INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

WSNs: CHALLENGES AND INDEMNITY

[1]I.AnandaBabu, [2]G.Anitha, [3]Md.Imran

[1, 2, 3] Asst.Prof in the Department of I.T
Gudlavalleru Engineering College, Andhra Pradesh

Abstract: *Wireless Sensor networks have made a tremendous growth, so does the need to enhance security mechanisms. Wireless sensor network is an emerging technology that has great potential for various futuristic applications. In this paper we are surveying all the security related issues, the challenges and to propose some solutions to secure the WSN against these security threats. This paper is organized where we first analyze the important topics in WSN security, what the barriers are and how to overcome those barriers to attain security and finally list there corresponding defensive measures.*

1. INTRODUCTION

One of fundamental goals for Wireless Sensor Networks (WSNs) is to collect information from the physical world. Comparing to existing infrastructure – based networks, wireless sensor networks can virtually work in any environment, especially those where wired connections are not possible. WSNs are often deployed to sense, process and disseminate information of targeted physical environments. Wireless Sensor Networks (WSN) are emerging as both an important new tier in the IT ecosystem and a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management, security and social factors [1], [2], [3]. The basic idea of sensor network is to disperse 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 [4]. 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. 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. We classify the main aspects of wireless sensor network security into four major categories: *the obstacles to sensor network security*, *the requirements of a secure wireless sensor network*, *attacks*, and *defensive measures*. The organization then follows this classification. For the completeness of the chapter, we also give a brief introduction of related security techniques, while providing appropriate citations for those interested in a more detailed discussion of a particular topic. This paper is outlined as follows. Section I provides the introduction to WSN and also covers the basic components and architecture of WSN. Section II describes various security threats of WSN. Section III describes the security challenges in implementing WSN. Section IV provides goals of security in WSN. Section V describes some security mechanism against these security threats. Section VI provides the conclusion of highlighted issues.

1.1 WSN Architecture

A **wireless sensor network (WSN)** of spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling *control* of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. In a typical WSN we see following network components –

Sensor nodes (Field devices) – Each sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for

a) Interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

b) Gateway or Access points – A Gateway enables communication between Host application and field devices.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

c) Network manager – A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network.

d) Security manager – The Security Manager is responsible for the generation, storage, and management of keys.

