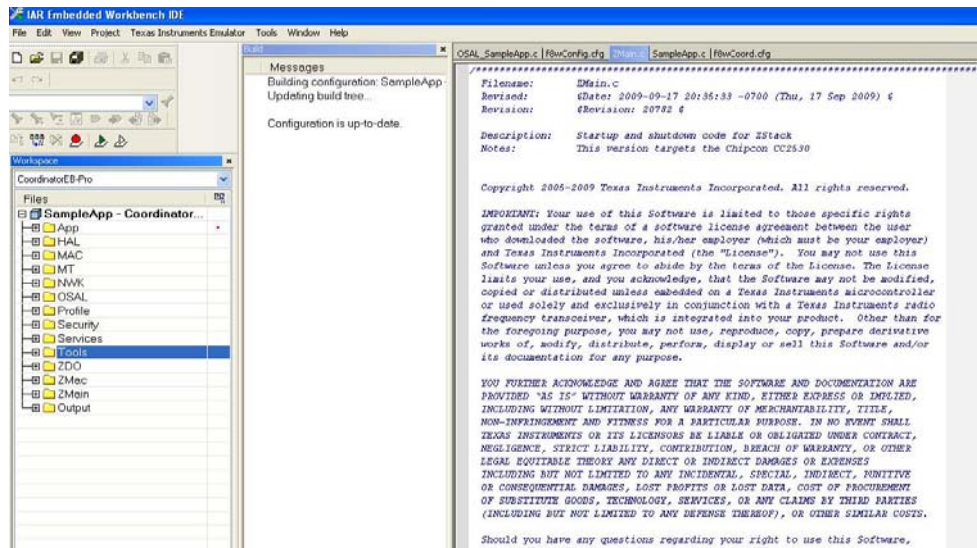


Figure 6-2: IAR EW

Figure 6-2 depicts the IAR Embedded Workbench IDE which is applied to compile the code. As can be seen, the ZigBee code has been classified into several components. This program allows the researcher to change, compile and upload the code to ZigBee devices.

## 6.4 Software Application Development

We developed a system to control the data from end-devices to the coordinator. This system allows us to send data (0 or 1) to the Coordinator by manipulating a joystick on an end device. Using this system, the packet, which is detected by Coordinator, appears on the LCD of the Coordinator. As a result of this code, the data sent from the end device to the Coordinator is displayed on the coordinator LCD.



Figure 6-3: Data on Coordinator LCD

Figure 6-3 shows the visual information that allows us to determine the number of packets received and accepted by the Coordinator. As it can be seen the temperature is appeared on the LCD of coordinator. The temperature is shown 18 in the above diagram.

The application includes two functions such as `SampleApp_Send_Data()` and `SampleApp_HandleKeys( )`.

This function `SampleApp_Send_Data()` processes indicating data (0 or 1) to the LCD of the Coordinator. Both functions are defined in the application layer of the Z-Stack, applied network layer and MAC layer for routing protocol and data transmission.

The code can be represented as follows:

```
void SampleApp_Send_Data(uint8 temp)
{
    if (AF_DataRequest(&SampleApp_Data_DstAddr, &SampleApp_epDesc,
        SAMPLEAPP_DATA_CLUSTERID,
        1,
        (uint8*)&data,
        &SampleApp_TransID,
        AF_DISCV_ROUTE,
        AF_DEFAULT_RADIUS ) == afStatus_SUCCESS )
    }
    else
    {
```

```
// Error occurred in the request to send
}
```

The SampleApp\_HandleKeys() function processes the sent data (0 or 1) from the end-device to Coordinator manually. In fact, this is the function of the key toggle on the devices. By playing the joystick to the right, the number on the LCD is increased and by playing the joystick to the left the number is decreased. The code below, which is developed in the application layers, handles this process.

```
void SampleApp_HandleKeys( uint8 shift, uint8 keys )

{
if( Joystick turns Left )
{
SampleDat sends Data(0);
HAL_TURN_ON_LED1();
else
HAL_TURN_OFF_LED1();
messages++;
}
if(Joystick turns Right)
{
SampleApp sends Data(1);
HAL_TURN_OFF_LED2();
else
HAL_TURN_ON_LED2();
messages++;
}
}
```

## 6.5 Network Configuration

The roles of devices such as the coordinator, routers and end devices are explained in order to define the network. The network channel, PAN ID, security schema and role of devices as well as other configurations are defined by the IAR Workbench.

- **Configuring PAN ID:** Routers and end devices can be configured to join any ZigBee PAN, or to join a specific PAN with a certain PAN ID. However, end devices must always find a coordinator or router to allow them to join the network.
- PAN ID configurations:
  - If PAN\_ID = 0xFFFF and device = Coordinator  
Device uses IEEE address to choose a PAN\_ID (last 2 bytes)
  - If PAN\_ID = 0xFFFF and device = Router or End Device  
Device will join any available PAN
  - If PAN\_ID ? 0xFFFF and device = Coordinator  
Device will use the set value for the PAN\_ID
  - If PAN\_ID ? 0xFFFF and device = Router or End Device  
Device will ONLY join a PAN that has this PAN\_ID

- **Turn Security Key Exchange ON:** In order to have a secure network, firstly, all device images must be built with the pre-processor flag SECURE set equal to 1. This can be found in the "f8wConfig.cfg" file.

As can be seen in Figure 6-2, Sample Application includes many Workspaces. One of these workspaces is Tools, which contains a Config file. To set up the security schema, the f8wConfig.cfg (config file) must be opened in the Tools workspace folder and set - DSECURE=1.

Open ZGlobals.c in the NWK workspace group and note that gPreConfigKeys = FALSE;.

This means that only the Coordinator stores the preconfigured key because the key is passed once per join, in the clear during the joining process. Hence, an out-of-band transfer might be involved.

When gPreConfigKeys = TRUE;, all devices in the network must be preconfigured at build time with the security key.

Set the default TC Link Key in nwk\_globals.c. in the NWK group. Replace the Key for In-House:

```
// Key for In-House Testing  
0x54, 0x45, 0x58, 0x41, 0x53, 0x49, 0x4E, 0x53  
0x54, 0x52, 0x55, 0x4D, 0x45, 0x4E, 0x54, 0x53
```

A Coordinator will initiate the network and accept join requests originating from the router or end-devices. Only the Coordinator or other ZRs which already have joined the network can accept join requests and forward packets [167]. Joining and identifying each device to the network is a very important step. Once a device has joined the ZigBee network, before communications begin, a message is sent to the Coordinator. At this stage, a decision is made about whether the device is authorized to join the network or not. This decision is based on the type of key and the configuration of the Coordinator [157]. As shown in Table 6.1, there are four options for configuring the Coordinator in ZigBee PRO, whereas only the two first options are available for the Coordinator configuration in ZigBee standard.

Table 6.1: Coordinator Authentication Configuration Options

Option	Joiner required information	Description
1	No keys pre-configured	Master, Link or Network Key is transmitted unencrypted Over The Air (OTA).
2	Active Network Key	Since the device has joined the network, the active Network Key should not change.
3	Coordinator address and Link Key	The secure connection is built using the Link Key and the address between Coordinator and the End Device. Then the Network Key is sent securely from the Coordinator.
4	Coordinator Address and Master Key	The Link Key for the device is generated using the Master Key. The Network Key is sent securely from the Coordinator.

- **Configuring Access Control List:** This is a table applied by the coordinator to determine which devices are authorized to perform a specific function. This table may also store the security material such as keys, frame counts, key counts, security level information, which are used for securely communicating with other devices within a network [108].
- **Turn Preconfigured Keys Off :** In a secure network, the Coordinator should be informed when a device joins the network. There is an option in the Coordinator that allows that device to enter the network or deny network access when a device wants to join.
- **Configure Network Access Control:** In a secure network, the coordinator is informed when a device joins the network. The coordinator has the option to allow that device to remain on the network or deny network access to that device.
  - 1) First, the SECURE schema, which is located in f8wConfig.cfg (config file) application in Tools workspace, should be activated.
  - 2) Find the ZDSecMgrDeviceValidate() function in ZDSecMgr.c in the ZDO workspace folder. In this function, the decision is made to either run high security mode (ZDSecMgrDeviceValidateCM()) or normal security mode (ZDSecMgrDeviceValidateRM()).
  - 3) Then find the ZDSecMgrDeviceValidateRM() function. The zgSecurityMode variable can control the Coordinator to reject any newly joining device [169].

4) Make sure that `gPreConfigKeys = FALSE` in `ZGlobals.c` so that key exchange is performed.

- **The white/black list features:** Comment out the `#if 0` and the `#endif` that surround the `ZDSecMgrDeviceValidateRM()` code. Now, if the joining device address matches the list, it is disallowed (black). So it should be changed to an allowed-device list (white). It is also possible to alter the address comparison to a portion of the IEEE address which all devices have in common [169].

Setting the Black IEEE Addresses: Find the list of IEEE addresses at `ZDSecMgrStoredDeviceList`. Comment out the `#if 0` and the `#endif` that surround the array. The IEEE addresses in the list, each one is broken into 8 groups of 8-bit addresses (64-bits total) [169]. For example, if the end device has this `20:bf:a7:d0:70:d6:1f:dc` IEEE address, it should be added to the Z-Stack at `ZDSecMgrStoredDeviceList` in this way:

```
uint8 ZDSecMgrStoredDeviceList[ZDSECMGR_STORED_DEVICES][Z_EXTADDR_LEN] =
{
  { 0xdc, 0x1f, 0xd6, 0x70, 0xd0, 0xa7, 0xbf, 0x20 },
};
```

Table 6.2: The security schema configurations

Descriptions	Configurations
Enabling Security	set <code>SECURE = 1</code> (in <code>f8wConfig.cfg</code> )
Enabling preconfigured Network key	set <code>gPreConfigKeys = TRUE</code> (in <code>nwk_globals.c</code> )
Setting preconfigured Network key	set <code>defaultKey = [170]</code> (in <code>nwk_globals.c</code> )
Setting the Black IEEE Addresses	call <code>ZDSecMgrStoredDeviceList</code> (in <code>ZDSecMgr.c</code> )
Specific device validation during joining	modify <code>ZDSecMgrDeviceValidate</code> (in <code>ZDSecMgr.c</code> )

Table 6:2 shows the summary of security schema configurations for enabling security, key distribution and network key setup, access control list, and device validation.

## 6.6 Configuring Destination Address and Performing Counter Attacks

In this section, it is explained how different configurations in the destination address, allows us to execute the DoS and replay attack. The destination address of the system is modified. Message's destination addresses can be toggled between broadcast or unicast.

```
SampleApp_Data_DstAddr.addr.mode = 0x0000 or 0xFFFF
```



We designed three different scenarios and configured the destination address of network devices to unicast and broadcast and then captured all transmission by the TI Packet Sniffer.

- Unicast: This addressing refers to a single sender or a single receiver, and can be used for both sending and receiving [171].
- Broadcast: This addressing permits the sender to send to all possible destinations, and all receivers receive a copy of it [171].

### 6.6.1 Defining of Scenarios

In this section, three different scenarios are defined and the behaviour of every single scenario is examined by sniffing the packets using a packet sniffer.

- **Scenario 1 Unicast address:**

This is the normal addressing mode and is used to send a packet to a single device whose network address is known. The `addrMode` is set to `Addr16Bit` and the destination network address is carried in the packet.

- **Scenario 2 Broadcast address:**

This address mode is used when the application intends to send a packet to all devices in the network. The address mode is set to `AddrBroadcast` and the destination address can be set to one of the following broadcast addresses: `NWK_BROADCAST_SHORTADDR_DEVALL` (0xFFFF). The message will be sent to all devices in the network (includes sleeping devices). For sleeping devices, the message is held at its parent until the sleeping device polls for it or the message has timed out (`NWK_INDIRECT_MSG_TIMEOUT` in `f8wConfig.cfg`).

`NWK_BROADCAST_SHORTADDR_DEVRXON` (0xFFFD) – The message will be sent to all devices that have the receiver on when idle (`RXONWHENIDLE`), that is, all devices except sleeping devices.

`NWK_BROADCAST_SHORTADDR_DEVZCZR` (0xFFFC) – The message is sent to all routers (including the coordinator).

- **Scenario 3 Unicast and Broadcast address:**

This scenario is combination of the last two scenarios, where the unicast address is set to coordinator and the broadcast address is set to the end devices. This means that the `addrMode` of the coordinator is set to `Addr16Bit` and the destination network address is carried in the

packet and the address mode of end devices are set to AddrBroadcast, which can be set to the following broadcast addresses: NWK\_BROADCAST\_SHORTADDR\_DEVALL (0xFFFF).

### 6.6.2 Implementation of Scenarios

In this section, the implementations of different scenarios are described in details and the behaviour of the network for each scenario is examined.

- **Scenario 1 Unicast only:**

Configure the end device and Coordinator with this:

SampleApp\_Data\_DstAddr.addr.shortAddr=0x0000;

In scenario 1, the Coordinator generates only one unicast packet for every single transmission, which does not allow us to execute a replay attack.

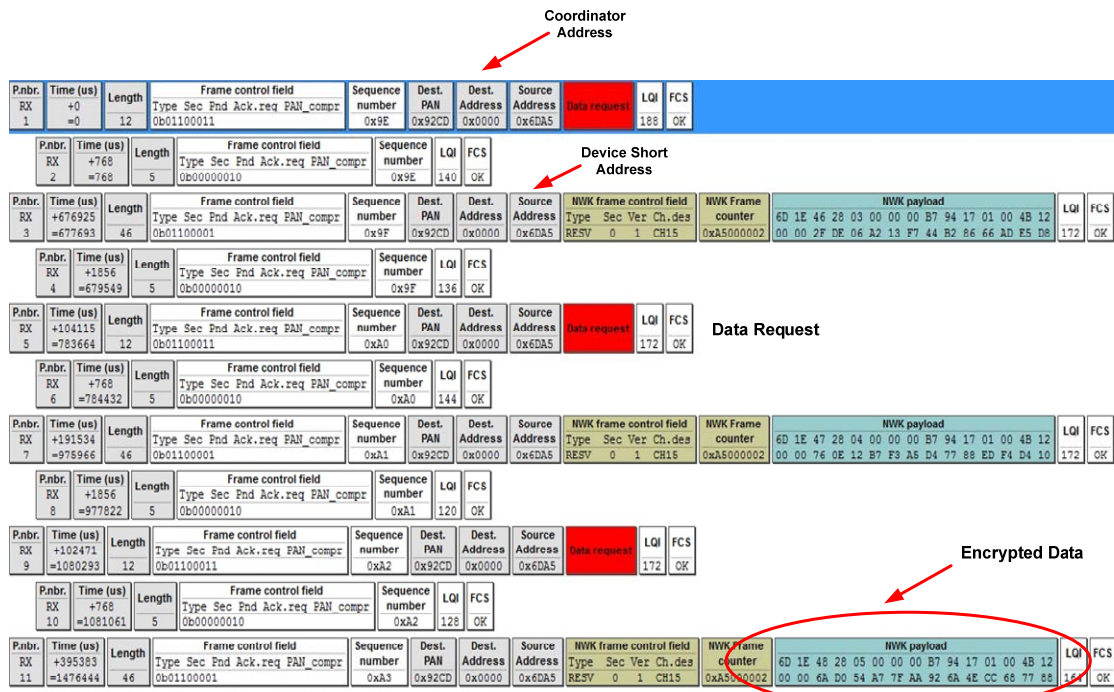


Figure 6-4: Encrypted packet unicast coordinator and unicast end device

Figure 6-4 depicts the screenshot from TI Packet Sniffer. It shows the IEEE 802.15.4 packets, which have a maximum MAC Payload Data Unit (MPDU) size of 127 bytes. The MPDU contains the Frame Control Field (FCF), sequence number, address field, frame payload, and Link Quality Indicator (LQI) metrics that are returned by the hardware platform for each packet and finally, the Frame Check Sequence (FCS). Texas Instruments has released

their Packet Sniffer that works with CC2530ZDK. It is capable of monitoring one channel at a time. The diagram below shows a screenshot of the Texas Instrument Packet Sniffer.

Figure 6-4 illustrates the screenshot of scenario 1. It shows encrypted packets where the unicast address has been set for the coordinator and end devices. The payload is encrypted and the address 0x0000 (Coordinator Address, which is indicated in the diagram) has been set to the coordinator and the address 0x6DA5 (Device Short Address, which is pointed in the diagram) has been set to the end device. The packets with no data payload are shown in the diagram as the Data Request. This frame does not carry any data. As can be seen, by addressing unicast to both coordinator and end devices, no broadcast address (0xFFFF) is generated in the coordinator.

- **Scenario 2 Broadcast only:**

Configure the end device and Coordinator with this:

SampleApp\_Data\_DstAddr.addr.shortAddr=0xFFFF;

In scenario 2, the Coordinator generates three broadcast packets for each transmission. These packets include 0xFFFF Dest Address, which is indicated as the Broadcast Address in Figure 6-5. These broadcast packets allow us to execute replay attack.

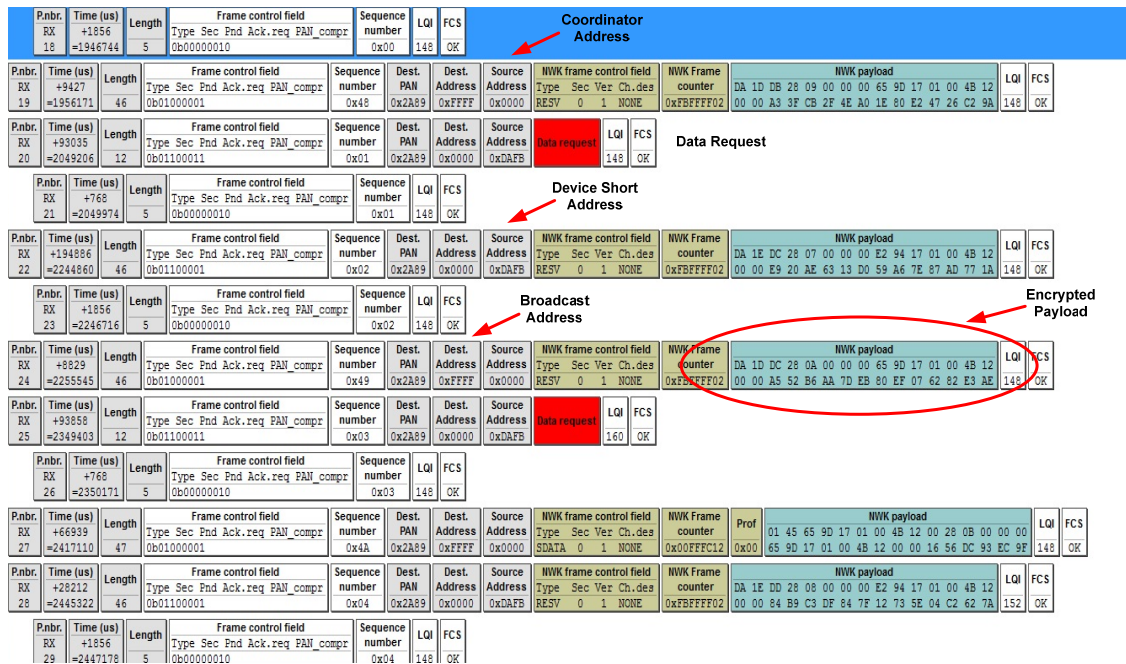


Figure 6-5: Encrypted payload coordinator and end-devices broadcast

Figure 6-5 shows the screenshot of scenario 2. It shows the encrypted packet where the broadcast addressed has been set for the coordinator and End-devices. The payload is encrypted by AES-128 encryption algorithm and the address 0x0000 (Coordinator Address, which is pointed in the diagram) has been set to the coordinator and the address 0xDAFB (Device Short Address, which is pointed in the diagram) has been set to the end device. As can be seen in Figure 6-5, by addressing broadcast to both coordinator and end devices, some broadcast packets (Dest Address 0xFFFF) are generated in the destination address of the coordinator. Through this broadcast address, the replay attack is executable.

- **Scenario 3 Unicast and Broadcast:**

Configure the end device with this:

SampleApp\_Data\_DstAddr.addr.shortAddr=0xFFFF;

Configure the Coordinator with this:

SampleApp\_Data\_DstAddr.addr.shortAddr=0x0000;

Pnbr.	Time (us)	Length	Frame control field	Sequence number	LQI	FCS	Device Short Address	Coordinator Address	Source Address	NWK frame control field	NWK Frame counter	NWK payload	LQI	FCS
RX 4	+768 =1004854	5	Type Sec Pnd Ack.req PAN_compr 0b00000010	0x24	136	OK								
RX 5	+364010 =1368864	46	Type Sec Pnd Ack.req PAN_compr 0b01100001	0x25	0xD6FB	0x0000	0x91B4	0x0000	RESV 0 1 NONE	0xB4FFFFF02	91 1E 5C 28 06 00 00 00 E2 94 17 01 00 4B 12 00 00 19 4B 7E 79 AA 8E 45 36 F2 A6 EF 9E C7	204	OK	
RX 6	+1856 =1370720	5	Type Sec Pnd Ack.req PAN_compr 0b00000010	0x25	112	OK								
RX 7	+8857 =1379577	46	Type Sec Pnd Ack.req PAN_compr 0b01100001	0x26	0xD6FB	0xFFFF	0x0000	0x0000	RESV 0 1 NONE	0xB4FFFFF02	91 1D 5C 28 08 00 00 00 00 BB 9E 17 01 00 4B 12 00 00 05 24 2C C5 60 74 AB 31 C1 51 0E C0 7A	112	OK	
RX 8	+93999 =1473576	12	Type Sec Pnd Ack.req PAN_compr 0b01100011	0x26	0xD6FB	0x0000	0x91B4		Data request				204	OK
RX 9	+768 =1474344	5	Type Sec Pnd Ack.req PAN_compr 0b00000010	0x26	120	OK								
RX 10	+194317 =1668661	46	Type Sec Pnd Ack.req PAN_compr 0b01100001	0x27	0xD6FB	0x0000	0x91B4	0x0000	RESV 0 1 NONE	0xB4FFFFF02	91 1E 5D 28 07 00 00 00 00 E2 94 17 01 00 4B 12 00 00 E9 20 AE 63 13 D0 59 A6 7E 69 DC CE EC	204	OK	
RX 11	+1856 =1670517	5	Type Sec Pnd Ack.req PAN_compr 0b00000010	0x27	116	OK								
RX 12	+8750 =1679267	46	Type Sec Pnd Ack.req PAN_compr 0b01100001	0x2F	0xD6FB	0xFFFF	0x0000	0x0000	RESV 0 1 NONE	0xB4FFFFF02	91 1D 5D 28 09 00 00 00 00 8B 9E 17 01 00 4B 12 00 00 68 CC 61 BA 56 A9 D5 72 FB 9F 0D 63 00	128	OK	
RX 13	+94074 =1773341	12	Type Sec Pnd Ack.req PAN_compr 0b01100011	0x28	0xD6FB	0x0000	0x91B4		Data request				204	OK
RX 14	+768 =1774109	5	Type Sec Pnd Ack.req PAN_compr 0b00000010	0x28	116	OK								
RX 15	+194718 =1968827	46	Type Sec Pnd Ack.req PAN_compr 0b01100001	0x29	0xD6FB	0x0000	0x91B4	0x0000	RESV 0 1 NONE	0xB4FFFFF02	91 1E 5E 28 08 00 00 00 00 E2 94 17 01 00 4B 12 00 00 84 B9 C3 DF 84 7F 12 73 5E 88 73 1D D6	204	OK	

Figure 6-6: Encrypted payload coordinator unicast end-device broadcast

Figure 6-6 shows the screenshot of scenario 3. It illustrates the encrypted packet where the unicast addressed has been set for the coordinator and the broadcast address has been set for end devices. The payload is encrypted and the address 0x0000 (Coordinator Address, which is indicated in the diagram) has been set to the coordinator and the address 0x91B4 (Device Short Address, which is indicated in the diagram) has been set to the end device. As can be



seen, by addressing broadcast to end devices, some broadcast packets are generated in the destination address of the coordinator. Through this broadcast address (Dest Address 0xFFFF), the replay attack is executable.

In scenario 3, Coordinator generates one unicast and one broadcast packet for every transmission. The broadcast packet allows us to execute a replay attack.

- **Removing the security schema:**

We removed the security schema in the Z-Stack to ensure that the replay attack is doable.

Firstly, we configured the destination address of both coordinator and end devices to unicast.

SampleApp\_Data\_DstAddr.addr.shortAddr=0x0000;

Figure 6-7 indicates that only one frame with the Source address of 0x1D9A frame (Device Short Address, which is pointed in the diagram) and destination address of 0x0000 is generated.

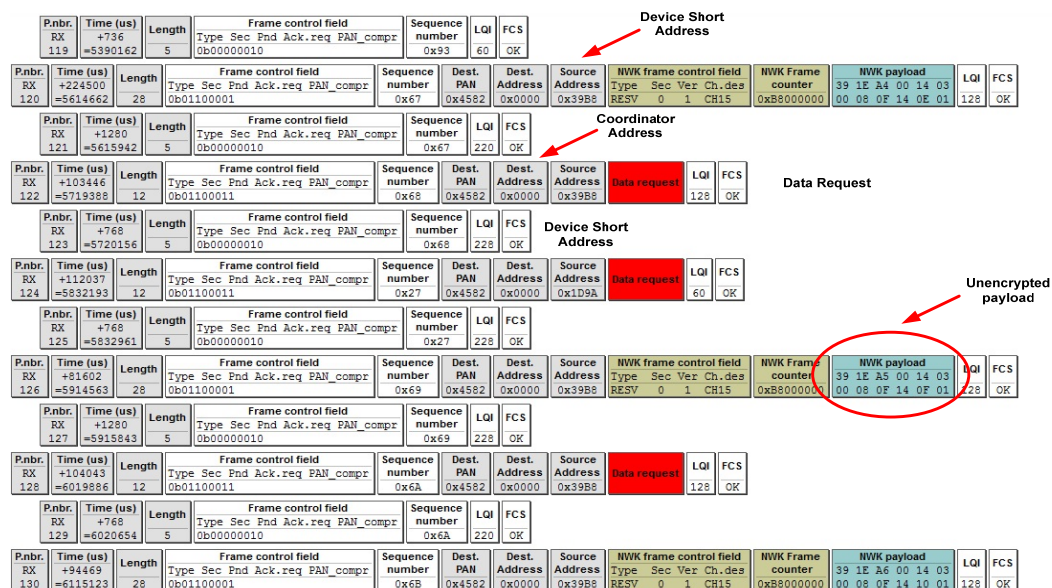


Figure 6-7: Packet captured no security with unicast address

Figure 6-7 shows the screenshot when the security schema is removed. This diagram illustrates that the packet is captured where the security schema is not enabled, and the unicast address has been set on both coordinator and end devices. As can be seen, the payload is not encrypted and the address 0x0000 has been set to the coordinator and the address 0x39DB and

0x1D9A (Device Short Address, which is indicated in the diagram) have been set to the end devices. However, there is no broadcast packet, but the attacker is able to execute the replay attack.

Secondly, the destination address of coordinator to unicast and the destination address of end devices to broadcast is configured.

SampleApp\_Data\_DstAddr.addr.shortAddr=0x0000;

SampleApp\_Data\_DstAddr.addr.shortAddr=0xFFFF;

Figure 6-7 indicates that two different frames are generated:

One frame with: Source address 0x1D9A and Dest Address 0x0000

Second frame with: Source address 0x0000 and Dest address 0xFFFF

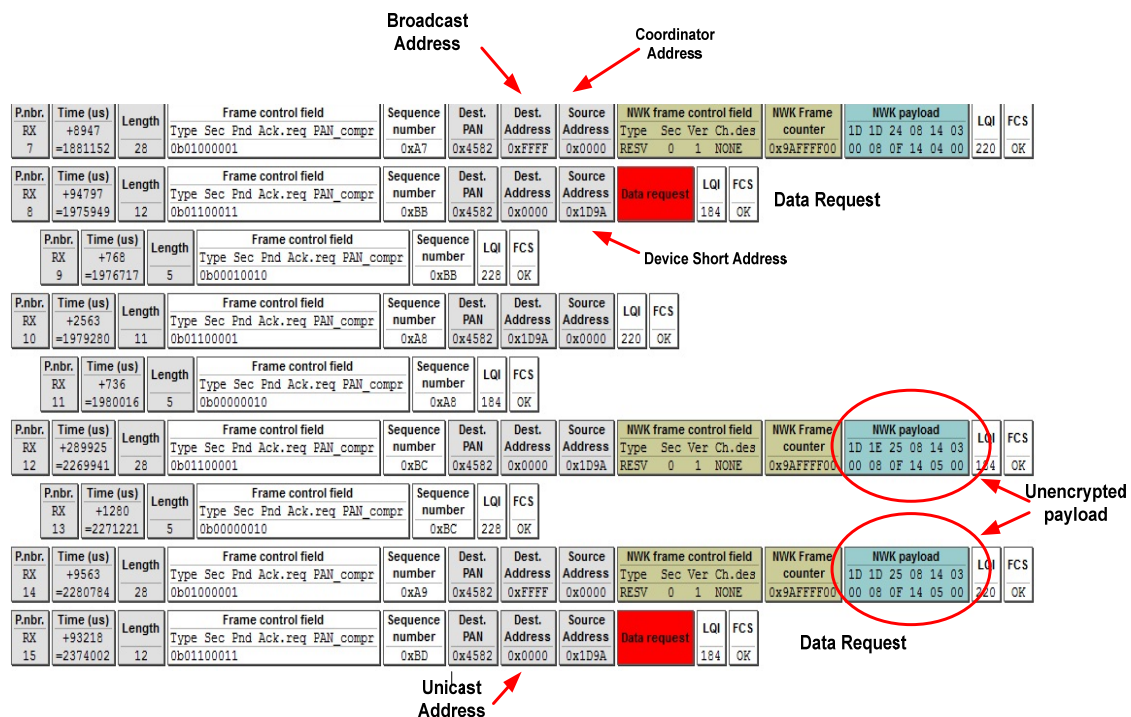


Figure 6-8: Packet captured no security unicast coordinator broad cast end-device

Figure 6-8 shows the screenshot when the security schema is removed. It indicates that the packet captured where the security schema is not enabled and broadcast address has been set on both coordinator and end devices. As can be seen, the payload is not encrypted and the address 0x0000 (Coordinator Address, which is indicated in the diagram) has been set to the coordinator and the address 0x1D9A (Device Short Address, which is indicated in the diagram) has been set to the end devices. The attacker is able to execute the replay attack.

As can be seen in Figures 6-7 and 6-8, payloads are unencrypted by removing the security schema in the Z-Stack. As long as the security schema is not activated in ZigBee, an adversary is able to execute the replay attack whether the network has been set up with a unicast or broadcast address.

## 6.7 Summary of Implementation

This chapter contained a description of the necessary hardware and software and an explanation of how we get started with the ZigBee Sample application for CC2530 and how we configure the sample application to control data by adding some codes to the Z-Stack. Three scenarios have been described, implemented and the behaviour of scenarios have been examined by the TI Packet Sniffer. We found that by setting up the broadcast address (0xFFFF) to the destination of end devices (Scenario 2, 3), we are able to force the coordinator to generate a broadcast address, which allows us to inject them back to the coordinator and execute the replay attack. In addition, we found that by configuring the unicast address of nodes within the ZigBee network, we are able to prevent the replay attack. Also, the behaviour of the ZigBee network without a security schema has been examined. It was proved that ZigBee with no security schema is easily susceptible to the replay attack, whether the addresses of nodes are configured as broadcast address or unicast address.

## 6.8 Conclusion

In this chapter, the attack scenario was described and the important details of the attacks were given including why these attacks were selected, what was expected to be investigated, how attacks would be measured, whether successful or not. The choice of a ZigBee development kit and source code from Texas Instrument was explained. Also, in this chapter, all the software and hardware required for setting up the test-bed to conduct the experiment were explained in detail. It was shown how the Z-Stack code was changed to control the communication. The network configuration for applying the security schema in ZigBee was presented to show how all the security requirements in ZigBee are employed. Different authentication options for key distribution in ZigBee coordinator was shown, and we discussed why the automatic key distribution by the coordinator is preferred to setting up the key in the factory in an out-of-band method.

## 7 Evaluation of the Security Risk and Execution Counter Attack

### 7.1 Introduction

In this chapter, the attack scenario is described; important details of the attacks are given including why these attacks were selected, what was expected to be investigated, and how the success or otherwise of the attacks would be measured. Also, it explains our objectives and how these are achieved. A solution is implemented for each remaining attack, and a flow chart is provided showing how the attack is launched, including all steps that were followed when attacking.

The security risks are evaluated by executing the remaining attacks such as replay, DoS and physical tampering attack within the ZigBee network and the strategy for controlling such attacks is explained. The exploitation of the ZigBee Coordinator is detailed: two approaches are developed namely, manual approach and automatic approach, for replay attack, and the solution to such attack is explained in detail. Flooding and jamming attacks are examined and solutions for controlling these two types of attack are discussed.

A few steps are required to execute the DoS and replay attacks. These steps include the application development, device configuration and network set-up. These steps are applied to execute DoS and replay attacks on the Coordinator, either automatically or manually. At the end of this chapter, the Quality of Service (QoS) in ZigBee-based wireless communication, where the security schema is activated, is examined.

### 7.2 Manual-based Network Set-up for Replay Counter Attack

This section describes how to set up a ZigBee sensor network demo which consists of Coordinator and end devices, using the pre-programmed devices of the CC2530ZDK. The last chapter explained the software and hardware that are required and how there are configured for the experiment. Below is a list of required hardware and software for a manual-based network setup for replay counter attack:

**Hardware:**

1 - 2 x SmartRF05EB (the large boards)

2 - 3 x CC2530EM

3 - 1x CC2430DB



## Software:

- 1 - Z-Stack
- 2 - Compiler from IAR
- 3 - TI Packet Sniffer
- 4 - Smart RF Studio (Flash Programmer)

The CC2530EM evaluation modules can be plugged into SmartRF05EB and SmartRF05BB boards, which are included in the development kit. The network contains two CC2530EMs programmed as collector devices, which can be used as a gateway, and the CC2530EMs are programmed as sensor devices. The listed software for executing our attack is required. The Z-Stack is a Texas Instrument ZigBee compliant protocol stack for the portfolio of IEEE 802.15.4 products and platforms.

The sensors periodically report their temperature and the routers ensure that the data gets routed to the collector node that functions as a gateway. The collector node configured as a gateway is connected to the PC running the PC application that visualizes the network topology and the sensor data. The TI packet sniffer and Smart RF Studio for listening and injecting are applied in this attack.

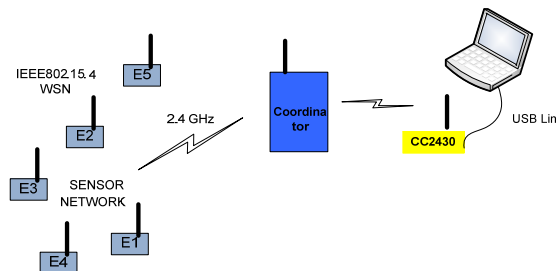


Figure 7-1: Test-bed for Manual Attack

The test-bed for executing replay attack is shown in Figure 7-1. As depicted, the laptop is equipped with the CC2430 as the listener and injector, in addition to the TI packet sniffer and Smart RF Studio software from TI.

### 7.3 Automated method through Network Set-up for Counter Replay Attack

As mentioned earlier, the KillerBee application was designed by Josh Wright to exploit the ZigBee/ZigBee network. Based on his talk, we set up the KillerBee test-bed at our wireless lab to prove the claims regarding the exploitation of the ZigBee/ZigBeePRO network through the KillerBee application. This attack is launched using the KillerBee framework, which

comprises tools for attacking ZigBee and IEEE 802.15.4 networks. Below is a list of required hardware and software for automated method using the network set-up for counter replay attack.

**Hardware:**

- 1- SmartRF05 Evaluation Boards
- 2- SmartRF05 Battery Board
- 3- CC2430DB Listener from Texas Instrument
- 4- Atmel RZ Raven USB Stick
- 5- Atmel JTAGICE mkII On-Chip Programmer

**Software:**

- 1- Z-Stack
- 2- IAR Workbench Compiler
- 3- KillerBee framework
- 4- Linux OS
- 5- Wireshark or Daintree SNA
- 6- AVR Studio for Windows
- 7- KillerBee Firmware for the RZUSBSTICK

- **KillerBee framework:** This is a Python-based framework and tool set to used to exploit the security of ZigBee and IEEE 802.15.4 networks. This framework includes several tools for eavesdropping on ZigBee networks, replaying traffic, and attacking cryptosystems, to name just a few. The KillerBee framework allows us to build our own tools and implement ZigBee fuzzing, emulate and attack the network [172].

KillerBee is designed to simplify the process of sniffing packets from the air interface or a supported packet capture file by Wireshark or Daintree SNA to inject arbitrary packets.

The KillerBee framework is currently based on the Atmel RZ RAVEN USB Stick. This hardware is convenient as the base firmware is open source with a freely-available IDE. The KillerBee firmware for the RZ RAVEN included in the firmware/ directory is a modified version of the stock firmware distributed by Atmel to include attack functionality [172]. This framework is intended for developers and advanced analysts who are attacking ZigBee and IEEE 802.15.4 networks. KillerBee is developed and tested on Linux systems.

The stock firmware of RZ RAVEN USB allows the researcher to leverage the passive functionality such as receiving frames, but does not include injection. To obtain the full functionality including injection in KillerBee, the RZ RAVEN USB Stick must be flashed with by Atmel JTAGICE mkll. This device is required to flash the KillerBee firmware onto a RZ RAVEN USB Stick using the included 10-pin header interface [172].

