Technical Report 2008N3-SP-NL

Security in Wireless Sensor Networks: Prospects, Challenges, and Future

Al-Sakib Khan Pathan and Choong Seon Hong
Department of Computer Engineering, Kyung Hee University
1 Seocheon, Giheung, Yongin, 449701 Gyeonggi, South Korea
spathan@networking.khu.ac.kr, cshong@khu.ac.kr

CHAPTER ABSTRACT

With the advancements of networking technologies and miniaturization of electronic devices, wireless sensor network (WSN) has become an emerging area of research in academic, industrial, and defense sectors. Different types of sensing technologies combined with processing power and wireless communication capability make sensor networks very lucrative for their abundant use in near future. However, many issues are yet to be solved before their full-scale practical implementations. Among all the research issues in WSN, security is one of the most challenging topics to deal with. The major hurdle of securing a WSN is imposed by the limited resources of the sensors participating in the network. Again, the reliance on wireless communication technology opens the door for various types of security threats and attacks. Considering the special features of this type of network, in this chapter we address the critical security issues in wireless sensor networks. We talk about cryptography, steganography, and other basics of network security and their applicability in WSN. We explore various types of threats and attacks against wireless sensor networks, possible countermeasures, mentionable works done so far, other research issues, etc. We also introduce the view of holistic security and future trends towards research in wireless sensor network security.

In a nutshell, in this chapter we will learn about the following topics:

- Basics of security in wireless sensor networks
- Feasibility of applying various security approaches in WSN
- Threats and attacks against wireless sensor networks
- Key management issues
- Secure routing in WSN
- Holistic view of security in WSN
- Future research issues and challenges

Table of Contents

Security in Wireless Sensor Networks: Prospects, Challenges, and Future

1. INTRODUCTION

Wireless Sensor Network (WSN) offers a unique way of extracting data from hazardous geographical regions where human intervention is extremely difficult, the network is often unattended, and where a good level of security has to be maintained for each step of the network's operation. Among all varieties of wireless networks, WSN is the type of network that demands high-level security as one of its core features. In practical terms, WSN is considered as a class of ad hoc networks which could be formed whenever needed and sometimes without a fixed infra-structure. We define a sensor network as a network consisting of a set of small sensor devices that are deployed in an ad hoc fashion to cooperate with each other for sensing certain physical phenomenon. Typically a WSN has one or more base stations (sometimes called as *sink*) and relatively a great number of tiny sensing devices.

Various issues in WSN are still under investigation and most of them are yet to reach the desired standards. Over the past few decades, with the advancements of ad hoc networking technologies, the research works on WSN have also been benefited. However, because of the differences in the nature of works and constrained resources of the sensors, a lot of issues simply could not be solved with the solutions that are devised for traditional ad hoc networks. '*Security in WSN*' is one of such issues that should be handled with special care.

Security in wireless sensor network has a great number of challenges, ranging from the nature of wireless communications, constrained resources of the sensors, unknown topologies of the deployed networks, unattended environment where sensors might be susceptible to physical attacks, dense and large networks, etc [1], [2]. In fact, each of these issues leads to different research direction. Whenever we think about any feasible security scheme for WSNs, we focus on a specific aspect and often ignore the other associated threats. It is in reality impossible to deal with all the security threats with a single mechanism. Hence, our approach often is to choose the most apposite mechanism among all the available mechanisms, based on the situation at hand and the settings of the network.

From the high-level point of view, we consider the following six principles while considering security for any system. These are collectively known as the *philosophy of mistrust*:

- *Don't talk to any one you don't know*
- *Accept nothing without a guarantee*
- *Take everyone as an enemy until proved otherwise*
- *Don't trust your friend for long*
- *Use well-tried solutions*
- *Watch the ground you are standing on for cracks*

Maintaining all these principles at the same time requires a lot of computational, memory, and energy resources which could often not be afforded for a security solution for wireless sensor networks. Sometimes we have to consider the schemes simply based on trust, the well-established solutions for other networks are often extremely difficult to think of, and sometimes employing periodic renewal for any security component is not at all viable. All these points make the research works on security in WSN very interesting as well as very challenging.