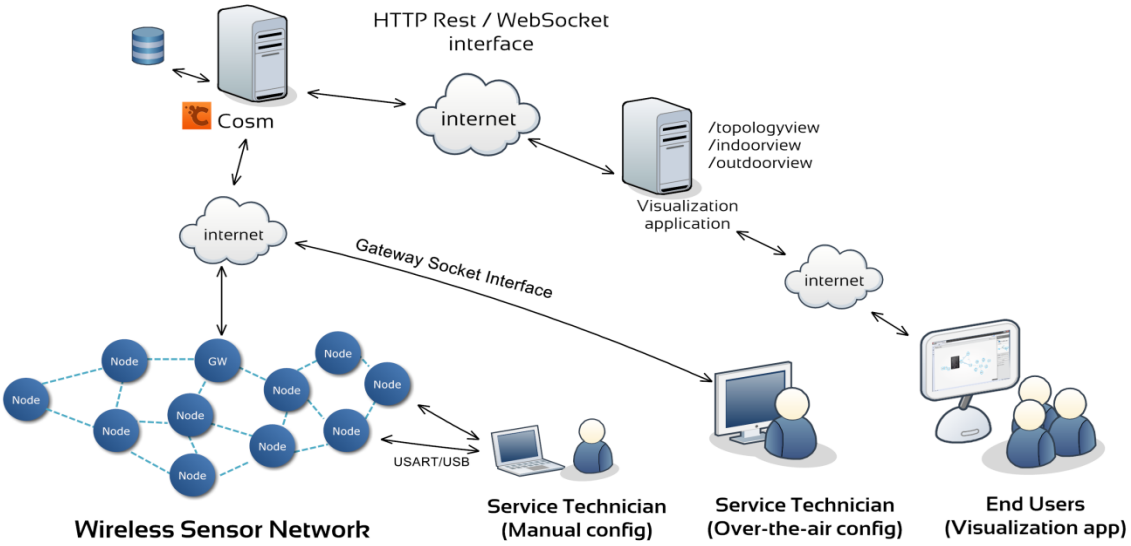


Figure1: WSN Architecture

2. FEASIBILITY OF BASIC SECURITY SCHEMES IN WIRELESS SENSOR NETWORKS

Security is a broadly used term encompassing the characteristics of authentication, integrity, privacy, non repudiation, and anti-playback [5]. 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. For the secure transmission of various types of information over networks, several cryptographic, steganographic and other techniques are used which are well known. In this section, we discuss the network security fundamentals and how the techniques are meant for wireless sensor networks.

2.1 Cryptography

The encryption-decryption techniques devised for the traditional wired networks are not feasible to be applied directly for the wireless networks and in particular for wireless sensor networks. WSNs consist of tiny sensors which really suffer from the lack of processing, memory and battery power [6], [7], [8], [9]. Applying any encryption scheme requires transmission of extra bits, hence extra processing, memory and battery power which are very important resources for the sensors' longevity. Applying the security mechanisms such as encryption could also increase delay, jitter and packet loss in wireless sensor networks [10]. Moreover, some critical questions arise when applying encryption schemes to WSNs like, how the keys are generated or disseminated. How the keys are managed, revoked, assigned to a new sensor added to the network or renewed for ensuring robust security for the network. As minimal (or no) human interaction for the sensors, is a fundamental feature of wireless sensor networks, it becomes an important issue how the keys could be modified time to time for encryption. Adoption of pre-loaded keys or embedded keys could not be an efficient solution.

2.2. Steganography

While cryptography aims at hiding the content of a message, steganography [11], [12] aims at hiding the existence of the message. Steganography is the art of covert communication by embedding a message into the multimedia data (image, sound, video, etc.) [13]. The main objective of steganography is to modify the carrier in a way that is not perceptible and hence, it looks just like ordinary. It hides the existence of the

covert channel, and furthermore, in the case that we want to send a secret data without sender information or when we want to distribute secret data publicly, it is very useful. However, securing wireless sensor networks is not directly related to steganography and processing multimedia data (like audio, video) with the inadequate resources [14] of the sensors is difficult and an open research issue.

2.3 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 [15] could also be utilized which introduces secure physical layer access employing the singular vectors with the channel synthesized modulation.

3. OBSTACLES OF SENSOR SECURITY

A wireless sensor network is a special network which has many constraints compared to a traditional computer network. Due to these constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks. Therefore, to develop useful security mechanisms while borrowing the ideas from the current security techniques, it is necessary to know and understand these constraints first [10].

3.1 Very Limited Resources

All security approaches require a certain amount of resources for the implementation, including data memory, code space, and energy to power the sensor. However, currently these resources are very limited in a tiny wireless sensor.

• *Limited Memory and Storage Space*

A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm. For example, one common sensor type (TelosB) has an 16-bit, 8 MHz RISC CPU with only 10K RAM, 48K program memory, and 1024K flash storage [14]. With such a limitation, the software built for the sensor must also be quite small. The total code space of Tiny OS, the de-facto standard operating system for wireless sensors, is approximately 4K [23], and the core scheduler occupies only 178 bytes. Therefore, the code size for the all security related code must also be small.

• *Power Limitation*

Energy is the biggest constraint to wireless sensor capabilities. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced (high operating cost) or recharged (high cost of sensors). Therefore, the battery charge taken with them to the field must be conserved to extend the life of the individual sensor node and the entire sensor network. When implementing a cryptographic function or protocol within a sensor node, the energy impact of the added security code must be considered. When adding security to a sensor node, we are interested in the impact that security has on the lifespan of a sensor (i.e., its battery life). The extra power consumed by sensor nodes due to security is related to the processing required for security functions (e.g., encryption, decryption, signing data, verifying signatures), the energy required to transmit the security related data or overhead (e.g., initialization vectors needed for encryption/decryption), and the energy required to store security parameters in a secure manner (e.g., cryptographic key storage).