- **KillerBee tools:** KillerBee includes several tools which are designed to attack ZigBee and IEEE 802.15.4 networks.
  - Zbassocflood: This is associated to the target PANID in an effort to cause the device to crash from too many connected stations.
  - Zbconver: Converts a packet capture from Libpcap to Daintree SNA format, or vice-versa.
  - Zbdsniff: Captures ZigBee traffic, looking for NWK frames and over-the-air key provisioning. When a key is found, zbdnsniff prints the key to stdout.
  - Zbdump: This is similar to tcpdump and captures IEEE 802.15.4 frames to a libpcap or Daintree SNA packet capture file. There is no display real-time stats like tcpdump when not writing to a file.
  - Zbgoodfind: Implements a key search function by using an encrypted packet capture and memory dump from a legitimate ZigBee or IEEE 802.15.4 device. The search file of this must be in binary format and convert from the hexfile format to a binary file, use the objcopy tool: `objcopy -I ihex -O binary mem.hex mem.bin`
  - Zbid: Identifies available interfaces that can be used by KillerBee and associated tools.
  - Zbreplay: This tool is applied to implement the replay attack, reading from a specified Daintree DCF or libpcap packet capture file and injecting it into the network.
  - Zbstumbler: Active ZigBee and IEEE 802.15.4 network discovery tool. Zbstumbler sends out beacon request frames while channel hopping, recording and displaying summarized information about discovered devices. Can also log results to a CSV file.
- **RZ RAVEN USB:** This device belongs to the family of AVR's with a low and full speed USB macro device. The microcontroller is AT86RF230, which is a 2.4GHz radio for a wide range of wireless applications [173].

The RZ RAVEN USB device is a sniffer by default; to change this device to the injector, the appropriate firmware is required. The right firmware for programming RZ RAVEN USB from the developer of KillerBee was received. Then the device was programmed by Atmel JTAGICE mkII On-Chip Programmer and AVR Studio Software and changed to an injector.



Figure 7-2: Programming RZ RAVEN USB by Atmel JTAGICE mkII

Figure 7-2 shows the programming of RZ RAVEN USB through Atmel JTAGICE mkII. This device changes the role of RZ RAVEN USB to injector rather than sniffer, which is programmed by default on RZ RAVEN USB.

- **AVR Studio:** Atmel AVR Studio is the Integrated Development Environment (IDE) for developing and debugging embedded Atmel AVR applications. The AVR Studio IDE provides a seamless and easy-to-use environment to write, build and debug C/C++ and assembler code [174].
- **Wireshark:** Wireshark is a network packet analyser which is able to capture network packets and tries to display that packet data in as much detail as possible. Wireshark packet sniffer recently supports IEEE 802.15.4 as a medium for a wide variety of network protocols, including ZigBee [175].
- **Daintree SNA:** Daintree's Sensor Network Analyser (SNA) provides solutions for developing, decoding, debugging and deploying wireless embedded networks. This is an expert tool for IEEE 802.15.4 and ZigBee. The SNA has extended to additional standards protocols such as ZigBee RF4CE, 6LoWPAN, JenNet (from Jennic), SimpliciTI (from Texas Instruments) and Synkro (from Freescale Semiconductor) [176].

Figure 7-3 shows the design of the KillerBee test-bed. This network is a combination of Texas Instrument devices and Atmel devices. This figure shows how the KillerBee machine communicates with the CC2530 development kit through RZ RAVEN USB devices.

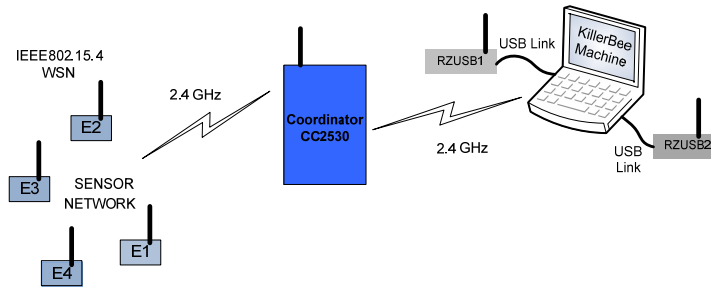


Figure 7-3: Test-bed for Automatic Attack

## 7.4 Implementation of Counter Measure against Attacks

In this section, the different approaches, whether manual or automatic, to executing DoS and replay attacks are explained.

### 7.4.1 Eavesdropping

As previously stated, over-the-air key set-up is unsecured and vulnerable to a one-time eavesdropper attack. This key can be grabbed by a packet sniffer such as the TI Packet Sniffer or one of the tools in the KillerBee framework. By applying the TI packet sniffer, it is possible to grab the key in plain text if the coordinator is configured to distribute the key to the network.

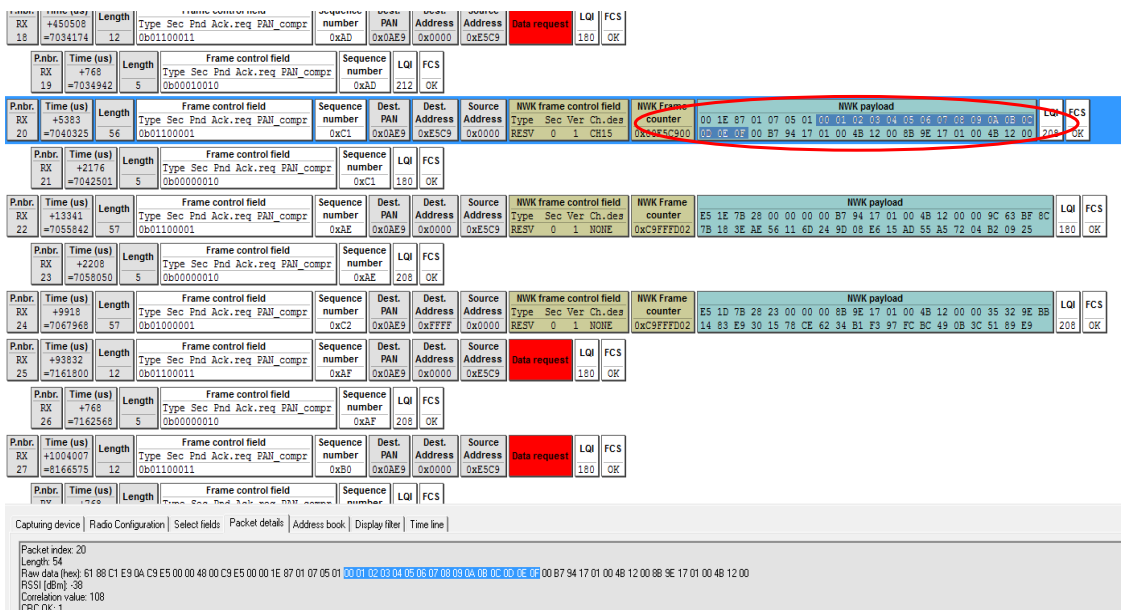
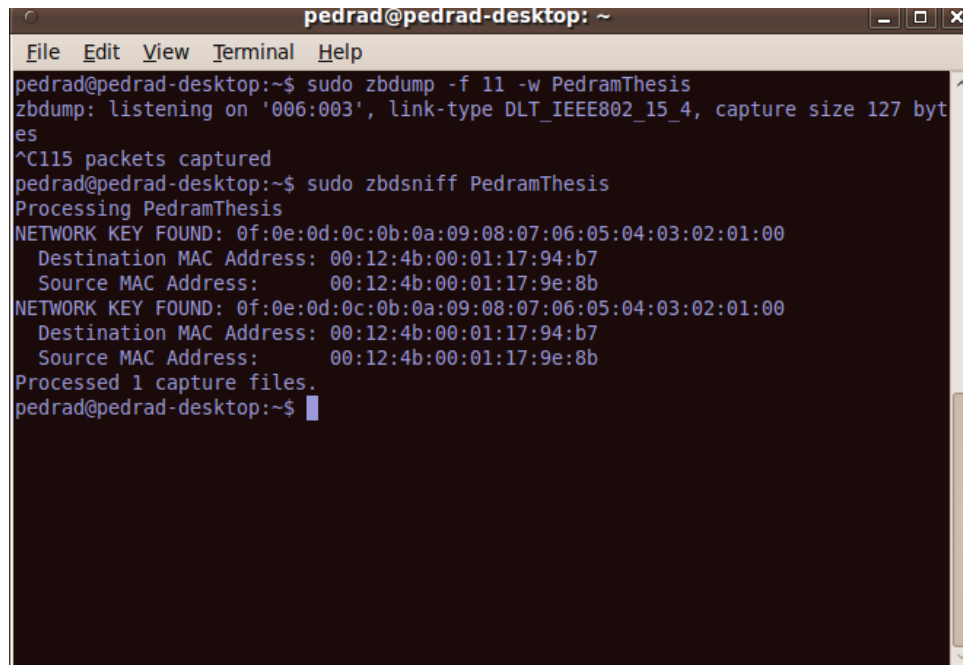


Figure 7-4: Grabbing the key by packet sniffer.

Figure 7-4 shows the screenshot of the TI Packet Sniffer. It shows how it is possible for the packet sniffer to grab the key. As can be seen, the key, which is highlighted in the above diagram, was captured in the first row of the data packet. The network key is shown in the red circle in Figure 7-4. The key is readable 000102030405060708090A080C0D0E0F and is sent from Coordinator to the end devices in plain text.

By applying the KillerBee tool Zbdsniff, it is possible to capture ZigBee traffic, looking for NWK frames and over-the-air key provisioning. Also, this tool allows us to access the key and destination and source addresses of two communicating nodes. Figure 7-5 depicts the key and MAC address which were obtained by the Zbdsniff tool.



```
pedrad@pedrad-desktop: ~  
File Edit View Terminal Help  
pedrad@pedrad-desktop:~$ sudo zbdump -f 11 -w PedramThesis  
zbdump: listening on '006:003', link-type DLT_IEEE802_15_4, capture size 127 bytes  
^C115 packets captured  
pedrad@pedrad-desktop:~$ sudo zbdsniff PedramThesis  
Processing PedramThesis  
NETWORK KEY FOUND: 0f:0e:0d:0c:0b:0a:09:08:07:06:05:04:03:02:01:00  
  Destination MAC Address: 00:12:4b:00:01:17:94:b7  
  Source MAC Address:    00:12:4b:00:01:17:9e:8b  
NETWORK KEY FOUND: 0f:0e:0d:0c:0b:0a:09:08:07:06:05:04:03:02:01:00  
  Destination MAC Address: 00:12:4b:00:01:17:94:b7  
  Source MAC Address:    00:12:4b:00:01:17:9e:8b  
Processed 1 capture files.  
pedrad@pedrad-desktop:~$
```

Figure 7-5: KillerBee tool for grabbing keys.

Figure 7-5 shows the KillerBee tools for grabbing keys. As illustrated, the key is readable and captured by the zbdsniff tools.

Once a device intends to join the network, the key is sent in plain text for the first time. As can be seen in Figure 7-5 “NETWORK KEY FOUND”, “Destination MAC Address” and “Source MAC Address” are shown twice. This means, that twice the device tried to join the network, and the Coordinator was configured to distribute the key to the network over air rather than out-of-band configuration, which sets the key in the factory and key distribution from the Coordinator is disabled.

The key is readable 0F0E0D0C0B0A090807060504030201000. If this key is read from right to left, we can find that the key in Figure 7-5 is the same as the key in Figure 7-4, which was obtained using different software and approach.

The key in both methods is sniffed, as both methods are able to capture the key at the beginning of handshaking. Note that the key grabbed by the KillerBee method should be read from right to left similarly to the key grabbed by the TI Packet Sniffer. The network key in this experiment is “00:01:02:03:04:05:06:07:08:09:0a:0b:0c:0d:0e:0f”.

#### 7.4.2 Eavesdropping Solution

This problem can be solved by using a key which is pre-installed at the factory, added by the final user in an out-of-band manner instead of having it sent from the coordinator to other devices, trusting them with the distribution of security keys.

ZGlobals.c in the NWK workspace group configure `gPreConfigKeys = TRUE;`, all devices in the network must be preconfigured at build time with the security key.

Setup the key in `defaultTCLinkKey` in `nwk_globals.c` in the NWK group.

```
// Key for In-House Testing
```

```
0x54, 0x45, 0x58, 0x41, 0x53, 0x49, 0x4E, 0x53
```

```
0x54, 0x52, 0x55, 0x4D, 0x45, 0x4E, 0x54, 0x53
```

By configuring this, the key in all devices within the network is set up, without any key exchange over the air through the coordinator.

However, an out-of-band transfer method is recommended because of the security implications of passing the key in the clear, but key transfer in a dense network would create some issues such as key management, costly maintenance and security. So in a dense network, it is recommended to leave the key distribution to coordinators and focus on this issue of concern.

#### 7.4.3 DoS Attack

The steps below show the attack procedure:

1. Run the Smart RF Studio on the laptop, which has the plugged to CC2430 device.
2. Click the TXT Test modes tab in the Smart RF Studio.
3. Select the packet from the Packet Sniffer.
4. Copy and paste the packet to the TXT Test modes in Smart RF Studio.
5. Click Start TX test.

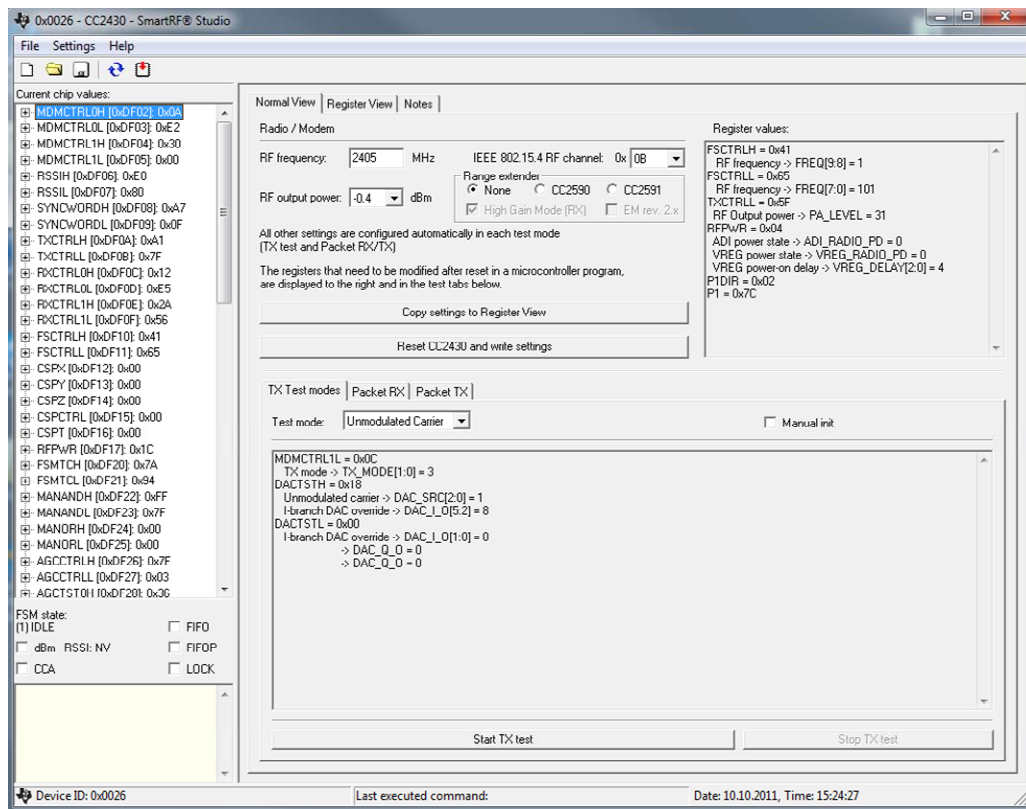


Figure 7-6: Packet injection by Smart RF Studio

Figure 7-6 depicts the Smart RF Studio software which was applied for DoS attack by the researcher. By sending a great many packets through the TX Test modes tab in this software, the process in the coordinator is halted.

By means of this injection, numerous packets are sent to the network and the Coordinator, and the communication between end devices and Coordinator is interrupted.

#### 7.4.4 DoS Solution

By configuring Scenarios 1 and 2, two different results are obtained.

##### a) Configuring the network by Scenario 1

In this scenario, the communication is interrupted by the injection and the Coordinator does not detect any packets. This means that only the communication is distorted and the communication channel is full, but the buffer of the coordinator is not full because, by playing the joystick, we are able to generate data destined for the coordinator and we can see the packets are counted. When the injection stops, communication resumes.



## b) Configuring the network by scenario 2

In this scenario, the communication is interrupted by the injection and Coordinator does not detect any packets. The coordinator buffer overflows and no packet is processed even by playing the coordinator joystick to send packets. This means that the communication channels as well as the coordinator buffer are exhausted.

The CC2530 combines an enhanced 8051 MCU, in-system programmable flash memory, 8-KB RAM, and many other powerful features [161].

- **Microcontroller 8051:** The Intel 8051 microcontroller is one of the most popular, general purpose ones. The Intel 8051 is an 8-bit microcontroller since most available operations are limited to 8 bits [177].

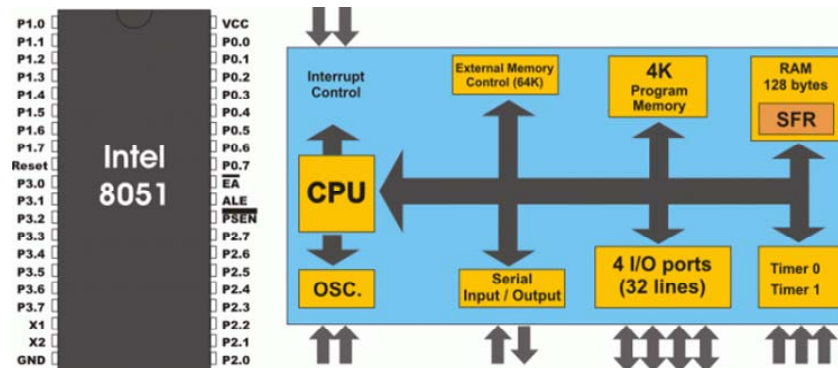


Figure 7-7: Intel 8051 Microcontroller [178].

Figure 7-7 shows the Intel 8051 Microcontroller which includes several parts. Each part of this microcontroller is explained below.

- **4k Program Memory:** 4 Kb of ROM.
- **4 I/O ports:** The 8051 microcontroller has 4 Input/output ports each comprising 8 bits which can be configured as inputs or outputs. 32 input/output pins enable the microcontroller to be connected to peripheral devices for use [177].
- **Special Function Registers (SFRs):** This is a sort of control table that runs and monitors the operation of the microcontroller. SFRs are similar to an internal RAM. The difference between them is that an internal RAM is from address 00h through to 7Fh, whereas SFR is from 80h through to FFh. It is the upper area of addressable memory. SFRs are a set of registers in a microcontroller, which controls various aspect of function. There are 128 memory locations and 21 registers [177]. One of the registers in SFR is called Program Status Word (PSW) Register.

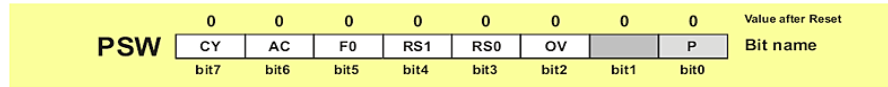


Figure 7-8: Program Status Word Register Flags [178].

- P - Parity bit: This for accumulating a number in the accumulator.
- OV Overflow: This flag sets to 1, if the result of an arithmetical operation is larger than 255. This large numerical operation cannot be stored in one register.
- RS0, RS1 - These two bits are applied to select one of four register banks of RAM. By setting and clearing these bits, registers R0-R7 are stored in one of four banks of RAM.
- F0 - Flag 0. This means bits are available for use.
- AC - Auxiliary Carry Flag is applied for BCD (Binary Coded Decimal) operations.
- CY - Carry Flag is the auxiliary bit which is applied for all arithmetical operations and shift instructions [177].

Figure 7-8 illustrates the Program Status Word Register Flags in the SFR section of 8051 microcontroller. The PSW is the most important register in SFR and contains several status bits such as Carry bit, Auxiliary Carry; two register bank select bits, Overflow flag, parity bit and user-definable status flag.

Since microcontroller has limited RAM memory, by sending a great deal of data to the Coordinator, overflow occurs because the arithmetical operation is becoming larger than 255 and the flag is set to 1 and the CPU processing of microcontroller is stopped.

#### 7.4.5 Replay Attack

In this section, both the manual and automatic replay attacks were described. Both attacks were launched when the security schema was activated. This security measure is supposed to prevent any attack including a replay attack. The flowchart below shows how replay attack on actual devices is executed in the lab.

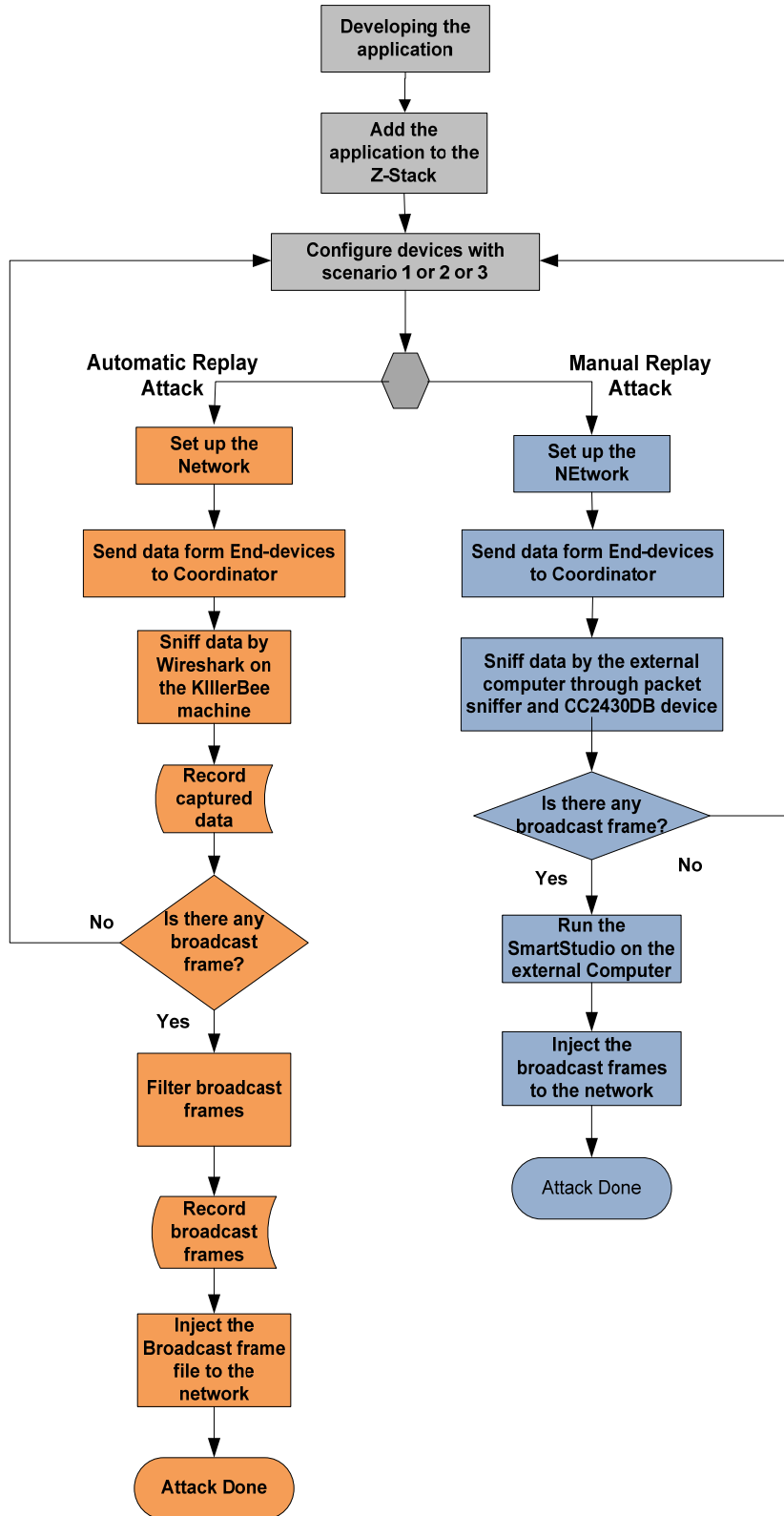


Figure 7-9: The procedure of executing replay attack.

Figure 7-9 shows the step-by-step procedure for executing replay attack. The application, which controls the data from end-device to the coordinator, should be added to the Z-Stack and compiled. Scenarios 1, 2, 3 should be implemented separately. As can be seen, manual and automatic replay attacks each require a different approach.

### a) Manual Replay Attack Execution

In this attack, the replay attack is manually executed. Firstly, we set up the network and then develop and upload the application with one of the above scenarios. In fact, the goal of this attack is to force the coordinator to generate a broadcast packet, whether an encrypted or unencrypted packet, and then through the broadcast packet execute the replay attack. The steps below show the attack procedure:

1. Scenarios 2 and 3, which generate broadcast packets on the coordinator, are implemented.
2. Send manually packets from end device to the coordinator by playing the joystick.
3. Capture transmitted data using a packet sniffer.
4. Select the broadcasted packets from the packet sniffer and inject them by the Smart RF Studio software and the CC2430 device to the network. This step is shown in Figures 7-10 and 7-11.

Inbr.	Time (us)	Length	Frame control field	Sequence number	Dest. PAN	Dest. Address	Source Address	NWK frame control field	NWK Frame counter	NWK payload	LQI	FCS
RX	+9999	46	Type Sec Pnd Ack.req PAN_compr 0b01100001	0xB8	0x0D9C	0xFFFF	0x0000	Type Sec Ver Ch.dea RESV 0 1 NONE	0x40FFFF02	17 1D C7 28 B8 00 00 00 8B 9E 17 01 00 4B 12 00 00 06 EC B8 4D 47 27 5F A9 3D 42 13 D7 B0	212	OK
RX	+93709	12	Type Sec Pnd Ack.req PAN_compr 0b01100011	0x8F	0x0D9C	0x0000	0x1740	Data request			160	OK
Pnbr.	+768	5	Type Sec Pnd Ack.req PAN_compr 0b00000010								212	OK
RX	+395121	46	Type Sec Pnd Ack.req PAN_compr 0b01100001	0x90	0x0D9C	0xFFFF	0x0000	Type Sec Ver Ch.dea RESV 0 1 NONE	0x40FFFF02	17 1E C8 28 02 00 00 00 E2 94 17 01 00 4B 12 00 00 BB BD 41 9B 10 6B B3 59 27 E2 A8 B9 13	140	OK
Pnbr.	+1856	5	Type Sec Pnd Ack.req PAN_compr 0b00000010								212	OK
RX	+9100	46	Type Sec Pnd Ack.req PAN_compr 0b01100001	0xB9	0x0D9C	0xFFFF	0x0000	Type Sec Ver Ch.dea RESV 0 1 NONE	0x40FFFF02	17 1D C7 28 B9 00 00 00 8B 9E 17 01 00 4B 12 00 00 E0 21 41 BB D9 BC 64 25 D5 CC A2 65 07	212	OK
RX	+2076228	46	Type Sec Pnd Ack.req PAN_compr 0b01100001	0xB9	0x0D9C	0xFFFF	0x0000	Type Sec Ver Ch.dea RESV 0 1 NONE	0x40FFFF02	17 1D C7 28 B9 00 00 00 8B 9E 17 01 00 4B 12 00 00 E0 21 41 BB D9 BC 64 25 D5 CC A2 65 07	212	OK

Packet 7 details (Raw data): 11 88 88 9C 0D FF FF 00 00 08 02 FF FF 40 17 1D C7 28 B8 00 00 00 8B 9E 17 01 00 4B 12 00 00 06 EC B8 4D 47 27 5F A9 3D 42 13 D7 B0

Copy & Paste To the Studio RF software for injection

Figure 7-10: Selecting packets from the packet sniffer

Figure 7-10 depicts the packet details. This numerical string represents the whole of the packet including length, Frame Control, Dst and Src address, NWK Frame counter, NWK

payload and FCS. By capturing this string, it is assumed that the whole packet has been captured.

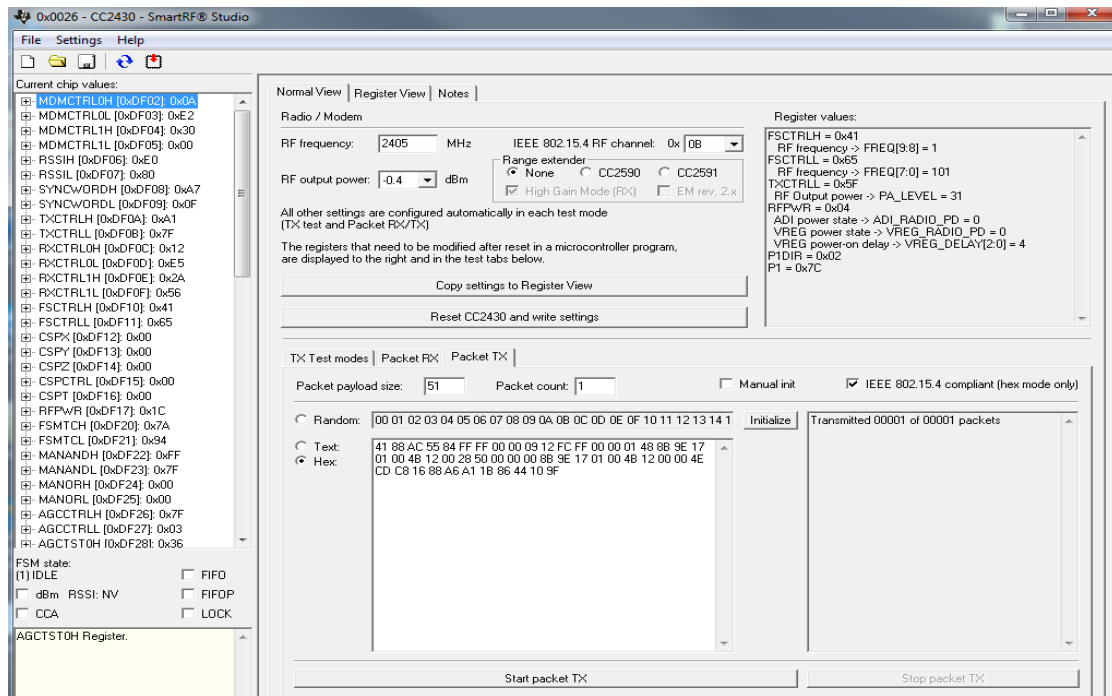


Figure 7-11: Packet injection by the Smart RF Studio packet

Figure 7-11 shows the packet injection by the Smart RF Studio packet. As indicated in the last diagram, the whole of the packet size can be captured through the packet sniffer and numerical string. By copying and pasting this string to the packet TX tab in this software, the relay attack is executed manually.

Using these steps, the out-dated data (repeated data) can be sent to the coordinator.

In Figure 7-10, a few frames include flags Source Address 0x0000 and Dest Address 0xFFFF. By dissecting these frames and injecting them into the network, we are able to force execute replay attacks and send out-dated data to the Coordinator. These kinds of frames, which include 0x0000 and 0xFFFF, are not detected in the Coordinator as a repeated frame.

Configure the network according to Scenario 1:

This scenario does not generate any broadcast attack on the coordinator, so we are not able to execute the replay attack.

Configure the network according to Scenario 2:

As three broadcast packets are generated for each transmission, by capturing the broadcast packet, we are able to execute the replay attack.

Configure the network according to Scenario 3:

As one broadcast packet is generated for each transmission by capturing the broadcast packet, we are able to execute the replay attack.

#### **b) Automatic Replay Attack**

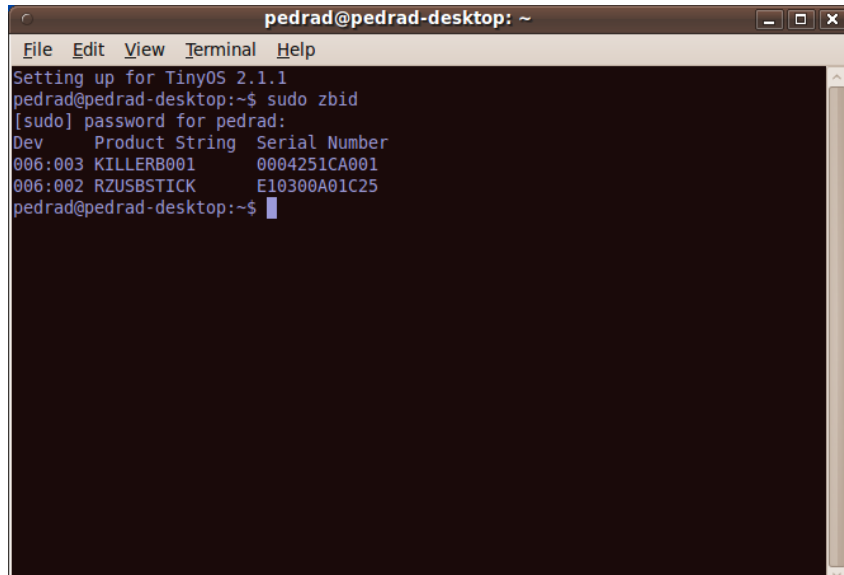
In this attack, the replay attack on the coordinator is automatically executed. The network was developed, and the application and one of the scenarios was uploaded to the devices. Once the KillerBee network had been set up and an attempt was made to execute a replay attack, it was found that when the security schema is activated in the ZigBee network, the KillerBee's replay tool does not work and the replay attack is not executed. This tool works only when the security schema is not activated. However, Joshua Wright, who developed this framework, claimed that it is possible to launch a replay attack using the KillerBee.

Therefore, there is a need to find another way to apply these tools in order to execute replay attack and exploit the network. Based on what was found in the manual replay attack, the ZigBee is susceptible to a replay attack if the coordinator generates broadcast packets. Thus, an attempt was made to force the coordinator to generate broadcast packets, select the broadcast packets and inject them into the network.

Steps below show the attack procedure:

1. Implement Scenarios 2 and 3, which generate broadcast packets on the coordinator.
2. Manually send packets from the end device to the coordinator by playing the joystick.
3. Equip the Laptop with two RZ RAVEN USB devices, one as the sniffer and the other as the injector.
4. Run the KilleBee framework.
5. Deploy the Zbid tool from the KillerBee.

This tool helps to determine which RZ RAVEN USB is recognised as the sniffer and which one as the injector. This recognition is done through the serial number which is mapped to the name of devices.



```
pedrad@pedrad-desktop: ~  
File Edit View Terminal Help  
Setting up for TinyOS 2.1.1  
pedrad@pedrad-desktop:~$ sudo zbid  
[sudo] password for pedrad:  
Dev      Product String  Serial Number  
006:003  KILLERB001     0004251CA001  
006:002  RZUSBSTICK     E10300A01C25  
pedrad@pedrad-desktop:~$
```

Figure 7-12: KillerBee tool for recognizing devices.

6. Execute the Zbdump tool from the Killerbee framework.

This tool Zbdump along with RZ RAVEN USB sniffer and Wireshark packet analyser help to capture packets.



```
pedrad@pedrad-desktop: ~  
File Edit View Terminal Help  
pedrad@pedrad-desktop:~$ sudo zbdump -f 11 -w test01  
zbdump: listening on '006:003', link-type DLT_IEEE802_15_4, capture size 127 bytes  
^C116 packets captured  
pedrad@pedrad-desktop:~$
```

Figure 7-13: KillerBee tool for capturing packets

7. Filter the broadcast packets from the packet sniffer and import them to a separate Wireshark file.

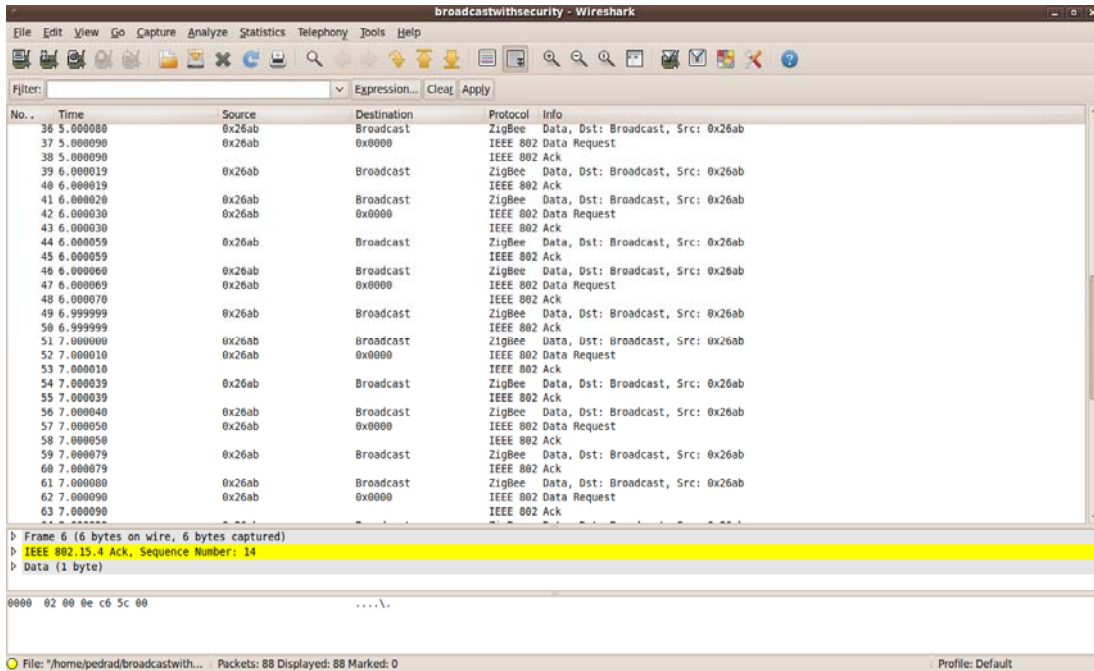


Figure 7-14: Wireshark packet captured with security schema

8. Execute the Zbreplay tool from the KillerBee and inject the new Wireshark file, which was created in the last step.

This new Wireshark file includes broadcast packets. By injecting this file, all broadcast packets are injected into the network and the coordinator cannot recognise them as repeated or out-dated packets. The Wireshark packet captured with security schema is shown in Figure 7-14.

