4th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2010)

Secure Communication in Wireless Multimedia Sensor Networks using Watermarking

Bambang Harjito[1,2] , Song Han[1], Vidyasagar Potdar[1], Elizabeth Chang[1], Miao Xie[1]
[1]*Digital Ecosystem and Business Intelligence Institute*
Curtin University of Technology, Perth, Western Australia
harjito.bambang@student.curtin.edu.au
{Song.Han;Vidysagar.Potdar; Elizabeth.Chang}@cbs.curtin.edu.au
Miao.X@curtin.edu.au
[2]*Computer Science Department, Faculty of Mathematics and Natural Science*
Sebelas Maret University, Surakarta, Indonesia
bambangcs@.mipa.uns.ac.id

Abstract- *Wireless multimedia sensor networks (WMSNs) are an emerging type of sensor networks which contain sensor nodes equipped with microphones, cameras, and other sensors that producing multimedia content. These networks have the potential to enable a large class of applications ranging from military to modern healthcare. Since in WMSNs information is multimedia by nature and it uses wireless link as mode of communication so this posse's serious security threat to this network. Thereby, the security mechanisms to protect WMSNs communication have found importance lately. However given the fact that WMSN nodes are resources constrained, so the traditionally intensive security algorithm is not well suited for WMSNs. Hence in this research, we aim to a develop lightweight digital watermarking enabled techniques as a security approach to ensure secure wireless communication. Finally aim is to provide a secure communication framework for WMSNs by developing new.*

Index terms - *Wireless Multimedia Sensor Networks, Watermark, Digital watermarking*

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have the capability for sensing, processing and wireless communication all built into a tiny embedded device. This type of network has drawn increasing interest in the research community over the last few years. This is driven by theoretical and practical problems in embedded operating systems, network protocols, wireless communications and distributed signal processing. The primary function of WSNs is to collect and disseminate critical data that characterize the physical phenomena within the target area. Depending on the application scenario WSNs can be categorized into two main streams: Wireless Scalar Sensor Networks (WSSNs) and Wireless Multimedia Sensor Networks (WMSNs) [1]. In addition, The availability of low-cost cameras, CMOS image sensor and microphones, also their broad application opportunities that are able to ubiquitously capture multimedia content from the environment has fostered the development of WMSNs, i.e., networks of wirelessly interconnected devices that allow retrieving video and audio streams, still images, and scalar sensor data from the environment. To the ability to retrieve multimedia data, WMSNs will also be able to store, process in real-time, correlate and fuse multimedia data originated from heterogeneous sources. WMSNs will not only change enhance existing sensor applications such as tracking, and environment monitoring [2], but they also will enable several new applications. For example they range over systems supporting telemedicine, attendance to disabled and elderly people as means to identify the causes of illnesses that affect them such as dementia [3], localization and recognition of services and users, and control of manufacturing processes in industry [4].

WMSNs have some novel features which stem the fact that some of the sensor node will have video cameras and higher computation capabilities. Consequently, the WMSNs bring new security of challenges as well as new opportunities. Security is a key concern in such application like traffic monitoring and enforcement [2] and monitoring process in industry [4]. However given the problems including the limited power resources and computational capabilities, it is difficult to implement strong cryptography algorithm. Hence, this paper aims to investigate the possibility of digital watermarking technique as an alternative method for providing security. The paper is structured as follows : Section 2 present review all the aspects of secure WMSNs, Section 3 describes proposed framework for watermarking enabled secure communication in WMSNs, Section 4 describe framework implementation, Section 5 evaluation and finally we have concluded and future work the paper in section 6.

2. RELATED WORKS

WMSNs security is still a very young research field. Tavli et al [1] provided a survey and analysis of the different security issues that will have to take into account in the design of WMSNs platforms and protocol. Grieco et al [5] summarize the main findings on secure WMSNs and forecasts future perspectives of such a technology. Both of them will be spurred new research ideas. Here, we integrate prior research results and investigate the following sub categories: which includes privacy, authentication

mechanisms, secure communication channels and Secure Compression and aggregation of multimedia data contents.

