

© 2010 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Taxonomy of Wireless Sensor Network Cyber Security Attacks in the Oil and Gas Industries

Pedram Radmand¹, Alex Talevski¹, Stig Petersen² and Simon Carlsen³

¹Digital Ecosystems and Business Intelligence Institute, Curtin University of Technology, Perth, Australia
Pedram.Radmand@student.curtin.edu.au, Alex.Talevski@cbs.curtin.edu.au

²SINTEF ICT, Trondheim, Norway
stig.petersen@sintef.no

³Statoil 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].

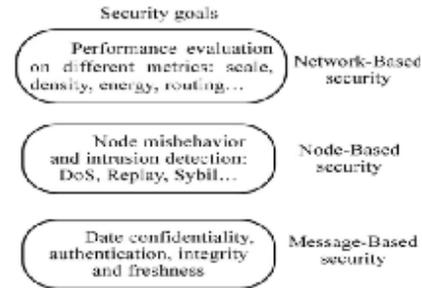


Figure 1: WSN Security Concerns [12]

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

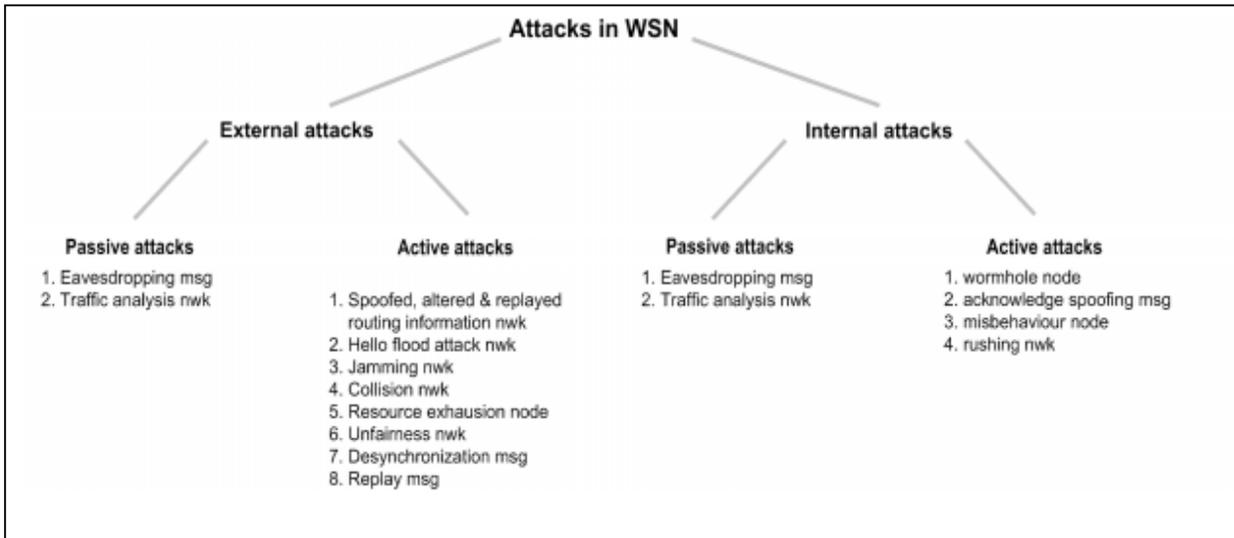
- **Wormhole Attack** - A wormhole is a low latency link between two portions of the network over which an attacker replays network messages. This link may either be a single node forwarding messages between two adjacent but otherwise non-neighboring nodes or a pair of nodes in different parts of the 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. Varadarajan, "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 μm CMOS Technology," *ETRI Journal*, vol. 30, pp. 33-46, February 2008.