International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 2 No. 2 Jun. 2014, pp. 301-307

http://www.ijisr.issr-journals.org/

Improving Security Connection in Wireless Sensor Networks

Abdalraouf Hassan[1] and Christian Bach[2]

[1]dept. Of Computer Science and Engineering
University of Bridgeport
Bridgeport, USA

[2]dept. of Technology Management
University of Bridgeport
Bridgeport, USA

ABSTRACT: Wireless Sensor Networks (WSNs) have concerned much attention in recent years. The prospective applications of WSNs are massive. They are used for collecting, storing and sharing sensed data. WSNs have been used for various applications including habitat monitoring, agriculture, nuclear reactor control, security and tactical surveillance. Wireless sensor networks are threatened by numerous attacks. Therefore, security is now becoming a significant new path of research and attempts to counter these attacks.

KEYWORDS: Cryptography; Steganography; Nodes; WSN's; Authentication; Integrity; Confidentiality.

1 INTRODUCTION

Wireless Sensor Networks (WSN) are rising as both an imperative new level in the IT ecosystem and a rich domain of active research relating hardware and system design, networking, distributed algorithms, programming models, data management, security and social factors[1]. The basic idea of sensor network is to scatter tiny sensing devices; which are capable of sensing some changes of incidents/parameters and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc. Today's sensors can monitor temperature, pressure, humidity, soil makeup, vehicular movement, noise levels, lighting conditions, the presence or absence of certain kinds of objects or substances, mechanical stress levels on attached objects, and other properties [2], [6]. In case of wireless sensor network, the communication among the sensors is done using wireless transceivers. The attractive features of the wireless sensor networks attracted many researchers to work on various issues related to these types of networks. However, while the routing strategies and wireless sensor network modeling are getting much preference, the security issues are yet to receive extensive focus [3], [4]. In this paper, we explore the security issues and challenges for next generation wireless sensor networks and discuss the crucial parameters that require extensive investigations.

Basically the major challenge for employing any efficient security scheme in wireless sensor networks is created by the size of sensors, consequently the processing power, memory and type of tasks expected from the sensors. We discuss these issues and challenges in this paper. To address the critical security issues in wireless sensor networks we talk about cryptography, steganography and other basics of network security and their applicability in Section 2. We explore various types of threats and attacks against wireless sensor network in Section 3. Section 4 reviews the related works and proposed schemes concerning security in WSN and also introduces the view of holistic security in WSN. Finally Section 5 concludes the paper delineating the research challenges and future trends toward the research in wireless sensor network security

Corresponding Author: Abdalraouf Hassan (abdalrah@my.bridgeport.edu)

2 WIRELESS SENSOR NETWORKS

Wireless sensor networks are becoming more and more popular day by day as they revolutionize many segments of our economy and life. The research into this field has expanded to include all relevant topics imaginable. This chapter gives a small overview of the general operations and technologies involved for better understanding of this research [1].

3 EVOLUTION OF WIRELESS SENSOR NETWORK

3.1 SENSOR NETWORKS ARCHITECTURE

A system of acoustic sensors called the Sound Surveillance System (SOSUS) was placed at strategic locations on the bottom of the ocean. Around the same time the United States also deployed networks of radars for air defense [2], [4]. These sensor networks had a hierarchical architecture and they were in fact wired sensor networks. They were not fully automated, human operators played an important role in maintaining the network. Wireless sensor networks were introduced by the Defense Advanced Research Projects Agency (DARPA) in the early 1980's [3]. It was called the Distributed Sensor Networks (DSN) program where many low-cost sensing nodes were spatially distributed and they processed data collaboratively. By the mid 1980's the Massachusetts Institute of Technology (MIT) started developing a DSN to track lowing aircrafts [5].

3.2 SECURITY IN WIRELESS SENSOR NETWORK ISSUES AND CHALLENGES

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE and SI do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable [7].

- Reliability is one of the most important factors. a sensor node can fail due to several
- Reasons such as environmental interference, physical damage, depleted energy source and etc [8]. The failure of a single node should not affect the overall network performance. Reliability in a WSN is the ability of the network to sustain its functionality regardless of the failure of nodes.
- Scalability a WSN may consist of hundreds of nodes in a single network. WSN protocols have to be designed to be able to work with these large numbers of nodes and also utilize the high density of nodes [5].
- The density of a WSN can be anything from a few nodes to a few hundred nodes per square meter. The density can be defined as the number of nodes within the transmission range of a specific node.