2.1 Privacy

In WMSNs collect and handle a great amount of data of different nature, which may provide some kind of information on individuals in both an indirect or direct form. The kind of information may specify explicit information on individuals. Therefore, under some circumstances, data may be used to violate the privacy of individuals. Privacy is a key requirement for numerous application scenarios of WMSN[5]. WMSNs run the risk of individual privacy violation due to possible unauthorized access to the data that are handled by the network. This treat is mainly attributable to vulnerabilities of WMSN, for example the remote access data and the huge quantity of multimedia data that are exchanged within the network [5]. Attacks versus privacy which exploit these vulnerabilities can be categories into distinct macro-types of techniques: Eavesdropping and Masquerading [6]. The design of privacy protecting mechanisms is a challenging problem for the intrinsic characteristic of WMSNs. There are two different types of solutions that aim at hindering such as attacks: The first of types is privacy aware mechanisms based on *data cloaking*. The aim of data cloaking anonymity mechanisms is hiding the informative content of messages by perturbing data according to specific patterns. There are only a few more prior studies on the issue of data cloaking , mainly considering the privacy such as [7] is expressed designed to enable privacy in vision rich system built in WMSN, [8] proposed a novel paradigm for securing privacy and confidently in a distributed manner, [9] presented attacks that affect the data privacy in visual sensor networks and proposed privacy-promoting security solutions established upon a detected-adversary using a game-theoretic analysis and keyless encryption. The second of types is privacy policy. The references of [10] propose privacy policy and they state who can use individuals data, which data can be collected, for what purpose the data can be used, and how they can be distributed. A privacy-preserving video surveillance system that monitor subjects in an observation region using video cameras along with localized sensors is presented in [11] . The localized sensors include RFID tags placed within the observation environment. The motion detectors are used to turn the video cameras on or off, while the RFIDs of the subjects provide information that specifies which individuals are entitled to privacy. The video data accommodates the information from the various sensors, and the result is in a video stream with only authorized subjects being masked through image processing. At present, the solutions that guarantee the privacy of data in the context of WMSNs are still in a primitive state and many open problems still exist such as lack of privacy and process data complements based on digital watermarking technique and are yet to be discovered, hence, further research work is required.

2.2 Authentication mechanisms

Wireless communications make security and privacy requirements critical take into account they increase the vulnerabilities and the threats on the integrity and confidentiality of the transmitted data. With these reasons, there are many studies on the issue of an authentication mechanisms such as Honggang W et al [12] presented an authentication mechanisms that it is used to guarantee the correctness and the confidentiality of data and Zhang W et al [13] proposed an end-to-end, watermark statistical approach for data authentication that provides inherent support for in-network processing. Due to the high number of sensor nodes, such systems could contain control units that broadcast commands and data to the nodes. Consequence, the authenticity of these data and commands is a critical requirement for the correct behaviour of WMSNs. It is really a complex problem to guarantee the correct broadcast authentication of the messages transmitted by control units, because the broadcast authentication algorithms that are currently available in the literature [14, 15] do not adequately satisfy the QoS requirements of multimedia signals. At present there is no solution to deploy for WMSNs. Therefore, exploiting the characteristics of multimedia nodes should be developed.

2.3 Secure Communication Channel

The usage of secure communication protocols to hinder active attacks and eavesdropping is presented. In this case the cloaking is executed by means of encryption methods. The objective of these methods is to guarantee the confidentiality of data by hiding their content. There has been a lot work for securing routing protocol for WSN. A suite of security protocols for sensor networks called SPIN was recently proposed [16]. The SPIN family of protocols permits only valid key holders access to encrypted data; but as soon as this data is decrypted, tracking the reproduction or re-transmission of the data is not possible. The protocol SPIN originally designed for generic WSN can also be applied to WMSN. Like Fidaleo et al [17] introduce the Networked Sensor Tapestry (NeST) architecture which is designed for the secure sharing, capture, distributed processing, and archiving of multimedia data. The infrastructure of the NeST is developed to facilitate the fast prototyping and deployment of WMSNs for a wide variety of surveillance applications including structural monitoring and battlefield assistance. In order to facilitate trust in WMSNs, [5] presents the notion of subjective privacy in video where the behaviour of an individual under surveillance is conveyed but not identify it.