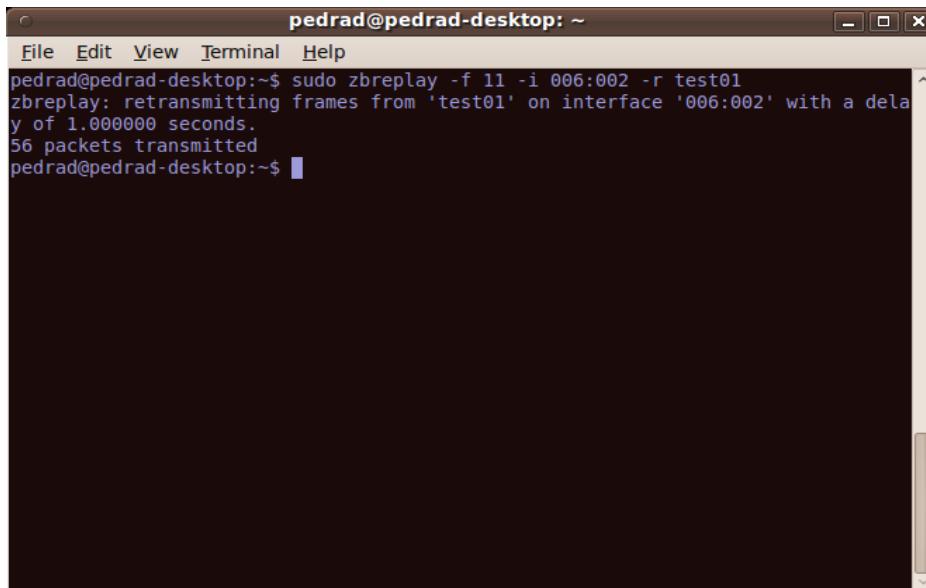


Figure 7-15: KillerBee tool for replaying packets



As was explained earlier, one of the RZ RAVEN USB devices was configured as the injector. This is done by programming the RZUSB with injector firmware. By programming this device, two RZUSB devices, one as the sniffer and the other one as the injector, are provided. Scenarios 2 and 3 are configured, which forces the coordinator to generate broadcast packets, on the end devices and Coordinator. The KillerBee framework is run on the computer (laptop in Figure 7-3), and KillerBee tools are deployed while data is being sent manually from the end device to the coordinator. By running the KillerBee sniffing tool, the packets can be sniffed and captured using the RZUSB Sniffer and recorded with Wireshark.

Then the packets on the captured Wireshark file are examined. If there are broadcast packets in the captured packets, they are selected and imported to a separate Wireshark file and the new file is injected into the network and coordinator. This injection shows that all the broadcast packets are accepted by the Coordinator for a single injection.

#### 7.4.6 Solutions for Replay Attack

As can be seen, if the destination address on the coordinator, which usually has some form of physical security, routers and end-devices, are configured with the specific destination address through unicast addressing, the coordinator will not generate any broadcast packet. This is depicted in Figure 7-16:

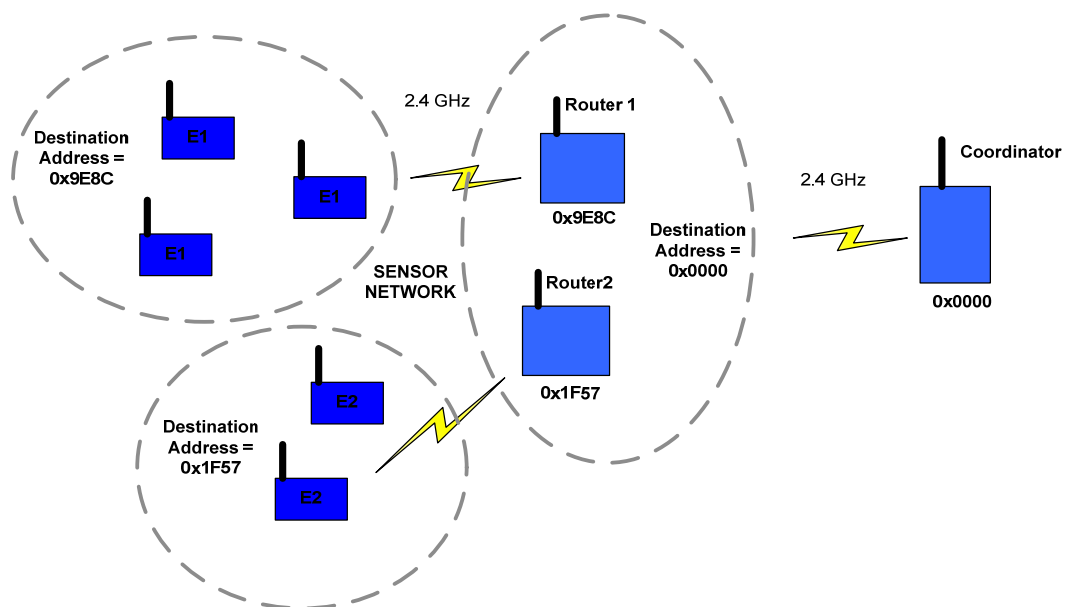


Figure 7-16: Network Addressing.

By addressing the destination address in the network for every single device, this issue will be resolved. In Figure 7-16, there are one coordinator and two routers and five end devices.

To prevent replay attack, the destination address of end devices should be set to the closest router's address and router's destination address should be set to the Coordinator's address. As can be seen, three end devices in network 1 communicate to router 1 because they are close to router one and two end devices in network 2 communicate to router 2. Both routers communicate to the coordinator. In this design, if the network communication is captured, the captured file shows there is no broadcast packet, which allows the attacker to execute a replay attack.

So in this case, an attack scenario needs to be created which includes social engineering, to force the Coordinator to generate broadcast packets in order to execute the replay attack through them.

**Social Engineering:** This is a non-technical intrusion that is based on human factors and often involves deceiving people into breaking normal security procedure. In fact, it is the use of deception and manipulation to obtain confidential information. Social engineering is, generally, the manipulation by hackers of the natural human tendency to trust, in order to obtain unauthorized access to a system and thence the information of the system [179].

By launching a DoS attack, if the Coordinator is configured to store the keys, it might be possible to deceive the network administrator who is responsible for maintaining the network, to restart the Coordinator in order to grab the network key on restart.

The flowchart below shows how it is possible to execute the replay attack in the network, where the network addressed properly to prevent replay attack like Figure 7-16 above.

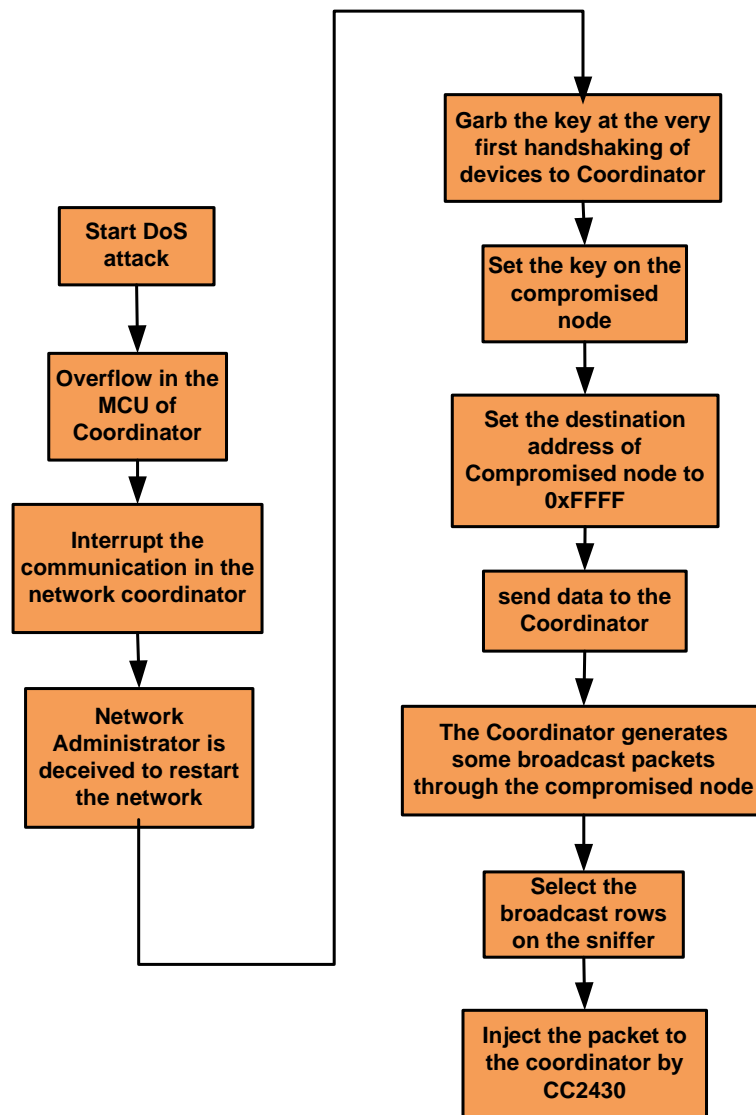


Figure 7-17: Attack Scenario

In this scenario, the DoS attack is executed and an overflow occurs in the microcontroller of the coordinator in order to halt communication. This means that the coordinator cannot receive any packets from the network; hence, the network administrator notices the issue in the coordinator and the coordinator process is halted, but this may deceive the network administrator into restarting the coordinator. By restarting the coordinator, because the key was distributed clearly at the very first handshaking with nodes in the network, the attacker is able to sniff the key.

By grabbing the key, the attacker is authenticated by a compromised node to access the network, giving the intruder the ability to communicate with the network nodes and coordinator. In this case, even if the node destination address has been designed properly to

prevent replay attack, such as in Figure 7-18, the attacker is able to implement Scenario 3, and by setting the destination address of compromised node to 0xFFFF, to force the coordinator to generate broadcast packets.

```
"SampleApp_Data_DstAddr.addr.shortAddr=0xFFFF;"
```

If the packets are captured by a sniffer, while the compromised node is sending messages to the coordinator, the attacker notices that there is one broadcast packet for every single transmission. These broadcast packets allow the attacker to inject them into the coordinator and replay attack is executed. Figure 7-18 shows the network architecture to execute the replay and DoS attacks.

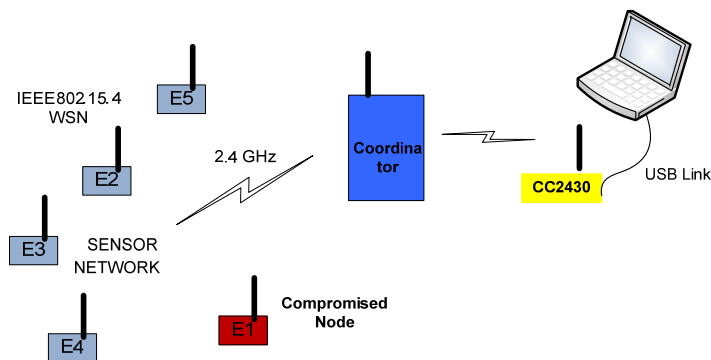


Figure 7-18: Replay Attack architecture

In the Z-Stack, MT workspace in the MT\_ZDO.c application, there is a code which is supposed to fix this problem, but it does not.

The Code:

```
if ( destAddr.addrMode == AddrBroadcast )
{
    destAddr.addrMode = Addr16Bit;
    destAddr.addr.shortAddr = _NIB.nwkDevAddress;
    retValue = (uint8) ZDP_MgmtNwkUpdateReq( &destAddr, channelMask, scanDuration,
        scanCount, _NIB.nwkUpdateId+1, nwkManagerAddr );
}
```

This code is supposed to change all the broadcast addresses which are stated in the destination address on devices within the network, to a unicast address. In Scenario 3, the destination address was changed to broadcast, thereby forcing the Coordinator to generate a broadcast address and through this configuration, a replay attack could be executed.

The code above shows that `destAddr.addrMode = Addr16Bit`; this means that all

dest.AddrMode must be changed to Addr16Bit, which is a unicast address which protects the network against replay attack.

By using the SmatRF Studio Flash Programmer software, which is applied for injecting packets in this experiment, it is observed that frames are injected into the network and the Coordinator cannot recognise these frames as being repeated and out-dated. This proves that there is a bug in the implementation of the Z-Stack from Texas Instruments. If this part of the code works properly, all broadcast addresses, which allows us to inject them back to the coordinator and execute replay attack within a ZigBee network, should be changed to unicast, which protects the ZigBee network from replay attack.

Due to this bug in the Z-Stack, the adversary is able to force the coordinator to generate broadcast packets in order to execute a replay attack. This bug is addressed in the code above.

#### **7.4.7 Physical attack**

Physical attacks are feasible by dumping device firmware using existing available hardware[148]. ZigBee chips, typified by the CC2530 evaluation board from Texas Instruments, are vulnerable to local key extraction. Currently, there is no protection against an external access which tries to steal keys using unprotected data memory and exploiting flash memory.

Specifically, it is possible to attack micro-controllers and ZigBee radios by exploiting their Pseudo-Random Number Generator (PRNG). This attack is called a side-channel timing attack, which is an attack against the MSP430 micro-controller by exploiting and programming the Joint Test Action Group (JTAG), a 4-wire Test Access Port (TAP) controller or a serial bootstrap loader (BSL) which resides in masked ROM [180].

The MSP430 is a low-power micro-controller popular in ZigBee/802.15.4 and is found in many wireless sensor development kits. The PRNG uses a 16-bit Linear Feedback Shift Register (LFSR), as shown in Figure 7-19, which can be advanced by writing to the RaNDom High (RNDH) register or overwritten by writing to the RaNDom Low (RNDL) register, to generate pseudo-random numbers. RNDH and RNDL are the high and low bytes in a 16-bit Cyclic Redundancy Check (CRC) of the LFSR, used to calculate the CRC value of a sequence of bytes and read the 16-bit shift register in the LFSR. In other words, the 802.15.4 low radio frequency randomizes the seed by mixing 32 values into the Random Number Generation (RNG), for  $i$  0 to 8. Once the RNG has been seeded, it has an initially random 16-bit state [146]. This random number can be read by the CPU and used to generate random cryptographic keys. In fact, the state of this random number is initialized in the Hardware

Abstraction Library (HAL) by feeding 32 bytes from the Analog Digital Converter (ADC), a device that converts continuous signals to discrete digital ones, into the RNDH register.

The random values generated by the ADC are read from the Radio Frequency (RF) registers ADCTSTH and ADCTSTL, which correspond to ADC test high and low, respectively. Unfortunately, bytes from the ADCTSTH register are physically random, but poorly distributed [146]. This problem in ADCTSH has been inherited from one of the flaws in the PRNG.

There are two flaws in the PRNG: the pool is extremely small (16 bits) and it is not seeded with very much entropy. The first flaw is that the PRNG is not cryptographically secure because the pool is extremely small (16 bits). Nevertheless, even if the pool were much larger, it is still vulnerable because the LFSR is not a cryptographically-secure PRNG and an attacker can recreate the LFSR taps and then generate any future sequence from it. The second problem is that it is seeded from a random source that has very little entropy. This could be exploited even if it were used in a cryptographically-secure PRNG. These problems are enough to make the system slightly insecure against a simple brute-force attack [181]. In order to prove the existence both flaws in the PRNG, a dumping of a random byte sequence from the ZigBee evaluation was developed by Travis Goodspeed through employing GoodFET to debug the chip. GoodFET is an open-source Joint Test Action Group (JTAG) interface adapter[180]. It is based upon the TI MSP430 micro-controller and is provided with a USB bus adapter. The firmware was compiled with the Small Device C Compiler and flashed by the GoodFET. A quick Python script is then used by the GoodFET library to debug the target micro-controller and dump random values through the JTAG interface [181].

As a result, it was found that by exploiting the PRNG through its flaws and access to LFSR, which does not have high entropy, obtaining the key stored in the MSP430 microcontroller of ZigBee devices is achievable. From this security test, it may be concluded that it is feasible, even though not necessarily easy, to crack the cryptographic key stored in individual ZigBee devices. Once an attacker has gained hold of the cryptographic keys, s/he can easily perform eavesdropping and spoofing attacks [181].



Figure 7-19: The Random Number Generator structure

#### **7.4.8 Physical Attack Solution**

Physical security is extremely important to securely maintain a network. For implementing ZigBee technology in the network, the physical security should be implemented and paid attention to properly. In a network, apart from proper design and configuration, a physical security policy plays a very important role in maintaining a secure network. For implementing ZigBee within a network, controlling unauthorised access to the ZigBee coordinator is of utmost importance. As was shown, via an unauthorised access to the coordinator, an intruder is able to take over the coordinator. By dumping device firmware and using existing available hardware, an attacker is able to exploit the flaws of PRNG and gain access to LFSR, which does not have high entropy, and the key stored in the microcontroller of ZigBee devices can be obtained [159].

The defence against a physical attack on the ZigBee MCU can be established by programmed JTAG or a serial bootstrap loader (BSL) which resides in a masked ROM along with appropriate physical security. By design, JTAG may be disabled by blowing a fuse. The BSL may be disabled by setting a value in the flash memory. When enabled, the BSL is protected by a 32-byte password. If these access controls are circumvented, a device's firmware may be extracted or replaced [159].

### **7.5 ZigBee Security Quality of Services**

In this section, the way that the security schema affects Quality of Services in ZigBee technology, is explained. Information security is usually a trade-off between using something and protecting it from undesired usage. Thus, the security in ZigBee can be defined as the process of achieving a balance between secure communication and high quality communication [183]. This section delineates a preliminary performance study of the ZigBee security IEEE 802.15.4 wireless standard via actual devices in the CC2530ZDK kit.

#### **7.5.1 Design of the Network**

A simple point-to-point topology between one end-device and one coordinator was designed. This study has been conducted thirty-three times without security and thirty-three times with security. To measure the impact of implementation of the security schema on ZigBee, the test-bed below was designed.

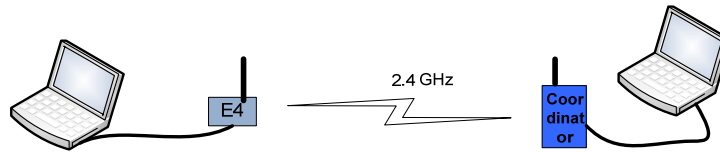


Figure 7-20: The point-to-point communication

Figure 7-20 depicts the simple point-to-point communication between a coordinator and an end device. The reason for setting up a point-to-point communication is to ensure that the routing protocol algorithm and other factors do not interfere with this experiment and that only the quality of service, whether with security schema or without security schema, is controlled.

### 7.5.2 Configuration of the network

The coordinator and device were configured to send 600 packets for each round. In the SampleApp in App workspace, the code below should be added to SampleApp.c application local variables.

```
* LOCAL VARIABLES
*/
uint8 SampleApp_TaskID; // Task ID for internal task/event processing
// This variable will be received when
// SampleApp_Init() is called.

devStates_t SampleApp_NwkState;

uint8 SampleApp_TransID; // This is the unique message ID (counter)

afAddrType_t SampleApp_Periodic_DstAddr;
afAddrType_t SampleApp_Flash_DstAddr;

aps_Group_t SampleApp_Group;

uint8 SampleAppPeriodicCounter = 0;
uint8 SampleAppFlashCounter = 0;

int messages=600;
int sendMessages=1;
```

Also, for controlling sent message timeout from the end device to the coordinator, in the same Workspace in SampleApp.h, the Send Message Timeout should be changed to 300 in the Constants section.

```
#define SAMLEAP_SEND_PERIODIC_MSG_TIMEOUT 300
```



This timeout is set for every packet which travels to the destination and returns. So for 600 packets, the timeout should be set to 300.

Table 7-1: The average lost packet ratio in ZigBee with and without security schema

Lost packages ZigBee	Total frames	Received frames	Error frames	Lost frames	% lost frames	% error (total)	% error (received)	% received (OK&ERR)
With Security	600	435.93	39.54	164.06	27.34%	6.59%	10.64%	72.65%
Without Security	600	463.54	24.03	136.45	22.74%	4.00%	5.78%	77.25%

According to Table 7-1, the removal of security schema causes the lost packet ratio to be reduced. As can be seen, on average, about 463 out of 600 packets are received where there is no security schema. On the other hand, once the security is ON, this amount is decreased to 435 out of 600 packets. The table also indicates that once the security is removed the number of errors is reduced from 39 packets to 24 packets. The last two columns illustrate that 77% of packets successfully reach the destination, whereas this percentage is slightly decreased to 72%, by adding the security schema in ZigBee. The results demonstrate that even though the quality of services is affected by adding the security schema in ZigBee, this security algorithm does not impact significantly on QoS in ZigBee technology.

## 7.6 Summary of the risk evaluation and counter measure

In Chapter 6, it was found that by setting up the broadcast address (0xFFFF) to the destination of end devices (Scenarios 2, 3), the coordinator can be forced to generate broadcast address, which allows them to be injected back to the coordinator, thereby executing the replay attack. Based on this finding, the test-bed was set up to execute those remaining attacks which were mentioned in Chapter 3 - Eavesdropping, Replay Attack, Physical Tampering and DoS attack including jamming and flooding attacks. It was found that if the coordinator is configured to distribute the key within the network, at the very first handshaking, the key can be grabbed using two different methods. In addition, it was revealed that there is a bug in the implementation of the Z-Stack from Texas Instruments which allows us to play with destination address of end devices to execute the replay attack. In this chapter, the possible solutions to protect the network against physical tampering have been explained. Also, the possible solution to control DoS attack by jamming and flooding was discussed. At the end of this chapter, the ZigBee security schema in terms of Quality of Services was examined.

## 7.7 Conclusion

In this chapter, it was shown how we executed remaining attacks, which were selected from Chapter 3. Three different scenarios were presented to execute these attacks, producing different results. Solutions, which were recommended by the researcher for controlling and mitigating the risk of relay and DoS attacks, were arrived at through these scenarios. The architecture of MCU in ZigBee was explained, and the method of obtaining the key by physical attack was described. Also, the KillerBee network was set up and all available tools, which were designed for executing several attacks, were applied. It was proven that the KillerBee application is not able to execute replay attack when the ZigBee security schema is activated and the replay attack by KillerBee was executed by the researcher by making changes in the sniffed files. At the end, it was proven that the ZigBee security schema does not impact significantly on the quality of services. To substantiate this claim, we established a point-to point communication in both cases (with security and without security) and examined the QoS. The impact of implementing the security schema on ZigBee was examined. The effect of implementing AES-128 has been measured in terms of lost packet and error frames. This laboratory experiment demonstrates that security schema does seem to affect quality of service and proves that by implementing the security schema in ZigBee, the number of lost packets raises the degree of lost packet ratios.

## **8 Evaluation of the Proposed Architecture Framework in Statoil Remote Operation Environment**

### **8.1 Introduction**

The chapter presents a case study which examines the cyber security issues surrounding WSNs in the oil and gas industry and specific Statoil installations. Statoil is a fully integrated petroleum company with production operations in thirteen countries and retail operations in eight [184]. After careful consideration and planning, some experiments are conducted to validate the project findings.

### **8.2 The case study**

WSNs will be a significant part of the picture when the oil and gas industry moves into the wireless domain. Such technology has the potential to be beneficial in many regards. Eliminating the need for cables contributes to reduced installation and operating costs, it enables installations in remote areas, and it allows for cost-efficient, temporary and mobile systems. WSNs are now potentially suitable for deployment in oil and gas production environments.

The monitoring of oil and gas plants using sensors allows for greater insight into safety and operational performance. However, as a result of strict installation regulations of powered sensors near oil and gas fittings, the introduction of new sensors to optimise plant operations has been expensive, complex and time consuming. Recent advances in wireless technology have enabled low-cost Wireless Sensor Networks (WSNs) capable of robust and reliable communication as an alternative solution to their wired counterparts. However, the critical WSN security issues have not been investigated properly in industry or academia.

This case study defines the cyber security issues surrounding WSNs in the oil and gas industry and specific Statoil installations. It focuses on the assessment stages of WSN security in the oil and gas industry. The recommendations that are produced aim to guide Statoil in the process, policy creation, enforcement and implementation of security measures as well as monitoring stages surrounding WSNs installations. This case study also aims to assist Statoil with the evaluations of the risks associated with such technology.

### **8.3 Project Scope**

The scope of the project is delineated by the points given below. These will contribute to achieving the overall objective of the project.

- Investigations into the security vulnerabilities of the existing Statoil technical with corporate networks are outside of the scope of this study. It is assumed that the existing wired network is secure.
- It is also assumed that the physical access to the wireless sensors and their configurations/setup is restricted to authorised persons who will not intentionally or otherwise introduce specific configurations which obviously introduce vulnerabilities clearly outside of regular secure operation and/or maintenance processes.
- The physical security of the devices is also not considered and it cannot be assumed that the device readings cannot be physically manipulated.
- It also assumed that the devices perform as specified by their standard and manufacturer. Any faults or operation outside of standard and manufacturer specification is not considered.

#### 8.4 Statoil WSN Lifecycle

This section details the WSN lifecycle in the oil and gas industry and documents the specific Statoil existing and planned WSN installations. The oil and gas development project lifecycle can be broken down into five basic phases. The WSN considerations apply to all phases of the lifecycle.

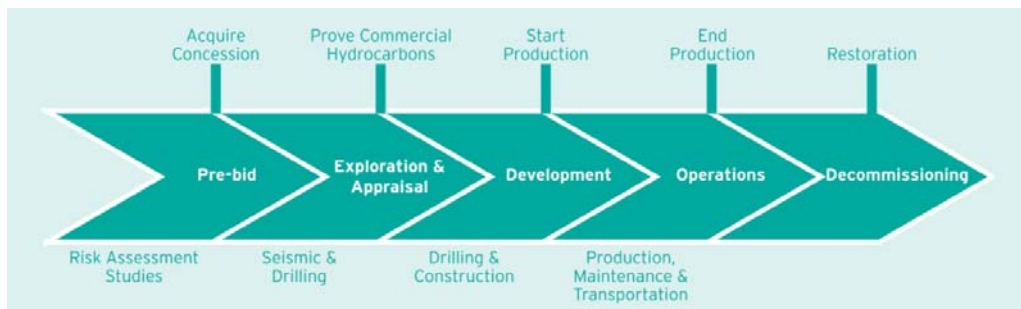


Figure 8-1: The life cycle of Oil and Gas [185].

- **Pre-Bid** - There would be needed a series of preliminary high-level identifications and assessments of potential business, environmental and social risks that acquiring the interest may present to future company operations and reputation.
- **Exploration and Appraisal** - This stage is to explore the concession area, to gain an understanding of the subsurface. For example, seismic surveying and, if justified, exploratory drilling are conducted with the objective of proving or disproving the presence of commercially viable quantities of hydrocarbons.

- **Development** - After that, if the exploration and appraisal phase reveals the presence of commercially viable quantities of hydrocarbons, the company can make the decision to develop the field, which includes drilling of production wells and construction of facilities such as pipelines and terminals to process hydrocarbons.

- **Operations** - After development of the field, the operations phase begins, which encompasses the day-to-day production of oil and/or gas and maintenance of facilities and transportation of the hydrocarbons via pipelines.

- **Decommissioning** - Once the commercial life of the field has concluded, the decommissioning process is initiated which may involve the removal of facilities and the restoration of project sites or other actions appropriate to the site's next intended use [186].

By integrating their operations, oil and gas companies like Statoil will be able to accelerate and increase production, reduce operating cost of maintenance, improve safety and extend the life of their oilfields. As its name suggests, TAIL IO (Integrated Operation), which is aimed at improving integrated operations of offshore assets at the tail end of their useful life, is a major challenge facing all oil and gas companies. It is the stage where the production rate is declining, the facilities are aging, and operation costs are high [114].

The implementation of TAIL IO requires both short- and long-term strategies. In the short term, the focus is on making improvements in daily operations and maintenance. These range from establishing support centres onshore, improving existing work processes, training staff in TAIL IO and cross-border cooperation, and investing in ICT to make real-time collaboration possible [187].

TAIL IO consists of a number of sub-projects on which Statoil and the ABB consortium collaborate. They range across a broad range of technologies which include:

- Condition-based maintenance and performance monitoring
- Wireless communication and sensor systems
- Corporate decision support model for strategic planning of turnarounds and shutdowns
- Collaborative visualization tools for preparation, training, executing and supporting maintenance operations

- Mobile ICT and - from wireless communications and sensor systems to robotics and mobile ICT

- Robotics

The ultimate objective of this project is to protect critical assets, improve productivity and safety, and prevent shutdowns [188].

Wireless devices are making an entry into the oil and gas industrial environment because of their numerous benefits including flexibility, redundancy, visibility, cabling, cost reduction and extending measurements to critical information, amongst others. This technology plays a vital role in increasing the efficiency of production of oil and gas because production of oil and gas needs networked sensors and actuators to monitor the production process, to either prevent or detect oil and gas leakage or to enhance the production flow and yield of the wells [189].

There are three WSN standards - ZigBee, WirelessHART and ISA 100 - which all work on IEEE 802.15.4. Using open WirelessHART products, Emerson Process Management's Smart Wireless network is automating flow monitoring to increase production on the Statoil platforms of Gullfaks and Grane in the northern part of the Norwegian North Sea. Needing a monitoring approach able to be installed without interrupting flow, operators are using wireless devices to transmit real-time temperature data that indirectly monitors flow, allowing quick reaction to any loss of well pressure and maximizing throughput from the well. The wireless devices are used to transmit data from clamp-on temperature sensors mounted on the surface of the flow pipes. The wellhead was already a very crowded area and for safety reasons it had to be kept as clear as possible. The introduction of additional equipment such as new cabling, cable trays and junction boxes was not possible [190].

## 8.5 Information Security in Integrated Operations

Wireless technology brings a great deal of advantages to the oil and gas industries, but due to the numerous challenges and concerns among end users in terms of reliability, security and safety, the rate of adoption has been slow. Information security must be considered for the successful integration of operations in the oil and gas industry [190].

Integrated operations leads to a change in technology where production and support systems are connected, and people on- and offshore cooperate in controlling processes offshore. Production and support systems include all kinds of electronic hardware and software. The trend is to connect the different kinds of systems, which introduces a set of threats and vulnerabilities that has previously not been relevant to the industry [191].

## 8.6 Security Requirements

The goal of security services in WSNs is to protect the information and resources from attacks and misbehaviour. The security requirements in WSNs include [46]:

- **Availability** - Ensures that the desired network services are available.

- **Authorization** - Only authorized sensors can be involved in providing information to network services.
- **Authentication** - Communication from one node to another node is genuine and a malicious node cannot masquerade as a trusted network node and compromise the network.
- **Confidentiality** - A given message cannot be understood by anyone other than the desired recipients.
- **Integrity** - A message sent from one node to another is not changed and modified by malicious intermediate nodes.
- **Non-repudiation** - Denotes that a node cannot deny sending a message that has been sent previously.
- **Freshness** - Implies that the data is recent and ensures that no adversary can replay old messages. Moreover, as new sensors are deployed and old sensors fail, it is suggested that forward and backward secrecy should also be considered.
- **Forward Secrecy** - A sensor should not be able to read any future messages after it leaves the network.
- **Backward Secrecy** - A joining sensor should not be able to read any previously transmitted message.
- **Self-Organisation** - A WSN is typically an ad hoc network, comprised of wireless sensor nodes which operate independently and are self-organising and self-healing according to different situations.
- **Time Synchronisation** - Some applications in WSN rely on time synchronization. This is increasingly used in WSN communication as sensor nodes may turn off their radio transceiver/receiver for some period of time in order to conserve power.
- **Secure Localisation** - In some cases, the utility of a WSN relies on its ability to accurately locate each sensor node in the network. A sensor node that is placed in a particular location to monitor its environment will need to relay its readings along with the location data for it to be truly useful.

It should be mentioned that cryptography is central to security service in WSNs and due to the constraints in WSNs, many existing secure algorithms are not practical for use [46].

In order to investigate the security vulnerabilities of WSNs in the oil and gas industry, we must consider the following in terms of both theory and practice:

- The network connections, devices and backend systems that can be accessed by the WSN or vice versa.
- The various scenarios and states that the WSN devices may achieve during their lifetime or lifecycle of operation.
- Wireless devices are far more susceptible to environmental changes and interference compared to their wired counterparts. Their radio performance and indeed the vast number of possible vulnerabilities are dependent on the available signal strength (or availability), environmental conditions and noise. The various changes in environmental conditions and potential intruder proximity must be considered.
- Wireless devices operate using radio transmission. Any party within range of that transmission may potentially exploit any security vulnerabilities that may exist.

The following network connections are carefully considered:

- The gateway connection to the technical network.
- The gateway connection to the control room.
- The sensor connections to the gateway.
- Interaction with the gateway and sensors through the terminal server.

The following WSN events are carefully considered:

- The installation and initiation of a gateway.
- The installation and initiation of a sensor.
- The removal of a sensor.
- The removal of a gateway.
- The regular maintenance of a gateway.
- The regular maintenance of a sensor (like battery update).
- The power outage / software crash / reboot of a gateway.
- The power outage / software crash / reboot of a sensor.
- Regular gateway operation.
- Regular sensor operation.

The following operational events are carefully considered:

All events where any foreign (and indeed familiar) vehicles and personnel are within radio range of the WSN.



## 8.7 Generic Attacks on Oil and Gas Wireless Network Installations

Wireless networks are susceptible to various security issues; hence, security should be assured in such a sensitive industry. Security processes, procedures, standards, risks, third-party agreements, change management, references, monitoring and maintenance, update, culture, including attitudes, knowledge and values, must be developed among all employees who are involved in this technology. The organisation has a significant job to do when it comes to increasing awareness related to information security. The challenges are on many levels; technical, human and organisational aspects must be taken into consideration [191].

## 8.8 Taxonomy of Applicable Attacks on Oil and Gas WSN Installations

In this section, all the existing attacks in WSN are categorized into two overarching attacks, Active and Passive, along with the security architecture of sensor networks.

### 8.8.1 Active and Passive Attacks

A passive attack occurs when an attacker eavesdrops but does not modify the data stream. An active attack occurs when an attacker modifies the data stream by transmitting messages, replaying old messages, modifying messages in transit, or deleting selected data [192].

Passive attacks should be examined as the first step because it is through these that Active attacks are launched. Eavesdropping and traffic analysis are examples of passive attack. Both of these attacks can be executed through a packet sniffer, which is computer software and/or hardware that can intercept and log network traffic [45].

Thus, it is extremely important to recognise when these types of attack are occurring.

Specific WSN attacks in the oil and gas industry include any action that intentionally or unintentionally aims to cause any damage to the organisational network. Based on the security architecture which was mentioned in Chapter 2, attacks can be divided according to their origin or their nature.

#### a) Applicable Passive Attacks

Both eavesdropping and traffic analysis attacks can be executed using a packet sniffer, which is computer software and/or hardware that can intercept and log network traffic [43]. Running a packet sniffer, an attacker may intercept 802.15.4 network traffic and employ passive attacks, whether internal or external.

## b) Applicable Active Attacks

- **Jamming** - A typical jamming attack can disrupt the entire WSN with a few randomly distributed jamming nodes. This type of attack is simple to implement and is very effective against single frequency networks. Wi-Fi devices which provide Internet via IEEE 802.11b/g/n wireless protocol, would increase the risk of jamming in such a network because both these two technologies operate within the 2.4 GHz frequency band.
- **Spoofed, Altered, or Replayed Information** - An unprotected sensor routing is vulnerable to these types of attacks, as every node acts as a router, and can therefore directly affect routing information [46].
- **Hello Flood Attack** - A malicious node can send, record or replay hello messages with high transmission power. It creates an illusion of being a neighbour to many nodes in the network. Laptop attackers can also use a hello flood attack [48].
- **Wormhole Attack** - A wormhole is a low latency link between two portions of the network over which an attacker replays network messages. This link may be either a single node forwarding messages between two adjacent but otherwise non-neighbouring nodes or a pair of nodes in different parts of the network with the ability to communicate with each other [46].
- **Replay** - This is an attack against the message which is repeated or delayed. It could be using duplicated authentication or malicious data. In a WSN, replay attack can be used to create a new session or to bypass authentication [38].
- **De-Synchronization** - This attack tries to disrupt a transport-layer connection by forging packets from either side. An attacker forges messages carrying a wrong sequence number to one or both end points [48].
- **Collision** - An attacker can induce a collision in the WSN to create a costly exponential back-off in some MAC protocols [48].
- **Unfairness** - Intermittent application of these attacks or abusing a cooperative MAC-layer priority scheme can cause this attack [48].
- **Resource Exhaustion** - A simple link-layer protocol may attempt repeated retransmissions due to collision. This will lead to exhaustion of battery resources in sensor nodes as well as delays in transmission [48].
- **Acknowledge Spoofing** - An attacking node can spoof the acknowledgments of overheard packets destined for neighbouring nodes in order to provide false information [46].

- **Misbehaviour** - This is the result of unintentional damage to other nodes [10].
- **Rushing** - This attack is performed against the routing protocol to employ a duplicate suppression technique and control flooding.

### 8.8.2 The security architecture of sensor networks

The security architecture of sensor networks, giving a general view of security issues addressed in sensor networks, is presented. There are three-level security requirements that outline the principles of algorithm design for security mechanisms.

- **Message-based Level** - Similar to that in conventional networks, this level deals with data confidentiality, authentication, integrity and freshness. Symmetric key cryptography and message authentication codes are important to support information flow security. Also data freshness is necessarily to provide content-correlative information to transmit on a sensor network during a specific time.
- **Node-based Level** – On this level, situations such as node compromise or capture are investigated. In case that a node is compromised, loaded secret information might be applied by adversaries.
- **Network-based Level** - On this level, more network-related issues are addressed, as well as security itself. Protecting it is critical. The security issue is becoming more challenging when applied in specific network environments. Firstly, securing a single sensor is completely different from securing the entire network; thus the network-based security should to be estimated. Secondly, network parameters such as routing, node's energy consumption, signal range, network density and so on should be considered correlatively. Moreover, the scalability issue is also important in the redeployment of node addition and revocation [27].

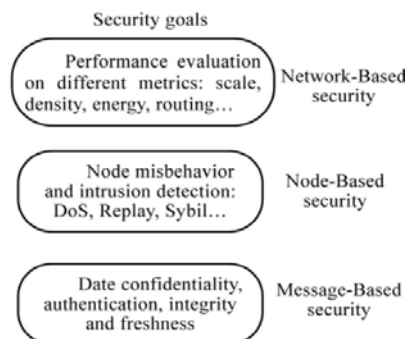


Figure 8-2: WSN Security Concerns [27].

Based on the above categories, the existing exposure attacks in the oil and gas industry are categorised. Figure 8-3 below classifies these attacks.