4 CRYPTOGRAPHY

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you?

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

4.1 ABBREVIATIONS AND ACRONYMS

Since data aggregation is done at intermediate nodes, it is necessary to ensure confidentiality, integrity, authentication, etc. Symmetric Key Cryptography is easy to compute and the

Public Key Cryptography is more secure compared to symmetric but it is slow. By combining the advantages of these two cryptographic methods, the level of security can be enhanced [10].

4.2 SECURITY GOALS

- Security of a system addresses three major concerns namely confidentiality, integrity and authenticity [3].
- Cryptography is the basic technique to provide security services such as authentication, confidentiality, integrity in data networks as well as sensor network.
- In sensor network security, an open research problem is to design a bootstrapping protocol that establishes a secure communication infrastructure
- from a collection of sensor nodes where the nodes are pre-initialized with some secret information without having any prior direct contact with each other [7].
- This is often referred as the bootstrapping problem. The complexity of the bootstrapping problem stems from the numerous restrictions of sensor network.
- A bootstrapping protocol should enable a newly deployed sensor network as well as it should support the addition deletion of nodes after deployment.
- Key management scheme is a basic building block to ensure security in sensor network.
- Traditional key management techniques are not suitable for sensor networks since sensor nodes are resource constrained devices and also can be physically captured [12].
- Security in communication system has become increasingly prominent and its key technology cryptography technology develops rapidly.
- Wireless network has been experiencing an explosive growth in recent years and offering attractive flexibility to network operators and users [11].
- There have been a few recent attempts to use PKC in wireless sensor networks, which demonstrate that it is feasible to perform limited PKC operations on the current sensor platforms such as MIC motes [5].
- Elliptic Curve Cryptography (ECC) has been the top choice among various PKC options due to its fast computation, small key size, and compact signatures. For example, to provide equivalent security to 1024-bit RSA, an ECC scheme only needs 160 bits on various parameters, such as 160-bit unite held operations and 160-bit key size [2].

4.3 SECURITY FUNDAMENTALS

Security is a broadly used term encompassing the characteristics of authentication, integrity [13] Privacy, no repudiation, and anti-playback. The more the dependency on the information provided by the networks has been increased, the more the risk of secure transmission of information over the networks has increased [15]. For the secure transmission of various types of information over networks, several cryptographic, steganography and other techniques are used which are well known. In this section [14].

4.4 SECURITY SCHEMES IN WIRELESS SENSOR NETWORKS

- Confidentiality, integrity, and authentication have an important role in security
- Most of the threats and attacks against security in wireless networks are almost similar to their wired counterparts
- While some are exacerbated with the inclusion of wireless connectivity.
- In fact, wireless networks are usually more vulnerable to various security threats as the unguided transmission medium is more susceptible to security attacks than those of the guided transmission medium [8].

5 STEGANOGRAPHY

The abundant availability of multimedia devices such as small microphones and low-cost complementary metal oxide semiconductors (CMOS) has fostered the development of wireless multimedia sensor network (WMSN) [11]. This type of network has drawn increasing interest in the research community over the last few years. Wireless multimedia sensor networks (WMSN) are a new low-cost and emerging type of sensor network that is facilitated by digital signal processing containing sensor nodes equipped with ubiquitously capturing cameras, microphones, and other sensors producing multimedia content that respond to sensory information such as humidity and temperature. Hence, a WMSN will have the ability to transmit and to receive multimedia information such as monitoring data, image and stream video [3], [7], [9]. Since,

there is functionality to retrieve multimedia information, the WMSN will also be able to store, process in real time, correlate and amalgamate multimedia information from different sources. The primary function of WMSNs is to garner and disseminate critical data that characterize the physical phenomena secluded in the target area. Depending on the application scenario, WMSNs are used in many contexts and therefore their application domains are continuously growing [3].