3.2 Unreliable Communication

Certainly, unreliable communication is another threat to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication.

• *Unreliable Transfer*- Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable. Packets may get damaged due to channel errors or dropped at highly congested nodes. The result is lost or missing packets. Furthermore, the unreliable wireless communication channel also results in damaged packets. Higher channel error rate also forces the software developer to devote resources to error handling. More importantly, if the protocol lacks the appropriate error handling it is possible to lose critical security packets. This may include, for example, a cryptographic key.

• Conflicts- Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network. If packets meet in the middle of transfer, conflicts will occur and the transfer itself will fail. In a crowded (high density) sensor network, this can be a major problem. More details about the effect of wireless communication can be found at [1].

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

• Latency-The multi-hop routing, network congestion and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes. The synchronization issues can be critical to sensor security where the security mechanism relies on critical event reports and cryptographic key distribution.

3.3 Unattended Operation

Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. There are three main caveats to unattended sensor nodes:

• *Exposure to Physical Attacks* -The sensor may be deployed in an environment open to adversaries, bad weather, and so on. The likelihood that a sensor suffers a physical attack in such an environment is therefore much higher than the typical PCs, which is located in a secure place and mainly faces attacks from a network.

• *Managed Remotely*- Remote management of a sensor network makes it virtually impossible to detect physical tampering (i.e., through tamperproof seals) and physical maintenance issues (e.g., battery replacement).Perhaps the most extreme example of this is a sensor node used for remote reconnaissance missions behind enemy lines. In such a case, the node may not have any physical contact with friendly forces once deployed.

• *No Central Management* Point A sensor network should be a distributed network without a central management point. This will increase the vitality of the sensor network. However, if designed incorrectly, it will make the network organization difficult, inefficient, and fragile. Perhaps most importantly, the longer that a sensor is left unattended the more likely that an adversary has compromised the node.

4. SECURITY THREATS AND ISSUES IN WSN

Wireless Sensor Networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Basically attacks are broadly classified in two categories i.e. active attacks and passive attacks. This paper points out both of these attacks in details.

4.1 Passive Attacks

The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. Some of the more common attacks against sensor privacy are:

4.1.1 Monitor and Eavesdropping:

This is the most common attack to privacy. By snooping to the data, the adversary could easily discover the communication contents.

4.1.2 Traffic Analysis:

Even when the messages transferred are encrypted, it still leaves a high possibility analysis of the communication patterns. Sensor activities can potentially reveal enough information to enable an adversary to cause malicious harm to the sensor network.

4.1.3 Camouflage Adversaries:

One can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can copy as a normal node to attract the packets, then misroute the packets, conducting the privacy analysis.

4.2 Active Attacks

The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. The following attacks are active in nature.

4.2.1 Routing Attacks in Sensor Networks:

The attacks which act on the network layer are called routing attacks. The following are the attacks that happen while routing the messages.

4.2.1.1 Attacks on Information in transit:

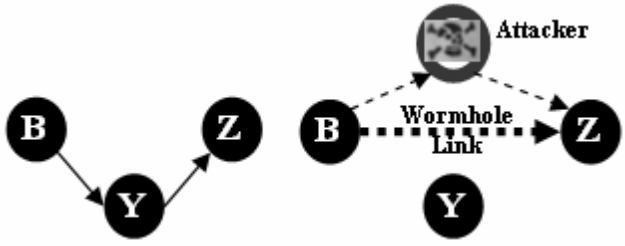
In a sense or network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be altered, spoofed, replayed again or vanished. As wireless communication is vulnerable to eavesdropping, 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.

4.2.1.2 Selective Forwarding:

A malicious node can selectively drop only certain packets. Especially effective if combined with an attack that gathers much traffic via the node. In sensor networks it is assumed that nodes faithfully forward received messages. But some compromised node might refuse to forward packets, however neighbors might start using another route.