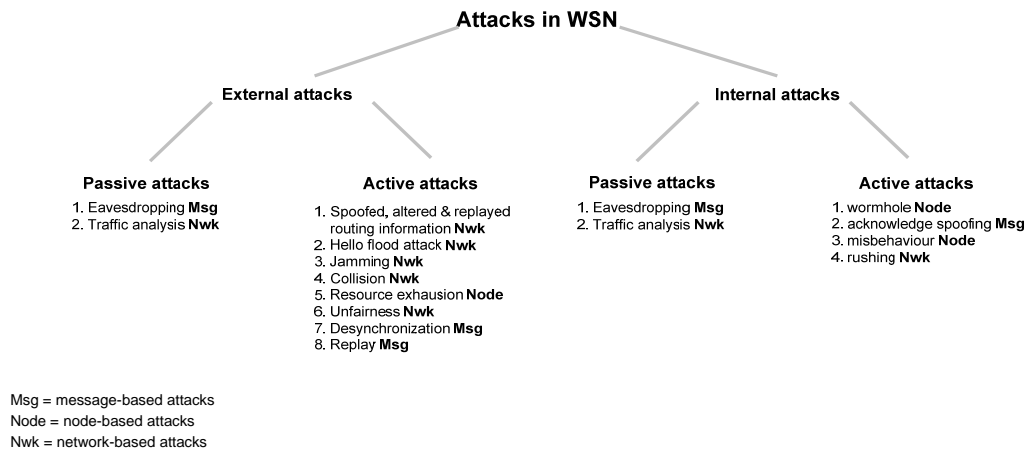


Figure 8-3: Taxonomy of WSN exposure attacks

Figure 8-3 illustrates the taxonomy of WSN exposure attacks. All attacks are divided into two overarching internal and external attacks. Attacks, whether internal or external, are classified into passive and active attacks. Finally, they are categorized into the security architecture of sensor networks that gives a general view on security issues in sensor networks.

Several Statoil applicable WSN security threats were outlined in this section and previous areas of the thesis.

## 8.9 Information Security Management System

There is a common strategy used by Statoil to integrate and enhance their relationships using information technology. Several initiatives have been introduced to help organizations implement and maintain their Information Security Management System (ISMS) which is a systematic approach to ensure the selection and use of adequate security controls to protect information, manage information assets and keep them secure for Statoil [193].

In order to implement successful ISMS, a company requires the commitment of the entire organization with the especial support of management. It is a good approach to base the development of the ISMS on standards established by international and government institutions because that certifies that a company is going to implement best practices. Even though it is a complex process, the benefits have been recognized by several companies around the world that have implemented their ISMS and been certified according to different standards [193].

ISMS can be established by a regulatory compliance like ISO 27001. This ISO basically is a certifiable standard that sets out the requirements for an ISMS and provides “a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System” [194].

ISO 27001 is relevant to all types of businesses and organizations regardless of type, size and nature, since the standard can be aligned with different business characteristics. It is vital that a company first identify the true value of a potential loss of information and then define processes and controls to mitigate the risk [195].

### **8.9.1 ISO 27001**

ISO 27001 has the list of control objectives and controls that need to be implemented, including: security policy, organization of information security, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, information security incident management, business continuity management and compliance. The implementation of ISO 27001 reduces the risk of incurring these costs [195].

The overall image of the company is improved with a certification and can be a differentiator between the company and its competitors.

This section presents the overall information technology WSN configuration within Statoil operations. This section builds upon the semantics and definitions found in OLF document 104 - Information Security Baseline Requirements for Process Control, Safety, and Support ICT Systems [196]. For reducing the risk in Statoil production operations, ISO 27001-based information security requirements for process control, safety and support ICT systems are applied.

In addition, the ISO 27001 family provides guidelines for securing wireless networking to define the risks, design techniques and control issues for securing wireless and radio networks. These guidelines are found in ISO27033-7 [159].

### **8.9.2 Information Security Requirements for Process Control, Safety and Support**

This section explains the OLF Information Security Baseline Requirements (ISBR) for ICT systems in process control, safety and support networks. The controls documented are considered as the best practice for information security, and it is recommended that all of the measures be implemented [196].

The controls are founded on ISO/IEC 27001:2005 (formerly BS 7799-2), which is adapted to the oil and gas sector. It should be mentioned that implementing all the controls in this ISBR will not guarantee that security incidents cannot occur. Each organization has to implement and customize additional controls and security measures to obtain the optimum level of information security. The Information Security Baseline Requirements do not require any prioritizing.

- An Information Security Policy for process control, safety and support ICT systems environments should be documented.
- An Information Security Policy is an overall management document that embraces the foundations for information security in the production environment. The policy describes the intention of management for information security.
- Risk assessments should be implemented for process control, safety and support ICT systems and networks.
- The risk assessments should identify probabilities and consequences of security incidents, taking into account the security actions that mitigate potential risks.
- Process control, safety and support ICT systems should specify the selected system and data owners.
- The function should have the overall system responsibility and ensure that only authorised people, applications and services are authorised in the ICT systems.
- The infrastructure should be able to provide divided networks; also, all communication should be controlled.
- The ICT infrastructure must be able to provide divided networks so that ICT systems with different levels of security, which require a guaranteed network throughput, can be installed in separately divided networks.
- Users of process control, safety and support ICT systems should be trained in the information security requirements.
- The organisation should develop training programs for operating ICT-based process control, safety and support systems. This includes how to implement and maintain the information security in the systems.
- Process control, safety and support ICT systems should be applied only for designated purposes.
- ICT equipment configuration should be customised to its specific requirements.
- All the authorised and tested configuration of the process control, safety and support ICTsystem should be documented and be kept updated.

- Disaster recovery plans should be documented and tested for critical process control, safety and support ICT systems.
- The organisation should be able to restore all critical operational processes within a specified timeframe in the production environment.
- Information security requirements for ICT components should be integrated in the engineering, procurement and commissioning processes.
- The requirements should include a minimum required information security baseline.
- The vendors, suppliers and contractors should document their degree of compliance [196].
- Critical process control, safety and support ICT systems should have defined and documented service and support levels.
- As a result of risk management, process control, safety and support ICT systems should have been identified as critical to the operations and they should have documented solutions for service and support lifecycles [196].
- Change management processes and work permit procedures should be followed for all connections to and changes in the process control, safety and support ICT systems and networks.
- No changes to the operational ICT infrastructure. For example, all hardware and software should be executed unless a work permit exists and any changes are performed in accordance with the change management process [196].
- An updated network topology diagram including all system components and interfaces to other systems should be available.
- The level of details should identify all critical components in the operational and supporting ICT infrastructure [196].
- ICT systems should be kept updated when connected to process control, safety and support networks.
- Security patches and other relevant security updates should all the time be implemented when available and approved, as long as they do not introduce higher business risks. If a system cannot be updated for any reason, it should be logically isolated or security measures should be installed to protect the vulnerable system. All changes must be done according to the requirements for change management and work permit procedures [196].
- Process control, safety and support ICT systems should be adequate against malicious software, and should be updated.

- The protection software should be configured to automatically update itself, when available and approved. However, systems that are part of critical real-time operations may be excluded from this requirement if there is a protected system by other security measures [196].
- All access requests should be denied unless explicitly granted.
- The ICT systems should be configured to give access to user for required resources and functions only. In the overall system access principle, everything should be forbidden, unless explicitly permitted. System and network access should always be granted from the inside, only by users having higher privileges/rights and as the result of a formal authorization process [196].
- Required operational and maintenance procedures should be documented and kept updated.
- Operational routines and maintenance schedules, which include the back-up and restoring procedures should be documented and specified for all system activities [196].
- All procedures for reporting of security events and incidents should be clearly specified, documented and implemented in the organisation.
- The organisation is responsible for handling and managing information security events[196].

### **8.10 Statoil WSN Networks**

This section describes several network configurations involving wireless sensor networks in Statoil. Four slightly different scenarios are presented, two of them utilizing the gateway's serial MODBUS port for transferring sensor data. The other two set-ups use the gateway's secondary Ethernet port for transferring sensor data from the gateway into the plant's Process Control and Data Acquisition (PCDA) system.

### **8.11 ICT Equipment in Technical Networks**

At the time of writing, Statoil have wireless sensor networks only from one single vendor in operation. All wireless sensor networks are delivered from Emerson Process Management, and are a part of the WirelessHART enabled SmartWireless product series [196].

- Wireless gateways: Emerson hg1420
- Wireless sensor nodes:
  - Rosemount 648 Wireless Temperature Transmitter
  - Rosemount 3051S Pressure, Flow, and Level Transmitter



Different set-ups and networks sizes are found at the different facilities. Statoil's overall strategy for establishing facilities for ICT equipment is grounded in the internal Technical Requirement 1658 (TR 1658) document [196].

### 8.11.1 Smart Wireless Gateway

There are some characteristics in Smart Wireless Gateway:

- **Self-Organizing Networks** - Self-organizing networks are perfect in any environment. Multiple communication paths and automatic path configuration show ninety-nine percent reliability, which allows deploying the instrumentation without a site survey and leads to saving time and money [197].
- **Open Integration** - The Smart Wireless Gateway gives a variety of options and the freedom to choose the Smart Wireless Solutions which is suited for installation [197].
- **Flexible** - Modbus TPC allows integration of the wireless network with any host system. Modbus TCP Modbus protocol is used on top of Ethernet-TCP/IP [197].
- **Serial** - The Smart Wireless Gateway supports Modbus RTU, which is connected to a supervisory computer with a remote terminal unit (RTU), for integration into legacy host systems.
- **PlantWeb** - The Smart Wireless Gateway integrates into any PlantWeb architecture for commissioning of a wireless network. Every gateway has a web interface to provide a standalone host interface to manage the wireless network, without a dedicated host system [197].
- **Layered Security Keeps Network Safe**- Emerson Process Management's layered approach to wireless network security ensures that the network stays protected. As Emerson Process Management claims, the network devices implement encryption, authentication, verification, anti-jamming and key management methods to ensure that data transmissions are secure [197]. However, this claim has not been proved universally yet.
- **AMS Wireless Configurator** - AMS Wireless Configurator uses the power of Enhanced to the Electronic Device Description Language (EDDL) for assistant setup and configuration of the Smart Wireless Field Devices. This is shipped with every Smart Wireless Gateway [197].
- **Powers PlantWeb**- The Smart Wireless Gateway powers PlantWeb by giving the access to intelligent devices using WirelessHART technology [197]. Gateway connects WirelessHART self-organizing networks with any host system.

### 8.11.2 SMARTMESH IA-510

SMARTMESH IA-510 is a WirelessHART compliant Wireless Sensor Network system. The SmartMesh IA-510 system offers industrial automation to deliver flexible solutions. The SmartMesh IA-510 system consists of the PM2510 embedded network manager and two mote form factors: the DN2510 Mote-on-Chip and the M2510 RF-certified mote module. SmartMesh IA-510 systems are easy for industrial automation vendors to integrate and simple for end users to deploy [198].

- **The PM2510:** This provides industrial automation vendors with a complete embedded wireless sensor networking solution for WirelessHART applications that assures multi-vendor interoperability and offers forward compatibility[198].
- **The DN2510 Mote-on-Chip:** Intelligent Networking Platform and industry-leading low power radio technology in an easy-to-integrate 12 mm x 12 mm System-in-Package (SiP). This is part of the SmartMesh IAR-510 system and provides industrial automation vendors with a complete embedded wireless sensor networking solution for WirelessHART applications that assures integration to multivendor interoperability[199].
- **The M2510 RF-certified mote module:** Intelligent Networking Platform and industry-leading low-power radio technology in an easy-to-integrate 22-pin module. This is part of the SmartMesh IA-510 system and provides industrial automation vendors with an embedded wireless system complete with modular radio certifications for easy integration and reuse in developing multiple WirelessHART products [200].

### 8.12 Overview of WirelessHART Framework Experiment Set-up

The basic elements of a typical WirelessHART network include:

- **Field Devices** that are attached to the plant process.
- **Handheld** which is a portable WirelessHART-enabled computer used to configure devices, run diagnostics, and perform calibrations.
- **Gateway** that connects host applications with field devices, and
- **Network Manager** that is responsible for configuring the network, scheduling and managing communication between WirelessHART devices.

To support the mesh communication technology, each WirelessHART device must be able to forward packets on behalf of other devices [127].

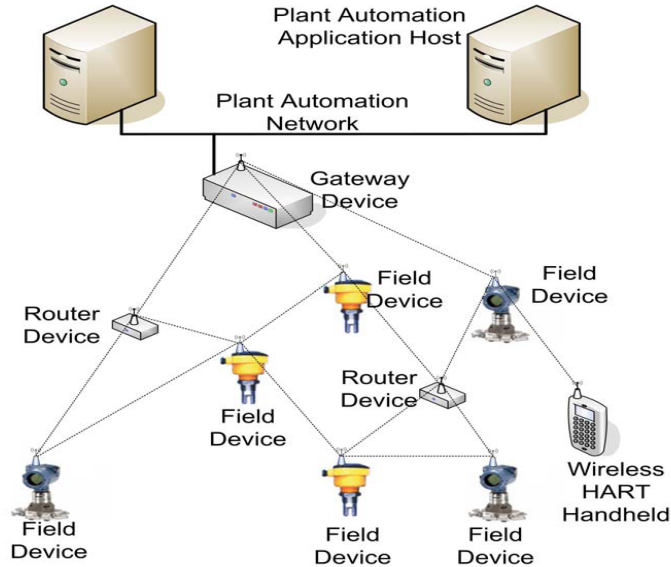


Figure 8-4: WirelessHART Mesh Networking [127].

As shown in Figure 8-4, the basic elements of a typical WirelessHART network include: (1) field devices that are attached to the plant process, (2) handheld which is a portable WirelessHART-enabled computer used to configure devices, run diagnostics, and perform calibrations, (3) A gateway that connects host applications with field devices, and (4) a network manager that is responsible for configuring the network, scheduling and managing communication between WirelessHART devices.

### 8.12.1 WirelessHART Routing Protocols

One will serve as the gateway and access point, which is connected to a laptop. The laptop is the host and runs the network manager. The *WirelessHART* network operates in the following way.

A device follows a strict process to join the network. Only after the network manager provisions it can a new device become a part of the network. A device has the flexibility to choose any neighbour with the best signal-to-noise ratio (or some other parameters) to join the network. In addition, once a device is set up, it publishes process data to the host periodically. The data will be routed via other neighbouring devices. *WirelessHART* is mainly intended for monitoring applications to send sensor data to the host [201].

- **Graph Routing** - A graph is a collection of paths that connect network nodes. The paths in each graph are explicitly created by the network manager and downloaded to each individual network device. To send a packet, the source device writes a specific graph ID (determined by the destination) in the network header. All network devices on the way to the destination must be pre-configured with graph information that specifies the neighbours to which the packets may be forwarded [127].
- **Source Routing** - Source Routing is a supplement of the graph routing aiming at network diagnostics. To send a packet to its destination, the source device includes in the header an ordered list of devices through which the packet must travel. As the packet is routed, each routing device utilizes the next network device address in the list to determine the next hop until the destination device is reached [127].

There are two different scenarios in terms of key management in WirelessHART:

- 1) Joining a new network device.
- 2) Communicating with an existing network device.

In the first scenario, the joining device will use the public key to generate the MIC on the MAC layer and use the join key to generate the network layer MIC and encrypt the join request. After the joining device is authenticated, the network manager will create a Session Key for the device and thus establish a secure session between them [127].

In the second scenario, on the MAC layer, the DLPDU (Data Link Protocol Data Unit) is authenticated with the network key; on the network layer, the packet is authenticated and encrypted by the session key.

### 8.12.2 Installation and Configuration of WirelessHART

- **Initial Connection and Configuration** - To configure the gateway, a local connection between a PC/laptop and the gateway needs to be established.
- **Establishing a Connection** - Connect the PC/laptop to the ethernet port of gateway through a crossover cable. After this, an IP address should be set up for the gateway by PC/laptop [202].
- Browse the IP address of gateway and configure the network settings.
- Restart the application and disconnect the power and ethernet from gateway.
- The gateway then connects to a host automation or asset management system using common industry communications standards such as OPC, MODBUS and MODBUS TCP.

- **Installation and Configuration of Wireless Sensor** - Wireless devices should also be powered up in order of proximity from the gateway, beginning with the closest. This will result in a simpler and faster network installation. Enable active advertising on the gateway to ensure that new devices join the network faster [203].

It should be mentioned that if the device was ordered with a factory configured network ID and join key, it should be able to join the network with no user input. If unsure, the network ID and the join key may be manually entered to match the gateway's ID. The network ID and join key may be changed in the wireless device. It should be mentioned that sensors' inputs can be configured for different sensor types [203].

### 8.12.3 Access@Plant

Access@Plant is the name for the technical solutions that provide access to networked systems in technical networks. Key components are [204]:

- Firewall (with redundancy) splitting networks into office network, (Demilitarized Zone) DMZ and technical networks
- Terminal server located in the DMZ.
- Active Directory server, maintaining user accounts for users that have been granted access to Terminal server.
- Backup server, maintaining backup of systems in technical networks.
- Antivirus and Software updates, OS Patches and services.

The hardware listed above forming the Access@Plant solution is normally physically located locally at the facility.

According to the Access@Plant specification, technical networks are segregated into dedicated subnets, one for each system. For instance, the plant's vibration analysis systems are placed in a dedicated subnet, while wireless gateways serving WSNs are designated their own subnet [204].

In general, all data flow between different systems on different technical networks should be passed through the firewall.

All communication from corporate network to technical systems is routed via the Terminal server. All network communication between corporate network and technical networks is initiated from the corporate network [204].

If a user in the corporate network needs access to a system in a plant's technical network, the following procedure applies:

- The user applies for access through Statoil's internal AccessIT service. The user's role in the organization and reasons for requiring access must be passed along with the request. For technical systems, local key persons at the actual facility are involved in the approval process [204].

If the request is approved:

- Access@Plant user account (in AD) is created.
- Logon information to the specific system is sent to the user. For systems incorporated in Access@Plant AD, the AD account is used. For other systems or devices, local username/passwords are commonly used [204].

#### **8.12.4 Access to the Wireless Gateway**

Administrative access to the wireless gateway is provided by the gateway's internal web server. The user authentication on the gateway is username/password. The gateway provides four access levels. Normally, a user in the corporate network will be granted "read-only" access. A typical procedure for accessing the wireless gateway at a producing facility is as follows [204]:

- Log on to the Terminal server, over Remote Desktop, with the Access@Plant AD account, which is different from the standard "office" user account.
- At the Terminal server, the user will meet a tailored desktop/start-menu, only containing icons for connecting to the technical systems to which access is granted. For wireless gateway access, an IE icon preconfigured to point to the gateway's IP address utilizing the https protocol is presented to the user.
- Clicking on the IE icon, the user reaches the logon screen on the gateway. The local username/password internally stored in the gateway must be used here.

### **8.13 Common Statoil Configurations**

The wireless gateway provides two Ethernet interfaces: Eth0 and Eth1 [204]. Eth0 is commonly used for administrative access, and the internal web server of the gateway is reached via this port. Eth0 is a part of a dedicated technical subnet. Depending on the user credentials, the user can monitor sensor data, collect network performance statistics and configure different WSN parameters such as network join key, encryption etc.

#### **8.13.1 Set-up 1: Sensor Data to PCDA over Serial MODBUS**

The transfer of sensor data into the PCDA system is conducted using the gateways RS-485 serial port. The protocol is MODBUS. At the control room side, the RS485 is terminated in a

Controller Node, which is a part of the plant's Safety & Automation System (SAS). The operator station collects sensor data from an interface in the Controller Node/SAS system. Obviously, in this setup, sensor data bypasses the firewall [204].

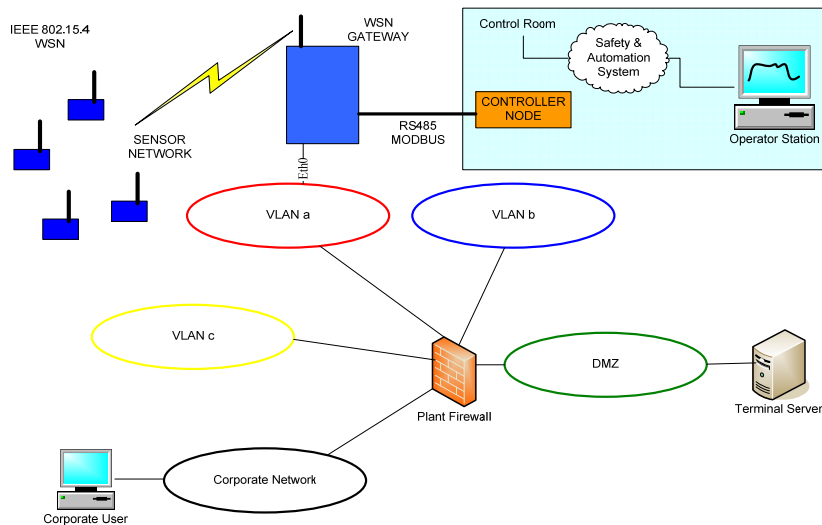


Figure 8-5: Sensor data to PCDA over serial MODBUS.

Note: All communication from corporate network into technical systems is routed via the firewall through segregated networks. This means that all data flow between different systems on different networks should pass through the firewall and the network should be segregated by VLAN (Virtual Local Area Network) to several different networks.

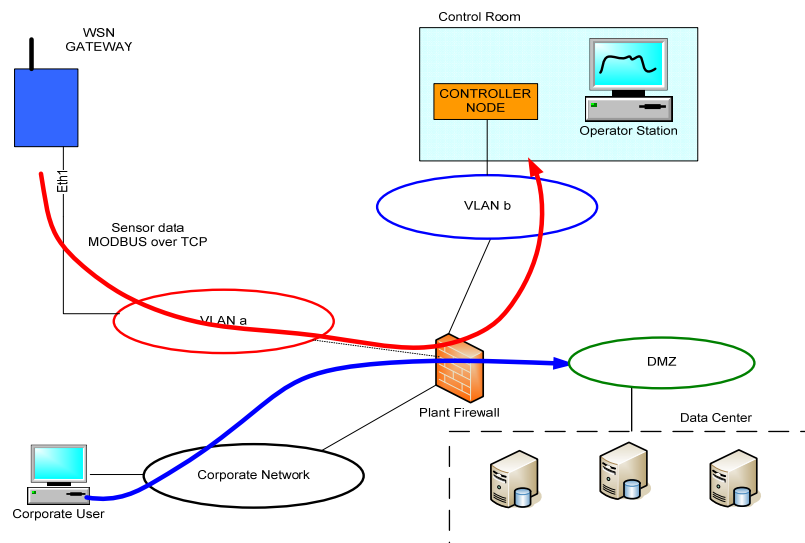


Figure 8-6: WSN Dataflow through firewall

Figure 8.6 illustrates the flow of data through the Firewall from different VLANs. As it can be seen, the network is segregated by several VLANs through the firewall. The dataflow from

Wireless gateway travels from VLAN a to VLAN b and then to Control room. This configuration provides the segmentation with a group of sensors and gateway, which have a common set of requirements, to communicate together, regardless of their physical location.

### 8.13.2 Set-up 2: Sensor Data via MODBUS over TCP 1

This configuration uses the gateway's secondary Ethernet port (Eth1) for transmitting sensor data to the control room. The implementation of MODBUS over TCP is utilized. In this set-up, Eth1 is connected directly to the technical subnet where the PCDA is located, implying that Eth0 and Eth1 are configured to operate in different IP subnets. Thus, sensor data flow from the gateway to the PCDA bypasses the firewall [204].

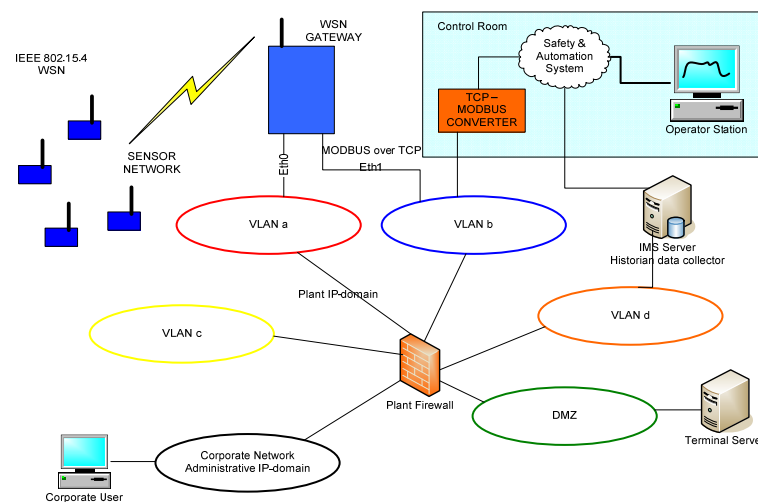


Figure 8-7: Sensor data via MODBUS over TCP, wireless gateway and PCDA in the same LAN.

### 8.13.3 Set-up 3: Sensor Data to PCDA via MODBUS over TCP 2

Like Set-up 2, this configuration utilizes MODBUS over TCP. Sensor data are transmitted to PCDA from Eth1 on the wireless gateway. Both Eth0 and Eth1 are connected to the same technical subnet, implying they are configured with IP addresses in the same range. In this set-up, all sensor data flow from gateway to PCDA must be routed through the firewall [204].



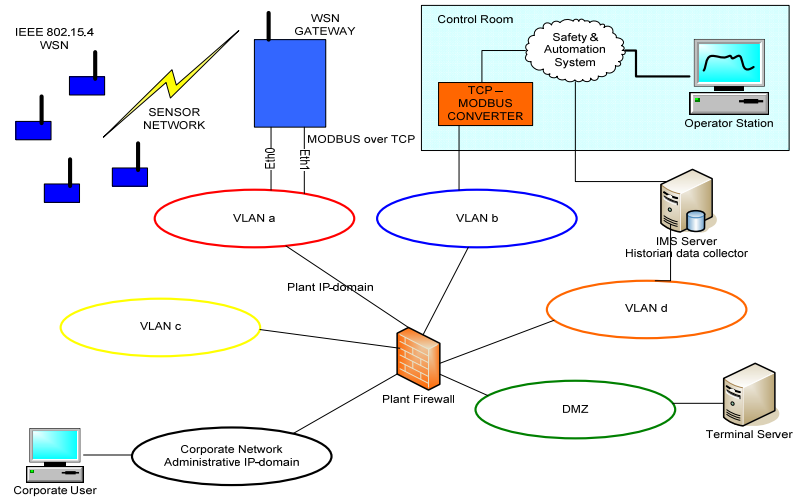


Figure 8-8: Sensor data to PCDA via MODBUS over TCP, wireless gateway and PCDA in separate LANs.

## 8.14 Summary of the case study

The monitoring of oil and gas platform performance through sensors allows for greater insight into potential safety problems and operational requirements. Through the use of intelligent techniques and key historical operation data, it is possible realize certain operational patterns, promote a safe workplace and optimize performance. However, as a result of very strict regulations pertaining to the installation of powered and networked sensors on oil and gas platforms, the installations of new sensors has been expensive, complex and time consuming [3].

WSNs in oil and gas industry must implement strict encryption, transmitter authentication and data consistency validation with possible constraints on energy, memory, computation and network bandwidth as countermeasures against cyber threats.

Wireless Sensor Networks (WSNs) have the potential to eliminate the need for cables and contribute to reduced installation and operating costs. They enable installations in difficult areas and allow for cost-efficient, temporary and mobile systems. The technical requirements for the effective deployment of wireless technology in Statoil installations have been identified [28].

Unfortunately, two factors make WSN cyber security a critical issue in this field:

- Wireless systems are quite vulnerable to cyber threats
- The oil and gas industry is an attractive target for cyber attacks

The cyber security issues of WSN installations raise serious concerns about the use of this technology in industrial settings. In a commercial environment, such networks must operate in

a secure manner. A security breach may cause significant production, safety and privacy issues.

As a result of the fundamental design constraints of WSNs, such systems have very many real and significant security concerns with potentially serious consequences if they are not managed.

Studies during this period could only be theoretically performed on WirelessHART specifications and devices. The ISA100 specification was only ratified well into the project and no development kits are currently available.

However, all of these standards are advertised as being open and public. We experienced serious issues with the supply of WirelessHART development equipment and software from Emerson and Dust Networks. Ideally, being a core Statoil technology, WirelessHART experimentation would have been preferable. However, to this day, such equipment, while theoretically open, is highly elusive. When our testing intentions were outlined, publically advertised development systems, which have been previously invoiced to Statoil and SINTEF, were only then not permitted to be purchased by non-OEM customers. Furthermore, promised documents outlining third-party security tests never emerged. After several attempts using personal contact, phone and email by Statoil, SINTEF and Curtin University, Emerson and Dust Networks simply no longer answered any correspondence. This raises serious concerns about WirelessHART solutions, ongoing development, collaboration, tailoring to Statoil requirements, performance and security.

It is concluded that as a direct result of our inability to independently source or verify the WirelessHART security aspects, WirelessHART offers highly questionable security and performance in an industrial environment outside of Emerson, Dust Networks and HART marketing.

In the oil and gas industry and Statoil's specific configurations, this may mean that:

WSN devices are not ultimately relied on for critical tasks where potential attacks are within theoretical radio range.

1. WSN devices are used exclusively for non-critical functions in all circumstances.
2. WSN devices are only used as a form of redundancy for wired counterparts.
3. Use of WSN is open to any function and the risks of such use are managed.

We leave it to Statoil to carefully consider the complete impact of such issues on their operation. This investigation certainly leads to further work on wireless process control.

## 8.15 Conclusion

In this chapter, the potential of WSN technology to benefit many aspects of the oil and gas industry was described. The case study examined the Statoil WSN lifecycle, which is broken down into five basic phases. The information security management and existing security standard ISO 27001 with its list of control objectives and controls that need to be implemented, have been explored.

It was shown that WSN technology brings a great deal of advantages for oil and gas industries, but due to the numerous challenges and concerns among end users in terms of security, the rate of adoption has been slow. As discussed earlier, the specific WSN attacks include any action that intentionally or unintentionally manipulates the WSN's performance. Hence, the potential attacks that could take place in this industry were introduced and categorized.

In this chapter, the device installation procedures of WirelessHART and the overview of WirelessHART Framework have been explained in detail. At the end, the common Statoil configuration through three set-up networks have been shown and described.

As mentioned earlier, the WirelessHART is applied in the Statoil to automate flow monitoring and increase production on its platforms. All three standards – ZigBee, WirelessHART and ISA100 – work on IEEE 802.15.4. Hence, we believe that applying our framework, which mitigates the risk of attacks in the ZigBee network, in the Statoil Company may reduce the risk of attacks within the WirelessHART network.

However, the WirelessHART technology was designed to enable secure industrial wireless sensor network communications while ensuring that ease-of-use is not compromised and security is built in and cannot be disabled. However, we believe that it would be useful to follow the recommendations from our proposed framework, which was designed to mitigate the ZigBee network security issues because both standards are based on the IEEE802.15.4 protocol.

## 9 Guidelines and Recommendations

### 9.1 Introduction

Finally, the risk evaluation guidelines are recommended in this chapter. In this research, nineteen attacks have been examined. It was found that the current ZigBee security schema is not able to remove the risk of all existing attacks. A few attacks can be avoided by activating ZigBee security schema. Those attacks have been identified and possible solutions to control them have been raised.

### 9.2 Guidelines and Recommendations

In this section, we gathered together all solutions for remaining attacks as recommendations and guidelines for organizations who are intending to implement a secure ZigBee network.

#### 9.2.1 Jamming Recommendation

Wireless Sensor Networks and indeed all other wireless networks are inherently and ultimately insecure simply because their availability can be selectively and strategically modified at will by manipulating the radio environment using jamming techniques. This, to a much lesser extent, is certainly also the case with their wired counterparts. This is the very reason why we are asked to switch off our mobile phones on airplane flights even though airplane sensors are of the wired variety. When considering jamming as a security issue, no currently available commercial solution is both practical and secure. It is obvious that where jamming is concerned, WSN security cannot be effectively deal with it when powerful jamming equipment is used.

Radio frequency interference is a disturbance that affects a radio environment with electromagnetic conduction or electromagnetic radiation as emitted from an external source. The disturbance may interrupt, totally obstruct, or otherwise degrade the effective performance of a wireless connection. Interference may be caused by an artificial or natural object that carries rapidly changing electrical currents, such as an electrical circuit. Furthermore, as demonstrated in this research, WSNs are subject to many security concerns beyond simple jamming.

In particular, we were able to confirm that network function could be halted or interrupted using radio interference (jamming) and man-in-the-middle type of attacks were indeed possible.

In a Wireless Sensor Network (WSN) environment, interference is considered a Quality of Service (QoS) issue. Unfortunately, in a security sense, radio frequency interference can be intentionally used for radio jamming as a form of electronic warfare. Therefore, jamming can be viewed as a form of malicious interference and is the most serious of security threats facing ZigBee network for two reasons:

1. It is very easy and very cheap to achieve.
2. It can strategically bring down a network in a timely, quick, effective, sustained and uncontrollable manner.

### **9.2.2 Physical Tampering Recommendation**

Physical security is the solution for a physical tampering attack. This countermeasure prevents intruders from gaining physical access to the devices by providing a facility which sets up a physical barrier to prevent intrusion. Physical security is more critical than network security configuration, but it is sometimes ignored by network administrators. Despite all the high-level safeguard measures, a compromise of physical access will almost always result in a complete compromise. Having a secured physical facility that is available only to authorized personnel is extremely important.

Physical attacks can impact on the coverage of the ZigBee network and in many cases make the ZigBee network inoperable. Due to the widespread placement of the individual nodes in an often non-secure and unmonitored area, individual nodes are susceptible to capture. An attacker is able to crack the key located in the node microcontroller by physically accessing the node and learning crucial security information from the node itself.

Device hardening is one of the fundamental security modules that should be practised to protect the device from unauthorized users and activity. An intruder gaining unauthorized access to a device can take over the devices and attack them, like the physical attack on the coordinator.

Every organization must have a device security policy that dictates the rules to protect device access and access control and outlines the minimal security configuration for all devices in the network.

### **9.2.3 Eavesdropping Recommendation**

However, an out-of-band transfer method is recommended because of the security implications of passing the key in the clear, but key management in a dense network would create some issues including costly maintenance. This means that in a network with too many

devices, it would be very challenging to add the correct key via the out-of-band method on devices which must be added or replaced in the network. In this case, proper key data management is required in order for the network administrator to maintain the network. This management raises several issues. For example, imagine that the network administrator has constructed a table containing the keys information which includes all the keys for encrypting and decrypting. If the network administrator decides to leave the company and work elsewhere, he/she still has knowledge of the keys of the whole network. If the company decides to change all of the network's keys, this will cost it money. Imagine another scenario where the network administrator has stored all the keys in a back-up tape. A few years later, disclosure is required due to a legal action and data needs to be recovered. If the keys file has been lost, then data cannot be accessed and this could become a major issue for the company.

The key management of a dense network, which has several coordinators and routers, is very complicated. Every single coordinator has its own key and PAN ID to communicate with its own routers and end-devices, which are in the same PAN ID, within the network. Therefore, in an out-of-band key management mechanism, the network administrator has to ascertain which key is applied by which coordinator in order to set up the appropriate key on the routers and end-devices which are willing to communicate with that coordinator. This process is costly and time consuming and not as efficient as automatic key distribution because a ZigBee node first scans the available channels to find operating networks and identifies which one it should join. In a dense network, multiple networks may operate in the same channel and are differentiated by their PAN IDs. Hence, the node may be able to see multiple routers and a coordinator from the same network, in which case the node selects the one to which it should be connected and this is usually the one with the best signal. Then the node sends a message to the relevant router or coordinator for handshaking and asks it to join the network. The router or coordinator decides whether the node is a permitted device, whether the router or coordinator is currently allowing devices to join, and whether it has address space available. If all these criteria are satisfied, the router or coordinator allows the device to join and an address is allocated.

As explained, the joining process of the node to the coordinator or router is usually done by the one with the best signal; distance is not the determining factor for the joining process. Therefore, the design of the network and the setting up of appropriate keys on nodes to communicate with the appropriate coordinator (the one with the best signal), would not be an easy job for the administrator who has to ensure that all nodes communicate with their coordinators or routers.

In addition, the network administrator must make sure that only authorized people have access to the key management information. If this information is kept in a database, some security schema to access this information are required, and an authentication and authorization mechanism allowing access to this information must be implemented, which is usually costly for the company.

Therefore, for a company which has a dense ZigBee network, the out-of-band method is too challenging, time consuming, costly, and prone to error; moreover, it introduces several security issues.

On the other hand, key distribution by the coordinator does not introduce these issues and all the joining processes and key distribution are done automatically by the coordinator, and data gathering by the coordinator is more efficient.

Due to these issues, the out-of-band method cannot be considered as appropriate for a dense network. Hence, we designed and configured the network to store the preconfigured key on the coordinators, and keys are distributed by coordinators to devices within the network.

#### **9.2.4 Flooding Attack Recommendation**

Flooding attack, like jamming, is inevitable to be removed. Three different scenarios in terms of addressing nodes within ZigBee network have been examined. It was found that we are only able to mitigate risk of attack rather than completely removing the risk of attack. In fact, by addressing the destination of nodes to a unicast address (Addr16Bit), an adversary is only able to interrupt the communication, not the buffer flow. This means that the communication will continue once an adversary stops the flooding attack, and the coordinator will not have to be restarted. Remember, that restarting the coordinator means the key is distributed at the very first handshaking in plain text, which produces a huge risk for the network.

Being a malicious activity, flooding is a security concern because it is an intentional, timely, strategic, unpredictable, modification of network performance.

#### **9.2.5 Replay Attack Recommendation**

By addressing the destination of nodes to a unicast address (Addr16Bit), an adversary is not able to force the coordinator to generate a broadcast packet and then execute a reply attack. Therefore, the unicast address is recommended to remove the risk of this attack.

We find that the key to a productive and secure environment in ZigBee is one where the security issues outlined in this research are identified, understood, accepted, related to particular functions and mitigated within the ZigBee network.

### **9.3 Conclusion**

In this chapter, we described all the solutions included in our framework as guidelines and recommendations. We believe that these solutions are better able to control all the exposure attacks against the ZigBee network. However, it cannot be stated with absolute certainty that all threats of these attacks have been eliminated completely, as the only certainty is uncertainty in the cyber security area.



## 10 Recapitulation and Future Work

### 10.1 Introduction

Security is one of the most talked about topics in the ICT area. The implementation of security protocols in WSNs, as a way of increasing the efficiency and performance of business, would be very useful and would enable industries to reduce the risk of losing data and information, which are considered as assets for firms. Moreover, WSNs are susceptible to other security breaches because they are usually deployed in unattended environments with no physical protection and use unreliable radio communication.

We experienced serious issues with the supply of WirelessHART and ISA 100 development equipment and software, so the only choice was for the researcher to conduct experiments using the Texas Instruments ZigBeePRO development kit.

The vulnerability of ZigBee was studied. All the existing exposure attacks were executed and the security schema in ZigBee was examined. It was found that ZigBee is still susceptible to a few attacks. Those exposure attacks were identified and an attempt was made to find solutions in order to control and mitigate such attacks.