5.1 ATTACKS IN WIRELESS SENSOR NETWORKS

Attacks against wireless sensor networks could be broadly considered from two different levels of views. One is the attack against the security mechanisms and another is against the basic mechanisms (like routing mechanisms). Here we point out the major attacks in wireless sensor networks [12].

Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service [19], [23], [26].

In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be altered, spoofed, replayed again or vanished. As wireless communication is vulnerable to eavesdropping, any attacker can monitor the traffic flow and get into action to interrupt, intercept, modify or fabricate packets thus, provide wrong information to the base stations or sinks [18], [22], [25]. As sensor nodes typically have short range of transmission and scarce resource, an attacker with high processing power and larger communication range could attack several sensors at the same time to modify the actual information during transmission.

The progressive nature of the Information Age creates increasing demands for processed data, and the consistent hlfillment of Moore's Law produces smaller hardware devices with improved capabilities to gather and process new data.

In the ideal world, a secure routing protocol should guarantee the integrity, authenticity, and availability of messages in the presence of adversaries of arbitrary power. Every eligible receiver should receive all messages intended for it and be able to verify the integrity of every message as well as the identity of the sender [12], [14].

5.2 PHYSICAL LAYER SECURE ACCESS

Physical layer secure access in wireless sensor networks could be provided by using frequency hopping. A dynamic combination of the parameters like hopping set (available frequencies for hopping), dwell time (time interval per hop) and hopping pattern (the sequence in which the frequencies from the available hopping set is used) could be used with a little expense of memory, processing and energy resources. Important points in physical layer secure access are the efficient design so that the hopping sequence is modified in less time than is required to discover it and for employing this both the sender and receiver should maintain a synchronized clock. A scheme as proposed in could also be utilized which introduces secure physical layer access

Employing the singular vectors with the channel synthesized modulation [14], [15], [17], [18].

Physical layer security has been established on the information-theoretic security that was initiated by the seminal work. In particular, physical layer security has been studied to understand the intrinsic security induced by physical layer capabilities such as randomness of wireless channels, signal-to-noise ratio gap, intended jamming, etc. Among the efforts, the study on a wiretap channel model, first introduced by Wiener, showed that secure communication over a broadcast channel is possible even [8].

Without resorting to secret key sharing. Wiener showed that a positive transmission rate of confidentiality messages can be achievable with the total ignorance at a passive eavesdropper. Meanwhile, the randomness of wireless channels was utilized as a common randomness shared among legitimate parities from which secret keys are extracted [24], [26]. This unique feature in physical layer provides a solution to a long lasting issue in secure communications, namely, the key distribution problem.

Wireless links are susceptible to eavesdropping, impersonation and message distortion. Poorly protected nodes that move into hostile environments can be easily compromised. Authorization of administration becomes difficult due to dynamic

topology [32], [33]. The scale of deployment of a WSN requires careful decision about trade-offs among various security measures. These issues are discussed and mechanisms to achieve secure communication in WSNs are presented in. Various security challenges in wireless sensor networks are analyzed and key issues that need to be addressed for ensuring adequate security are summarized in. Secure routing is a major research area [7].

Secure routing is a major research area. Types of routing attacks and their countermeasures are presented in. Secure routing in an ad hoc network is a daunting task because of some contradictions between the nature of the network and the associated applications. Various routing protocols have

Been presented with a focus on finding security vulnerabilities a survey of secure ad hoc routing protocols for mobile wireless networks is presented [29], [30], [33].

In WSNs, for the data confidentiality in distributed detection, capabilities of physical layer can also be exploited. In the presence of a passive eavesdropper called an enemy fusion center (EFC), sensors in a WSN individually or collaboratively transmit their local decisions on a target state to an ally fusion center (AFC), where a final decision is made. In this case, the central issue is how to design a physical layer scheme at the sensors to achieve reliable transmissions to the AFC, while preventing information leakage to the EFC. Two encryption methods, stochastic encryption and channel aware encryption, have been proposed to achieve reliability and security simultaneously. In this paper, we review existing physical layer security schemes for WSNs when there is an EFC performing passive attacks (i.e., eavesdropping). As most physical layer security schemes do not require expensive cryptographic techniques (in terms of computation and energy cost) for secure communications the encryption methods built based on physical layer are well-suited to WSNs [26], [28], [31].