2.4. Secure Compression and aggregation of multimedia data contents

Aggregation algorithms and compression technique for multimedia contents are crucial to reduce the amount of transmitted data and to save energy and processing resources in WMSNs. The problem of aggregating multiple compressed frames coming from different video sensors while guaranteeing the expected security level is still open research area. Even though, many compression schemes have been proposed as described in the surveys [19]. Because of the complex compression operations, the distributed elaborate of the multimedia contents and the limited bandwidth and power resources of WMSN, so it is needed to introduce secure aggregation algorithms that decrease the total amount of information to transmit, elaborate and protect at the same time the quality of the multimedia message. There has been a lot of work in the

area of secure data aggregation such as Hani A et al [20] discussed the security issue in data aggregation in the WSN. A novel framework for secure information aggregation in large sensor networks is proposed by Bartosz P et al [21] . Wang et al [22] propose a survey on the most important solutions, but they can be hardly applied to multimedia data. In the case of WMSN, aggregation is probably, only going to be useful with abstract information extracted from sensed media. This is because it is extremely complex to aggregate different multimedia sources into a single aggregated multimedia stream [6]. To take into account the cost deriving from the secure aggregation of multimedia contents, [23] proposed a methods to optimize the placement of aggregation node. At present, research on secure aggregation of multimedia contents is still separated and that more efforts are required to address it in a comprehensive way.

2.5. Research issues for WMSNs Security

After doing the literature review, we identify the gaps in the following area.

1. Lack of privacy based on digital watermarking technique**.**
2. Lack of data authentication based on digital watermarking technique**.**
3. Lack of the processed data complement**s.**
4. Lack of secure communication model based on watermarking technique for WMSNs.

In this context of this research, we will address and then issues. The next section will provide a conceptual framework to solve the open problem

3. CONCEPTUAL FRAMEWORK FOR SECURE COMMUNICATION IN WMSNS USING WATERMARKING

3.1. Overview Digital Watermarking and WSNs

The objective of digital watermarking is to protect the intellectual property of multimedia contents such as copy right protection, contents archiving, Meta-data insertion, broadcast monitoring, tamper detection and digital fingerprinting [18]. Digital watermarking techniques have been extensively studied in the multimedia domain [19, 20]. However, rarely this technique has been used in WSNs. Zhang W et al [13] propose a watermarking-based authentication schemes for WSNs. The key idea is to hide certain information about the multimedia material within that material itself. As illustrated in Fig. 1, a generic watermarking system is usually composed of two components: an embedder and a detector [13]. The embedder takes three inputs: (1) messages that are encoded as the watermark; (2) cover data that are used to embed the watermark; and (3) key

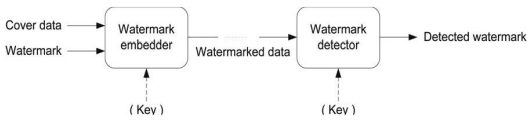

Fig. 1, A generic watermarking system [13]

That is optional for enforcing secure watermark generation. As an embedder's output, the watermarked data is distributed. It is presented as the detector's input, with the key information (depending on whether employed), the detector can determine whether a watermark exists and decode it. The watermark detection schemes can be categorized into two classes: *informed detection* and *blind detection*. The difference lies in that the original cover data is accessible in the former case while it is not required in the latter case. Although watermarking technique has been widely used in the multimedia domain, its direct adoption to wireless sensor networks is often not feasible. First, often in multimedia applications, both the watermark embedder and detector (shown in Fig. 1) possess the knowledge of the whole multimedia material, which can be leveraged to watermark embedding. On the contrary, in sensor networks, each sensor node only has knowledge of its own local sensory data without a global view of the whole ''sensory image''. This requires the sensor node to embed its watermark in a distributed fashion [13] Second, most watermarking schemes for multimedia applications operates in the frequency domain, for example, after certain time to frequency transform. However, in sensor networks, only the sink that performs the compression can obtain such information.

3.2. Research method

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. This research approach commonly identifies problems and proposes solutions to these problems. [21] and [22] provide a concise conceptual framework for design-science research and state that design-science research deals with understanding the problem domain and design a solution by building application or some design artifacts.

3.3. Research Stages

The work in [1] gives a vision of the research challenges and the future trend focusing on their security aspects in WMSNs and the work [5] gives a driving directions for future research in secure WMSNs. In [5] shows that privacy, trust management and authentication mechanisms are not separated components of security in WMSNs.