This research focused on developing advanced solutions to address problems relating to:

- The extent to which the ZigBee security schema is secure;
- The exposure attacks that have not been successfully addressed by the current security schema in ZigBee technology;
- Mitigating the risk of eavesdropping attack in ZigBee;
- Mitigating the risk of replay attack in ZigBee;
- Mitigating the risk of physical tampering attack in ZigBee;
- Mitigating the risk of DoS attack such as jamming and flooding in ZigBee;

The hypothesis on which this research is based, that “The ZigBee standard is secured against all existing exposure attacks by activating the ZigBee security schema”, has proven to be incorrect. It was discovered that the ZigBee security schema is not secure against all existing exposure attacks and there are a few attacks that still threaten the ZigBee network. Then, the solutions to deal with those attacks were discussed, evaluated and recommended. These solutions enabled a better control of all existing exposure attacks by providing an architect framework with an appropriate design and configurations to improve security in the ZigBee network.

In order to resolve the issues in WSNs as discussed above, in the next section, we will recapitulate on the different issues that have been identified and addressed in this thesis. In

Section 10.3, the contributions, which have been made by the thesis to the literature, are highlighted as a result of having successfully addressed the different issues. In Section 10.4, some areas for future work have been identified. Section 10.5 concludes the chapter.

## 10.2 Recapitulation of Research Issues

As mentioned in Chapter 2, a comprehensive overview of WSN security, including protocol and existing standards and applications have been discussed. WSN attacks are a relatively recent phenomenon and include any action that intentionally or unintentionally manipulates the WSN's performance. In this thesis, the security of ZigBee has been studied and examined. Also, it was proved that the stated hypothesis in Chapter 3 is not correct and the ZigBee security schema is not able to protect the ZigBee network from all current exposure attacks.

The experiment was conducted on the actual devices and results were obtained through ZigBee CC2530 development kit. However, ZigBee standard presented a security schema to protect the ZigBee network against those attacks, but this technology is still susceptible to a few exposure attacks. It has been found that ZigBee is still vulnerable to eavesdropping and key management, replay attack, physical tampering as well as DoS such as jamming and flooding. We recommended solutions to control these attacks and contributed to improving the security in the cyber security area.

In summary, the research issues addressed in this thesis are as follows:

- The key can be achieved by capturing plain text traffic sent from a ZigBee Coordinator through eavesdropping.
- The key can be achieved by dumping device firmware using existing available hardware to steal keys by using unprotected data memory and exploiting flash memory.
- By sending a forged packet with key counter 0xFFFF by an adversary, the coordinator generates some broadcast packets, whether encrypted packets or unencrypted, and allows an adversary, through the broadcast packets, to execute or inject the out-dated data into the network.
- ZigBee is very susceptible to DoS attacks which may be conducted at the PHY/MAC/NWK/APS layers.
- ZigBee cannot be practically dealt with when powerful jamming equipment is used and this attack interrupts the communication in the network.

- ZigBee is vulnerable to flooding attack. This attack attempts to bring down the network or critical components such as the Coordinator by overwhelming it with excessive traffic.

### **10.3 Contribution of the Thesis**

The major contribution of this thesis to existing literature is that it proposes an architecture to enhance the security of WSNs. Following the conceptual model, several solutions are developed for specific research issues.

#### **10.3.1 Contribution 1:**

The first major contribution of this thesis is the development of an end-to-end WSN Architecture Framework with an approach for identifying the security vulnerability, by examining the extent of the security of the ZigBee schema. This examination includes specific areas such as key establishment, key transport, frame protection and device authorization. Due to the weakness in one of these specific areas, all mentioned exposure attacks are introduced in ZigBee.

#### **10.3.2 Contribution 2:**

The second major contribution of this thesis is the development of an end-to-end WSN Architecture Framework with an approach that is capable of identifying the number of exposure attacks that have not yet been removed by the current ZigBee security schema. WSNs are vulnerable to security attacks due to the broadcast nature of the transmission medium. Also, they have an additional vulnerability because nodes are often placed in an environment where they are not physically protected. So, several attacks introduced in WSN area can be categorised as two overarching passive and active attacks. In this thesis, nineteen attacks have been studied and executed in one of the WSN standards - ZigBee. It was found that, although the ZigBee Alliance has tried to develop a proper security schema to secure the ZigBee network, there are still some exposure attacks which have not yet been removed by the ZigBee security schema.

#### **10.3.3 Contribution 3:**

The third major contribution of this thesis is the development of an end-to-end WSN Architecture Framework capable of mitigating the risk of eavesdropping attack in ZigBee. It was found that the unsecured transport-key command provides a means for initializing a device with an initial key. This command does not cryptographically protect and a key is sent in plain text. By configuring the key at the factory through a physical interface, rather than

distributing keys from the coordinator over the air, this issue is resolved and the risk of this attack is mitigated.

However, due to the key management and costly maintenance, an out-of-band transfer method in a dense WSN network is not recommended.

#### **10.3.4 Contribution 4:**

The fourth major contribution of this thesis is the development of a solution to mitigate the risk of replay attack in the ZigBee network. By sending a forged packet with key counter 0xFFFF in ZigBee network, by an adversary, the coordinator generates some broadcast packets, whether encrypted packets or unencrypted. Through these broadcast attacks, an adversary is able to execute the replay attack and inject the broadcast packet into the network again. An attempt was made by ZigBee Alliance to address this issue through a Frame Counter mechanism, which is categorised as the frame protection in the ZigBee security schema.

It was found that the ZigBee is susceptible to attack, and if the destination addresses of network devices including coordinator and end-devices are properly addressed, this issue can be controlled and the risk of this attack is mitigated.

#### **10.3.5 Contribution 5:**

The fifth major contribution of this thesis is the development of a solution to mitigate the risk of physical tampering attack in ZigBee. The key can be achieved by dumping device firmware using existing available hardware to steal keys by using unprotected data memory and exploiting flash memory. This issue can be controlled through programmed JTAG or a serial bootstrap loader (BSL), which resides in masked ROM along with a proper physical security.

#### **10.3.6 Contribution 6:**

The sixth major contribution of this thesis is the development of a solution to mitigate the risk of a DoS attack which may be conducted at the PHY/MAC/NWK/APS layers. It was found that ZigBee is still susceptible to jamming and flooding attacks.

However, the spread-spectrum communication has introduced a way to control this attack as presented in an earlier chapter, but this defence mechanism cannot be applied to WSNs and therefore to ZigBee, as it requires greater complexity and power, thus making it unsuitable for WSNs. So, no currently available commercial solution is capable of securing the ZigBee network against this attack.

ZigBee is vulnerable to flooding attack and the network or critical components such as a coordinator may be able to bring it down by overwhelming it with excessive traffic. This issue can be controlled by limiting the number of connections thereby preventing complete resource exhaustion, which interferes with all other processes at the victim end by addressing properly the destination address of nodes.

The results can be of great help in ZigBee environments under DoS attacks. The effects of DoS attacks on the performance of ZigBee are considered in order to critically analyse these issues.

#### **10.4 Contribution against research Question**

It is concluded that all the following questions and that have been formulated for the research are answered through our contributions.

- 1- How secure is the ZigBee security schema?
- 2- Does the ZigBee security schema cover all security requirements?
- 3- How many existing exposure attacks can be removed by adding ZigBee security schema?
- 4- Is the ZigBee standard secured against all existing exposure attacks by activating the ZigBee security schema?
  - Questions 1 and 2 are answered through contribution 1 which identifies the ZigBee security vulnerability.
  - Questions 3 and 4 are answered through contribution 2 which identifies the number of exposure attacks that have not been removed by the current ZigBee security.
  - Contributions 3, 4, 5 and 6 answered the recommended solutions for those attacks, which are still vulnerable by activating the ZigBee security schema.

#### **10.5 Future Work**

It was demonstrated that this thesis has successfully achieved the research objectives to examine ZigBee security schema and find its vulnerabilities along with some solutions to address them. However, further investigation is needed in order to strengthen the proposed solutions.

The weaknesses of the ZigBee security schema were identified and in Chapter 4 a solution was proposed for enhanced security. WirelessHART and ISA100 are two standards for WSNs and are attracting increasing attention these days. Both of them provide a stronger security

schema than that of ZigBee standard. However, the ISA100 security schema is still inadequate, especially for certain environments with high security requirements. In future, the security weaknesses of WirelessHART and ISA100 standards must be investigated and solutions proposed for them.

Integration with Internet (IP) architecture is of utmost importance for the commercial development of sensor networks in order to provide services that allow querying the network to retrieve useful information from anywhere and at any time. In order to integrate the ZigBee network into the IP network, the use of application level gateways or an overlaying of IP networks is the best approach to integrate WSNs and the Internet. The ZigBee Gateway Device is a stand-alone device that can meet the IP connectivity requirements of most applications. ZigBeePRO is based on a different stack layer than with IP. Therefore, for connecting any ZigBee device to the Internet, an adaptor must be used to convert ZigBeePRO technology to ZigBee IP technology. This adaption is done by 6lowpan technology, which is already located within ZigBee IP and does not need any further development for integration into an IP network. The 6lowpan standard is the international Open Standard that enables IEEE802.15.4 and IP to communicate in a simple way. It defines encapsulation and header compression mechanisms that allow IPv6 packets to be sent to and received from IEEE 802.15.4-based networks. Using 6lowpan, it is possible to communicate with the Internet without any adapter. In future work, it is intended to investigate the security weaknesses of 6lowpan and propose the solutions for them.

## **10.6 Conclusion**

This chapter recapitulated the work that has been undertaken in this thesis. The research achievements according to the identified research issues have been highlighted. Also presented was a brief description of intended further work in order to strengthen the proposed solutions.

The work in this thesis has been reported to and approved by the Statoil Company and published as a part of proceedings in peer-reviewed international conferences.

Some selected publications were attached in Appendix. A complete list of all the publications arising as a result of the work documented in this thesis is attached at the beginning of the thesis.

## 11 References

- [1] H. Balakrishnan, V. Padmanabhan, S. Seshan, and R. Katz, "A comparison of mechanisms for improving TCP performance over wireless links", presented at the Networking, IEEE/ACM Transactions on Berkeley California, 2002.
- [2] SATS. (2007, 19 October). *Information security in integrated operations*. Available: <http://www.sintef.no/Home/Information-and-Communication-Technology-ICT/Software-Engineering-Safety-and-Security/Research-groups/Information-Security/Information-security-in-integrated-operations/>
- [3] "WSN Security Project Overview and Scope-Internal Statoil Document " Statoil2009.
- [4] S. Avancha, J. Undercoffer, A. Joshi, and J. Pinkston, "Security for Wireless Sensor Networks", in *Wireless Sensor Networks*, ed, 2004, pp. 253-275.
- [5] A. Barns, "Is Implementation of Voice Over Internet Protocol (VoIP) More Economical for Businesses with Large Call Centers", *Springerlink*, vol. 1, pp. 3-19, 2005.
- [6] Cisco. (2010, May). *Optimizing Branch Office Network Infrastructure TCO with Cisco ISR*. Available: [http://www.cisco.com/en/US/prod/collateral/routers/ps5855/prod\\_white\\_paper0900aecd805898e5.html](http://www.cisco.com/en/US/prod/collateral/routers/ps5855/prod_white_paper0900aecd805898e5.html)
- [7] Cisco. (2008, May). *How Cisco WLAN Became Primary Corporate User Network*. Available: [http://www.cisco.com/web/about/ciscoitnetwork/mobility/wireless\\_lan\\_benefits\\_web.html](http://www.cisco.com/web/about/ciscoitnetwork/mobility/wireless_lan_benefits_web.html)
- [8] W. Lehr and L. W. McKnight, "Wireless Internet access: 3G vs. WiFi?", *Telecommunications Policy*, vol. 27, pp. 351-370, 2003.
- [9] P. S. Henry and H. Luo. (2002) WiFi: what's next? *Communications Magazine, IEEE* 66 - 72.
- [10] J. C. Haartsen, "The Bluetooth radio system", presented at the Personal Communications, IEEE, Emmen, Netherlands 2000.
- [11] I. Howitt and J. A. Gutierrez, " IEEE 802.15.4 low rate - wireless personal area network coexistence issues", presented at the Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE New Orleans, USA 2003.
- [12] J. Zhang and V. Varadharajan, "A New Security Scheme for Wireless Sensor Networks", in *IEEE Global Telecommunications Conference*, 2008, pp. 1-5.
- [13] J. Wu and I. Stojmenovic, "Ad Hoc Networks", *The IEEE Computer Society*, vol. 04, 2004.
- [14] R. Wattenhofer, N. Burri, R. Flury, and P. v. Rickenbach. (August 30). *Wireless Ad Hoc And sensor netWorks*. Available: [http://www.disco.ethz.ch/misc/DCG\\_Sensor.pdf](http://www.disco.ethz.ch/misc/DCG_Sensor.pdf)
- [15] S. Petersen, S. Carlsen, and A. Skavhaug, "Layered Software Challenge of Wireless Technology in the Oil & Gas Industry", in *19th Australian Conference on Software Engineering*, Perth Australia, 2008, pp. 37-46.
- [16] T. He, S. Krishnamurthy, J. A. Stankovic, Tarek Abdelzaher, L. Luo, R. Stoleru, T. Yan, and L. Gu, "Energy-Efficient Surveillance System Using Wireless Sensor Networks", presented at the Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services, MobiSys'04, New York, USA, 2004.
- [17] D. C. Steere, A. Baptista, D. McNamee, C. Pu, and J. Walpole, "Research challenges in environmental observation and forecasting systems", in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, MobiCom'00*, New York, USA, 2000.
- [18] P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards", *Wired/Wireless Internet Communications*, vol. 30, pp. 1655-1695, 2007.
- [19] A. Talevski, S. Carlsen, and S. Petersen, "Intelligent Wireless Methodologies and Technologies for the Oil, Gas and Resources Industries", presented at the Industrial Informatics, 2009. INDIN 2009. 7th IEEE International Conference on Perth Australia, 2009.
- [20] J. Lopez and J. Zhou, *Wireless Sensor Network Security* vol. 1: IOS Press, Apr. 2008.
- [21] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey", in *Network*. vol. 1, ed: Auerbach Publications, 2007, pp. 1-50.
- [22] P. Radmand, A. Talevski, S. Petersen, and S. Carlsen, "Taxonomy of Wireless Sensor Network Cyber Security Attacks in the Oil and Gas Industries", presented at the 24th IEEE International Conference on Advanced Information Networking and Applications, Australia Perth, 2010.
- [23] C. Pearce, V. Y.-M. Ma, and P. Bertok, "A secure communication protocol for ad-hoc wireless sensor networks", in *Proceedings of the 2004 Intelligent Sensors, Sensor Networks and Information Processing Conference*, Melbourne, Australia, 2004, pp. 79-84.
- [24] S. Avancha, J. Undercoffer, A. Joshi, and J. Pinkston, "Security for wireless sensor networks", *Wireless Sensor Networks*, pp. 253-275-253-275.



- [25] R. Singh, S. D.K., and L. Kumar, "A review on security issues in wireless sensor network " *Journal of Information Systems and Communication*, vol. 1, 2010.
- [26] Y. Zhang, W. Liu, and Y. Fang;, "Secure localization in wireless sensor networks", presented at the Military Communications Conference, 2005. MILCOM 2005. IEEE Atlantic City USA, 2006.
- [27] P. Li, Y. Lin, and W. Zeng, "Search on Security in Sensor Networks", *Journal of Software*, vol. 17, pp. 2577-2588, Dec. 2006.
- [28] Y. Zhou, Y. Fang, and Y. Zhang, "Securing Wireless Sensor Networks: A Survey", *IEEE Communications Surveys & Tutorials*, vol. 10, pp. 6-28, 2008.
- [29] D. Kotz and K. Essien, "Analysis of a campus-wide wireless network", *Wireless Networks*, vol. 11, 2005.
- [30] I. F. Akyildiz, S. Weilian, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", *Communications Magazine, IEEE*, vol. 40, pp. 102-114, 2002.
- [31] J. A. Stankovic, T. E. Abdelzاهر, C. Lu, L. Sha, and J. C. Hou, "Real-time communication and coordination in embedded sensor networks", *Proceedings of the IEEE*, vol. 91, pp. 1002-1022, 2003.
- [32] I. Atakli, H. Hu, Y. Chen, and Z. Su, "Malicious node detection in wireless sensor networks using weighted trust evaluation", in *Proceedings of the 2008 Spring simulation multicongference*, USA San Diego, 2008.
- [33] S. K. Udgate, A. Mubeen, and S. L. Sabat, "Wireless Sensor Network Security Model Using Zero Knowledge Protocol", presented at the Communications (ICC), 2011 IEEE International Conference on Japan Kyoto, 2011.
- [34] D. Raymond and S. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses", vol. 7, pp. 74 - 81 2008.
- [35] J. Geier. (2002, September). *Minimizing 802.11 Interference Issues*. Available: <http://www.wi-fiplanet.com/tutorials/article.php/953511>
- [36] A. C. Alvaro, R. Tanya, and S. Shankar, "Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems", *Ad Hoc Netw.*, vol. 7, pp. 1434-1447, 2009.
- [37] S. Marano, V. Matta, and L. Tong, "Distributed Detection in the Presence of Byzantine Attack in Large Wireless Sensor Networks", presented at the Military Communications Conference, 2006. MILCOM 2006. IEEE Washington USA, 2007.
- [38] M. Saraogi, "Security in wireless sensor networks", Department of Computer Science, University of Tennessee, Knoxville2005.
- [39] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks", in *2005 IEEE Symposium on Security and Privacy*, 2005, pp. 49-63.
- [40] M. Gaurav, D. Peter, G. Deepak, and S. Prashant, "Capsule: an energy-optimized object storage system for memory-constrained sensor devices", presented at the Proceedings of the 4th international conference on Embedded networked sensor systems, Boulder, Colorado, USA, 2006.
- [41] C. Alippi, G. Anastasi, M. D. Francesco, and M. Roveri, "Energy Management in Wireless Sensor Networks with Energy-hungry Sensors", *IEEE Instrumentation and Measurement Magazine*, vol. 12, pp. 16-23, 2009.
- [42] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor Network Security: A Survey", *IEEE Communications Surveys & Tutorials*, vol. 11, 2009.
- [43] A. D. Wood and J. A. Stankovic, "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks."
- [44] M. Drozda, S. Schaust, and H. Szczerbicka, "AIS for misbehavior detection in wireless sensor networks: Performance and design principles", presented at the Evolutionary Computation, 2007. CEC 2007. IEEE Congress on Singapore 2008.
- [45] J. Stankovic and A. Wood, *A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks*: CRC Press, 2008.
- [46] W. Yong, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks", *Communications Surveys & Tutorials, IEEE*, vol. 8, pp. 2-23, 2006.
- [47] T.-G. Lupu, "Main types of attacks in wireless sensor networks", in *SSIP '09/MIV'09 Proceedings of the 9th WSEAS international conference on signal, speech and image processing, and 9th WSEAS international conference on Multimedia, Internet & video technologies*, Timisoara, Romania, 2009.
- [48] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks", *Computer*, vol. 35, pp. 54-62, 2002.
- [49] S. Kaplantzis, "Security Models for Wireless Sensor Networks", Master, Monash University, Monash University, 2006
- [50] R. Sandro and H. David, "A survey of key management for secure group communication", *ACM Comput. Surv.*, vol. 35, pp. 309-329, 2003.



- [51] Y. Mun and C. Shin, "Secure Routing in Sensor Networks: Security Problem Analysis and Countermeasures", in *Computational Science and Its Applications – ICCSA 2005*, ed, 2005, pp. 459-467.
- [52] H. Yih-Chun, P. Adrian, and B. J. David, "Rushing attacks and defense in wireless ad hoc network routing protocols", presented at the Proceedings of the 2nd ACM workshop on Wireless security, San Diego, CA, USA, 2003.
- [53] T. Zia and A. Zomaya, "Security Issues in Wireless Sensor Networks", presented at the Systems and Networks Communications, 2006. ICSNC '06. International Conference on Tahiti, 2006.
- [54] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: analysis & defenses", in *Information Processing in Sensor Networks, 2004. IPSN 2004. Third International Symposium on*, 2004, pp. 259-268.
- [55] N. Ahmed, S. Kanhere, and S. Jha, "The holes problem in wireless sensor networks: a survey", *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 9, pp. 4-18, 2005.
- [56] K. Xing, S. S. R. Srinivasan, M. Rivera, J. Li, and X. Cheng, "Attacks and Countermeasures in Sensor Networks A Survey", in *Network Security*, ed Springer: Springer, 2005, p. 370.
- [57] P. Li, Y. Lin, and W. Zeng, "Research on security in sensor networks", *Journal of Software*, vol. 17, pp. 2577-2588, 2006.
- [58] D. George, "Introducing Traffic Analysis: Attacks, Defences and Public Policy Issues", ed. Kasteelpark, Arenberg, 2005.
- [59] ([http://en.wikipedia.org/wiki/Traffic\\_analysis](http://en.wikipedia.org/wiki/Traffic_analysis)). *Traffic analysis*. Available: [http://en.wikipedia.org/wiki/Traffic\\_analysis](http://en.wikipedia.org/wiki/Traffic_analysis)
- [60] D. G. Peterson. (2008, October). *S4 Preview: Jamming and Interference on 802.15.4 Wireless*. Available: <http://www.digitalbond.com/2008/10/23/s4-preview-jamming-and-interference-on-802154-wireless/>
- [61] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", in *Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on*, 2003, pp. 113-127.
- [62] S. Misra, I. Woungang, and M. S. Chandra, *Guide to Wireless Ad Hoc Networks*, 2009.
- [63] "Wireless Sensor Network Sniffer/Analyser (IEEE 802.15.4 / ZigBee™ version)", BzWorks Pte Ltd, Singapore2003.
- [64] G. Padmavathi and D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", *International Journal of Computer Science and Information Security*, vol. 4, pp. 117-125, 2009.
- [65] D. R. Raymond and S. F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses", *Pervasive Computing, IEEE*, vol. 7, pp. 74-81, 2008.
- [66] "Wireless Sensor Network Sniffer/Analyser (IEEE 802.15.4/ZigBee Version)", BzWorks Pte Ltd, Singapore2003.
- [67] P. Radha, W. Cliff, and R. Sumit, *Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks (Advances in Information Security)*: Springer-Verlag New York, Inc., 2006.
- [68] W. Znaidi, M. Minier, and J.-P. Babau, "An Ontology for Attacks in Wireless Sensor Networks", ed: HAL - CCSD, 2008.
- [69] T. Masao and A. Masaki, "Preventing Resource Exhaustion Attacks in Ad Hoc Networks", presented at the Proceedings of the Eighth International Symposium on Autonomous Decentralized Systems, 2007.
- [70] M. Roche. ([http://www.cse.wustl.edu/~jain/cse571-07/ftp/wireless\\_hacking/](http://www.cse.wustl.edu/~jain/cse571-07/ftp/wireless_hacking/)). *Wireless Hacking Tools*. Available: [http://www.cse.wustl.edu/~jain/cse571-07/ftp/wireless\\_hacking/](http://www.cse.wustl.edu/~jain/cse571-07/ftp/wireless_hacking/)
- [71] A. George, T. Leandros, and S. Y. Gregory, "Overcoming misbehavior in mobile ad hoc networks: an overview", *Crossroads*, vol. 11, pp. 5-5, 2005.
- [72] N. Hoang Lan and N. Uyen Trang, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks", in *Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006. International Conference on*, 2006, pp. 149-149.
- [73] M. A. Khan, G. A. Shah, and M. Sher, "Challenges for Security in Wireless sensor Networks (WSNs)", presented at the World Academy of Science, Engineering and Technology, 2011.
- [74] A. B. Becher, Z. Dornseif, M., "Tampering with Motes: Real-World Attacks on Wireless Sensor Networks", RWTH Aachen University.
- [75] L. K. Bysani and A. K. Turuk, "A Survey On Selective Forwarding Attack in Wireless Sensor Networks", presented at the Devices and Communications (ICDeCom), 2011 International Conference on Mesra, 2011.
- [76] Jennic. (2008, September 30). *ZigBee Stack User Guide*. Available: [http://www.jennic.com/files/support\\_files/JN-UG-3017-ZigBeeStackUserGuide-1v6.pdf](http://www.jennic.com/files/support_files/JN-UG-3017-ZigBeeStackUserGuide-1v6.pdf)
- [77] (2007, Nov 23rd). *HART Communication Foundation*. Available: <http://www.hartcomm.org/index.html>
- [78] ISA. (2008, September). *ISA100.11a Release 1* Available: <http://www.isa.org/isa100/>

- [79] V. Ahuja, in *Network and Internet Security*, ed: DIANE Publishing Company, 1999.
- [80] J. Rehana, "Security of Wireless Sensor Network", presented at the Seminar on Internet Working, 2009-04-27.
- [81] L. Yee Wei, D. Jeroen, and H. Pieter, "Survey and benchmark of block ciphers for wireless sensor networks", *ACM Trans. Sen. Netw.*, vol. 2, pp. 65-93, 2006.
- [82] M. Sharifnejad, M. Sharifi, M. Ghiasabadi, and S. Beheshti, "A Survey on Wireless Sensor Networks Security", presented at the The 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, TUNISIA, 2007.
- [83] N. Gura, A. Patel, A. Wander, H. Eberle, and S. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs", in *Cryptographic Hardware and Embedded Systems - CHES 2004*, ed, 2004, pp. 119-132.
- [84] H. Jason, S. Robert, W. Alec, H. Seth, C. David, and P. Kristofer, "System architecture directions for networked sensors", *SIGPLAN Not.*, vol. 35, pp. 93-104, 2000.
- [85] V. Gupta, M. Wurm, Y. Zhu, M. Millard, S. Fung, N. Gura, H. Eberle, and S. C. Shantz, "Sizzle: A Standards-based End-to-End Security Architecture for the Embedded Internet", June 2005.
- [86] B. Duncan and D. Malan, "Low-Power, Secure Routing for MICA2 Mote", 2004.
- [87] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "TinyPK: securing sensor networks with public key technology", in *SASN'04 -- Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, 2004, pp. 59-64.
- [88] O. M. Dahl, "Limitations and Differences of using IPsec, TLS/SSL or SSH as VPN-solution", Oct. 29 2004.
- [89] F. Tang, M. Guo, M. Li, C.-l. Wang, and M. Dong, "Secure Routing for Wireless Mesh Sensor Networks in Pervasive Environments", *INTERNATIONAL JOURNAL OF INTELLIGENT CONTROL AND SYSTEMS*, vol. 12, pp. 293-306, 2007.
- [90] Wei. Zhang, S. K. Das, and Y. Liu, "Security in Wireless Sensor Networks: A Survry", in *Security in Sensor Networks*, Y. Xiao, Ed., ed: Taylor & Fancis Group LLC, 2007, pp. 237-272.
- [91] L. E. Bassham, "The Keyed-Hash Message Authentication Code Validation System (HMACVS)", December 3, 2004.
- [92] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless Sensor Network Security: A Survey", 2006.
- [93] G. Saurabh, Srdjan, apkun, H. Chih-Chieh, and B. S. Mani, "Secure time synchronization service for sensor networks", presented at the Proceedings of the 4th ACM workshop on Wireless security, Cologne, Germany, 2005.
- [94] K. Masica, "Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments", Lawrence Livermore National Laboratory, April 2007.
- [95] T.-K. Nguyen, V.-H. Le, Q.-H. Duong, S.-K. Han, S.-G. Lee, N.-S. Seong, N.-S. Kim, and C.-S. Pyo, "Low-Power Direct Conversion Transceiver for 915 MHz Band IEEE 802.15.4b Standard Based on 0.18  $\mu\text{m}$  CMOS Technology", *ETRI Journal*, vol. 30, pp. 33-46, February 2008.
- [96] T. Hailun, O. Diethelm, Z. John, and J. Sanjay, "A confidential and DoS-resistant multi-hop code dissemination protocol for wireless sensor networks", presented at the Proceedings of the second ACM conference on Wireless network security, Zurich, Switzerland, 2009.
- [97] R. Struik. (Jun .09 2009). *Re: [6lowpan] ND and MAC-level security*. Available: <http://www.mail-archive.com/6lowpan@ietf.org/msg01612.html>
- [98] "IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)", *IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003)*, pp. 0\_1-305, 2006.
- [99] A.Miguel and A.Arzuaga, "STATE-OF-THE-ART TECHNOLOGIES & PROTOCOLS DESCRIPTION OF STATE-OF-THE-ART WIRELESS ACCESS TECHNOLOGIES", Project Funded by the European Commission under the 7th Framework Programme 2009.
- [100] N. Sastry and D. Wagner, "Security considerations for IEEE 802.15.4 networks", in *Proceedings of the 3rd ACM workshop on Wireless security*, New York, NY, USA, 2004.
- [101] N. Chayat and V. Yanover, "Proposal on changes in the 802.16 MAC Reference Model and PHY Service definition", 08-12-2000.
- [102] R. Struik, "Security Clauses-Streamlines Version, with Security Level Set", Certicom Corp, Mississauga 2006.
- [103] D. Gascón. (2009, November 10). *Security in 802.15.4 and ZigBee networks*. Available: <http://www.sensor-networks.org/index.php?page=0903503549>
- [104] A. Mishra, C. Na, and D. Rosenburgh, "On Scheduling Guaranteed Time Slots for Time Sensitive Transactions in IEEE 802.15.4 Networks", presented at the Military Communications Conference, 2007. MILCOM 2007. IEEE USA Orlando, 2008.

- [105] TI. (2010, September). *CC2530 ZigBee Development Kit* Available: <http://www.ti.com/tool/cc2530zdk>
- [106] R. R. Garcia. Understanding of ZigBee Stack. Available: [http://www.eetasia.com/ARTICLES/2006JAN/PDF/EEOL\\_2006JAN02\\_RFD\\_NETD\\_TA\\_01.pdf](http://www.eetasia.com/ARTICLES/2006JAN/PDF/EEOL_2006JAN02_RFD_NETD_TA_01.pdf)
- [107] A. Elahi and A. Gschwender, *ZigBee Wireless Sensor and Control Network*. Prentice Hall, 2009.
- [108] Daintree. (2010, September ). *Getting Started with ZigBee and IEEE 802.15.4* Available: [http://www.daintree.net/downloads/whitepapers/ZigBee\\_primer.pdf](http://www.daintree.net/downloads/whitepapers/ZigBee_primer.pdf)
- [109] S. Tian-Wen and Y. Chu-Sing, "A Connectivity Improving Mechanism for ZigBee Wireless Sensor Networks", in *Embedded and Ubiquitous Computing, 2008. EUC '08. IEEE/IFIP International Conference on*, 2008, pp. 495-500.
- [110] X. Xianghua, Y. Daomin, and W. Jian, "An Enhanced Routing Protocol for ZigBee/IEEE 802.15.4 Wireless Networks", in *Future Generation Communication and Networking, 2008. FGCN '08. Second International Conference on*, 2008, pp. 294-298.
- [111] "ZigBee Stack Advanced User Guide.", Jennic Technology for a Changing World Mar. 2008.
- [112] G. Thonet. (2006, May). *ZigBee FAQ*. Available: <http://wsnet.files.wordpress.com/2006/08/ZigBee-faq.pdf>
- [113] S. Farahani, "ZigBee wireless networks and transceivers", illustrated ed: Newnes, 2008.
- [114] Jennic, "An Introduction to Smart Energy", Jennic Limited, Jennic Limited 2009.
- [115] ZigBee. (2008, September 30). *ZIGBEE CLUSTER LIBRARY SPECIFICATION*. Available: [www.ZigBee.org/ZigBee/en/spec\\_download/spec\\_download.asp?](http://www.ZigBee.org/ZigBee/en/spec_download/spec_download.asp?).
- [116] ZigBee. (2005, September 30). *ZigBee Specification*. Available: <http://www.ZigBee.org/Specifications.aspx>
- [117] S. Jing and Z. Xiaofen, "Study of ZigBee Wireless Mesh Networks", in *Hybrid Intelligent Systems, 2009. HIS '09. Ninth International Conference on*, 2009, pp. 264-267.
- [118] "ZigBee Standards Organization", Network Specification, 2005.
- [119] (Feb 2008). *Getting Started with ZigBee and IEEE 802.15.4*.
- [120] P. Ocenasek, "Towards Security Issues in ZigBee Architecture", in *Human Interface and the Management of Information. Designing Information Environments*, ed, 2009, pp. 587-593.
- [121] S. Farahani, *ZigBee Wireless Networks and Transceivers* Elsevier Science & Technology Books, Sep. 2008.
- [122] R. Silva and S. Nunes, "Security Issues on ZigBee", 2005.
- [123] R. Silva and S. Nunes, "Security in IEEE 802.15.4 Standard", Inescid Lisboa, Matera Italy Jan. 18 2006.
- [124] S. C. Ergen and P. Varaiya, "TDMA scheduling algorithms for wireless sensor networks", *Wireless Networks*, vol. 16, 2010.
- [125] (2009). *The Components of WirelessHART technology*. Available: [http://www.hartcomm.org/protocol/wihart/wireless\\_components.html](http://www.hartcomm.org/protocol/wihart/wireless_components.html)
- [126] H. C. Fundation. (2011, September). *HART Specification*. Available: [http://www.hartcomm.org/protocol/about/aboutprotocol\\_specs.html](http://www.hartcomm.org/protocol/about/aboutprotocol_specs.html)
- [127] S. Jianping, H. Song, A. K. Mok, C. Deji, M. Lucas, and M. Nixon, "WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control", in *Real-Time and Embedded Technology and Applications Symposium, 2008. RTAS '08. IEEE*, 2008, pp. 377-386.
- [128] T. Lennvall, S. Svensson, and F. Hekland, "A Comparison of WirelessHART and ZigBee for Industrial Applications", presented at the Factory Communication Systems, 2008. WFCS 2008. IEEE International Workshop on Dresden 2008.
- [129] A. Lehto, "WirelessHART™ Smart Wireless Solutions", Emerson Process Management Oy.
- [130] S. Raza, T. Voigt, A. Slabbert, and K. Landernäs, "Design and Implementation of a Security Manager for WirelessHART Networks", presented at the The 5th IEEE International Workshop on Wireless and Sensor Networks Security (WSN'S 2009), Macau SAR, P.R.C, 2009.
- [131] (2009). *ISA-100.11a-2009 Wireless systems for industrial automation: Process control and related applications*. Available: <http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=10766>
- [132] D. Sexton, "Understanding the unique nature of the universal family of ISA100 Wireless Standards", ISAAug. 28 2007.
- [133] H. Rodriguez, B. Ontiveros, I. Soto, and R. Carrasco, "A public key encryption model for wireless sensor networks", in *Communication Systems, Networks and Digital Signal Processing, 2008. CNSDSP 2008. 6th International Symposium on*, 2008, pp. 373-377.
- [134] G. WAN, "Comparison and Evaluation of Industrial Wireless Sensor Network Standards ISA100.11a and WirelessHART", CHALMERS UNIVERSITY OF TECHNOLOG EX036/201, 2011.
- [135] T. Lennvall, S. Svensson, and F. Hekland, "A comparison of WirelessHART and ZigBee for industrial applications", in *Factory Communication Systems, 2008. WFCS 2008. IEEE International Workshop on*, 2008, pp. 85-88.