4.3 Wormholes Attacks:

Wormhole attack is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location.



(a) (b)

Figure 2: Wormhole Attack

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Figure 2 (a and b) shows a situation where a wormhole attack takes place. When a node B (for example, the base station or any other sensor) broadcasts the routing request packet, the attacker receives this packet and replays it in its neighborhood. Each neighboring node receiving this replayed packet will consider itself to be in the range of Node B, and will mark this node as its parent. Hence, even if the victim nodes are multi-hop apart from B, attacker in this case convinces them that B is only a single hop away from them, thus creates a wormhole.

4.3.1 HELLO flood attacks:

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.

4.3.2 Denial of Services:

Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action. In wireless sensor networks, several types of DoS attacks in different layers might be performed.

4.3.3 Node Subversion:

Capture of a node may reveal its information including disclosure of cryptographic keys and thus compromise the whole sensor network. A particular sensor might be captured, and information (key) stored on it might be obtained by an adversary.

4.3.4 Node Malfunction:

A malfunctioning node will generate inaccurate data that could expose the integrity of sensor network especially if it is a data-aggregating node such as a cluster leader.

4.4 Node Outage:

Node outage is the situation that occurs when a node stops its function. In the case where a cluster leader stops functioning, the sensor network protocols should be robust enough to mitigate the effects of node outages by providing an alternate route.

4.5 Physical Attacks:

Unlike many other attacks mentioned above, physical attacks destroy sensors permanently, so the losses are irreversible. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker.

4.6 Message Corruption:

Any modification of the content of a message by an attacker compromises its integrity.

4.7 False Node:

A false node involves the addition of a node by an adversary and causes the injection of malicious data. An intruder might add a node to the system that feeds false data or prevents the passage of true data. Insertion of malicious node is one of the most dangerous attacks that can occur.

4.8 Node Replication Attacks:

Conceptually, a node replication attack is quite simple; an attacker seeks to add a node to an existing sensor network by copying the node ID of an existing sensor node. A node replicated in this approach can severely disrupt a sensor network's performance. Packets can be corrupted or even misrouted.

4.9 Passive Information Gathering:

An adversary with powerful resources can collect information from the sensor networks if it is not encrypted. To minimize the threats of passive information gathering, strong encryption techniques needs to be used.

5. PROPOSED SECURITY SCHEMES AND RELATED WORK

In the recent years, wireless sensor network security has been able to attract the attentions of a number of researchers around the world. In this section we review and map various security schemes proposed or implemented so far for wireless sensor networks.

5.1. Security Schemes for Wireless Sensor Networks

[17] Gives an analysis of secure routing in wireless sensor networks. [25] Studies how to design secure distributed sensor networks with multiple supply voltages to reduce the energy consumption on computation and therefore to extend the network's life time. [7] aims at increasing energy efficiency for key management in wireless sensor networks and uses Younis et. al. [27] network model for its application. Wood et al. [22] studies DoS attacks against different layers of sensor protocol stack. JAM [29] presents a mapping protocol which detects a jammed region in the sensor network and helps to avoid the faulty region to continue routing within the network, thus handles DoS attacks caused by jamming. In [30] the authors show that wormholes those are so far considered harmful for WSN could effectively be used as a reactive defense mechanism for preventing jamming DoS attacks. Ye et. al. [24] presents a statistical en-route filtering (SEF) mechanism to detect injected false data in sensor network and focus mainly on how to filter false data using collective secret and thus preventing any single compromised node from breaking the entire system. SNEP & μTESLA [6] are two secure building blocks for providing data confidentiality, data freshness and broadcast authentication. Tiny Sec [26] proposes a link layer security mechanism for sensor networks which uses an efficient symmetric key encryption

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

protocol. Newsome et. al. [16] proposes some defense mechanisms against Sybil attack in sensor networks. Kulkarni et al. [19] analyzes the problem of assigning initial secrets to users in ad-hoc sensor networks to ensure authentication and privacy during their communication and points out possible ways of sharing the secrets. [31] presents a probabilistic secret sharing protocol to defend Hello flood attacks. The scheme uses a bidirectional verification technique and also introduces multi-path multi-base station routing if bidirectional verification is not sufficient to defend the attack.