Digital watermarking technique is an effective vehicle to assure and assert the image data authentication and is not inherently pose risk to privacy. At the same time, it relies on other security services. Digital watermarking technique and other security services together make up security architecture for WMSNs. Therefore, a comprehensive consideration is compulsory when designing digital watermarking for WMSN. Here we will propose a conceptual framework for watermarking enabled secure communication in WMSNs. It can be depicted in Figure 2. The conceptual will provide a guideline to design watermarking technique for WMSNs. The concept consists of 8 stages.

Stage 1 : **Application scenarios extraction.**

This step defines QoS requirement for different application scenarios extraction. WMSNs are application-specific networks. Except from some common features, a sensor network for a specific application has some features and the secure communication requirements. Suppose a multimedia

sensor network is deployed in the hospital surveillance environment [3] and the other in military [23]. Both network secure communication requirement should be different based on the resource of node can be used. The risks they face with. Therefore, we have to fully understand application background. The acquirement information in this step includes the size of the network and the densities, the available software and hardware resources, and some special knowledge that can be used in a real time, for example location information

Stage 2: **The secure communication model**.

This step develops the secure communication model. Since the protocol SPIN [16] originally designed for WSN and it can also be applied for WMSNs. So the secure communication model will be developed according to security requirements [16]. So far we know that it is the first time to define secure communication model with this terminology. Development of metrics, measurement and evaluation of approach are of great importance in order to establish a scientific methodology for the WMSNs area.

Stage 3: **Privacy protection for WMSNs.**

This step develops a privacy protection. WMSN collect a great amount of data, which may be used to violate individual's privacy, privacy protection is required. There are many existing privacy protection [24] but there is no the privacy of data in the context of WMSNs. [25] states that digital watermarking does not inherently pose risk to privacy and suggestions specific privacy principles for digital watermarking. One of the suggestions is privacy by design. Here, the privacy protection will be incorporated into the design of digital watermarking. The developing of digital watermarking considers and addresses privacy issues in the early design.

Stage 4: Authentication for WMSNs: This step defines an authentication mechanism. Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. Since data is easy to threat in wireless communication, so it is needed an authentication mechanism. The authentication mechanism rules privacy and security. [12] and [13] proposed authentication mechanism based on the digital watermarking technique. Here, we also addressed the digital watermarking technique as an authentication mechanism. This mechanism is used to guarantee the correctness and the confidentiality data for WMSNs.

Stage 5: **Trust management for WMSNs**. This step develops a trust management for WMSNs. The concept of trust is to increase security and reliability in sensor networks [26, 27]. We know that reputation is the opinion of one WSN node about another. The trust is a derivative of the reputation of an entity. The sensor network may be deployed in entrusted locations. We assume that individual sensors network is entrusted. Using SPIN [16], we compromise of a node to other nodes. Here the developing of digital watermarking considers and addresses trust management.

Stage 6: Initializes system parameter.

This step initializes system parameter. An authentication mechanism, used to guarantee the correctness and the confidentiality of data, is fixed in this step. To assert and assure the data authentication digital watermarking technique is applied. Digital watermarking consists of two components: an embbeder and a detector [13]. There are two inputs in the embedder. ie., messages that are encoded as the watermark, data comes from physical world. The watermark detector can determine whether a watermark exist and decode it. A fully integrated view of the design factors promotes the development of protocol for WMSNs

Stage 7: Digital watermarking technique for WMSNs : This step explains how digital watermarking works for WMSNs. In this step, there are three stages. The first stage is generating watermark. Here, a watermark binary stream is generated by using Linear Feed Back Shift Register [20] , then it is converted to watermark constraint using a particular low of the kolmogorov rule [28]. The second stage is the process of embedding. Here, the watermark constraint and the original data which comes from physical world flow into the sensor node are processed into a format suitable for using multi-modal fusion. After that a non linear system equation is obtained using atomic acoustic trileteraton,. Furthermore, the non linear system equation is solved by using the standard non linear programming approach to get watermarked solution. At last, the watermarked solution flows from sensor node to receiver sensor node. There are some watermark attacks which also flows from another sensor node into receiver sensor node. The third stage is the process of detecting watermark. Watermarked solution is detected in receiver sensor node whether it exists or not by applying the blind detection. This stage corresponds to perceptual level of the science and engineering research method.