In this chapter, we present a detailed review of security in wireless sensor network considering all the challenges, prospects, and the futuristic views. As we will mainly focus on the ins and outs of security in WSN, other introductory aspects of sensor networks will not be discussed. Interested readers are suggested to go through [3] for a good survey on the basics of wireless sensor networks.

We have started this chapter with a brief introduction of wireless sensor network, its characteristics, and the major challenges that it faces to get an efficient security solution. In the rest of this chapter, we will first learn about the key aspects to consider for WSN security, various security approaches, whether they are directly applicable for WSN or not, major threats and attacks in WSN, their detection, prevention, and countermeasures, key management issues, and secure routing issues. Before concluding the chapter, we will talk about holistic view of security and what we can expect in the near future for research on WSN security.

2. BACKGROUND

Before an in-depth investigation of the security threats and attacks in wireless sensor networks, let us first have a look at the major aspects that make the issue of maintaining security so difficult for wireless sensor networks.

2.1. Key Aspects to Consider for WSN Security

2.1.1. Constrained Resources of Sensors

The sensors that build up the network are usually of inadequate memory, processing, and communication capabilities that cannot support the execution of large amount of codes. Their energy sources are also very limited. As an example, Crossbow MICA2 mote [4] is a well-known sensor node with an ATmega128L 8-bit processor at 8 MHz, 128KB program memory (flash), 512KB additional data flash memory, 433, 868/916, or 310 MHz multi-channel radio transceiver, 38.4 kpbs radio, 500-1000 feet outdoor range (depending on versions) with a size of only 58 x 32 x 7 (mm). Usually it is run by TinyOS operating system and powered by 2 AA sized batteries. Hence, it is understandable that such a device with this configuration cannot support the security mechanisms that require executing huge amount of instructions. Again, usually a sensor network contains a large number of sensor nodes. The number of sensors in the network might directly affect the use of memory space of a particular node participating in the network. This is because the memory is frequently used to store pre-distributed secret keys or keying information or the codes to find out pairwise secret keys between any two nodes in the network. Node failure is another problem that could also affect the network severely. If a node is alive relatively longer than the other nodes in the network (say for performing huge calculations related to security), it might lose its energy rapidly and can be non-functional relatively earlier than the other less active nodes.

2.1.2. Nature of Work of WSN

Many applications of wireless sensor networks require deployment of sensors in remote, unattended, hostile, or hazardous areas. The sensors are often exposed to various types of adversaries and could be attacked physically. Even if they are deployed over a field, a passing vehicle can run over and physically damage them. An adversary can physically search and destroy the nodes [5]. Environmental conditions might also affect the performance of the sensors or can cause physical damage. All these unintentional or intentional events that can cause physical damage to a sensor are considered as physical security issues. Sometimes physical attacks (like capture or destruction of nodes) can also cause several types of logical security attacks. A good deployment or management policy, tamper-proofing mechanisms of the physical package of the sensors, camouflaging, protective shields, or other available techniques [6] could

be used for dealing with physical security threats in wireless sensor network. More discussions on these issues will be provided later in this chapter.

2.1.3. Use of Wireless Communications

Wireless technology is used for communications among the nodes in a wireless sensor network. Hence, similar to any other kind of wireless network, it is also prone to various types of threats related to the unreliable nature of wireless links like; undelivered packets, collisions of packets, latency, etc. Because of the broadcast nature of wireless channels, any adversary can even eavesdrop or passively listen to the transmissions of any legitimate node. In case of wired communication, the guided media could be well-protected by using various means and usually the end devices come with sufficient protective mechanisms. On the contrary, in case of wireless communication, because of its unguided medium and open nature, many new types of attacks could be launched. In fact, many of the security threats in WSN exist because of the use of wireless technology for communications among the nodes.

2.2. Feasibility of Different Security Approaches in WSN

Security is a broadly used term encompassing the characteristics of authentication, integrity, privacy, non-repudiation, and anti-playback [7]. Over the past few decades, the more the dependency on network-provided information has increased, the more the risk has increased for secure transmission of information over the networks. To ensure various aspects of security (i.e., authenticity, integrity, privacy, etc.), we use various approaches like cryptography, steganography, physical layer security, and so on. In this section, we will examine which of the major security approaches can be viable for wireless sensor networks.