Table 1: Summary of various security schemes for wireless sensor

SECURITY SCHEMA	ATTACKS DETERRED	NETWORK ARCHITECTURE	MAJOR FEATURES
JAM [29]	DoS Attack (Jamming)	Traditional wireless sensor network	Avoidance of jammed region by using coalesced neighbor nodes
Wormhole based [30]	DoS Attack (Jamming)	Wormhole based [30]	Uses wormholes to avoid jamming
Statistical En-Route Filtering [24]	Information Spoofing	Large number of sensors, highly dense wireless sensor network	Detects and drops false reports during forwarding process
Radio Resource Testing, Random Key Pre-distribution etc. [16]	Sybil Attack	Traditional wireless sensor network	Uses radio resource, Random key pre-distribution, Registration procedure, Position verification and Code attestation for detecting sybil entity
Bidirectional Verification, Multi-path multi-base station routing [31]	Hello Flood Attack	Traditional wireless sensor network	Adopts probabilistic secret sharing, Uses bidirectional verification and multi-path multi-base station routing
TIK [18]	Wormhole Attack, Information or Data Spoofing	Traditional wireless sensor network	Based on symmetric cryptography, Requires accurate time synchronization between all communicating parties, implements temporal leashes
Random Key Predistribution[20],[21], [32]	Data and information spoofing, Attacks in information in Transit	Traditional wireless sensor network	Provide resilience of the network, Protect the network even if part of the network is compromised, Provide authentication measures for sensor nodes
REWARD [34]	Blackhole attacks	Traditional wireless sensor network	Uses geographic routing, Takes advantage of the broadcast inter-radio behavior to watch neighbor transmissions and detect black hole attacks
TinySec [26]	Data and Information spoofing, Message Replay Attack	Traditional wireless sensor network	Focuses on providing message authenticity, integrity and confidentiality, Works in the link layer
SNEP & μTESLA [6]	Data and Information Spoofing, Message Replay Attacks	Traditional wireless sensor network	Semantic security, Data authentication, Replay protection, Weak freshness, Low communication overhead

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

REWARD [34] is a routing algorithm which fights against blackholes in the network. [23] proposes separate security schemes for data with various sensitivity levels and a location-based scheme for wireless sensor networks that protects the rest of the network, even when parts of the network are compromised. [18] implements symmetric key cryptographic algorithms with delayed key disclosure on motes to establish secure communication channels between a base station and sensors within its range. [32], [33], [20] and [21] propose key pre-distribution schemes, which target to improve the resilience of the network. In Table 1 we summarize various security schemes along with their main properties proposed so far for wireless sensor networks.

5.2. Holistic Security in Wireless Sensor Networks

A holistic approach [28] aims at improving the performance of wireless sensor networks with respect to security, longevity and connectivity under changing environmental conditions. The holistic approach of security concerns about involving all the layers for ensuring overall security in a network. For such a network, a single security solution for a single layer might not be an efficient solution rather employing a holistic approach could be the best option.

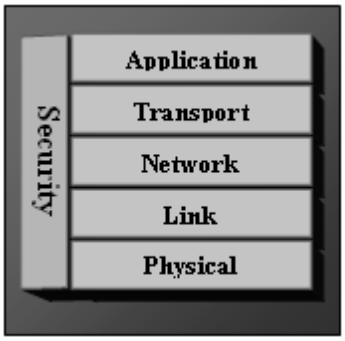


Figure 3: Holistic view of Security in wireless sensor networks

The holistic approach has some basic principles like, in a given network; security is to be ensured for all the layers of the protocol stack, the cost for ensuring security should not surpass the assessed security risk at a specific time, if there is no physical security ensured for the sensors, the security measures must be able to exhibit a graceful degradation if some of the sensors in the network are compromised, out of order or captured by the enemy and the security measures should be developed to work in a decentralized fashion. If security is not considered for all of the security layers, for example; if a sensor is somehow captured or jammed in the physical layer, the security for the overall network breaks despite the fact that, there are some efficient security mechanisms working in other layers. By building security layers as in the holistic approach, protection could be established for the overall network.