Stage 8: Theoretical analysis and simulation: Both theoretical analysis and simulation are good tools to test the designed schemes. Only by these tools can we prove the validity of the schemes and, at the same time, find deficiencies of the scheme. The step 6, 7, and 8 proceed in turn. They form a loop and perform numerous times before the error minimization is obtained. This stage corresponds to the practical level of the science and engineering research methods

4. FRAMEWORK IMPLEMENTATION

Based on the conceptual framework proposed in the first research stage, the main task in this stage would be to design secure communication protocols in WMSNs using digital watermarking. Each of these schemes has some specialties according to watermarking attacks. It is not the final aim and it is impossible to design one of type protocol which will outperform all other for all watermarking attacks. We devote to designing secure communication in WMSNs using digital watermarking which matches the abstracted model in Fig. 2. This design can be categorized into two paths: the process of embedding into sensor node, and the process of detecting from receiver sensor node. The process of embedding consists of two stages: firstly, generating a watermark binary by using Linear Feedback Shift Register (LFSR)[20]. Then converting the watermark stream into watermarking constraints using a particular low of the Kolmogorov complexity rule [28]. Secondly, the original data, gathered

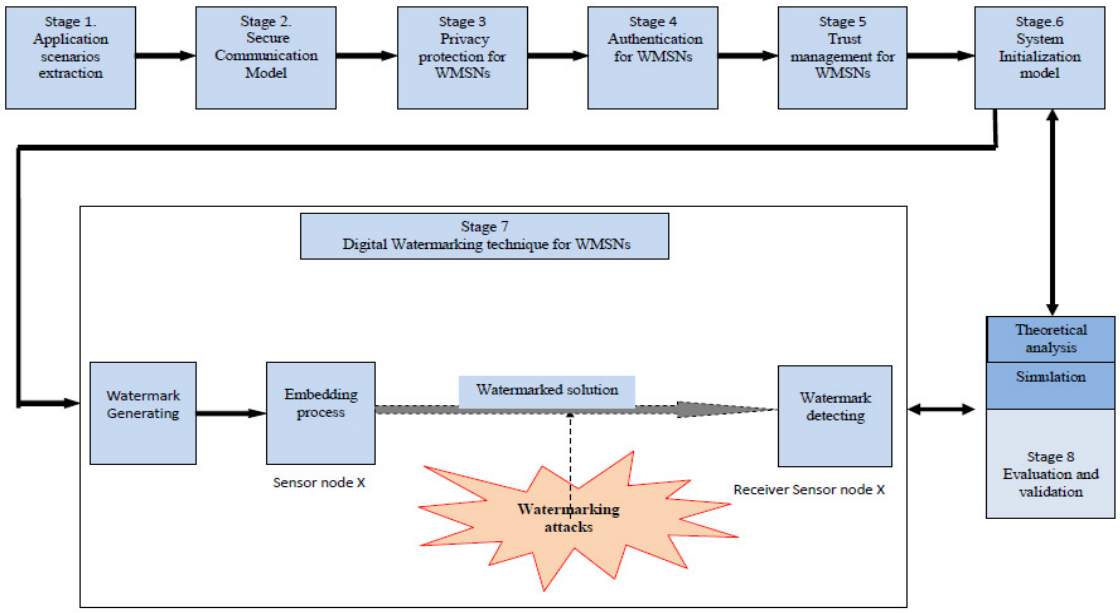

Figure 2 : framework for secure communication in WMSNs using watermarking

from physical world, flows into the sensor node and then process, that data into a format suitable for multi-modal sensor fusion [29]. Here we use atomic acoustic trileteraton [30]. In order to get non linear system equations those consists of objective FN, constraints and add constraints. To get a watermarked data, we have to solve the non linear system equation by using a gradient projection or the standard non linear programming approach. The process of detecting watermark uses *blind detection*. The blind detection means that we do not use the original data for watermarking detection. Here we approach by statistically analyzing the relationship between correctness, strength of authorship and measurement error [31].