2.2.1. Cryptography

Most of the encryption-decryption techniques devised for traditional wired networks are not fit for direct use in wireless networks. We know that WSNs consist of tiny low-cost devices which possess very scarce processing, memory, and battery power. Applying any kind of encryption scheme requires transmission of extra bits, and thus it needs extra processing, memory, and battery power which are very important resources for the sensors' longevity. Applying the encryption and decryption operations can also increase delay, jitter, and packet loss in wireless sensor networks. Moreover, some critical questions arise when applying an encryption-decryption scheme to WSN like; how the keys should be generated, how the keys should be disseminated, how the keys should be managed, revoked, or assigned to a newly added sensor in the network,

and so on. As minimal (or no) human interaction is one of the fundamental features of WSN, it is also a crucial point to decide how the keys could be modified/refreshed time to time for encryption. Adoption of pre-loaded keys or embedded keys might always not be the best solution. Overall, the schemes that are based on cryptographic techniques must be lightweight so that the sensors can support them along with other mechanisms, which are running and sharing the same available resources in the tiny devices.

2.2.2. Steganography

While cryptography aims at hiding the content of a message, steganography [8], [9] 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.) [10]. The main objective of steganography is to modify the carrier in a way so that it is not perceptible and hence, looks just like ordinary. It hides the existence of the covert channel, and furthermore, if we want to send a secret data without sender information or 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 of the sensors is difficult. Instead, it still remains as an open research issue. We might have to wait until the sensors acquire enough capabilities to support extensive computations associated with steganography.

2.2.3. 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 point in physical layer secure access is the efficient design so that the hopping sequence is modified in less time than is required to discover it. One drawback for employing this is that both the sender and receiver should maintain a synchronized clock. Time synchronization in wireless sensor network [11] is another research issue that might relatively be easier or harder based on the application requirements at hand.

Considering all the basic security approaches, lightweight cryptography related or logical or algorithmic schemes could be the best choice for WSN security. We must keep in mind that, the

higher is the level of security of a WSN, the higher is the amount of resources needed to support it.

3. Security Issues in Wireless Sensor Networks

Let us now investigate the security threats and attacks in wireless sensor networks. We can consider several factors for categorizing the attacks like; the approach of attack, target of the attack, position of attacker, role of attacker, etc. Overall, we can classify all of the known attacks into three basic types:

Type I

- ***Attacks on the Basic Mechanism*** (e.g., attacks against routing in the network)
- ***Attacks on the Security Mechanisms*** (e.g., against cryptographic scheme or against key management scheme)

Type II

- ***Passive Attack*** – It typically means eavesdropping of data. In this case, the attacker passively listens to the transmitted data in the network and can use the collected information later for launching other types of attacks.
- ***Active Attack*** – It means any type of direct attack caused by an adversary. The attacker actively participates in the collection, modification, and fabrication of data. Sometimes, the information collected by passive attacks can be used for active attacks.

Type III

- ***External Attack*** – In external attack, an outsider is involved. These attacks can cause denial of service (DoS) situation, congestion, propagation of wrong routing information, etc. Typically external attacks can be resisted using firewalls, encryption mechanisms, good security management policy, and other available techniques.
- ***Internal Attack*** – Internal attack sometimes could be very harmful for the network as any node within the network works as an attacker in this case. Internal attack is performed by compromising node(s) in the network. Compromising a node means convincing a legitimate node to help the attacker or persuading a node in the network to work on behalf of the attacking entity. Often it is difficult to detect an internal attacker within the network which shows a legitimate identity. Various kinds of authentication schemes,

intrusion detection schemes, or membership verification schemes can be used for preventing internal attacks.

Other than these basic categories of attacks, depending upon the working principles and attack methods, several attacks are given some formal names. Here, we will learn about all the known attacks in WSN with their major features and possible defense mechanisms.

3.1. Denial of Service (DoS) Attack

Strictly speaking, we consider any kind of attempt of an adversary to disrupt, subvert, or destroy the network as Denial of Service (DoS) attack. In reality, any kind of incident that diminishes or eliminates or hinders the normal activities of the network can cause a DoS situation. It means that any kinds of hardware failures, software bugs, resource exhaustion, environmental conditions, or any type of complicated interaction of these factors can cause DoS. Note that, *DoS* (Denial of Service) is basically a given formal name of a particular condition of the network but when it occurs as a result of an intentional attempt of an adversary, it is called *DoS attack*. In general, '*Denial of Service (DoS)*' is an umbrella term that can indicate many kinds of events in the network with the fact that the legitimate nodes are deprived of getting their expected legitimate services for some reasons (intentional attempts or unintentional incidents).