6. CONCLUSION

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. In this chapter we have described the four main aspects of wireless sensor network security: obstacles, requirements, attacks, and defenses. Within each of those categories we have also sub-categorized the major topics including routing, trust, denial of service, and so on. Our aim is to provide both a general overview of the rather broad area of wireless sensor network security, and give the main citations such that further review of the relevant literature can be completed by the interested researcher. As wireless sensor networks continue to grow and become more common, we expect that further expectations of security will be required of these wireless sensor network applications. We also expect that the current and future work in privacy and trust will make wireless sensor networks a more attractive option in a variety of new arenas.

REFERENCES

[1] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[2] Akyildiz, I. F., Su, W., Sankara subramaniam, Y, and Cayirci, E., "Wireless Sensor Networks: A Survey", Computer Networks, 38, 2002, pp. 393-422.

[3] Dai, S, Jing, X, and Li, L, "Research and analysis on routing protocols for wireless sensor networks", Proc. International Conference on

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Communications, Circuits and Systems, Volume 1, 27-30 May, 2005, pp.407-411.

[4] Pathan, A-S. K., Islam, H. K., Sayeed, S. A., Ahmed, F. and Hong, C. S., "A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks", to appear in IEEE ICNEWS 2006.

[5] Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J., "Security for Sensor Networks", CADIP Research Symposium, 2002, available at, http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf

[6] Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D., "SPINS: Security Protocols for Sensor Networks", Wireless Networks, vol. 8, no.5, 2002, pp. 521-534.

[7] Jolly, G., Kuscu, M.C., Kokate, P., and Younis, M., "A Low-Energy Key Management Protocol for Wireless Sensor Networks", Proc. Eighth IEEE International Symposium on Computers and Communication, 2003.(ISCC 2003). vol.1, pp. 335 - 340.

[8] Rabaey, J.M., Ammer, J., Karalar, T., Suetfei Li., Otis, B., Sheets, Mand Tuan, T., "PicoRadios for wireless sensor networks: the next challenge in ultra-low power design" 2002 IEEE International Solid-State Circuits Conference (ISSCC 2002), Volume 1, 3-7 Feb. 2002, pp. 200 –201.

[9] Hollar, S, "COTS Dust", Master's Thesis, Electrical Engineering and Computer Science Department, UC Berkeley, 2000.

[10] Saleh, M. and Khatib, I. A., "Throughput Analysis of WEP Security in Ad Hoc Sensor Networks", Proc. The Second International Conference on Innovations in Information Technology (IIT'05), September 26-28, Dubai, 2005.

[11] Kurak, C and McHugh, J, "A Cautionary Note on Image Downgrading in Computer Security Applications", Proceedings of the 8th Computer Security Applications Conference, San Antonio, December, 1992, pp. 153-159.

[12] Mokowitz, I. S., Longdon, G. E., and Chang, L., "A New Paradigm Hidden in Steganography", Proc. of the 2000 workshop on New security paradigms, Ballycotton, County Cork, Ireland, 2001, pp. 41 – 50.

[13] Kim, C. H., O, S. C., Lee, S., Yang, W. I., and Lee, H-W., "Steganalysis on BPCS Steganography", Pacific Rim Workshop on Digital Steganography (STEG'03), July 3-4, Japan , 2003.

[14] Younis, M., Akkaya, K., Eltoweissy, M., and Wadaa, A., "On handling QoS traffic in wireless sensor networks", Proc. of the 37th Annual Hawaii International Conference on System Sciences, 2004, 5-8 January, 2004, pp. 292 – 301.

[15] Orihashi, M., Nakagawa, Y., Murakami, Y., and Kobayashi, K., "Channel synthesized modulation employing singular vector for secured access on physical layer", IEEE GLOBECOM 2003, Volume 3, 1-5 December, 2003, pp. 1226 – 1230.