5. VALIDATION

The schemes and protocol will be evaluated by using experimental simulation which can be divided into three stages: Stage 1, Here we will verify whether the schemes satisfy the secure communication data requirements against different watermarking attacks, such as Ghost signature, addition of a new signature, removal of the author's signature and de-Synchronization with the help of software Mathematica and Matlab. To this time there were limited references existed in experimental simulation, namely [30] and [32]. Both of them developed the system of watermarking techniques for embedding signatures into data and information acquired by embedded WSNs. However, [30] and [32] do not provide any attempt to handle some watermarking attacks. Thus, this research will contribute to the source studies on the field, providing digital watermarking schemes for WMSNs through experimental simulation. With regards to protocols, it is necessary to have comprehensive guidelines for evaluating a specific protocol and compare it against others. Based on the proposed secure communication model, appropriate performance metrics would then be used to evaluate the strength and weakness of each protocol. Stage 2, The performance of the proposed secure communication schemes will be further simulated by NS-2. Stage 3, The security of the watermarking enabled secure communication schemes will be validated by mathematical security proof.

6. CONCLUSION AND FUTURE WORK

This paper aims to address the problem of secure communication in wireless multimedia sensor networks using digital watermarking. Although some work has been done in this area, there is no security in application on wireless multimedia sensor networks. The unique idea proposed in this paper aims to address the problem from a scientific and systematic process. Our future work is to provide watermarking enabled secure communication framework in WMSNs. This framework is focusing on establishing multimedia data authentication, and ensuring privacy perseveration in WMSNs.

REFERENCES

[1] Manel Guerrero Zapata, R.Z., Jos´e M. Barcel´o-Ordinas, Kemal Bicakci, Bulent Tavli, *The Future of Security in Wireless Multimedia Sensor Networks*. 2009.

[2] Jason, C., Phillip, B. Gibbons, Suman, Nath, Padmanabhan, Pillai Srinivasan, Seshan Rahul, Sukthankar, *IrisNet: an internet-scale architecture for multimedia sensors*, in *Proceedings of the 13th annual ACM international conference on Multimedia*. 2005, ACM: Hilton, Singapore.

[3] Reeves, A.A., *Remote monitoring of patients suffering from early symptoms of dementia.* in Proc. Int. Workshop Wearable

Implantable Body Sensor Networks: p. London, U.K., Apr. 2005.

[4] Besma, R.A., Nash, R. Aragam, Yi, Yao Mongi, A. Abidi, *Survey and analysis of multimodal sensor planning and integration for wide area surveillance.* ACM Comput. Surv., 2008. **41**(1): p. 1-36.

[5] Grieco, L.A., Boggia, G, Sicari, S, Colombo, P. *Secure Wireless Multimedia Sensor Networks: A Survey*. in *Mobile Ubiquitous Computing, Systems, Services and Technologies, 2009. UBICOMM '09. Third International Conference on*. 2009.

[6] Marco, G.G., Schelle. Ashish, Jain Rick, Han Dirk, Grunwald, *Privacy-aware location sensor networks*, in *Proceedings of the 9th conference on Hot Topics in Operating Systems - Volume 9*. 2003, USENIX Association: Lihue, Hawaii.

[7] Kundur, D., et al., *Security and Privacy for Distributed Multimedia Sensor Networks.* Proceedings of the IEEE, 2008. **96**(1): p. 112-130.

[8] Czarlinska, A. and D. Kundur, *Reliable Event-Detection in Wireless Visual Sensor Networks Through Scalar Collaboration and Game-Theoretic Consideration.* Multimedia, IEEE Transactions on, 2008. **10**(5): p. 675-690.

[9] Czarlinska, A., W. Huh, and D. Kundur. *On privacy and security in distributed visual sensor networks*. in *Image Processing, 2008. ICIP 2008. 15th IEEE International Conference on*. 2008.

[10] Sastry, D., Marco, Gruteser, Xuan, Liu, Paul, Moskowitz, Ronald, Perez , Moninder, Singh, Jung-Mu, Tang, *Framework for security and privacy in automotive telematics*, in *Proceedings of the 2nd international workshop on Mobile commerce*. 2002, ACM: Atlanta, Georgia, USA.

[11] Jehan, W., et al., *Privacy protecting data collection in media spaces*, in *Proceedings of the 12th annual ACM international conference on Multimedia*. 2004, ACM: New York, NY, USA.