DoS attacks can mainly be categorized into three types:

(1) Consumption of scarce, limited, or non-renewable resources
(2) Destruction or alteration of configuration information
(3) Physical destruction or alteration of network resources

Among these types of DoS attacks, the first one is the most significant for wireless sensor networks as the sensors in the network suffer from the lack of enough and renewable resources. Other than these basic types, layer wise categorization of DoS attacks can be done [12]. An attacker can choose different targets at different layers to stop proper functioning of legitimate nodes so that they cannot get the services they are entitled to. Though it is quite difficult to know whether any particular DoS situation is caused intentionally or unintentionally, there are some common prevention and detection methods for each of the DoS attacks.

Let us now have a look at the layer wise DoS attacks in wireless sensor networks:

3.1.1. DoS Attacks in Physical Layer

Jamming – Jamming means the deliberate interference with radio reception to deny a target's use of a communication channel. For single-frequency networks, it is simple and effective, causing the jammed node unable to communicate or coordinate with others in the network. Due to their very nature, wireless sensor networks are probably the category of wireless networks most vulnerable to "radio channel jamming"-based Denial of Service (DoS) attacks [13]. Mainly two types of jamming could be possible; constant and sporadic. In case of constant jamming, attacker interferes with the signals of a legitimate node continuously for a certain period of time while in case of sporadic jamming, the attacker intermittently causes jamming. Sporadic jamming in the network is often more difficult to detect than detecting constant jamming. Some solutions to deal with jamming in WSN are proposed in [13], [14], and [15].

Tampering – Due to the unattended feature of wireless sensor networks, an attacker can physically damage/replace sensors, parts of computational and sensitive hardware, even can extract cryptographic keys to gain unrestricted access to higher communication layers. Tampering is actually any type of physical attack on sensors in the network. Success in tampering depends on:

- how accurately and efficiently the designer considered the potential threats at design time
- resources available for design, construction, and test
- attacker's cleverness and determination

3.1.2. DoS Attacks in Link Layer

Collision – Adversaries may only need to induce a collision in one octet of a transmission to disrupt even a relatively longer packet. As the resources of the sensors are scarce, such loss could be significant in many cases. Also it is a great hurdle for acquiring timely and accurate data from the sensors. Unfortunately, in wireless networks, detection of a collision with a node's own transmission is difficult. Standard collision avoidance mechanisms also cannot help as they are cooperative by nature. An attacker simply can ignore the avoidance protocol and transmit at the same time as the victim. One possible solution could be the use of error correction codes (ECC) but with the use of ECC, more processing and communication overheads are incurred in such resource-constrained networks.

Exhaustion – Battery exhaustion attack could be launched with repeated requests for using the channel. A naive link layer implementation could be a target for this type of attack. Feasible defense mechanisms against battery exhaustion caused by repeated transmissions could be the use of time division multiple access (TDMA) or rate limitation. Additional logics could also be developed to help these mechanisms.

Unfairness – Unfairness is a weaker form of DoS attack. This threat may not entirely prevent legitimate access to the channel, but could degrade service for real time MAC protocols. In fact, ensuring fairness in WSN is often viewed as a separate research issue. Use of small frames might be helpful in this case. However this would also incur some framing overheads.

3.1.3. DoS Attacks in Network Layer

Neglect and Greed – If a node drops packets or denies transmitting legitimate packets or if a node is very greedy to give undue priority to its own messages, these could be considered as '*neglect and greed*'. Dynamic Source Routing (DSR) protocol or the protocols that are based on DSR are especially vulnerable to this type of attack. Use of multipath routing or redundant message transmission could be the solutions for handling such attacks. However, for WSNs these solutions might not be feasible. Instead, use of some other routing mechanisms could help.