[16] Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensor networks: analysis & defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268.

[17] Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks:Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.

[18] Hu, Y.-C., Perrig, A., and Johnson, D.B., "Packet leashes: a defense against wormhole attacks in wireless networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 – 1986.

[19] Kulkarni, S. S., Gouda, M. G., and Arora, A., "Secret instantiation in adhoc networks," Special Issue of Elsevier Journal of Computer Communications on Dependable Wireless Sensor Networks, May 2005, pp. 1–15.

[20] Du, W., Deng, J., Han, Y. S., and Varshney, P. K., "A pairwise key pre-distribution scheme for wireless sensor networks", Proc. of the 10th ACM conference on Computer and communications security, 2003, pp.42-51.

[21] Oniz, C. C, Tasci, S. E, Savas, E., Ercetin, O., and Levi, A, "SeFER: Secure, Flexible and Efficient Routing Protocol for Distributed Sensor Networks",fromHttp://people.sabanciuniv.edu/~levi/SeFER_EWSN.pdf

[22] Wood, A. D. and Stankovic, J. A., "Denial of Service in Sensor Networks", Computer, Volume 35, Issue 10, Oct. 2002 pp. 54 - 62.

[23] Slijepcevic, S., Potkonjak, M., Tsiatsis, V., Zimbeck, S., and Srivastava, M.B., "On communication security in wireless ad-hoc sensor networks", 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002, 10-12 June 2002, pp.139 – 144.

[24] Ye, F., Luo, H., Lu, S, and Zhang, L, "Statistical en-route filtering of injected false data in sensor networks", IEEE Journal on Selected Areas in Communications, Volume 23, Issue 4, April 2005, pp. 839 – 850.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

[25] Yuan, L. and Qu, G., "Design space exploration for energy-efficient secure sensor network", Proc. The IEEE International Conference on Application-Specific Systems, Architectures and Processors, 2002, 17-19 July 2002, pp. 88 – 97.

[26] Karlof, C., Sastry, N., and Wagner, D., "TinySec: a link layer security architecture for wireless sensor networks", Proc. of the 2nd international conference on Embedded networked sensor systems, Baltimore, MD, USA, 2004, pp. 162 – 175.

[27] Younis, M., Youssef, M., and Arisha, K., "Energy-aware routing in cluster-based sensor networks" Proc. 10th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunications Systems, 1-16 Oct. 2002 pp. 129 – 136.

[28] Avancha, S, "A Holistic Approach to Secure Sensor Networks", PhD Dissertition, University of Maryland, 2005.

[29] Wood, A.D., Stankovic, J.A., and Son, S.H., "JAM: A Jammed-Area Mapping Service for Sensor Networks", 24th IEEE Real-Time Systems Symposium, RTSS 2003, pp. 286-297.

[30] Cagalj, M., Capkun, S., and Hubaux, J-P., "Wormhole-based Anti-Jamming Techniques in Sensor Networks" from http://lcawww.epfl.ch/ Publications/Cagalj/CagaljCH05-worm.pdf

[31] Hamid, M. A., Rashid, M-O., and Hong, C. S., "Routing Security in Sensor Network: Hello Flood Attack and Defense", to appear in IEEE ICNEWS 2006, 2-4 January, Dhaka.

[32] Chan, H, Perrig, A., and Song, D., "Random key predistribution schemes for sensor networks", In IEEE Symposium on Security and Privacy, Berkeley, California, May 11-14 2003, pp. 197–213.

[33] Eschenauer, L. and Gligor, V. D., "A key-management scheme for distributed sensor networks", Proc. ACM CCS'02, 18-22 November 2002, pp. 41-47.

[34] Karakehayov, Z., "Using REWARD to detect team black-hole attacks in wireless sensor networks", in Workshop on Real-World Wireless Sensor Networks (REALWSN'05), 20-21 June, 2005, Stockholm, Sweden.