[12] Honggang, W., et al. *Energy-Aware Adaptive Watermarking for Real-Time Image Delivery in Wireless Sensor Networks*. in *Communications, 2008. ICC '08. IEEE International Conference on*. 2008.

[13] Zhang, W., Liu, Yonghe, Das, Sajal K, De, Pradip, *Secure data aggregation in wireless sensor networks: A watermark based authentication supportive approach.* Pervasive and Mobile Computing, 2008. **4**(5): p. 658-680.

[14] Liu, D. and P. Ning, *Efficient Distribution of Key Chain Commitments for Broadcast Authentication in Distributed Sensor Networks*. 2002, North Carolina State University at Raleigh.

[15] Liu, D. and P. Ning, *Multi-Level microTESLA: A Broadcast Authentication System for Distributed Sensor Networks*. 2003, North Carolina State University at Raleigh.

[16] Adrian, P., et al., *SPINS: security protocols for sensor networks.* Wirel. Netw., 2002. **8**(5): p. 521-534.

[17] Douglas, A.F., N. Hoang-Anh, and T. Mohan, *The networked sensor tapestry (NeST): a privacy enhanced software architecture for interactive analysis of data in video-sensor networks*, in *Proceedings of the ACM 2nd international workshop on Video surveillance \& sensor networks*. 2004, ACM: New York, NY, USA.

[18] M. Barni and F. Bartolini, *Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications.* Marcel Dekke, 2004.

[19] Harjito, B., *Watermarking of Image Reconstruct by Using Information Dispersal Algorithm* Master Thesis, Computer Science Department at James Cook University of queensland Australia 1999.

[20] Harjito, B., *Watermarking Technique based on Linear Feed Back Shift Register (LFSR),* . Seminar Nasional Konferda ke –9 Himpunan Matematika Wilayah Jateng dan DIY di FMIPA UNS 2003.

[21] T.M. Salvatore and F.S. Gerald, *Design and Natural Science Research on Information Technology.* Decision Support System. **Vol. 15**: p. 251-266, 1995.

[22] Herner A, M.S., Park J, Ram S, *Design Science in Information System Research.* MIS Quarterly. **Vol 28**(1): p. 75-105, 2004.

[23] Dan, L.W., K. D. Yu Hen, Hu Sayeed, A. M., *Detection, classification, and tracking of targets.* Signal Processing Magazine, IEEE, 2002. **19**(2): p. 17-29.

[24] Qun, N., Alberto, Trombetta, Elisa, Bertino, Jorge, Lobo, *Privacy-aware role based access control*, in *Proceedings of the 12th ACM symposium on Access control models and technologies*. 2007, ACM: Sophia Antipolis, France.

[25] Technology, C.f.D., *Privacy Principles for Digital Watermarking* Keeping the Internet Open, Innovative, and Free 1634 I St., NW, Suite 1100, Washington, DC 20006 • v. +1.202.637.9800. • f. +1.202.637.0968 • http://www.cdt.org, 2008. **1**(29 May).

[26] Saurabh, G., K.B. Laura, and B.S. Mani, *Reputation-based framework for high integrity sensor networks.* ACM Trans. Sen. Netw., 2008. **4**(3): p. 1-37.

[27] Avinash, S., T. Joshua, and W. Jie, *DRBTS: Distributed Reputation-based Beacon Trust System*, in *Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing*. 2006, IEEE Computer Society.

[28] Li, P.V.M., *An Introduction to Kolmogorov Complexity and Its Applications.* Graduate Texts in Computer Science. Springer, New York, second edition 1997.

[29] Richard, R.B. and S.S. Iyengar, *Multi-sensor fusion: fundamentals and applications with software*. 1998: Prentice-Hall, Inc. 488.

[30] F. Koushanfar, M.P., *Watermarking Technique for Sensor Networks: Foundations and Applications.* Book chapter, in 'Security in Sensor Networks', Yang Xiao (ed.),, 2007.

[31] Hernandez, J.R. and F. Perez-Gonzalez, *Statistical analysis of watermarking schemes for copyright protection of images.* Proceedings of the IEEE, 1999. **87**(7): p. 1142-1166.

[32] Fang Jessica, P.M., *Real-time watermarking techniques for sensor networks* ProceedingS-SPIE The international Society for Optical Engineering (5020): p. 391-402 2003.