- [136] P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards", *Computer Communications*, vol. 30, pp. 1655-1695, 2007.
- [137] A. Madhukar, I. Zachary, and L. Insup, "Quantifying eavesdropping vulnerability in sensor networks", presented at the Proceedings of the 2nd international workshop on Data management for sensor networks, Trondheim, Norway, 2005.
- [138] D. Jing, R. Han, and S. Mishra, "Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks", in *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*, 2005, pp. 113-126.
- [139] P. Kyasanur and N. H. Vaidya, "Detection and handling of MAC layer misbehavior in wireless networks", in *Dependable Systems and Networks, 2003. Proceedings. 2003 International Conference on*, 2003, pp. 173-182.
- [140] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. Culler, "SPINS: security protocols for sensor networks", *Wirel. Netw.*, vol. 8, pp. 521-534, 2002.
- [141] M. d. J. Marcel Breeuwsma, Coert Klaver, Ronald van der Knijff and Mark Roeloffs, "Forensic Data Recovery from Flash Memory", *Small Scale Digital Device Forensic Journal*, vol. 1, pp. 1-17, Jun 2007.
- [142] S. Sastry, J. Stankovic, and J. Sztipanovits, "New Vistas in CIP Research and Development: Secure Networked Embedded Systems", The NSF/OSTP Workshop on Innovative Information Technologies for Critical Infrastructure Aug. 25-30 2002.
- [143] Y. Zhang, J. Zheng, and M. Ma, *Handbook of Research on Wireless Security: Information Science Reference*, 2008.
- [144] A. Hamid, Mamun-Or-Rashid, and C. S. Hong, "Routing Security in Sensor Network: HELLO Flood Attack and Defense", presented at the Proceedings of First International Conference on Next-Generation Wireless Systems (ICNEWS 2006), Dhaka, Bangladesh, , 2006.
- [145] V. C. Giruka, M. Singhal, J. Royalty, and S. Varanasi, "Security in wireless sensor networks", in *Wireless Communications and Mobile Computing*. vol. 8, ed, Sep 12 2006, pp. 1-24.
- [146] "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)", IEEE Standard for Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements 2006.
- [147] J. y. Cache, J. Wright, and W. Liu, *Hacking Exposed Wireless: Wireless Security Secrets & Solutions: McGraw-Hill Prof Med/Tech*, 2007.
- [148] J. Wright. (2010, October). *Will Hack For SUSHI Hacking and Defending Wireless*. Available: <http://www.willhackforsushi.com/>
- [149] ZigBee. (September). *Understanding ZigBee RF4CE*. Available: <https://docs.ZigBee.org/ZigBee-docs/dcn/09-5231.PDF>
- [150] J. Wright. (2010, September). *KillerBee: Practical ZigBee Exploitation Framework or "Wireless Hacking and the Kinetic World"*. Available: <http://www.willhackforsushi.com/presentations/toorcon11-wright.pdf>
- [151] R. Muraleedharan and L. A. Osadciw, "Jamming attack detection and countermeasures in wireless sensor network using ant system " in *Proceeding of the SPIE*, 2006.
- [152] Peter Egli, "Susceptibility of wireless devices to denial of service attacks " net Module 2006.
- [153] P. Dell, "Acting Your Age: A Study of the Relationship between Online Social Interaction and Identity in Older Adults", PhD, Curtin Business School, Curtin University of Technology., Curtin University of Technology., 2008.
- [154] J. F. Nunamaker, M. Chen, and T. D. M. Purdin, "Systems development in information systems research.", *Journal of Management Information Systems*, vol. 7, pp. 89-106, 1990.
- [155] F. Burstein and S. Gregor, "The systems development or engineering approach to research in information systems: An action research perspective.", in *Proceedings of the 10th Australian Confenece on Information Systems, ACIS'99*, Wellington, NZ, 1999, pp. 122-134.
- [156] ISO/IEC, "Information technology — Security techniques — Information security management systems — Overview and vocabulary", in *Terms and Definitions*, ed. ISO/IEC: ISO/IEC, 2009, p. 7.
- [157] K. Lee, J. Lee, B. Zhang, J. Kim, and Y. Shin, "An Enhanced Trust Center Based Authentication in ZigBee Networks", in *ISA '09 Proceedings of the 3rd International Conference and Workshops on Advances in Information Security and Assurance*, Haidelberg Germany, 2009.
- [158] Y. Bhajji, *Network Security Technologies and Solutions*. Cisco System: Cisco Press, 2008.
- [159] BSi. (2010, September ). *BS ISO/IEC 27033-1:2009*. Available: <http://shop.bsigroup.com/en/ProductDetail/?pid=00000000030168527>
- [160] TI. (2009, July). *SmartRF05 Evaluation Board User's Guide*. Available: <http://www.ti.com/lit/ug/swru210a/swru210a.pdf>



- [161] TI. (2008, July). *CC2530 Development Kit User's Guide*. Available: <http://www.ti.com/lit/ug/swru208b/swru208b.pdf>
- [162] IAR. (July). *IAR Embedded Workbench*. Available: <http://www.iar.com/en/Products/>
- [163] TI. (2010, September). *Z-Stack - ZigBee Protocol Stack* Available: <http://www.ti.com/tool/z-stack>
- [164] Z. Kyaw. (2010, July). *Creating a ZigBee® Smart Energy Device with the MSP430F54xx and the CC2530-ZNP (ZigBee Pro Network Processor)*.
- [165] TI. (2009, July). *SmartRF Protocol Packet Sniffer*. Available: <http://www.ti.com/tool/packet-sniffer>
- [166] TI. (2009, May). *SmartRF Studio* Available: <http://www.ti.com/tool/smartrfstudio>
- [167] T. Y. Song, Ch., "A Connectivity Improving Mechanism for ZigBee Wireless Sensor Networks", vol. 2, pp. 495 - 500 2008.
- [168] Jennic. (May). *Joining a ZigBee Network*. Available: <http://www.jennic.com/elearning/ZigBee/files/html/module6/module6-4.htm>
- [169] TI. (2008, August). *Low Power RF Solutions - ZigBee Security Workshop*.
- [170] L. E. Bassham, "The Keyed-Hash Message Authentication Code Validation System (HMACVS)", Computer Security Division, National Institute of Standards and Technology, 2004.
- [171] T. Lammle, *CCNA: Cisco Certified Network Associate Study Guide, Third Edition*. Cisco Press: Cisco Press, 2008.
- [172] J. Wright. (2009, September). *killerbee*. Available: <http://code.google.com/p/killerbee/>
- [173] Atmel. (2008, July). *AVR2016: RZRAVEN Hardware User's Guide*. Available: [http://www.datasheetarchive.com/RZUSB\\*-datasheet.html](http://www.datasheetarchive.com/RZUSB*-datasheet.html)
- [174] Atmel. (May). *The New Atmel AVR Studio*. Available: [http://www.atmel.com/microsite/avr\\_studio\\_5/default.asp?source=redirect](http://www.atmel.com/microsite/avr_studio_5/default.asp?source=redirect)
- [175] Wireshark. (2009, July). *Wireshark IEEE\_802.15.4*. Available: <http://www.wireshark.org/about.html>
- [176] Daintree. (July). *Sensor Network Analyzer (SNA)*. Available: <http://www.daintree.net/sna/sna.php>
- [177] D. Calcutt, F. Cowan, and H. Parchizadeh, *8051 Microcontrollers: An Applications Based Introduction*: Elsevier, 2004.
- [178] MikroElektronika. (July). *Architecture and programming of 8051 MCU's*. Available: <http://www.mikroe.com/eng/chapters/view/65/chapter-2-8051-microcontroller-architecture/>
- [179] K. Mitnick, W. Simon, and S. Wozniak, *The Art of Deception: Controlling the Human Element of Security*. WILEY, 2002.
- [180] T. Goodspeed. (2009, September). *Extracting Keys from Second Generation ZigBee Chips*. Available: <http://www.scribd.com/doc/18225321/Extracting-Keys-From-Second-Generation-ZigBee-Chips>
- [181] N. Lawson. (2010, September). *Smart meter crypto flaw worse than thought*. Available: <http://rdist.root.org/2010/01/11/smart-meter-crypto-flaw-worse-than-thought/>
- [182] G. W. Skelton and A. Holton, "Survivability in Wireless Sensor Networks", in *SoutheastCon, 2006. Proceedings of the IEEE* Memphis, TN, 2006, pp. 341 - 341
- [183] M. Baar, "Security Amangement. Lecture Notes", ed. Macquarie University, 2007.
- [184] Statoil. (July 2011). *About Statoil*. Available: <http://www.statoil.com/en/Pages/default.aspx>
- [185] "Integrating Biodiversity Conservation into Oil and Gas Development", The Energy & Biodiversity Initiative, The Center for Environmental Leadership in Business (CELB) at Conservation International (CI)
- [186] "Integrating Biodiversity Conservation into Oil and Gas Development", The Energy & Biodiversity Initiative, Washington DC2003.
- [187] (2007). *Creating The Oil Company of The Future* Available: <http://www.abb.com/cawp/seitp202/a76b051c06a5a368c125737f00296336.aspx>
- [188] S. Vatland, P. Doyle, and T. M. Andersen. (2008). *Integrated operations*. Available: <http://www02.abb.com/global/gad/gad02077.nsf/lupLongContent/2B9754FEE49B7AD7C125734800319DCF>
- [189] M. Dalbro, E. Eikeland, A. J. i. t. Veld, Stein Gjessing, T. S. Lande, H. K. Riis, and O. Søråsen, "Wireless Sensor Networks for Off-shore Oil and Gas Installations", presented at the Sensor Technologies and Applications, 2008. SENSORCOMM '08. Second International Conference on, 2008.
- [190] (May 20, 2009). *Emerson's WirelessHART™ products monitor flow on StatoilHydro Gullfaks platforms following wireless success on company's Grane platform*
- [191] (Aug. 29 2007). *Information security in integrated operations*. Available: <http://sats-certification.org/Home/Information-and-Communication-Technology-ICT/Software-Engineering-Safety-and-Security/Research-groups/Information-Security/Information-security-in-integrated-operations/>
- [192] A. S. K. Pathan, *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*: CRC Press, 2010.
- [193] M. Baar, "Information Security Management System " in *Information Security Management*, ed. Macquarie University, 2008.
- [194] M. Baar, "ISO Standards", in *Information Security Management*, ed. Macquarie University, 2008.

- [195] PRAXIOM, "ISO IEC 27002 (17799) INFORMATION SECURITY CONTROL OBJECTIVES", in *ISO IEC 27001*, ed. PRAXIOM, 2005.
- [196] "OLF Guideline No.104: Information Security Baseline Requirements for Process Control, Safety, and Support ICT Systems-Internal Statoil Document", Integrated Operations2009.
- [197] "Smart Wireless Gateway", Emerson Process ManagementSep 2009.
- [198] M. Khan, F. Amini, and J. Mišić, "Key Exchange in 802.15.4 Networks and Its Performance Implications", in *Mobile Ad-hoc and Sensor Networks*, ed, 2006, pp. 497-508.
- [199] Dust. (July). *SMARTMESH IA-510 DN2510 2.4 GHz Mote-on-Chip (H)*. Available: [http://www.dustnetworks.com/products/list/?field\\_product\\_type\\_value\\_many\\_to\\_one=Mote-on-Chip](http://www.dustnetworks.com/products/list/?field_product_type_value_many_to_one=Mote-on-Chip)
- [200] Dust. (July). *SMARTMESH IA-510 M2510 2.4 GHz Wireless Mote (H)*. Available: [http://www.dustnetworks.com/products/list/?field\\_product\\_type\\_value\\_many\\_to\\_one=Mote-on-Chip](http://www.dustnetworks.com/products/list/?field_product_type_value_many_to_one=Mote-on-Chip)
- [201] J. Song, S. Han, X. Zhu, A. Mok, D. Chen, and M. Nixon, "Demo Abstract: A Complete WirelessHART Network."
- [202] "Quick Installation Guide of Smart Wireless Gateway (WirelessHART™)", Rosemount IncAug. 2009.
- [203] "Quick Installation Guide- Rosemount 848T Wireless Temperature Transmitter", Emerson Process ManagementMay 2009.
- [204] "Setup WSN Networks-Internal Statoil Document", Statoil2009.

Every reasonable effort has been made to acknowledge the owners of copyright material. I would be pleased to hear from any copyright owner who has been omitted or incorrectly acknowledged.

## 12 Appendix

### 12.1 Examining ZigBee Security Quality of Services

Table 12.1: ZigBee Security Lost Packets

Lost packages ZigBee	Total frames	Received frames	Error frames	Lost frames	% lost frames	% error (total)	% error (received)	% received (OK&ERR)
<b>With Security</b>								
1	600	483	45	117	19.50%	7.50%	9.32%	80.50%
2	600	434	39	166	27.67%	6.50%	8.99%	72.33%
3	600	284	60	316	52.67%	10.00%	21.13%	47.33%
4	600	583	18	17	2.83%	3.00%	3.09%	97.17%
5	600	552	70	48	8.00%	11.67%	12.68%	92.00%
6	600	486	44	114	19.00%	7.33%	9.05%	81.00%
7	600	575	25	25	4.17%	4.17%	4.35%	95.83%
8	600	563	36	37	6.17%	6.00%	6.39%	93.83%
9	600	551	29	49	8.17%	4.83%	5.26%	91.83%
10	600	428	62	172	28.67%	10.33%	14.49%	71.33%
11	600	412	56	188	31.33%	9.33%	13.59%	68.67%
12	600	586	20	14	2.33%	3.33%	3.41%	97.67%
13	600	598	3	2	0.33%	0.50%	0.50%	99.67%
14	600	563	19	37	6.17%	3.17%	3.37%	93.83%
15	600	598	2	2	0.33%	0.33%	0.33%	99.67%
16	600	299	58	301	50.17%	9.67%	19.40%	49.83%
17	600	377	41	223	37.17%	6.83%	10.88%	62.83%
18	600	344	55	256	42.67%	9.17%	15.99%	57.33%
19	600	502	22	98	16.33%	3.67%	4.38%	83.67%
20	600	435	37	165	27.50%	6.17%	8.51%	72.50%
21	600	423	37	177	29.50%	6.17%	8.75%	70.50%
22	600	520	14	80	13.33%	2.33%	2.69%	86.67%
23	600	223	59	377	62.83%	9.83%	26.46%	37.17%
24	600	223	59	377	62.83%	9.83%	26.46%	37.17%
25	600	451	36	149	24.83%	6.00%	7.98%	75.17%
26	600	460	40	140	23.33%	6.67%	8.70%	76.67%
27	600	341	42	259	43.17%	7.00%	12.32%	56.83%
28	600	357	63	243	40.50%	10.50%	17.65%	59.50%
29	600	409	31	191	31.83%	5.17%	7.58%	68.17%
30	600	323	64	277	46.17%	10.67%	19.81%	53.83%
31	600	357	27	243	40.50%	4.50%	7.56%	59.50%
32	600	278	59	322	53.67%	9.83%	21.22%	46.33%
33	600	368	33	232	38.67%	5.50%	8.97%	61.33%
<b>Without Security</b>								
1	600	551	21	49	8.17%	3.50%	3.81%	91.83%
2	600	449	33	151	25.17%	5.50%	7.35%	74.83%
3	600	452	47	148	24.67%	7.83%	10.40%	75.33%
4	600	554	9	46	7.67%	1.50%	1.62%	92.33%

5	600	555	36	45	7.50%	6.00%	6.49%	92.50%
6	600	491	25	109	18.17%	4.17%	5.09%	81.83%
7	600	535	32	65	10.83%	5.33%	5.98%	89.17%
8	600	373	39	227	37.83%	6.50%	10.46%	62.17%
9	600	283	46	317	52.83%	7.67%	16.25%	47.17%
10	600	596	8	4	0.67%	1.33%	1.34%	99.33%
11	600	560	19	40	6.67%	3.17%	3.39%	93.33%
12	600	598	5	2	0.33%	0.83%	0.84%	99.67%
13	600	598	7	2	0.33%	1.17%	1.17%	99.67%
14	600	594	0	6	1.00%	0.00%	0.00%	99.00%
15	600	600	1	0	0.00%	0.17%	0.17%	100.00%
16	600	531	10	69	11.50%	1.67%	1.88%	88.50%
17	600	483	19	117	19.50%	3.17%	3.93%	80.50%
18	600	486	28	114	19.00%	4.67%	5.76%	81.00%
19	600	314	32	286	47.67%	5.33%	10.19%	52.33%
20	600	461	34	139	23.17%	5.67%	7.38%	76.83%
21	600	408	23	192	32.00%	3.83%	5.64%	68.00%
22	600	361	31	239	39.83%	5.17%	8.59%	60.17%
23	600	528	13	72	12.00%	2.17%	2.46%	88.00%
24	600	227	15	373	62.17%	2.50%	6.61%	37.83%
25	600	403	31	197	32.83%	5.17%	7.69%	67.17%
26	600	368	32	232	38.67%	5.33%	8.70%	61.33%
27	600	425	36	175	29.17%	6.00%	8.47%	70.83%
28	600	440	36	160	26.67%	6.00%	8.18%	73.33%
29	600	474	26	126	21.00%	4.33%	5.49%	79.00%
30	600	354	28	246	41.00%	4.67%	7.91%	59.00%
31	600	432	26	168	28.00%	4.33%	6.02%	72.00%
32	600	354	27	246	41.00%	4.50%	7.63%	59.00%
33	600	459	18	141	23.50%	3.00%	3.92%	76.50%
<b>Average RESULTS</b>								
<b>With Security</b>	600	435.93	39.54	164.06	27.34%	6.59%	10.64%	72.65%
<b>Without Security</b>	600	463.54	24.03	136.45	22.74%	4.00%	5.78%	77.25%



## 12.2 Z-Stack Sample Application

This application sends its messages either as broadcast or broadcast filtered group messages. The other (more normal) message addressing is unicast. Most of the other sample applications are written to support the unicast message model.

Key control:

SW1: Sends a flash command to all devices in Group 1.

SW2: Adds/Removes (toggles) this device in and out

of Group 1. This will enable and disable the reception of the flash command.

```
*****/
```

```
/******
```

```
* INCLUDES
```

```
*/
```

```
#include "OSAL.h"
```

```
#include "ZGlobals.h"
```

```
#include "AF.h"
```

```
#include "aps_groups.h"
```

```
#include "ZDApp.h"
```

```
#include "SampleApp.h"
```

```
#include "SampleAppHw.h"
```

```
#include "OnBoard.h"
```

```
/* HAL */
```

```
#include "hal_lcd.h"
```

```
#include "hal_led.h"
```

```
#include "hal_key.h"
```

```
*****
```

```
* MACROS
```

```
*/
```

```
*****
```

```
* CONSTANTS
```

```
*/
```

```
*****
```

```
* TYPEDEFS
```

```
*/
```

```
*****
```

```

* GLOBAL VARIABLES
*/
int messages=0;
int fmessages=0;

// This list should be filled with Application specific Cluster IDs.
const cld_t SampleApp_ClusterList[SAMPLEAPP_MAX_CLUSTERS] =
{
    SAMPLEAPP_PERIODIC_CLUSTERID,
    SAMPLEAPP_FLASH_CLUSTERID,
    SAMPLEAPP_TEMPERATURE_CLUSTERID
};

const SimpleDescriptionFormat_t SampleApp_SimpleDesc =
{
    SAMPLEAPP_ENDPOINT,      // int Endpoint;
    SAMPLEAPP_PROFID,        // uint16 AppProfId[2];
    SAMPLEAPP_DEVICEID,      // uint16 AppDeviceId[2];
    SAMPLEAPP_DEVICE_VERSION, // int AppDevVer:4;
    SAMPLEAPP_FLAGS,         // int AppFlags:4;
    SAMPLEAPP_MAX_CLUSTERS,  // uint8 AppNumInClusters;
    (cld_t *)SampleApp_ClusterList, // uint8 *pAppInClusterList;
    SAMPLEAPP_MAX_CLUSTERS,  // uint8 AppNumInClusters;
    (cld_t *)SampleApp_ClusterList // uint8 *pAppInClusterList;
};

// This is the Endpoint/Interface description. It is defined here, but
// filled-in in SampleApp_Init(). Another way to go would be to fill
// in the structure here and make it a "const" (in code space). The
// way it's defined in this sample app it is define in RAM.
endPointDesc_t SampleApp_epDesc;

/*****
* EXTERNAL VARIABLES
*/

/*****
* EXTERNAL FUNCTIONS
*/

/*****
* LOCAL VARIABLES
*/
uint8 SampleApp_TaskID; // Task ID for internal task/event processing
// This variable will be received when
// SampleApp_Init() is called.
devStates_t SampleApp_NwkState;

uint8 SampleApp_TransID; // This is the unique message ID (counter)

afAddrType_t SampleApp_Periodic_DstAddr;
afAddrType_t SampleApp_Flash_DstAddr;

aps_Group_t SampleApp_Group;

uint8 SampleAppPeriodicCounter = 0;
uint8 SampleAppFlashCounter = 0;

```

```

uint16 Temperature=22;

/*****
 * LOCAL FUNCTIONS
 */
void SampleApp_HandleKeys( uint8 shift, uint8 keys );
void SampleApp_MessageMSGCB( afIncomingMSGPacket_t *pkt );
void SampleApp_SendPeriodicMessage( void );
void SampleApp_SendFlashMessage( uint16 flashTime );

void SampleApp_Send_Temperature(uint8 temp);

/*****
 * NETWORK LAYER CALLBACKS
 */

/*****
 * PUBLIC FUNCTIONS
 */

/*****
 * @fn   SampleApp_Init
 *
 * @brief Initialization function for the Generic App Task.
 *        This is called during initialization and should contain
 *        any application specific initialization (ie. hardware
 *        initialization/setup, table initialization, power up
 *        notificaiton ... ).
 *
 * @param task_id - the ID assigned by OSAL. This ID should be
 *                used to send messages and set timers.
 *
 * @return none
 */
void SampleApp_Init( uint8 task_id )
{
    SampleApp_TaskID = task_id;
    SampleApp_NwkState = DEV_INIT;
    SampleApp_TransID = 0;

    // Device hardware initialization can be added here or in main() (Zmain.c).
    // If the hardware is application specific - add it here.
    // If the hardware is other parts of the device add it in main().

#if defined ( SOFT_START )
    // The "Demo" target is setup to have SOFT_START and HOLD_AUTO_START
    // SOFT_START is a compile option that allows the device to start
    // as a coordinator if one isn't found.
    // We are looking at a jumper (defined in SampleAppHw.c) to be jumpered
    // together - if they are - we will start up a coordinator. Otherwise,
    // the device will start as a router.
    if ( readCoordinatorJumper() )
        zgDeviceLogicalType = ZG_DEVICETYPE_COORDINATOR;
    else
        zgDeviceLogicalType = ZG_DEVICETYPE_ROUTER;
#endif // SOFT_START

#if defined ( HOLD_AUTO_START )

```

```

// HOLD_AUTO_START is a compile option that will surpress ZDApp
// from starting the device and wait for the application to
// start the device.
ZDOInitDevice(0);
#endif

// Setup for the periodic message's destination address
// Broadcast to everyone
SampleApp_Periodic_DstAddr.addrMode = (afAddrMode_t)AddrBroadcast;
SampleApp_Periodic_DstAddr.endPoint = SAMPLEAPP_ENDPOINT;
SampleApp_Periodic_DstAddr.addr.shortAddr = 0xFFFF;

// Setup for the flash command's destination address - Group 1
SampleApp_Flash_DstAddr.addrMode = (afAddrMode_t)afAddrGroup;
SampleApp_Flash_DstAddr.endPoint = SAMPLEAPP_ENDPOINT;
SampleApp_Flash_DstAddr.addr.shortAddr = SAMPLEAPP_FLASH_GROUP;

// Fill out the endpoint description.
SampleApp_epDesc.endPoint = SAMPLEAPP_ENDPOINT;
SampleApp_epDesc.task_id = &SampleApp_TaskID;
SampleApp_epDesc.simpleDesc
    = (SimpleDescriptionFormat_t *)&SampleApp_SimpleDesc;
SampleApp_epDesc.latencyReq = noLatencyReqs;

// Register the endpoint description with the AF
afRegister( &SampleApp_epDesc );

// Register for all key events - This app will handle all key events
RegisterForKeys( SampleApp_TaskID );

// By default, all devices start out in Group 1
SampleApp_Group.ID = 0x0001;
osal_memcpy( SampleApp_Group.name, "Group 1", 7 );
aps_AddGroup( SAMPLEAPP_ENDPOINT, &SampleApp_Group );

#if defined ( LCD_SUPPORTED )
    HalLcdWriteString( "SampleApp", HAL_LCD_LINE_1 );
#endif
}

/*****
 * @fn    SampleApp_ProcessEvent
 *
 * @brief  Generic Application Task event processor. This function
 *         is called to process all events for the task. Events
 *         include timers, messages and any other user defined events.
 *
 * @param  task_id - The OSAL assigned task ID.
 * @param  events - events to process. This is a bit map and can
 *                contain more than one event.
 *
 * @return none
 */
uint16 SampleApp_ProcessEvent( uint8 task_id, uint16 events )
{
    afIncomingMSGPacket_t *MSGpkt;

    if ( events & SYS_EVENT_MSG )
    {

```

```

MSGpkt = (afIncomingMSGPacket_t *)osal_msg_receive( SampleApp_TaskID );
while ( MSGpkt )
{
    switch ( MSGpkt->hdr.event )
    {
        // Received when a key is pressed
        case KEY_CHANGE:
            SampleApp_HandleKeys( ((keyChange_t *)MSGpkt)->state, ((keyChange_t *)MSGpkt)->keys );
            break;

        // Received when a messages is received (OTA) for this endpoint
        case AF_INCOMING_MSG_CMD:
            SampleApp_MessageMSGCB( MSGpkt );
            break;

        // Received whenever the device changes state in the network
        case ZDO_STATE_CHANGE:
            SampleApp_NwkState = (devStates_t)(MSGpkt->hdr.status);
            if ( (SampleApp_NwkState == DEV_ZB_COORD)
                || (SampleApp_NwkState == DEV_ROUTER)
                || (SampleApp_NwkState == DEV_END_DEVICE) )
            {
                // Start sending the periodic message in a regular interval.

                /*
                    osal_start_timerEx( SampleApp_TaskID,
                                        SAMPLEAPP_SEND_PERIODIC_MSG_EVT,
                                        SAMPLEAPP_SEND_PERIODIC_MSG_TIMEOUT );
                */
            }
            else
            {
                // Device is no longer in the network
            }
            break;

        default:
            break;
    }

    // Release the memory
    osal_msg_deallocate( (uint8 *)MSGpkt );

    // Next - if one is available
    MSGpkt = (afIncomingMSGPacket_t *)osal_msg_receive( SampleApp_TaskID );
}

// return unprocessed events
return (events ^ SYS_EVENT_MSG);
}

// Send a message out - This event is generated by a timer
// (setup in SampleApp_Init()).
if ( events & SAMPLEAPP_SEND_PERIODIC_MSG_EVT )
{
    // Send the periodic message
    SampleApp_SendPeriodicMessage();

    // Setup to send message again in normal period (+ a little jitter)
    osal_start_timerEx( SampleApp_TaskID, SAMPLEAPP_SEND_PERIODIC_MSG_EVT,

```

```

        (SAMPLEAPP_SEND_PERIODIC_MSG_TIMEOUT + (osal_rand() & 0x00FF));

    // return unprocessed events
    return (events ^ SAMPLEAPP_SEND_PERIODIC_MSG_EVT);
}

// Discard unknown events
return 0;
}

/*****
 * Event Generation Functions
 */
/*****
 * @fn   SampleApp_HandleKeys
 *
 * @brief Handles all key events for this device.
 *
 * @param shift - true if in shift/alt.
 * @param keys - bit field for key events. Valid entries:
 *             HAL_KEY_SW_2
 *             HAL_KEY_SW_1
 *
 * @return none
 */
void SampleApp_HandleKeys( uint8 shift, uint8 keys )
{
    if ( keys & HAL_KEY_SW_1 )
    {
        /* This key sends the Flash Command is sent to Group 1.
         * This device will not receive the Flash Command from this
         * device (even if it belongs to group 1).
         */
        //SampleApp_SendFlashMessage( SAMPLEAPP_FLASH_DURATION );
    }

    if ( keys & HAL_KEY_SW_2 )
    {
        /* The Flashr Command is sent to Group 1.
         * This key toggles this device in and out of group 1.
         * If this device doesn't belong to group 1, this application
         * will not receive the Flash command sent to group 1.
         */
        /* aps_Group_t *grp;
         grp = aps_FindGroup( SAMPLEAPP_ENDPOINT, SAMPLEAPP_FLASH_GROUP );
         if ( grp )
         {
             // Remove from the group
             aps_RemoveGroup( SAMPLEAPP_ENDPOINT, SAMPLEAPP_FLASH_GROUP );
         }
         else
         {
             // Add to the flash group
             aps_AddGroup( SAMPLEAPP_ENDPOINT, &SampleApp_Group );
         }
         */
    }

    if ( keys & HAL_KEY_LEFT )
    {

```

```

SampleApp_Send_Temperature(0);
if((messages%2)==0 )
    HAL_TURN_ON_LED1();
else
    HAL_TURN_OFF_LED1();
messages++;
}
if ( keys & HAL_KEY_RIGHT )
{
    SampleApp_Send_Temperature(1);
    if((fmessages%2)==0 )
        HAL_TURN_OFF_LED2();
    else
        HAL_TURN_ON_LED2();
    fmessages++;
}
}

/*****
* LOCAL FUNCTIONS
*/

/*****
* @fn   SampleApp_MessageMSGCB
*
* @brief Data message processor callback. This function processes
*        any incoming data - probably from other devices. So, based
*        on cluster ID, perform the intended action.
*
* @param none
*
* @return none
*/
void SampleApp_MessageMSGCB( afIncomingMSGPacket_t *pkt )
{
    uint16 flashTime;

    switch ( pkt->clusterId )
    {
        case SAMPLEAPP_PERIODIC_CLUSTERID:
            /*
            if((fmessages%2)==0 )
                HAL_TURN_OFF_LED2();
            else
                HAL_TURN_ON_LED2();
            fmessages++;
            */
            break;

        case SAMPLEAPP_FLASH_CLUSTERID:
            /*
            flashTime = BUILD_UINT16(pkt->cmd.Data[1], pkt->cmd.Data[2] );
            HalLedBlink( HAL_LED_4, 4, 50, (flashTime / 4) );
            */
            break;

        case SAMPLEAPP_TEMPERATURE_CLUSTERID:
            #if defined ( LCD_SUPPORTED )
                HalLcdWriteString( "Temperature", HAL_LCD_LINE_1 );
            #endif
    }
}

```

```

        //uint8 option=BUILD_UINT8(pkt->cmd.Data[1])
        if(pkt->cmd.Data[0]==0)
            //HalLcdWriteString( "0", HAL_LCD_LINE_2 );
            Temperature--;
        else
            //HalLcdWriteString( "1", HAL_LCD_LINE_2 );
            Temperature++;
        //HalLcdWriteValue (Temperature,8,HAL_LCD_LINE_2);
        HalLcdWriteStringValue("Temperature", (uint32)Temperature, 16, HAL_LCD_LINE_2 );
    #endif

    break;
}
}

/*****
 * @fn   SampleApp_SendPeriodicMessage
 *
 * @brief Send the periodic message.
 *
 * @param none
 *
 * @return none
 */
void SampleApp_SendPeriodicMessage( void )
{
    if ( AF_DataRequest( &SampleApp_Periodic_DstAddr, &SampleApp_epDesc,
                        SAMPLEAPP_PERIODIC_CLUSTERID,
                        1,
                        (uint8*)&SampleAppPeriodicCounter,
                        &SampleApp_TransID,
                        AF_DISCV_ROUTE,
                        AF_DEFAULT_RADIUS ) == afStatus_SUCCESS )
    {
    }
    else
    {
        // Error occurred in request to send.
    }

    /*
    if((messages%2)==0 )
    HAL_TURN_ON_LED1();
    else
    HAL_TURN_OFF_LED1();
    messages++;
    */
}

/*****
 * @fn   SampleApp_SendFlashMessage
 *
 * @brief Send the flash message to group 1.
 *
 * @param flashTime - in milliseconds
 */

```



```

* @return none
*/
void SampleApp_SendFlashMessage( uint16 flashTime )
{
    uint8 buffer[3];
    buffer[0] = (uint8)(SampleAppFlashCounter++);
    buffer[1] = LO_UINT16( flashTime );
    buffer[2] = HI_UINT16( flashTime );

    if ( AF_DataRequest( &SampleApp_Flash_DstAddr, &SampleApp_epDesc,
        SAMPLEAPP_FLASH_CLUSTERID,
        3,
        buffer,
&SampleApp_TransID,
        AF_DISCV_ROUTE,
        AF_DEFAULT_RADIUS ) == afStatus_SUCCESS )
    {
    }
    else
    {
        // Error occurred in request to send.
    }
}

/*****
*****/

void SampleApp_Send_Temperature(uint8 temp)
{
    if ( AF_DataRequest( &SampleApp_Periodic_DstAddr, &SampleApp_epDesc,
        SAMPLEAPP_TEMPERATURE_CLUSTERID,
        1,
        (uint8*)&temp,
&SampleApp_TransID,
        AF_DISCV_ROUTE,
        AF_DEFAULT_RADIUS ) == afStatus_SUCCESS )
    {
    }
    else
    {
        // Error occurred in request to send.
    }
}

```

# Taxonomy of Wireless Sensor Network Cyber Security Attacks in the Oil and Gas Industries

Pedram Radmand<sup>1</sup>, Alex Talevski<sup>1</sup>, Stig Petersen<sup>2</sup> and Simon Carlsen<sup>3</sup>

<sup>1</sup>Digital Ecosystems and Business Intelligence Institute, Curtin University of Technology, Perth, Australia  
Pedram.Radmand@student.curtin.edu.au, Alex.Talevski@cbs.curtin.edu.au

<sup>2</sup>SINTEF ICT, Trondheim, Norway  
stig.petersen@sintef.no

<sup>3</sup>Statoil ASA, Trondheim, Norway  
SCAR@StatoilHydro.com

**Abstract**— the monitoring of oil and gas plants using sensors allows for greater insight into safety and operational performance. However, as a result of strict installation regulations of powered sensors near oil and gas fittings, the introduction of new wired sensors to optimize end-of-lifecycle plants has been expensive, complex and time consuming. Recent advances in wireless technology have enabled low-cost Wireless Sensor Networks (WSNs) capable of robust and reliable communication. However, the critical WSN security issues have not been sparsely investigated. The goal of this paper is to define the security issues surrounding WSNs with specific focus on the oil and gas industry.

## I. INTRODUCTION

The monitoring of oil and gas platform performance through sensors allows for greater insight into potential safety problems and operational requirements. Sensors may monitor pipeline pressure, flow, temperature, vibration, humidity, gas leaks, fire outbreaks, equipment condition and others. Furthermore, through the use of intelligent techniques and the monitoring of key historical operation properties, sensor data may be used to realize certain characteristics and patterns in typical operations to further promote a safe workplace and optimize production. However, as a result of very strict regulations on the installation of wired sensors on oil and gas platforms, the installations of new sensors to optimize plant operation has been very expensive, complex and time consuming [1]. Recent advances in wireless technology have enabled low-cost wireless solutions capable of robust and reliable communication. International standards such as the IEEE 802.11a/b/g/n for wireless local area networks and the IEEE 802.15.4 for low-rate wireless personal area networks have facilitated many new applications [1].

Controlling oil and gas infrastructure is highly complex. It requires many sensors which monitor plant equipment. A delicate and accurate balance of flows, temperatures, pressures, and other parameters must be maintained to ensure safe and productive operation. Unfortunately, two factors have moved wireless network cyber security quickly up the list of priorities for oil and gas companies:

- Wireless systems are vulnerable to cyber threats.
- The oil and gas industry forms an attractive target for cyber-attacks.

## II. WIRELESS SENSOR NETWORKS (WSNs)

A sensor is a device that reacts to changes in conditions. It returns a value of a physical quantity or parameter and converts the value into a signal for visualization, processing, recording or automation. Such information can be used to monitor factory performance and optimize production. Wireless Sensor Networks (WSNs) comprise of a large number of spatially distributed autonomous devices that may collect data using a wireless medium. They may be used to cooperatively control and monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations [4]. WSNs exhibit several unique properties as compared to their wired counterparts such as large scale of deployment, mobility of nodes, node failures, communication failures and dynamic network topologies. In addition, each sensor node has constraints on resources such as energy, memory, computation speed and bandwidth as a result of their constraints on size, battery life and cost [4]. WSN have many applications in both military and civilian fields such as battlefield surveillance, habitat monitoring, healthcare, and traffic control and so on. Many WSN applications require secure communications. Due to absence of physical protection, the security in WSN is extremely important [4].

**IEEE Std 802.15.4** – Specifies the physical layer and media access control for low-rate wireless personal area networks (LR-WPANs). It is maintained by the IEEE 802.15 working group. It offers lower network layers which focus on low-power and low-cost ubiquitous communication between devices with little to no underlying infrastructure where interaction is performed over a conceptually simple wireless network [21]. The following layers are considered;

- **Physical Layer** – This layer provides the data transmission service along with the interface to the

physical layer management entity. This layer offers access to every layer management function and maintains the database of personal area network. The PHY layer manages the RF transceiver and performs channel selection, energy and signal management functions [21].

- **Media Access Control (MAC) Layer** – The MAC layer manages the interface as well as access to the physical channel and network beaconing. In addition, it handles network association and disassociation functions and applies unique 64-bit MAC hardware addresses assigned by the manufacturer. In addition, the MAC layer provides optional security services including frame encryption, integrity, and access control. The unit of transmission at this layer is the MAC frame. The standard Data Link Layer (DLL) layer in the IEEE model normally consists of two sub-layers such as MAC sub-layer and a Logical Link Control (LLC) sub-layer, which is the IEEE 802.2 standard. It should be mentioned that both the wired Ethernet network standard (802.3) and the wireless Ethernet standard (802.11) utilize the standard 802.2 sub-layer [21].
- **Higher Layers** – These layers and interoperability sub layers are not defined in the standard. There exist specifications, such as ZigBeePRO, WirelessHART and ISA100, which build on this standard [21].

There are four fundamental frame types (data, acknowledgment, beacon and MAC command frames), which provide a reasonable trade-off between simplicity and robustness. In IEEE 15.4 a super-frame structure, which is defined by the coordinator, may provide synchronization to other devices and configuration information. A super-frame consists of sixteen equal-length slots, which can be further divided into an active part and an inactive part and may be used to enter power saving mode [21].

Table 1: IEEE 802.15.4 Standard Specs [21]

Band	Frequency	Channels	Data Rate	Availability and Usage
868 MHz	868-868.6 MHz	1	20 Kbps	Most Europe Countries
915 MHz	902-923 MHz	10	40 Kbps	Americas, Australia and NZ
2.4 GHz	2.4-2.4835 GHz	16	250 Kbps	Most Countries Worldwide

Note: For the purposes of the 802.15.4 standard, the IEEE considers the 868 MHz and 915 MHz bands to be a single, contiguous band and vendors that choose to support either band must support both [21]. The IEEE 802.15.4 Standard defines a total of 27 channels, numbered 0 to 26. Channel 0 is in the 868 MHz band with a center frequency of 868.3 MHz Channels 1 through 10 are in the 915 MHz band, with a

channel spacing of 2 MHz, and channel 11 having a center frequency of 906 MHz Channels 11 through 26 are in the 2.4 GHz band with 5 MHz channel spacing and channel 11 (2.405 GHz) as the center frequency [22].

#### A. Communication Channel

A wireless channel is an open communication medium that can be accessed by everyone within its signal range. However, this openness is a great benefit as it reduces infrastructure costs, but it makes security a very important issue as access to the communication channel. These issues are explained in below:

- **Unreliable Transfer** - Unlike fixed wired network channels, the wireless channel is inherently unreliable. It is susceptible to interference, channel error, congestion and devices moving in and out of range. These conditions could be permanent or temporary and can lead to damaged or dropped packets on the wireless network. If a wireless protocol does not provide error handling, it can lead to incoherent communication or loss of critical security packets, leading to sensor nodes that are unable to communicate securely.
- **Conflicts** - WSN is susceptible to packet collision in the wireless channel. This occurs when two or more sensor nodes within each range of each other transmit packets at the same time. This is a major problem in a highly dense WSN. In such scenarios, the wireless protocol has to provide a mechanism for handling traffic collision/conflicts as retransmission of packets will use more of the limited sensor node resources [8].
- **Latency** - Multi-hop routing, network congestion and node processing can lead to greater latency in the network. This latency can cause synchronization issues among sensor nodes that impact WSN security such as event reporting and cryptographic key distribution [9].

#### B. Device Limitations

WSNs have additional constraints that hinder the usage of traditional network security features. Current WSN sensor nodes are low powered devices with very limited resources. Therefore, current sensor nodes cannot support complicated and computationally heavy applications such as the security algorithms that are used in devices. In fact, implementing strong security algorithms is a trade-off between security and performance.

- **Processing Power** - Alongside the limitations such sensor nodes have on power consumption, they are also naturally equipped with limited processors. This restricts the complexity of the functions that each node can perform which includes data processing, encoding and encryption [10].
- **Memory and Storage Space** - A sensor node has limited memory and storage space, thus communication packets need to be small and simple. On average, most sensor nodes have 8-16bit CPUs with 10-64K of program memory and 512K-4MB of flash storage [10]. With such

limited resources, the software codebase used in such devices has to be very small. Thus, any security and communication algorithms have to be very small [10].