Homing – Sometimes in wireless sensor networks, some nodes are given some special responsibilities like managing cryptographic keys, making gist of acquired data, maintaining a local group, etc. Often the adversaries are attracted to these leader nodes and try to eavesdrop on their activities. In case of homing attack, the adversaries try to hamper the normal functioning of such types of leader nodes within a WSN. Homing attack is especially dangerous for the location-aware routing protocols which rely on geographic information. Different types of cryptographic schemes, algorithms, hiding management messages, etc. could be used for preventing homing attack.

Misdirection – Misdirection means simply directing the legitimate packets to the wrong path. A malicious insider can cause misdirection of traffic. Egress filtering (in hierarchical routing protocols), authorization and monitoring, or any kind of intrusion detection scheme (IDS) [16] could be used to prevent this type of DoS attack.

Blackhole – Blackhole (or Sinkhole) attack itself is one of the major attacks in WSN. We will discuss this attack in detail later in this chapter. However, when this attack causes any sort of *denial of service* in the network, it is considered as a DoS attack in network layer.

3.1.4. Transport Layer DoS Attacks

Flooding – Protocols which must keep the states of both end-nodes are particularly vulnerable to this attack. It aims at memory exhaustion of the nodes by flooding of a great number of packets. Client puzzles or traceback mechanisms could be used to deal with such type of DoS attack.

Desynchronization – This attack means forging of packets during transmission. Existing connection between two endpoints could be effectively disrupted by desynchronization. Any kind of authentication mechanism for the packets could be used to handle desynchronization attack.

Other than these attacks, many other individually considered attacks like wormhole attack, hello flood attack, sybil attack etc. can also cause *denial of service* situation in the network. This is in fact true that, many of the methods of attacking and targets of attacks simply overlap with each other, but considering different circumstances, they are given different tags and names. It should be clear that, any sort of intentional attempt that causes any sort of *denial of service* situation in the network is considered as *DoS attack*. As we will examine all other attacks in the rest of the chapter, here we conclude this section with the names of the major types of DoS attacks only.

3.2. Attacks on Information in Transit

Basic task of the sensors is to monitor the changes of some specific parameters (like temperature, sound, magnetism, light level, etc.) and to report those to the base station. The readings from the sensors could be transmitted using various methods. But, while sending the readings, the packets may be altered, spoofed, or vanished on the way (this type of attack could also be considered as network layer DoS attack when it resists a valid node from getting its expected service). As wireless communication is susceptible to eavesdropping, any attacker can monitor the traffic flow and get into action to interrupt, intercept, modify, or fabricate packets. If the routing method does not have proper security measures, wrong information even can reach up to the base station and thus can influence the decision taken by the central authority. Such an event might be extremely dangerous for a military reconnaissance scenario which could lead to taking disastrous military decisions. As sensor nodes typically have short range of transmission and scarce resources, an attacker with adequate processing power and larger communication range can attack several

sensors at the same time to modify the actual information during transmission. Among several works, a good approach to tackle this and to filter out falsely injected data in sensor networks is presented in [88].

3.3. Sybil Attack

Sometimes the sensors in a wireless sensor network might need to work together to accomplish a task, hence the management policy of the network can use distribution of subtasks and redundancy of information. In such a situation, a node can pretend to be more than one node at the same time using the identities of other legitimate nodes. This type of attack where a node forges the identities of more than one node is called a *Sybil attack* [17]. The malicious device's additional identities are called the *Sybil nodes*. Sybil attack tries to degrade the integrity of data, level of security, and resource utilization that a distributed algorithm targets to achieve. This type of attack can be performed for downgrading the performances of distributed storage, routing mechanism, data aggregation, voting, fair resource allocation, and misbehavior detection mechanisms. A conceptual view of Sybil attack is shown in Figure 1. Basically, any peer-to-peer network (any kind of wireless ad hoc network) is vulnerable to Sybil attack. Newsome et al. [18] presented a taxonomy of sybil attacks in WSN based on three orthogonal dimensions.