6 ACKNOWLEDGMENT

Sensor networks are ideal candidates for applications such as target tracking, battlefield surveillance, and scientific exploration in hazardous environments. Typically, a sensor network consists of a potentially large number of resource constrained sensor nodes, which are mainly used to sense physical phenomena (e.g. temperature, humidity) from its immediate surroundings, process, and communicate the sensed data locally, and a few control nodes, which may have more resources and may be used to control the sensor nodes and/or connect the network to the outside world (e.g. a central data processing server).

Sensor nodes usually communicate with each other through wireless channels in short distances.

Sensor networks may be deployed in hostile environments, especially in military applications. In such situations, an adversary may physically capture sensor nodes, and intercept and/or modify data/control packets [13], [15]. Therefore, security services such as authentication and encryption are essential to maintain the normal network operations. However, due to the resource constraints on sensor nodes, many security mechanisms such as public key cryptography are not desirable, and sometimes infeasible in sensor networks.

Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. For defending the inclusion of false reports by compromised nodes, a means is required for detecting false reports. However, developing such a detection mechanism and making it efficient represents a great research challenge. Again, ensuring holistic security in wireless sensor network is a major research issue. Many of today's proposed security schemes are based on specific network models. As there is a lack of combined effort to take a common model to ensure security for each layer, in future though the security mechanisms become well-established for each individual layer, combining all the mechanisms together for making them work in collaboration with each other will incur a hard research challenge. Even if holistic security could be ensured for wireless sensor networks, the cost-effectiveness and energy efficiency to employ such mechanisms could still pose great research challenge in the coming days.

REFERENCES

[1] AboElFotoh, H.M.F., E.S. Elmallah, and H.S. Hassanein. *On The Reliability of Wireless Sensor Networks*. in *Communications, 2006. ICC '06. IEEE International Conference on*. 2006.

[2] Agah, A., S.K. Das, and K. Basu. *A game theory based approach for security in wireless sensor networks*. in *Performance, Computing, and Communications, 2004 IEEE International Conference on*. 2004.

[3] Ahmad Salehi, S., et al. *Security in Wireless Sensor Networks: Issues and challanges*. in *Space Science and Communication (IconSpace), 2013 IEEE International Conference on*. 2013.

[4] Ahmed, M.H., et al. *Security for WSN based on elliptic curve cryptography*. in *Computer Networks and Information Technology (ICCNIT), 2011 International Conference on*. 2011.

[5] Ahmed, M.R., H. Xu, and C. Hongyan. *A Novel Evidential Evaluation for Internal Attacks with Dempster-Shafer Theory in WSN*. in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on*. 2013.

[6] Aina, H. *Applications of environmental security monitoring based on WSN in substation*. in *Image and Signal Processing (CISP), 2011 4th International Congress on*. 2011.

[7] Akyildiz, I.F., et al., *Wireless sensor networks: a survey.* Computer networks, 2002. **38**(4): p. 393-422.

[8] Al-Obaisat, Y. and R. Braun, *On wireless sensor networks: architectures, protocols, applications, and management.* 2007.

[9] Ashraf, A., et al. *Design and analysis of the security assessment framework for achieving discrete security values in wireless sensor networks*. in *Electrical and Computer Engineering, 2008. CCECE 2008. Canadian Conference on*. 2008.

[10] Ashraf, A., et al. *A model for classifying threats and framework association in wireless sensor networks*. in *Anti-counterfeiting, Security, and Identification in Communication, 2009. ASID 2009. 3rd International Conference on*. 2009.

[11] Aslam, M.S., et al. *Wi-design, Wi-manage, why bother?* in *Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on*. 2011.

[12] Bekara, C., M. Laurent-Maknavicius, and K. Bekara. *Mitigating Resource-Draining DoS Attacks on Broadcast Source Authentication on Wireless Sensors Networks*. in *Security Technology, 2008. SECTECH '08. International Conference on*. 2008.

[13] Brownfield, M., Y. Gupta, and N. Davis. *Wireless sensor network denial of sleep attack*. in *Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC*. 2005. IEEE.

[14] Bruneo, D., A. Puliafito, and M. Scarpa. *Dependability evaluation of Wireless Sensor Networks: Redundancy and topological aspects*. in *Sensors, 2010 IEEE*. 2010.