- **Power** - Energy usage is another major constraint to security in WSN. These sensor nodes are physically small and autonomous, the power source is usually a battery. The deployment of many such devices would make replacing these batteries difficult and increase maintenance costs. Therefore, the batteries installed in these sensor nodes have to last for a long time (many years instead of days or hours). It should be mentioned that implementing security schema in these sensors require more processing overhead which increases energy usage and may reduce the overall performance [10].

### C. Unattended Operation

One of the major benefits of WSNs is the ability to place sensor nodes in an environment without any supervision. This can provide security drawbacks to the network and backend system if the sensor nodes are located in harsh environments or in an unsecured manner while being readily accessible to people.

- **Exposure to Environment/Physical Attacks** - Sensor nodes may be deployed in an environment open to physical attacks and bad weather. For example, sensor nodes in the ocean might be eaten by fish or washed away during storms. Since these nodes are in the open, they can also be attacked or stolen by malicious persons.
- **Remote Management** - One benefit of WSN is its ability to be managed remotely. This enables sensor nodes to be placed in hazardous or inaccessible environments. This requires security to protect the WSN, devices and the information that is relayed to the control center. Security is also required to protect the control center servers since the WSN might be used by attackers to gain access to the backend server systems.
- **No Fixed Infrastructure** - WSNs can self-organize to form a distributed network without a central management point among the sensor nodes. This provides a robust and dynamic communication network for information to be passed from the sensor nodes to the backend servers. However, if the WSN is improperly designed, it will make the network organization difficult, inefficient, and fragile. The peer-to-peer communication among the sensor nodes need to incorporate security features that will disallow malicious users to access or disrupt the sensor network.

## III. WIRELESS NETWORK SECURITY REQUIREMENTS

WSNs form a significant part of the picture as the oil and gas industry moves into the wireless domain. In a commercial environment, such networks must operate in a secure manner. A security breach may cause significant production, safety and privacy issues. The following sections define the typical wireless network security requirements in an industrial setting.

### A. Access Control

Access control prevents the participation of unauthorized parties in the network. Legitimate nodes are able to detect and reject messages from unauthorized nodes.

### B. Data Confidentiality

Data confidentiality is one of the most basic security requirements. The standard approach for providing confidentiality is to encrypt the data with a secret key that can only be decrypted by the receiving node [7]. Encryption should prevent message recovery, as well as preventing adversaries from learning any information about the messages. This type of encryption is known as semantic security. One implication of semantic security is that encrypting the same plaintext two times should give two different ciphertexts. If the encryption process is identical for two invocations on the same message, then semantic security is clearly violated and the resulting ciphertexts are identical [11]. A common technique for achieving semantic security is to use a unique nonce for each invocation of the encryption algorithm. A nonce can be thought of as a side input to the encryption algorithm. The main purpose of a nonce is to add variation to the encryption process when there is little variation in the set of messages. Since the receiver must use the nonce to decrypt messages, the security of most encryption schemes does not rely on nonces being secret. Nonces are typically sent in the clear and are included in the same packet with the encrypted data.

In sensor networks, the confidentiality relates to the following [11]:

- A sensor network should not leak sensor readings to its neighbors, as it may contain sensitive data.
- A sensor network requires a secure channel to transmit sensitive data, such as key distributions.
- Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.

### C. Data Authenticity

Another major security concern is the authenticity of the source providing the data received from the WSN. An attacker can feed false information by masquerading as a legitimate sensor node and transmitting this data to the receiver. So the receiver needs to ensure that the data used originates from the correct source and has not been tampered with. Besides information processing, authentication is required for administrative tasks over the network, such as network reprogramming or controlling of the sensor node duty cycle [11]. Thus, message authentication is important for networked devices to positively identify the source of the communication. The most common method of providing packet authentication is through a Message Authentication Code (MAC). When a sender and receiver share a secret key, the sender can compute the MAC of the data to be sent and embed it in the packet. When the destination node receives a packet with a correct

MAC, it knows the source of the packet and that the packet has not been modified in transit [7].

#### D. Data Integrity

The data transmitted by a legitimate source might be modified or corrupted in transit. Attackers can introduce interference, such as add or delete some bits, to transmitted packets. A malicious routing node can change important data in packets before forwarding them. The integrity of data ensures that the received data is complete and correct. The recipient of a message which has been tampered with whilst in transit will be able to detect that this has occurred. Message authentication and integrity will be increased by including a MAC with each packet. Only authorized senders and receivers will be able to view the message as they share a secret cryptographic key which computes MAC. Authentication methods like MAC are used so that the receiver can easily know if a packet has been tampered with or is corrupted. Due to the unreliable nature of the wireless medium, packet loss or damage can occur without the presence of a malicious node in the network. Data integrity ensures that any received data has not been altered in transit [11].

#### E. Data Freshness

Legitimate messages being sent between two nodes may at times be monitored by unauthorized parties which will later be replayed, and due to the fact that they are originating from an authorized sender, with a valid Message Authentication Code Message, they will be accepted. WSNs need to ensure the freshness of each message. For example, the data is recent, and that no old messages have been replayed. This requirement is important for key management since shared keys need to be changed over time. However, it takes time for new shared keys to be propagated to the entire network. In this case, it is easy for an attacker to use a replay attack, which protects against using sequential numbering, to join the network with an older key. The use of a nonce, or another time-related counter, can be added into the packet to ensure data freshness. These counters are reset every time a new key is created [11]. Besides security, data freshness is important in certain situations, such as using sensor nodes to monitor mission critical operations. Any disruption or delay to the data received can have a negative impact to the operations or safety of the personnel/equipment.

#### F. Availability

Traditional encryption algorithms used in fixed wired networking must be adapted to low powered sensor nodes to maximize the usage of the nodes in a WSN. Some adaptations modify the encryption/decryption code to reuse as much code as possible while others try to make use of additional communication to achieve the same goal. Some adaptations force strict limitations on the data access, or propose an unsuitable scheme (such as a central point scheme) in order to simplify the algorithm. However, all these approaches weaken the availability of a sensor node and WSN for the following reasons[11]:

Additional computation consumes additional energy. If no more energy exists, the data will no longer be available and increases the chance of incurring a communication conflict.

A single point failure will be introduced in the central point scheme. This greatly threatens the availability of the network.

#### G. Secure Localization

In some cases, the utility of a WSN relies on its ability to accurately locate each sensor node in the network. A sensor node that is placed in a particular location to monitor its environment will need to relay its readings along with the location data for it to be truly useful. Unfortunately, an attacker can easily manipulate non-secured location data by reporting false signal strengths or replaying signals.

Alongside the security requirements that were outlined in this section, there exist a number of threats on these concepts. It is required that WSNs employ strict security schemes to protect against the many WSN attacks that have been documented in the following section.

## IV. ATTACKS ON WIRELESS NETWORKS

WSNs must implement strict encryption, transmitter authentication and data consistency validation with constraints on energy, memory, computation and network bandwidth. The following sections define a cross section of the typical attacks that may affect WSN installations.

### A. Generic Wireless Network Attacks

In general, wireless networks are susceptible to various security issues. In such sensitive commercial environments it is essential that security is assured from generic attacks such as:

- **Accidental Association** - Refers to unintentional access to wireless networks where foreign computers or devices may inadvertently connect to an overlapping neighboring wireless network without being aware that this is even happening. This still represents a significant security breach in proprietary network and may expose sensitive company systems and data [1].
- **Malicious Association** - Is created when access to a network is obtained by hackers. This is typically performed through weak security measures and protocol loopholes. It may also be possible to lure computers to login to networks that impersonate the real thing by exploiting faults in the wireless protocol. By temporarily disrupting the response of a real network and simultaneously granting access to an impostor equivalent it is possible to involuntarily capture a user and transparently route all future communications through a central hacker point. This makes it possible to capture valid users, steal passwords and data, launch other attacks and install Trojans [1].
- **Man-in-the-Middle Attacks** – Man-in-the-Middle Attacks use the Malicious Association techniques to gain access to a network and its users and transparently monitor passing traffic. If data is unencrypted or is easy to

decipher then a hacker is given access to sensitive company information. A hacker may transparently listen to, remove and/or replace key network packets with others to provide false information [1].

- **Denial of Service** – A Denial-of-Service attack (DoS) attack occurs when a targeted access point or device is flooded with bogus protocol messages and data in an attempt to reduce or even suspend its responsiveness and ability to perform its regular functions. This is a very serious problem when wireless devices may be required to deliver time critical data. Jamming the wireless communication link utilizing dedicated jamming devices also falls into the Denial-of-Service category [16].
- **Network Injection** – A network injection attack makes use of access points that are exposed to non-filtered or broadcast network traffic, by introducing bogus network configuration commands that may affect routers, switches, and intelligent hubs. The network devices may crash, shutdown, restart or even require reprogramming.
- **Radio Interference** – As more and more wireless communication devices utilize the license free portions of the frequency spectrum, in particular the ISM bands, friendly coexistence between the different systems and technologies is of greatest importance.
- **Environment Tampering** – The adversary in principle can compromise the integrity of the sensor readings by tampering with the deployment area. For example, the adversary can place a magnet on top of a magnetometer, or temper with the temperature of the environment around temperature sensors. This is an effective attack against service integrity. The main drawback of this attack is the high risk of apprehension if the network is under some kind of surveillance [13].
- **Byzantine Attack** – Wireless sensor networks are vulnerable to Byzantine attacks in which a fraction of sensors are tampered. In this attack, the intruder can reprogram the compromised sensors and authenticate them and compromised sensors collaboratively send fictitious observations to the center. This attack eventually results in severe consequences as the network operation may seem to operate normal to the other nodes [14].

#### B. Specific Wireless Sensor Network (WSN) Attacks

Specific WSN attacks include any action that intentionally or unintentionally aims to cause any damage to the network. They can be divided according to their origin or their nature. An origin-based classification splits attacks into two categories, external and internal, whereas a nature-based classification splits them into passive attacks and active attacks.

#### C. External Attacks and Internal Attacks

Usually, a WSN is deployed and managed by one authority. All the nodes in the network can be seen as honest and cooperative entities, whereas attackers have no right to access the network. External attacks are those launched by a node that does not belong to the logical network, or is not allowed

to access to it. Such attacks are launched only from outside of the scope of the network. The impact of external attack is limited. If an attacker can obtain authorization to access the network, it becomes an internal attacker. In this case, the attacker can cause more severe damage because it is seen as a legitimate entity. Usually, an attacker can become an internal one by compromising a legitimate node or by deploying malicious nodes that can pass the network access control mechanism [3].

#### D. Passive Attacks

In a passive attack, the attacker's goal is to obtain information without being detected. Usually, the attacker remains quiet and eavesdrops on passing traffic. If it knows the communication protocols, the attacker can follow those protocols like normal sensor nodes. A passive attack is a continuous collection of information from one or multiple targets that might be used later when launching an active attack. By passively participating in the network, the attacker collects a large volume of traffic data and carries out analysis on the data such that some secret information can be extracted. It should be mentioned that due to the nature of the wireless communication medium which is widely shared, it is easier for an attacker to passively eavesdrop in this environment than in traditional wired environments [3].

- **Eavesdropping** - The confidentiality objective is required in sensors' environment to protect information travelling between the sensor nodes of the network or between the sensors and the base station from disclosure, since an adversary having the appropriate equipment may eavesdrop on the communication. By eavesdropping, the adversary could overhear critical information such as sensing data and routing information. Based on the sensitivity of the stolen data, an adversary may cause severe damage by using this data for many illegal purposes. By listening to the data, the adversary could easily discover the communication contents [12].
- **Traffic Analysis** - Traffic analysis attacks allow an adversary to deduce information about the network topology and the location of the base station by monitoring traffic transmission patterns. Once the topology of the network is known, the attacker can selectively target nodes to attack [12].

#### E. Active Attacks

In an active attack, the attacker exploits the security holes in the network protocol stack to launch various attacks such as packet modification, injection, or replaying. The impact of active attacks is more severe than passive attacks. However, additional anomalies can show evidence of malicious attacks because the attacker is actively involved in network communications [3].

Active attacks include almost all attacks launched by actively interacting with victims, such as: sleep deprivation torture, which targets the batteries; hijacking, in which the attacker takes control of a communication between two entities and masquerades as one of them; jamming, which causes channel

unavailability by overusing it, attacks against routing protocols that we will see in the next section, and so on. Most of these attacks result in a Denial of Service (DoS), which is degradation or a complete halt in communication between nodes.

- **Replay** - This attack happens when an adversary keeps messages and re-transmits the contents of those packets at a later time. Data freshness implies that the data is recent, and it ensures that an adversary has not replayed old messages [6].
- **Misbehavior** - Unauthorized behavior of an internal node that can result unintentionally in damage to other nodes. The aim of the node is not to launch an attack, but it may have other aims such as obtaining an unfair advantage compared with the other nodes. One may not correctly execute the MAC protocol, with the intent of getting higher bandwidth, or it may refuse to forward packets for others to save its resources, while using their resources and asking them to forward its own packets [15].

In addition, various security requirements on sensor networks are classified depend on those requirements, into three security levels:

- **Message-Based Level** - Similar with that in conventional networks, this level deals with data confidentiality, authentication, integrity and freshness. Symmetric key cryptography and message authentication codes are necessary security primitives to support information flow security. Also data freshness is necessarily required as lots of content-correlative information is transmitted on a sensor network during a specific time [12].
- **Node-Based Level** - Situations such as node compromise or capture are investigated on this level. In case that a node is compromised, loaded secret information may be improperly used by adversaries [12].
- **Network-Based Level** - On this level, more network-related issues are addressed, as well as security itself. A major benefit of sensor networks is that they perform in-network processing to reduce large streams of raw data into useful aggregated information. Protecting it is critical. The security issue becomes more challenging when discussed seriously in specific network environments. Firstly, securing a single sensor is completely different from securing the entire network, thus the network-based anti-intrusion abilities have to be estimated. Secondly, network parameters such as routing, node's energy consumption, signal range, network density and so on, should be discussed correlatively. Moreover, the scalability issue is also important with respect to the redeployment of node addition and revocation [12].

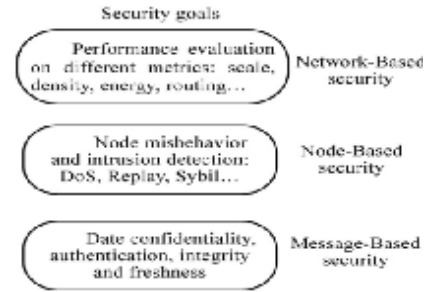


Figure 1: WSN Security Concerns [12]

## V. DENIAL OF SERVICE ATTACKS

A Denial-of-Service (DoS) attack is an active attack that occurs when a targeted access point or device is flooded with data in an attempt to reduce or even suspend its responsiveness and ability to perform its regular functions. This is a very serious problem when wireless devices may be required to deliver time critical data. A DoS attack is generally defined as an event that can diminish or eliminate a network's capacity to perform its expected function. Sensor networks are usually divided into layers, and this layered architecture makes WSNs vulnerable to DoS attacks as DoS attacks may occur in any layer of a sensor network [16]. Lists of these attacks are identified below:

### A. Physical Layer Attacks

- **Jamming** – This type of attack interferes with (disrupts) the radio frequencies a WSN uses. A typical jamming attack can disrupt the entire WSN with a few randomly distributed jamming nodes. This type of attack is simple to implement and is very effective against single frequency networks. There are two types of jamming, constant jamming and sporadic jamming. Both these attacks can cause major disruptions to networks, particularly if the communication is sensitive or time critical. A sensor node can easily distinguish jamming from other natural causes of communication disruption by determining that constant energy, not lack of response, impedes communication. If a sensor node does not know it is being jammed, it will increase its transmitter power, thus depleting its resources faster [17].

### B. Link Layer Attacks

- **Collision** – An attacker can induce a collision in the WSN to create a costly exponential back-off in some MAC protocols. The energy spent by an attacker is minute compared to the amount of energy that will be expanded by the WSN. The use of error-correcting codes can minimize collision errors, but they are very simple so as to reduce processing costs. A malicious node can

cause more collisions to occur than the error correcting codes can handle in a WSN [18].

- **Resource Exhaustion** - A naive link-layer protocol may attempt repeated retransmissions due to collision. This will lead to exhaustion of battery resources in sensor nodes in the WSN as well as delays in transmissions. Random back-offs only decrease the probability of inadvertent collision and would be ineffective at preventing this kind of attack. Time-division multiplexing gives each node a slot for transmission without requiring arbitration for each frame. A malicious node could constantly request for channel access or elicit a response from sensor nodes in the WSN. Although, constant transmission would exhaust the energy resources of both malicious nodes and targeted sensor nodes, the lifespan of the WSN would reduce significantly [18].
- **Unfairness** - Intermittent application of these attacks or abusing a cooperative MAC-layer priority scheme can cause unfairness, a weaker form of DoS. This threat may not entirely prevent legitimate access to the channel, but it could degrade service. For example, by causing users of a real-time MAC protocol to miss their deadlines [18].

#### C. Network Layer Attacks

- **Wormhole Attack** - A wormhole is a low latency link between two portions of the network over which an attacker replays network messages. This link may either be a single node forwarding messages between two adjacent but otherwise non-neighboring nodes or a pair of nodes in different parts of the network with the ability to communicate between each other. The latter of these cases is closely related to the sinkhole attack as an attacking node near the base station can provide a one hop link to that base station via the other attacking node in a distant part of the network [16]. A wormhole attack is one in which a malicious node eavesdrops on a packet or series of packets, tunnels them through the sensor network to another malicious node, and then replays the packets. This can be done to misrepresent the distance between the two colluding nodes. It can also be used to more generally disrupt the routing protocol by misleading the neighbor discovery process [19].
- **Rushing Attack** - Most on-demand routing protocols rely on broadcast ROUTE-REQUESTs to find routes. In a rushing attack, an attacker can forward ROUTE-REQUESTs more quickly than legitimate nodes so that it is more possible that the chosen route includes the adversary. If not overcome, the rushing attack can prevent secure on-demand routing protocols to find routes longer than two-hops [20]. The widely used duplicate suppression technique, when a node only considers the first copy of a given control packets and drops any further copies, makes the rushing attack possible.

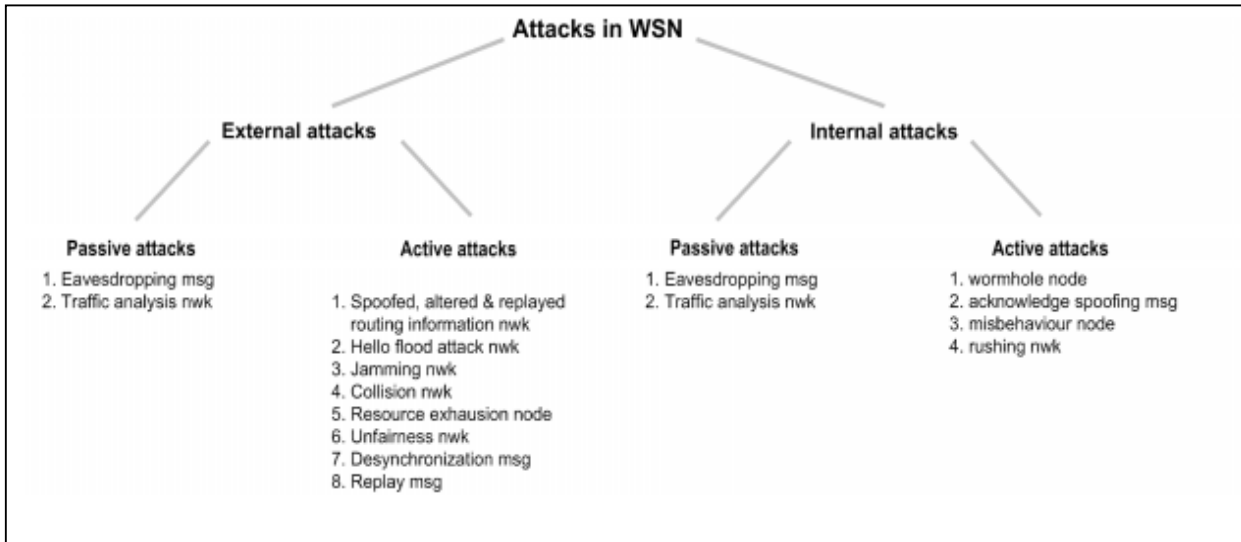
- **Acknowledgment Spoofing** - Routing algorithms used in sensor networks sometimes require acknowledgments to be used. An attacking node can spoof the acknowledgments of overheard packets destined for neighboring nodes in order to provide false information to those neighboring nodes. For instance, it can claim that false information like a node is alive when in fact it is dead [16].
- **Spoofed, Altered, or Replayed Routing Information** - The most direct attack against a routing protocol in any network is to target the routing information itself while it is being exchanged between nodes. An attacker may spoof, alter, or replay routing information in order to disrupt traffic in the network. These disruptions include the creation of routing loops, attracting or repelling network traffic from selecting nodes, extending and shortening source routes, generating fake error messages, partitioning the network, and increasing end-to-end latency [16].

#### D. Transport Layer Attacks

- **HELLO Flood Attack** - An attacker sends or replays a routing protocol's HELLO packets from one node to another with more energy. This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes that are isolated in a large area within a WSN. As a result, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker.
- **Desynchronization** - An existing connection between two end points can be disrupted by desynchronization. In this attack, the adversary repeatedly forges messages to one or both end points. These messages carry sequence numbers or control flags that cause the end points to request retransmission of missed frames. If the adversary can maintain proper timing, it can prevent the end points from exchanging any useful information, causing them to waste energy in an endless synchronization-recovery protocol [18].

In general, all attacks are classified in Figure 2 in below. The figure shows attacks may happen in Oil and Gas rigs, which WSNs devices installed.





Msg = message-based attacks

Node = node-based attacks

Nwk = network-based attacks

Figure 2: Taxonomy of WSN attacks

## VI. CONCLUSION

Wireless Sensor Networks (WSNs) are generating significant interest as the oil and gas industry moves into the wireless domain. Such technology has the potential to be beneficial in many regards. Eliminating the need for cables can contribute to reduced installation and operating costs; it enables installations in remote areas, and allows for cost-efficient, temporary and mobile systems.

A level of security risk must be accepted with WSNs. The key to a productive environment with WSNs is one where addressable security issues are dealt with and others are managed and accepted. In the oil and gas industry specific configurations, this may mean that WSN devices are not ultimately relied on for critical tasks, they are used only as a form of redundancy and appropriate contingency, management and mitigation plans exist if their function is interrupted or modified.

## VII. REFERENCES

- [1] "WSN Security Project Overview and Scope-Internal Statoil Document" Statoil 2009.
- [2] S. Avancha, J. Undercoffer, A. Joshi, and J. Pinkston, "Security for Wireless Sensor Networks," in *Wireless Sensor Networks*, 2004, pp. 253-275.
- [3] Y. Zhou, Y. Fang, and Y. Zhang, "Securing Wireless Sensor Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 10, pp. 6-28, 2008.
- [4] J. Zhang and V. Varadharajan, "A New Security Scheme for Wireless Sensor Networks," in *IEEE Global Telecommunications Conference*, 2008, pp. 1-5.
- [5] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. Culler, "SPINS: security protocols for sensor networks," *Wirel. Netw.*, vol. 8, pp. 521-534, 2002.
- [6] M. Saraogi, "Security in wireless sensor networks," Department of Computer Science, University of Tennessee, Knoxville 2005.
- [7] J. Lopez and J. Zhou, *Wireless Sensor Network Security* vol. 1: IOS Press, Apr. 2008.
- [8] I. F. Akyildiz, S. Weilian, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *Communications Magazine, IEEE*, vol. 40, pp. 102-114, 2002.
- [9] J. A. Stankovic, T. E. Abdelzaher, C. Lu, L. Sha, and J. C. Hou, "Real-time communication and coordination in embedded sensor networks," *Proceedings of the IEEE*, vol. 91, pp. 1002-1022, 2003.
- [10] M. Gaurav, D. Peter, G. Deepak, and S. Prashant, "Capsule: an energy-optimized object storage system for memory-constrained sensor devices," in *Proceedings of the 4th international conference on Embedded networked sensor systems* Boulder, Colorado, USA: ACM, 2006.
- [11] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless Sensor Network Security: A Survey," 2006.
- [12] P. Li, Y. Lin, and W. Zeng, "Search on Security in Sensor Networks," *Journal of Software*, vol. 17, pp. 2577-2588, Dec. 2006.
- [13] A. C. Alvaro, R. Tanya, and S. Shankar, "Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems," *Ad Hoc Netw.*, vol. 7, pp. 1434-1447, 2009.
- [14] H. Redwan and K. Ki-Hyung, "Survey of Security Requirements, Attacks and Network Integration in Wireless Mesh Networks," in *Frontier of Computer Science and*

*Technology, 2008. FCST '08. Japan-China Joint Workshop on, 2008, pp. 3-9.*

[15] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *2005 IEEE Symposium on Security and Privacy, 2005*, pp. 49-63.

[16] W. Yong, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *Communications Surveys & Tutorials, IEEE*, vol. 8, pp. 2-23, 2006.

[17] A. D. Wood and J. A. Stankovic, "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks."

[18] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, pp. 54-62, 2002.

[19] R. Sandro and H. David, "A survey of key management for secure group communication," *ACM Comput. Surv.*, vol. 35, pp. 309-329, 2003.

[20] H. Yih-Chun, P. Adrian, and B. J. David, "Rushing attacks and defense in wireless ad hoc network routing protocols," in *Proceedings of the 2nd ACM workshop on Wireless security* San Diego, CA, USA: ACM, 2003.

[21] K. Masica, "Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments," Lawrence Livermore National Laboratory, April 2007.

[22] T.-K. Nguyen, V.-H. Le, Q.-H. Duong, S.-K. Han, S.-G. Lee, N.-S. Seong, N.-S. Kim, and C.-S. Pyo, "Low-Power Direct Conversion Transceiver for 915 MHz Band IEEE 802.15.4b Standard Based on 0.18  $\mu\text{m}$  CMOS Technology," *ETRI Journal*, vol. 30, pp. 33-46, February 2008.

# Comparison of Industrial WSN Standards

Pedram Radmand<sup>1</sup>, Alex Talevski<sup>1</sup>, Stig Petersen<sup>2</sup> and Simon Carlsen<sup>3</sup>

<sup>1</sup>DEBII, Curtin University of Technology, Perth, Australia  
Pedram.Radmand@student.curtin.edu.au, A.Talevski@curtin.edu.au

<sup>2</sup>SINTEF ICT, Trondheim, Norway  
stig.petersen@sintef.no

<sup>3</sup>Statoil ASA, Trondheim, Norway  
SCAR@StatoilHydro.com

**Abstract**— This paper presents a comparison of the current Wireless Sensor Network (WSN) standards that are available for industrial applications. Zigbee, WirelessHART and the recently released ISA.100 are carefully considered. The comparison outlines how WirelessHART and ISA.100 address some of the ZigBee weaknesses in the oil and gas domain.

## I. INTRODUCTION

An accelerating energy crisis in the oil and gas industry is driving the development and investment in Wireless Sensor Network (WSN) technologies. WSN is a key investment area across the whole oil and gas supply chain including refineries, petrochemical plants, pipelines, exploration, production, and transportation. By providing secure and reliable two-way wireless communications, WSN enables automation and control solutions that are not feasible with wired systems to improve production, operational efficiency, safety, and asset management[1].

Wireless Sensor Networks (WSNs) comprise of a large number of spatially distributed autonomous devices that may collect data using a wireless medium. They may be used to cooperatively control and monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations [2]. WSNs exhibit several unique properties as compared to their wired counterparts such as large scale of deployment, mobility of nodes, temporary installations, redundancy, and dynamic network topologies. However, each sensor node has constraints on operational environment, energy, memory, computation speed and bandwidth [2].

International standards for wireless devices and networks, such as ZigBee, WirelessHART and ISA100.11a use stacks to provide a layered and abstract description of the network protocol design. Each layer in the stack is a collection of related functions, and each layer is responsible for providing services to the layer above it, while receiving services from the layer below it [3].

## II. INDUSTRIAL REQUIREMENTS

As a result of the strict regulations associated with the installation of wired sensors on oil and gas platforms, the introduction of such devices is complicated, time-consuming and expensive. The primary use cases for WSN in the oil and gas industries are associated with the integration of new sensors and strategies within existing end-of-lifecycle platforms while reducing complexity, time and costs. We have developed the following requirements for the industrial application of WSNs.

### A. Reliability

Reliability is a measure of the percentage of accurate data which reaches its destination. This usually is the gateway. Reliability is often used in conjunction with stability. It represents the percentage of successfully transmitted data packets in the network on an individual link basis (the measurement of loss packet). The transfer of data in IEEE 802.15.4 is acknowledge-based (ACK). The transmitter expects to receive an ACK from the receiver for each transmitted packet. The packet is transmitted, if the ACK is not received within a certain time. It is often possible to achieve 100% reliability with no lost packets along with 90% stability through the use of packet retransmission [4].

### B. Latency

Latency is a measure of time delay. It is defined as the time it takes from when a data packet is transmitted from the originating sensor to reach its final destination. In fact, there are several factors which effect on latency such as the link quality, which commonly relates to the signal-to-noise ratio in the RF (Radio Frequency) domain. A poor link increases the number of retransmissions and latency. Also, hop-count is another factor which increases latency.

In an IEEE 802.15.4-based full mesh sensor network every sensor is defined as a (FFD) full-function device. For instance, each sensor can work as a sensor unit and a routing device to forward from adjacent sensors toward the gateway [5].

### C. Sensor Data Update Rates

As the update rate of the sensor data affects power consumption, a trade-off between update rate and sensor battery life is required. For example, the update rate for temperature data may be 30 seconds for temperature data [5].

### D. Wireless Transmission Range

All flow lines on the process deck should be within radio range of one wireless gateway. According to Statoil, studying the proposed individual placements of the sensors showed a radio range of approximately 25 meters is required[5].

### E. Power Consumption

There are many factors which affect the power consumption of a wireless sensor node:

- **Update Rate:** The number of transmissions per time unit increases the rate of power consumption.
- **Routing Activity:** A sensor node which transmits more packets consumes more energy due to forwarding packets from remote sensors [5].
- **Link Quality:** Packet transmission in the network is ACK-based. Therefore, a poor link quality, which needs more retransmission, increases the power consumption.

Low power consumption is required to lengthen the intervals between battery replacements as much as possible. The general requirement is a battery life-time of five years at a once per minute update rate [5].

### F. Integration with PCDA System

To achieve efficient oil rig application, real-time wireless control and monitoring of platform and well performance is required. These systems are integrated with the plants existing PCDA system. This system is able to integrate sensor data with existing graphical views and monitor the sensor node remaining battery life. Using these data streams production is optimised while minimising safety concerns.

## III. WIRELESS STANDARDS

Several standards are currently ratified for wireless sensor networks. In addition to the standards, there are also several non-standard, proprietary mechanisms and specifications around.

### A. Zigbee

The ZigBee Alliance is a group of companies that develop and maintain the ZigBee standard. ZigBee is a specification for a suite of high level communication protocols using low-power digital radios based on IEEE 802.15.4. The technology defined by the ZigBee specification is intended to be simpler and less expensive than other consumer WPANs, such as Bluetooth. ZigBee is targeted at radio-frequency (RF) applications that require a low data rate, long battery life, and secure networking. The low cost allows the technology to be widely deployed in wireless control and monitoring applications .

#### 1) Basic Features

ZigBee is a specification for the higher protocol layer, and builds upon the physical (PHY) and medium-access control (MAC) layers in the 802.15.4 specification.

The protocol is based on the ad-hoc on-demand distance vector (AODV) algorithm. This means, routing, discovery, and peer-to-peer communication is possible through this routing protocol [16]. Mesh networking topologies are supported. All nodes share the same channel and frequency hopping is not available [15].

There are two classes of network devices in ZigBee standards such as Full-Function Devices (FFD) and Reduced-Function Devices (RFD). FFD can form networks of any desired type such as mesh, star and hybrid whereas; RFD can only connect to a full function node [15].

ZigBee can operate in both beaconed and non-beaconed mode. In beaconed mode, the nodes are synchronized and the superframe is divided into 16 slots. There is an option to use up to seven of these as dedicated slots to specific nodes to increase determinism, which is called Guaranteed Slot Time (GTS) [15].

#### 2) Protocol Devices

- **Coordinator** - This device starts and controls the network. The coordinator stores information about the network, which includes acting as a Trust Centre and being the repository for security keys [22] .
- **Router** - These devices extend network area coverage, dynamically route around obstacles, and provide backup routes in case of network congestion or device failure. They can connect to the coordinator and other routers, and also support child devices [22] .
- **End Devices** - These devices can transmit or receive a message, but cannot perform any routing operations. They must be connected to either the coordinator or a router, and do not support child devices [22] .

#### 3) Security

Support for authentication, integrity and encryptions are available, but security is not mandatory. ZigBee makes use of the security mechanisms in 802.15.4; Counter with CBC-MAC (CCM) with AES-128 encryption along with the option to employ encryption-only or integrity-only. However, MAC layer security is not explicitly addressed through the 802.15.4 [17]. Three key types are applied in Zigbee security mechanism: Master key, Link key and Network key. The master key is necessary to join the network. The link key is used for end-to-end encryption and provides the highest level of security at the price of higher storage requirements.

The network key is shared between all devices, and provides a lower level of security. The Network key brings the benefit of reduced storage requirements in devices. All keys can be set in trust centre or coordinator. In fact, the trust centre can control the joining of new devices and periodically update the network key [17]. It should be mentioned that Replay

attacks is protected by using sequential numbering techniques [15].

### B. *WirelessHART*

WirelessHART is a mesh networking technology operating in the 2.4GHz ISM radio band. It utilizes IEEE 802.15.4 compatible DSSS radios with channel hopping on a packet by packet basis. WirelessHART is backward compatible with core HART technology .

Communication is performed using Time Division Multiple Access (TDMA) technology to arbitrate and coordinate communications between network devices. The TDMA Data Link Layer establishes links specifying the timeslot and frequency to be used for communication between devices [18]. These links are organized into superframe that periodically repeats to support both cyclic and acyclic communication traffic. A link may be dedicated or shared to allow elastic utilization of communications bandwidth to assure process data with minimal latency.

#### 1) *Basic Features*

WirelessHART coexists in the shared 2.4GHz ISM band: Frequency Hopping Spread Spectrum (FHSS), which allows WirelessHART to hop across the 16 channels that are defined in the IEEE802.15.4 standard. CCA (Clear Channel Assessment) is an optional feature in WirelessHART and can be performed before transmitting a message [18]. Moreover, WirelessHART has another feature called transmit power. This feature disallows the use of certain channels, called Blacklisting. These features ensure WirelessHART does not interfere with other co-existing wireless systems, which have real-time constraints [15].

All WirelessHART devices have routing capability and can be treated equally in terms of networking capability, installation, formation, and expansion [15].

There are two different routing protocols in WirelessHART such as Graph routing and Source routing. Graph routing uses pre-determined paths to route a message from a source to a destination device.

Source routing employs ad-hoc created routes for the messages without providing any path diversity. This routing protocol is applied for network diagnostics, and not process related messages [19].

#### 2) *Protocol Devices*

The following are key components of WirelessHART;

- **Gateway** - Provides the connection to the host network. WirelessHART and the main host are interfaced using Modbus – Profibus – Ethernet. The Gateway also provides the network and security manager [20].
- **Network Manager** - Builds and maintains the mesh network. It identifies the best paths and manages distribution of slot time access (WirelessHART divides each second into 10msec slots) Slot access depends upon the required process value refresh rate and other access [20] .

- **Security Manager** - Distributes security encryption keys. It also holds the list of authorized devices to join the network [20] .

The Process includes measuring devices – the HART-enabled instrumentation.

- **Repeater** - Routes WirelessHART messages but may have no process connection of its own. Its main use would be to extend the range of a WirelessHART network. All instruments in a WirelessHART network have routing capability [21] .
- **Adapter** - Plugs into an existing HART-enabled instrument to pass the instrument data through a WirelessHART network to the host. The adapter could be located anywhere along the instrument 4-20mA cable; it could be battery powered or obtain its power from the 4-20Ma cable. Some adapters will be battery powered and use the same battery to power the instrument as well [21].
- **Terminal** - Used to join a new instrument to an existing WirelessHART network. The terminal has a connection to the gateway and then down to an instrument that can be used for diagnostics [21] .

#### 3) *Security*

Security is mandatory in WirelessHART. WirelessHART provides end-to-end and hop-to-hop security measures data encryption and message authentication on the Network and Data-link layers. AES-128 block cipher symmetric keys is used for the message authentication and encryption [15].

There are set of security key to ensure secure communication. A new device is provisioned by a join key before each device joins the network. The actual key generation and management are implemented by the Security manager and also Session and Network keys are provided by Network manager for further communication [15].

A Session key is used by the Network layer to authenticate the end-to-end communication between two devices. A Session key is applied for each pairwise communication.

The Data Link layer uses a Network key to authenticate messages on a one-hop basis [15].

### C. *ISA.100*

ISA-100 is the brainchild of the Instrumentation, Systems, and Automation Society (ISA). This standard aims to enable a single, integrated wireless infrastructure platform for plants and delivers a family of standards defining wireless systems for industrial automation and control applications [30]. The ISA 100 standard adheres to a comprehensive coexistence strategy, which provides “the ability of wireless networks to perform their tasks in an environment where there are other wireless networks that may or may not be based on the same standard”[31] .

#### 1) *Basic Features*

The architecture supports wireless systems that span the physical range from a single, small and isolated network; the

network may include many thousands of devices and multiple networks that can cover a multi-square-km plant [30].

The protocols in ISA.100 have capabilities to reserve for future use and version numbers in headers that allow future revisions to offer additional or enhanced functionality [30].

ISA.100 standard supports channel hopping to avoid any interference from other RF devices operating in the same band and provides the robustness to mitigate multipath interference. Moreover, this standard facilitates coexistence with other RF systems along with the use of adaptive channel hopping to detect occupied channels and/or those with poor performance [30].

Like WirelessHART, this standard, defines TDMA mechanism, which allows a device to access the RF medium without having to wait for other devices [30].

ISA.100 is fully redundant and self-healing and supports end-to-end network reliability [30].

This standard differs from other standards and the network layer uses header formats to be compatible with the IETF (Internet Engineering Task Forces) 6LoWPAN standard to facilitate potential use of 6LoWPAN networks as a backbone. It should be mentioned that by using this standard, the headers compatible with 6LoWPAN does need to be based on the Internet Protocol (IP).

Furthermore, the use of header formats based on 6LoWPAN and IP does not imply that a network based on this standard is open to internet hacking; in fact, networks based on this standard, devices will typically not even be connected to the Internet [30].

## 2) Security

The security services in ISA 100 are selected by policy. The policy is distributed with each cryptographic material, permitting focused policy application. Since a single key is used at a time at the Data Link, except for a brief period of the key handover, the entire sub-network is subject to the same policies at the Data Link [23]. The security manager controls the policies for all the cryptographic materials it generates.

One of the most important factors in the ISA 100 standard is to provide security mechanisms for Single Security System Management for the automation industry. ISA 100 provides simple, flexible, and scalable security that addresses major industrial threats by leveraging 802.15.4-2006 security [24].

Security is a major design facet of ISA100.11a that considers the entire WSN life cycle that includes configuration, operation and maintenance. Security is considered throughout the whole system not only at the PHY layer or MAC sub-layer. This standard allows for reduced costs and quicker implementations [24].

Types of keys using in ISA100 are both symmetrical and asymmetrical key variants. Session keys have a limited lifetime and are updated periodically, which is initiated by a device, to ensure that the session is kept alive. The key update process may be initiated by a device, although it should be pushed from the security manager between the soft and hard lifetime of a session key [25].

## IV. COMPARISON OF WIRELESS SENSOR STANDARD

ZigbeePRO and WirelessHART represent proven industry WSN technologies. However, ISA100 is an emerging technology which promises many new features. This section presents a comparison of these standards from the perspective of basic features and security.

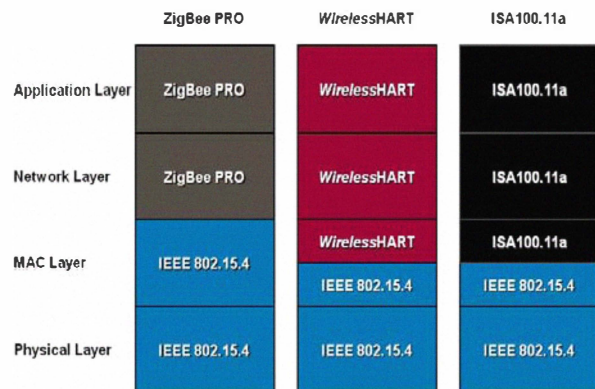


FIGURE 1: OVERALL SCHEMA OF WIRELESS STANDARDS [34].

There are some similarities and dissimilarities between WSN standards. All standards are based on IEEE 802.15.4 standards and the same frequency, which is 2.4 GHz. The WirelessHART, like ISA 100, supports mesh, star and combination of mesh and star topology, while Zigbee supports mesh, star and tree topologies. Three standards follow common objectives, such as: interoperability with other communication systems, scalability, energy-saving, communication reliability, compatibility with existing industrial devices, and security [32].

In the industrial market, the International Society of Automation's new ISA100a wireless standard is going to be a threat to ZigBee's future. ISA 100 is able to communicate simultaneously with most popular wired protocols and it can be easily integrated with other wired protocols while Zigbee doesn't support wired protocols. Furthermore, like WirelessHART, the ISA 100 standard incorporates several strategies that are used simultaneously to optimize coexistence with other users of the 2.4 GHz radio spectrum [32].

Like WirelessHART, ISA100 is based on the PHY layer specified in IEEE 802.15.4 but it specifies new Data-link (including MAC), Network, Transport, and Application layers, whereas ZigBee is a specification for the higher protocol layers only. It builds upon the Physical (PHY) and Medium-Access Control (MAC) layers in the 802.15.4 specification [15].

The Application Sub-Layer in ISA 100a is necessary. This promotes interoperability and it is a unique feature of the ISA100 specification that provides a set of common functions available to all applications. The Application Sub-Layer in ISA100a allows different applications in the Application Layer to communicate with each other in different stack layers through a common interface [33]. Table 1 illustrates the summary of features of these three standards:

TABLE 1 : WIRELESS SENSOR NETWORK STANDARDS COMPARISON.

Feature Set	Zigbee PRO	WirelessHART	ISA 100.11a
Topology	Mesh	Mesh, Star, Combined Mesh and Star	Mesh, Star, Combined Mesh and Star
Scalability	Yes	Yes	Yes
Radio Channel	CSMA-CD	TDMA	TDMA/CSMA
RF Channel Change	Yes	Yes	Yes
High Security	Yes	Yes	Yes
Keys	Symmetric	Symmetric	Symmetric/Asymmetric
Interface Control/ Noise	Yes	Yes	Yes
Energy Saving	Yes	Yes	Yes
Interoperability to other systems	Yes	Yes	Yes
Application Context	Commercial	Industrial	Industrial
Reliability Determinism	No	Yes	Yes
Latency determinism	No	Yes	Yes
Implementation	Easy	Challenging	Challenging

Most standards include protection against jamming and Denial of Service attacks through the use of frequency hopping techniques. As it is mentioned before, all protocols provide secure communication channels to assure the confidentiality, integrity, and authentication of data. However, it is still possible to include a malicious node inside the network to hinder the provisioning of services, but any effects of attacks perpetrated by malicious outsiders can be avoided and mitigated through the security schemas in these standards.

It should be mentioned that WirelessHART and ISA100 have tamper resistance package due to the critically of the environment. As any insider attacks can interrupt the functionality of the network, so the protocols should incorporate with some lightweight security mechanism as well as support for self-healing and intrusion detection system would be significantly useful. WirelessHART already provides support for self-healing. Applying security schema and Public Key Cryptography (PKC) to establish the security infrastructure is a challenge in these standards, but that would be extremely useful for industry.

However, it should be mentioned that applying security schema is the only challenge in such network but network design and users and other factors such as existing connections between the context of the application, its security requirements, and the security mechanisms.

## V. CONCLUSION

This paper presented different wireless sensor standards such as Zigbee, WirelessHART and ISA.100, which is recently released industrial wireless network standard and is interesting for industrial applications. The comparison shows that WirelessHART and ISA.100 addressed many of the ZigBee weaknesses and also indicated that WirelessHART and ISA.100 are more suitable for industry applications. The ISA.100, like WirelessHART standard, specifies the communication stack, as well as the interfaces and responsibilities for the various devices comprising an ISA.100 network. Also, it should be mentioned that all the standards protect the communication channel against external attackers, and the refresh keys in the network is provided through specific mechanism.

## VI. REFERENCES

- [1] M. G. Hatler, D. Chi, Ch., "Wireless Sensor Networks for Oil & Gas." vol. 2010, 2008.
- [2] J. Zhang and V. Varadharajan, "A New Security Scheme for Wireless Sensor Networks," in *IEEE Global Telecommunications Conference*, 2008, pp. 1-5.
- [3] "WSN Security Project Overview and Scope-Internal Statoil Document" Statoil 2009.
- [4] International Electrotechnical Commission, "'IEC 60079- 4: Electrical apparatus for explosive gas atmospheres –Part 4: Method of test for ignition temperature," 1995.
- [5] S. S. Carlsen, A. Petersen, S. Doyle, P., "Using wireless sensor networks to enable increased oil recovery," in *ETFA 2008*, pp.:1039 - 1048.
- [6] T. S. Lennvall, S.; Hekland, F., "A comparison of WirelessHART and ZigBee for industrial applications," in *WFCS*, 2008, pp. 85 - 88
- [7] "Getting Started with ZigBee and IEEE 802.15.4," Daintree Networks 2008.
- [8] "HART Communication Foundation," <http://www.hartcomm.org/index.html>, 2007.
- [9] "ISA100: Wireless Systems for Industrial Automation-Developing a Reliable, Universal Family of Wireless Standards," ISA, Standard 2007.
- [10] "ISA100.11a Release 1 Status," ISA 2008.
- [11] K. Masica, "Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments," Lawrence Livermore National Laboratory, April 2007.
- [12] "IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)," IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003), pp. 0\_1-305, 2006.
- [13] "Looking Ahead: ISA100 Heads to China," ISA, Mar. 2008.
- [14] "ZigBee Alliance to Incorporate IETF IT into Wireless Network Standards." vol. 2009: IHS, May 10. 2009.
- [15] T. Lennvall, S. Svensson, and F. Hekland, "A comparison of WirelessHART and ZigBee for industrial applications," in *Factory Communication Systems*, 2008. WFCS 2008. IEEE International Workshop on, 2008, pp. 85-88.
- [16] S. Tian-Wen and Y. Chu-Sing, "A Connectivity Improving Mechanism for ZigBee Wireless Sensor Networks," in *Embedded and Ubiquitous Computing*, 2008. *EUC '08. IEEE/IFIP International Conference on*, 2008, pp. 495-500.
- [17] S. Jing and Z. Xiaofen, "Study of ZigBee Wireless Mesh Networks," in *Hybrid Intelligent Systems*, 2009. *HIS '09. Ninth International Conference on*, 2009, pp. 264-267.
- [18] D. Wenliang, D. Jing, Y. S. Han, C. Shigang, and P. K. Varshney, "A key management scheme for wireless sensor networks using

- deployment knowledge," in *INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies*, 2004, p. 597.
- [19] A. K. D. C. L. Jianping Song; Song Han; Mok, M.; Nixon, M., "WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control," in *Real-Time and Embedded Technology and Applications Symposium, 2008. RTAS '08. IEEE*, 2008, pp. 377 - 386.
- [20] "HART Communication Foundation," <http://www.hartcomm.org/index.html>, 2007.
- [21] "The Components of WirelessHART Technology ": HART Communication Foundation, 2009.
- [22] "Getting Started with ZigBee and IEEE 802.15.4," Daintree Networks, Feb 2008.
- [23] "ISA100: Wireless Systems for Industrial Automation-Developing a Reliable, Universal Family of Wireless Standards," ISA, Standard 2007.
- [24] "ISA-100.11a-2009 Wireless systems for industrial automation: Process control and related applications," ISA, 2009.
- [25] D. Sexton, "Understanding the unique nature of the universal family of ISA100 Wireless Standards," ISA Aug. 28 2007.
- [26] "IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)," *IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003)*, pp. 0\_1-305, 2006.
- [27] "Looking Ahead: ISA100 Heads to China," ISA, Mar. 2008.
- [28] "ZigBee Alliance to Incorporate IETF IT into Wireless Network Standards." vol. 2009: IHS, May 10. 2009.
- [29] L. E. Bassham, "The Keyed-Hash Message Authentication Code Validation System (HMACVS)," December 3, 2004.
- [30] "ISA100: Wireless Systems for Industrial Automation-Developing a Reliable, Universal Family of Wireless Standards," ISA, Standard 2007.
- [31] "ISA100.11a Release 1 Status," ISA 2008.
- [32] "ZigBee Alliance to Incorporate IETF IT into Wireless Network Standards." vol. 2009: IHS, May 10. 2009.
- [33] "Looking Ahead: ISA100 Heads to China," ISA, Mar. 2008.
- [34] K. Masica, "Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments," Lawrence Livermore National Laboratory, April 2007.



# ZigBee/ZigBee PRO security assessment based on compromised cryptographic keys

Pedram Radmand<sup>1</sup>, Marc Domingo<sup>2</sup>, Jaipal Singh<sup>1</sup>, Joan Arnedo<sup>2</sup>, Alex Talevski<sup>2</sup>, Stig Petersen<sup>3</sup>, Simon Carlsen<sup>4</sup>

<sup>1</sup>Digital Ecosystem and Business intelligence Institute, Curtin University of Technology, Perth, Australia

e-mail: pedram.radmand@postgrad.curtin.edu.au, {J.Singh, A.Talevski}@curtin.edu.au

<sup>2</sup>Estudis d'Informàtica, Multimèdia i Telecomunicació, UOC, Barcelona, Spain

e-mail: {mdomingopr, jarnedo}@uoc.edu

<sup>3</sup>SINTEF ICT, Trondheim, Norway

e-mail: stig.petersen@sintef.no

<sup>4</sup>Statoil ASA, Trondheim, Norway

e-mail: SCAR@StatoilHydro.com

**Abstract**—Sensor networks have many applications in monitoring and controlling of environmental properties such as sound, acceleration, vibration and temperature. Due to limited resources in computation capability, memory and energy, they are vulnerable to many kinds of attacks. The ZigBee specification [1], based on the 802.15.4 standard [2], defines a set of layers specifically suited to sensor networks. These layers support secure messaging using symmetric cryptographic. This paper presents two different ways for grabbing the cryptographic key in ZigBee: remote attack and physical attack. It also surveys and categorizes some additional attacks which can be performed on ZigBee networks: eavesdropping, spoofing, replay and DoS attacks at different layers. From this analysis, it is shown that some vulnerabilities still in the existing security schema in ZigBee technology.

## I. INTRODUCTION

Wireless Sensor Networks (WSNs) comprise of a large number of spatially distributed autonomous devices that may collect data using a wireless medium. They may be used to cooperatively control and monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion and pollutants, at different locations. WSNs exhibit several unique properties as compared to their wired counterparts, such as large scale of deployment, mobility of nodes, temporary installations, redundancy and dynamic network topologies. However, each sensor node has constraints on its operational environment, energy, memory, computation speed and available bandwidth [3].

WSNs are generating significant interest in the industry area and moving into the wireless domain. This technology has the potential to be beneficial in many fields, such as oil and gas, military and medicine. Since information security is a very important factor for these industries, any WSN application requires secure communications. Due to the absence of physical protection, security in WSNs is extremely important [3]. Unfortunately, WSNs, and indeed all other wireless networks, are inherently and ultimately insecure, since their availability can be selectively and strategically modified by manipulating the radio environment.

This paper presents a survey on the existing security schema in the 802.15.4/ZigBee specification [1], focusing on vulnerabilities in this technology. We categorize and provide a detailed description of the different kinds of attacks in the related literature and as well as explaining how they may be actually executed by taking advantage of the current ZigBee specification weaknesses.

This paper is organized as follows. Section II provides an overview of the 802.15.4/ZigBee specification security. Section III explains the security assessment of this technology, which may be divided in attacks which require key compromise and attacks which do not. Finally, Section IV exposes the summary and conclusions of this paper.

## II. ZIGBEE SECURITY FEATURES OVERVIEW

The ZigBee Alliance is a group of companies that develop and maintain the ZigBee standard. ZigBee is a specification for a suite of high level communication protocols built over IEEE 802.15.4. One important characteristic of ZigBee is that tries to be simpler and less expensive than other Wireless Personal Area Networks (WPAN) standards, such as Bluetooth and IrDA. The main focus of the ZigBee standard is applications that require low data rate, long battery life and security.

The main difference between ZigBee and other WPAN definitions is the kind of devices that can be deployed in the network, namely: Full Function Devices (FFD) and Reduced Function Device (RFD). An FFD can receive and send messages over the 802.15.4, whereas an RFD is usually a sensor which sleeps most of the time and only wakes up in order to send messages.

Being based on the IEEE 802.15.4 standard [4], ZigBee shares its low level layers specification, defined as the physical (PHY) and the Medium Access Control (MAC) layers. Basically, the former handles the bit rate and communication channel whereas the latter handles the access to the physical radio channel, manages the radio synchronization and provides

Option	Joiner required information	Description
1	No keys pre-configured	Master, Link or Network Key are transmitted unencrypted Over The Air (OTA)
2	Active Network Key	Since the device has joined the network, the active Network Key should not change.
3	Trust Center address and Link Key	The secure connection is built using the Link Key and the address between Trust Center and the End Device. Then the Network Key is sent securely from the Trust Center.
4	Trust Center Address and Master Key	The Link Key for the device is generated using the Master Key. The Network key is sent securely from the Trust Center

TABLE I  
TRUST CENTER AUTHENTICATION CONFIGURATION OPTIONS

a reliable link between two nodes. As far as security is concerned, ZigBee shares the basic capabilities defined in IEEE 802.15.4, which operate at the MAC layer [5]. Unfortunately, these capabilities are partially constrained by the diverse range of potential applications which must be supported. They basically consist of maintaining an access control list (ACL) and using the Advanced Encryption Standard (AES) [6] to protect frame transmissions. Furthermore, both services are only optional and the IEEE 802.15.4 standard does not include key management and device authentication schemes, relying on final security policies defined by the higher layers.

However, the 802.15.4/ZigBee specification defines some particular additional security capabilities to avoid potential vulnerabilities such as message interception, modification and fabrication, as well as interruption of communication. The last specification of ZigBee at this date, redacted in 2007, defines two special security modes: Standard Security and High Security. The former is used in ordinary applications, while the latter, which is implemented in ZigBee PRO, provides higher security mechanisms at a cost in the demand on device resources. A general overview of such security features in ZigBee follows. Nevertheless, a more detailed description may be found in [7].

1) *ZigBee Keys*: ZigBee devices establish secure communications over the network by protecting messages through using symmetric keys. It should mention that the communication in the Standard Security mode in ZigBee is secured through the Network Key, which is shared among all devices in the network, while the communication in High Security mode in ZigBee PRO is secured through employing three different keys: Link Key, Master Key, and Network Key. The Link Key is a 128 bit key that is shared between two nodes and is applied for securing unicast communications. The generation of the Link Keys is made using the Master Key, which is pre-installed at the factory, added by the final user in an out-of-band manner or sent from a Trust Center, a special device which other devices trust for the distribution of security keys. The Network Key is a 128 bit long key that is shared between devices in the network and is used to secure the broadcast communications.

2) *Key Exchange*: Symmetric-key Key Exchange (SKKE) is a new security mechanism in ZigBee PRO which is used to periodically update the Link Key. SKKE employs the Master

Key to initialize a secure exchange, increasing the system's security.

3) *Additional Security Layers*: ZigBee basically provides security services at three different layers, MAC, Network (NWK) and Application Support (APS), in contrast with vanilla IEEE 802.15.4. On one hand, the NWK layer routes frames to their destination and discovers and maintains the routing table. On the other hand, the APS layer acts as an extension of the Application (APP) layer, which provides services to users, defines the role of devices and manages data reassembly.

At the MAC layer, ZigBee provides additional security to single hop messages using the AES encryption algorithm.

At the NWK layer, the Link and Network Keys are used to also provide privacy using AES encryption. Additionally, data integrity is also provided using a Message Integrity Code (MIC) security schema.

Finally, the APS sublayer performs the security functions of the APP layer. This security function is based on the Link and Network Keys. The APS sublayer adds an auxiliary header for carrying security information. At the APS layer, a MIC is also applied to determine the level of data integrity.

4) *Network Join Mechanism*: ZigBee defines three types of devices: ZigBee Coordinator (ZC), ZigBee Router (ZR), and ZigBee End Device (ZED). A ZC will initiate the network and accept join requests originating from ZRs or ZEDs. Only a ZC or other ZRs which already have joined the network can accept join requests and forward packets [8]. Joining and identifying each device to the network is a very important step. Once a device has joined the ZigBee network, before communications begin, a message is sent to the ZC or a Trust Center. At this stage, a decision is made about whether the device is authorized to join the network or not. This decision is based on the type of key and the configuration of the Trust Center [9]. As it is addressed in Table I there are four options to configure the Trust Center in ZigBee PRO, whereas only the two first options are available for the Trust Center configuration in ZigBee standard.

### III. ZIGBEE SECURITY ASSESSMENT

In this section, we analyze the current capabilities of the ZigBee standard in order to assess the security level currently provided by the platform. We categorize the existing

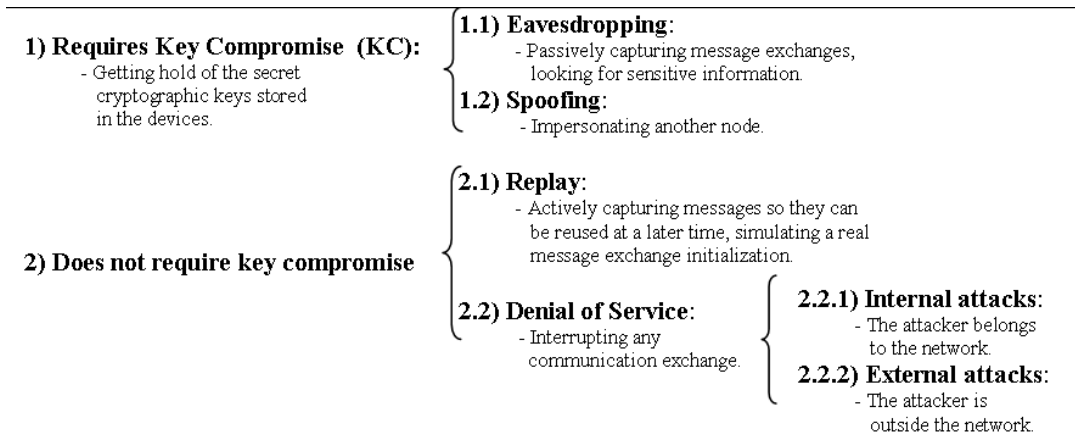


Fig. 1. Attack categories

vulnerabilities according to the following factors: constraints on performing a successful attack and the kind of disruption an attack may cause on the network. From our analysis, the existing vulnerabilities can be divided in two main categories: those which require knowledge of the ZigBee cryptographic keys (Link, Master or Network), and those which do not. Depending on this fact, the set of sub-scenarios varies, as shown in Figure 1.

#### A. Attacks Requiring Key Compromise

All unicast communications between ZigBee nodes are secured using a 128 bit Link Key shared between two devices at the APS layer. All broadcast communications are secured by a 128 bit Network Key shared among all devices in the network layer [9]. Therefore, a compromised key is a very important issue as far as security is concerned. Once an attacker gets hold of a key, he will be able to act at leisure within the network.

An attacker can obtain the Network Key through different methods such as remote attack or a physical attack [10]. In the former case, this feat may be achieved by intercepting the key during the out-of-band transmission or capturing plain text traffic sent from a ZigBee Coordinator. In the latter case, the physical device is stolen, extracting the information directly from its hardware.

Remote attacks rely on message interception and exploiting the out-of-band exchange key mechanisms, which may be executed through a social engineering attack. Hence, we focus on the much more complex physical attack rather than focus on the remote attack.

Physical attacks are feasible by dumping device firmware using existing available hardware [11]. ZigBee chips, typified by the CC2430 evaluation board from Texas Instruments, are vulnerable to local key extraction. Currently, there is no protection against an external access which tries to steal keys using unprotected data memory and exploiting flash memory.

Specifically, it is possible to attack micro-controllers and ZigBee radios by exploiting their Pseudo-Random Number

Generator (PRNG). This attack is called *side-channel timing attack*, which is an attack against the MSP430 micro-controller by exploiting and programming of Joint Test Action Group (JTAG), a 4-wire Test Access Port (TAP) controller or a serial bootstrap loader (BSL) which resides in masked ROM [12]. The MSP430 is a low-power micro-controller popular in ZigBee/802.15.4 and found in many wireless sensor development kits.

The PRNG uses a 16-bit Linear Feedback Shift Register (LFSR), as shown in Figure 2, which can be advanced by writing to the RaNDom High (RNDH) register or overwritten by writing to the RaNDom Low (RNDL) register, to generate pseudorandom numbers. RNDH and RNDL are the High and Low bytes in a 16-bit Cyclic Redundancy Check (CRC) of the LFSR, used to calculate the CRC value of a sequence of bytes and read the 16-bit shift register in the LFSR. In other words, the 802.15.4 Low radio frequency randomizes the seed by mixing 32 values into the Random Number Generation (RNG), for  $i$  0 to 8. Once the RNG has been seeded, it has an initially random 16-bit state [4].

This random number can be read by the CPU and used to generate random cryptographic keys. In fact, the state of this random number is initialized in the Hardware Abstraction Library (HAL) by feeding 32 bytes from the Analog Digital Converter (ADC), a device that converts continuous signals to discrete digital ones, into the RNDH register. The random values generated by the ADC are read from the Radio Frequency (RF) registers ADCTSTH and ADCTSTL, which correspond to ADC test high and low, respectively. Unfortunately, bytes from the ADCTSTH register are physically random, but poorly distributed [4]. This problem in ADCTSH has been inherited from one of the flaws in the PRNG.

There are two flaws in the PRNG: the pool is extremely small (16 bits) and it is not seeded with very much entropy. The first flaw is that the PRNG is not cryptographically secure because the pool is extremely small (16 bits). Nevertheless, even if the pool was much larger, it is still vulnerable because the LFSR is not a cryptographically-secure PRNG and attacker

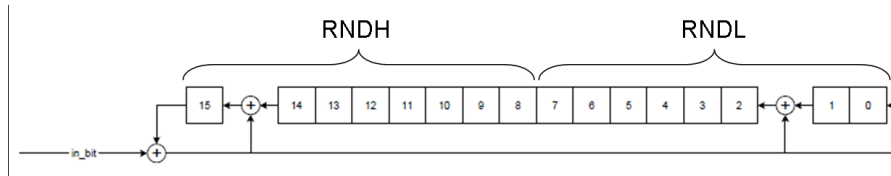


Fig. 2. The Random Number Generator structure

can recreate the LFSR taps and then generate any future sequence from it. The second problem is that it is seeded from a random source that has very little entropy. This could be exploited even if it was used in a cryptographically-secure PRNG. These problems are enough to make the system trivially insecure to a simple brute-force attack [13].

In order to prove both flaws in the PRNG, a dumping of a random byte sequence from the ZigBee evaluation was developed by Travis Goodspeed through employing GoodFET to debug the chip. GoodFET is an open-source Joint Test Action Group (JTAG) interface adapter [12]. It is based upon the TI MSP430 micro-controller and is provided with a USB bus adapter. The firmware was compiled with the Small Device C Compiler and flashed by the GoodFET. A quick Python script is then used by the GoodFET library to debug the target micro-controller and dump random values through the JTAG interface [13].

As a result, it was found that by exploiting the PRNG through its flaws and access to LFSR, which does not have high entropy, obtaining the key stored in the MSP430 micro-controller of ZigBee devices is achievable. From this security test, it may be concluded that it is feasible, even though not necessarily easy, to crack the cryptographic keystores in individual ZigBee devices. Once an attacker has gained hold of the cryptographic keys, he can easily perform eavesdropping and spoofing attacks.

1) *Eavesdropping*: In ZigBee, broadcast messages are encrypted using the Network Key, which is shared between all the devices in the network. Unfortunately, it is only necessary to compromise a single device in the network for the attacker to be able to compromise the entire network. By using this key the attacker is able to capture the content of broadcast messages in the network, and thus, this is one of the most important vulnerabilities in the ZigBee technology. This is a feasible feat, since an adversary may obtain the cryptographic keys remotely or physically, as mentioned in Section III-A.

In contrast, unicast communications are secured by a unique Link Key shared between two devices in the network. This means, if a device of the network is compromised by physical attack, an attacker is able to capture the content of all the direct unicast communication of the device.

In order to address this problem, a mechanism to protect the key exchange must be used. Also, the physical security of devices would be necessary to prevent this attack.

2) *Spoofing*: This attack is based on the same vulnerability mentioned in the previous one: all broadcast messages are encrypted using the same key, the Network Key. This allows attackers to impersonate the identity of any node in the broadcast messages, since there is no authentication check. Since this vulnerability only applies to broadcast messages, the risk of this vulnerability depends on the amount of broadcast data sent by each application.

In order to address this problem, a mechanism to secure the broadcast communications by enforcing an authentication process is proposed in [14], by using a modified one-way signature.

#### B. Attacks With Unrequired Key Compromise

Attacks which do not require for an attacker to gain access to the cryptographic keys stored in a ZigBee device are a bigger concern, since they can be performed remotely from the wireless space. It is not necessary to manipulate physical devices. The two existing main attacks which follow this condition are Replay and Denial of Service (DoS).

1) *Replay attack*: This kind of attack can apply to many applications. For example, in a server room where the temperature is controlled by ZigBee sensor and the data changed is only +1 or -1 degrees. By executing replay attack, the temperature can be changed by an adversary. It means, if an attacker, who implemented the Replay attack, sniff the sent packet from the ZigBee device to the Air Conditioning and replay it n-times, the temperature is added or decreased by n-degrees. This incorrect temperature can cause damage to servers.

ZigBee technology provides one mechanism to avoid replay attacks [15], called the *Frame Counter*, which has been added to the frame header at the Network layer. It consists of a counter that is employed in each transmission and is supposed to detect replicate data. Nevertheless, a replay attack has been successfully executed by Joshua Wright, a senior security analyst from InGuardian [16]. As he mentioned: "802.15.4 has no replay protection and ZigBee has meager replay protection" and "An attacker can replay any previously observed traffic until key rotation".

In fact, at the moment, Joshua Wright is working in KillerBee, an open source collection of python tools intended for testing the security of ZigBee networks. One of this tools is *zbreplay*, that produces a straightforward and unintelligent

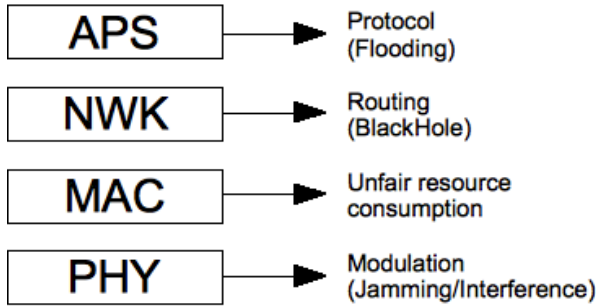


Fig. 3. Denial of Service attack

replay attack from stored data streams.

2) *DoS*: A great deal of effort has been done by the ZigBee Alliance to be able to perform authentication and provide confidentiality to transmitted data. However, no effort has been done to avoid Denial of Service (DoS) attacks. This attack can be performed at several layers and depends on whether the attacker has joined the network, being part of it (an insider) or not (an outsider). [17], [18].

If the attacker is an insider, the DoS attack may be conducted at the PHY/MAC/NWK/APS layers, whereas if the attacker is an outsider, DoS may only be conducted at the PHY/MAC layers. Figure 3 classifies all possible DoS attack according to each layer.

The possibility to perform the DoS attack at several layers is important because more complex attacks will be more difficult to detect, as an attacker always intends to be invisible.

*Insider Attacks:*

At the APS layer, DoS is performed by sending a great deal of messages to the device (flooding) to interrupt message processing. In addition, this action exhausts the device resources, such as battery. This attack can be easily detected, since all the messages are sent from an specific device.

At the NWK layer, DoS is executed by modifying the default routing protocol. If the attacker, which is placed within the network, is a compromised router, it can stop forwarding messages between nodes, which leads to changes to the routing protocol. Fortunately, this DoS attack may be directly detected and avoided by the default routing protocol. The sensor can just start sending messages via another router, if possible.

*Outsider Attacks:*

At the MAC layer, ZigBee uses CSMA/CA [10] (if it is running in non-beacon mode) to guarantee that all the devices can communicate through the same communication channel. Once a device intends to transmit data, the communication channel should be listened during the specific time. If the channel is sensed idle, then the node is permitted to begin the transmission. However, if the channel is sensed as busy,

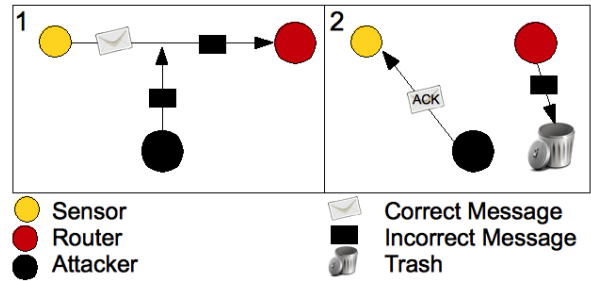


Fig. 4. ACK-MAC layer attack

the node defers its transmission for a random period of time. A DoS attack occurs if a device starts consuming bandwidth unfairly. For example, if the attacker starts continuously sending data over the communication channel, other devices cannot communicate to each other.

At the PHY layer, the DoS attack is performed by direct jamming of the channel. This attack can be executed through an outsider device by disrupting the signal of other devices by changing the Power Spectral Density (PSD). In fact, a jammer can never re-produce a signal nor it can pretend to be a receiver node. There are some parameters such as signal strength of a jammer as well as the location and its type which may influence the performance of the network.

To perform jamming, the attacker should be near to the device or use an adequate level of transmission power [18], [19]. This is since the transmitted signal loses energy as the distance increases. An algorithm to avoid the jamming attack has been proposed in [17].

Additionally, the MAC layer may also be interfered using an ACK attack, an optimized DoS attack that more difficult to be detected. Since ZigBee is built over the IEEE 802.15.4 stack, some of its vulnerabilities has been inherited. In ZigBee, the sender has the option to activate ACK by setting a flag inside of each message sent. If this flag is set, the receiver sends a new message containing an ACK answer. However, this message is not authenticated, so anyone may respond with an ACK message [20], [21]. The 802.15.4/ZigBee specification does not provide integrity and confidentiality protection for acknowledgment packets [21].

The scenario is shown in figure 4. There are three devices: the sensor (sender), the router (receiver) and an external device (attacker). (1) While the sensor is sending a message to the network, the attacker interferes and corrupts the transmitted data, so the receiver does not receive the complete message. (2) To ensure that the sensor does not resend the message again, the attacker generates an ACK message and sends it back to the sensor (sender). Due to not checking the authentication, the sensor assumes that the message has been sent to the router.

IV. CONCLUSIONS

As ZigBee technology is generating significant interest in the industry area. Therefore, the security of this standard becomes extremely important in its successful deployment.

In this paper, we presented a survey of the existing vulnerabilities in the security services available in ZigBee. From our analysis, it has been identified that ZigBee is still vulnerable to some attacks, specially those related to capturing its cryptographic keys. The MSP430 micro-controller from TI is still vulnerable to key theft because of unprotected data memory. Based on these vulnerabilities, some attacks such as eavesdropping, spoofing are feasible. It can also be concluded that, even when keys are not compromised, some attacks are still possible, such as replay and DoS attacks at different layers.

Further research will include developing and implementing new mechanisms to protect against the different attacks analyzed in this paper. To avoid Eavesdropping and Spoofing attacks, secure distribution of the keys, physical security of devices as well as authentication and confidentiality in broadcast communications should be implemented. Additionally, even though a protection for frame freshness exists in the ZigBee standard, we plan on improving this schema to protect this technology against Replay attacks.

#### REFERENCES

- [1] ZigBee Alliance, "ZigBee specification", 2007.
- [2] IEEE 802.11, "Wireless Medium Access Control (MAC) and Physical layer (PHY) specifications", 1999.
- [3] Junqi Zhang and Vijay Varadharajan, "A new security scheme for Wireless Sensor Networks", in *GLOBECOM*, 2008, pp. 128–132.
- [4] IEEE, "IEEE 802.15.4-2006 IEEE standard for information technology–telecommunications and information exchange between systems–local and metropolitan area networks– specific requirements part 15.4: Wireless Medium Access Control (MAC) and Physical layer (PHY) specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)", 2006.
- [5] Yang Xiao, Hsiao-Hwa Chen, Bo Sun, Ruhai Wang, and Sakshi Sethi, "MAC security and security overhead analysis in the IEEE 802.15.4 Wireless Sensor Networks", *EURASIP Journal on Wireless Communications and Networking*, vol. 2006, pp. 1–12, 2006.
- [6] "NIST. AES: Advanced Encryption Standard", <http://csrc.nist.gov/CryptoToolkit/aes/>.
- [7] Paolo Baronti, Prashant Pillai, Vince W. C. Chook, Stefano Chessa, Alberto Gotta, and Y. Fun Hu, "Wireless Sensor Networks: A survey on the state of the art and the 802.15.4 and ZigBee standards", *Computer Communications*, vol. 30, no. 7, pp. 1655–1695, 2007.
- [8] Tian-Wen Song and Chu-Sing Yang, "A connectivity improving mechanism for ZigBee Wireless Sensor Networks", *Embedded and Ubiquitous Computing, IEEE/IFIP International Conference on*, vol. 2, pp. 495 – 500, 2008.
- [9] Kyunghwa Lee, Joohyun Lee, Bongduk Zhang, Jaeho Kim, and Yongtae Shin, "An enhanced Trust Center based authentication in ZigBee networks", in *Advances in Information Security and Assurance*, pp. 471–484. SpringerLink, 2009.
- [10] "Wireless Medium Access Control (MAC) and Physical layer (PHY) specifications", 1999.
- [11] Joshua Wright, "Will hack for sushi - hacking and defending wireless", <http://www.willhackforsushi.com/>, 2009.
- [12] Travis Goodspeed, "Extracting keys from second generation ZigBee chips", in *Black hat*, 2009.
- [13] Nate Lawson, "Smart meter crypto flaw worse than thought", <http://rdist.root.org/2010/01/11/smart-meter-crypto-flaw-worse-than-thought/>, 2010.
- [14] Ji-Tsong Shieh and Li chun Ko, "Implementation of a broadcast authentication mechanism in ZigBee", in *The 2nd Workshop on Wireless, Ad Hoc, and Sensor Networks (WASN)*, August 10, 2006 2006.
- [15] ZigBee Alliance, "Understanding ZigBee RF4CE", July 2009 2009.
- [16] Joshua Wright, "KillerBee: Practical ZigBee exploitation framework", in *ToorCon*, 2009.
- [17] Rajani Muraleedharan and Lisa Ann Osadciw, "Jamming attack detection and countermeasures in Wireless Sensor Network using ant system", in *Proceedings of the SPIE*, Monday 17 April 2006 2006, vol. 6248.
- [18] Peter Egli, "Susceptibility of wireless devices to denial of service attacks", Technical white paper, Netmodule AG, 2006.
- [19] Jacob Brodsky and Anthony McConnell, "Jamming and interference induced denial-of-service attacks on IEEE 802.15.4-based Wireless Networks", Tech. Rep., Digital Bond's SCADA Security Scientific Symposium, 2009.
- [20] Radosveta Sokullu, Ilker Korkmaz, Orhan Dagdeviren, Anelia Mitsevax, and Neeli R.Prasad, "An investigation on IEEE 802.15.4 MAC layer attacks", in *Proceedings of The 10th International Symposium on Wireless Personal Multimedia Communications (WPMC) 2007*, 2007.
- [21] Naveen Sastry and David Wagner, "Security considerations for IEEE 802.15.4 networks", in *WiSe '04: Proceedings of the 3rd ACM workshop on Wireless security*, New York, NY, USA, 2004, pp. 32–42, ACM.