[15] Byunggil, L., B. Seungjo, and H. Dongwon. *Design of Network Management Platform and Security Framework for WSN*. in *Signal Image Technology and Internet Based Systems, 2008. SITIS '08. IEEE International Conference on*. 2008.

[16] Camtepe, S.A. and B. Yener, *Key distribution mechanisms for wireless sensor networks: a survey.* Rensselaer Polytechnic Institute, Troy, New York, Technical Report, 2005: p. 05-07.

[17] Camtepe, S.A. and B. Yener, *Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks.* Networking, IEEE/ACM Transactions on, 2007. **15**(2): p. 346-358.

[18] Chien-Wen, C., L. Chih-Chung, and I.C. Ray. *A new scheme of key distribution using implicit security in Wireless Sensor Networks*. in *Advanced Communication Technology (ICACT), 2010 The 12th International Conference on*. 2010.

[19] Corke, P., et al., *Environmental Wireless Sensor Networks.* Proceedings of the IEEE, 2010. **98**(11): p. 1903-1917.

[20] de los Angeles Cosio Leon, M., J.I.N. Hipolito, and J.L. Garcia. *A Security and Privacy Survey for WSN in e-Health Applications*. in *Electronics, Robotics and Automotive Mechanics Conference, 2009. CERMA '09.* 2009.

[21] Dey, H. and R. Datta. *Monitoring threshold cryptography based wireless sensor networks with projective plane*. in *Computers and Devices for Communication (CODEC), 2012 5th International Conference on*. 2012.

[22] Di Pietro, R., et al., *United We Stand: Intrusion Resilience in Mobile Unattended WSNs.* Mobile Computing, IEEE Transactions on, 2013. **12**(7): p. 1456-1468.

[23] Doriguzzi Corin, R., G. Russello, and E. Salvadori. *TinyKey: A light-weight architecture for Wireless Sensor Networks securing real-world applications*. in *Wireless On-Demand Network Systems and Services (WONS), 2011 Eighth International Conference on*. 2011.

[24] El Brak, M. and M. Essaaidi. *Wireless sensor network in home automation network and smart grid*. in *Complex Systems (ICCS), 2012 International Conference on*. 2012.

[25] El-din, A., R. Ramadan, and M. Fayek. *A novel fuzzy HEED security using VEGK for wireless sensor networks*. in *Mobile Adhoc and Sensor Systems (MASS), 2012 IEEE 9th International Conference on*. 2012.

[26] El-Din, A.E., R.A. Ramadan, and M.B. Fayek. *Secure clustering based SEP using Virtual ECC Group Key for Wireless Sensor Networks*. in *Engineering and Technology (ICET), 2012 International Conference on*. 2012.

[27] El-Din, A.E., R.A. Ramadan, and M.B. Fayek. *VEGK: Virtual ECC group key for wireless sensor networks*. in *Computing, Networking and Communications (ICNC), 2013 International Conference on*. 2013.

[28] Fei, H., et al. *Reliability Evaluation of Wireless Sensor Networks Using Logistic Regression*. in *Communications and Mobile Computing (CMC), 2010 International Conference on*. 2010.

[29] Fengyun, L., et al. *A Novel Cooperation Mechanism to Enforce Security in Wireless Sensor Networks*. in *Genetic and Evolutionary Computing (ICGEC), 2011 Fifth International Conference on*. 2011.

[30] Frantti, T., H. Hietalahti, and R. Savola. *A risk-driven security analysis and metrics development for WSN-MCN router*. in *ICT Convergence (ICTC), 2013 International Conference on*. 2013.

[31] Garcia-Morchon, O. and H. Baldus. *The ANGEL WSN Security Architecture*. in *Sensor Technologies and Applications, 2009. SENSORCOMM '09. Third International Conference on*. 2009.

[32] Gatti, N., M. Monga, and S. Sicari. *Localization security in Wireless Sensor Networks as a non-cooperative game*. in *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 International Congress on*. 2010.

[33] Gosda, U., *et* al. *Target tracking in wireless sensor networks by data fusion with video-based object detection*. in *Positioning Navigation and Communication (WPNC), 2013 10th Workshop on*. 2013.