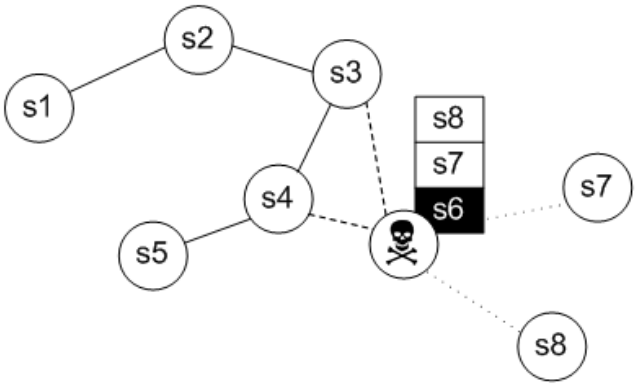

Figure 1: Conceptual view of a Sybil Attack. The node with id s6 is pretending to be three nodes at the same time (s6, s7, and s8), the nodes s3 and s4 do not have direct contacts with s7 and s8, so s6 can pretend to them as it is s7 or s8. Here, additional ids of s6 are called the 'Sybil nodes' (s7 and s8)

3.3.1. Dimension I

Direct Communication – In this case, Sybil nodes directly communicate with the legitimate nodes. When a legitimate node sends message to a Sybil node, malicious device listens to the message. In the same way, messages sent from the Sybil nodes are actually sent from the malicious device.

Indirect Communication – In this case, the legitimate nodes cannot directly communicate with the Sybil nodes rather a malicious device convinces them that it can reach to the Sybil nodes. Any message sent by a legitimate node to a Sybil node is routed through the malicious node and it can eventually do anything (modification, fabrication, dropping, etc.) with the received messages.

3.3.2. Dimension II

Identities used for the Sybil nodes could be obtained in one of two ways:

Fabricated Identities – Attacker can simply generate a fake identity supported by the network and perform Sybil attack.

Stolen Identities – Attacker in this case steals the identities of the legitimate nodes and uses those for launching attacks.

3.3.3. Dimension III

The identities of the Sybil nodes could be used in two ways:

Simultaneous – The malicious node or the attacker can pretend to have multiple identities at the same time (as shown in Figure 1).

Non-simultaneous – The attacker can somehow obtain a large number of valid identities but, instead of using all the identities at the same time, it can use those one after another in different time slots.

One advantage for WSN to face Sybil attack is that, it can have some sort of centralized entity (base station or cluster head) in the network. Hence, this attack could be prevented using efficient protocols. Douceur [17] showed that, without a logically centralized authority, sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities. However, detection of sybil nodes in a network is not so easy. Some of the recently proposed detection and prevention mechanisms could be found in [19], [20], [21], [22], and [90].

3.4. Blackhole/Sinkhole Attack

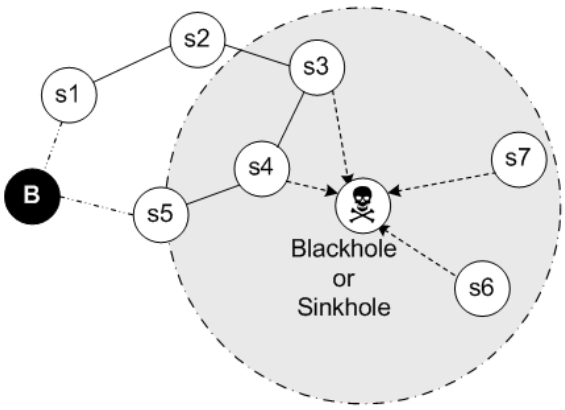

Figure 2: Conceptual view of a Blackhole/Sinkhole Attack. The attacker advertises high quality link through it which tempts s3, s4, s6, and s7 to select itself as a forwarding node for their packets. In the figure, B is the base station and the large gray circle is the attacker's radio range

In this attack, a malicious node acts as a blackhole [23] to attract all the traffic in the network. Especially in a flooding based protocol, the attacker listens to the route request and then replies to the target node saying that it has a high quality or shortest path to the base station. A victim node is thus lured to select it as a forwarder of its packets. Once the malicious device is able to insert itself between the communicating entities (between the base station and sensor node), it is able to do whatever it wishes with the packets that pass through it. The blackhole (i.e., malicious node or the attacker) can drop the packets, selectively forward those to the base station or to the next node, or even can change the content of the packets. This type of attack could be very harmful for those nodes that are considerably far from the base station. We should keep in mind that blackhole attack and sinkhole attack are basically the same attack but these two terms are often used interchangeably. As mentioned earlier, this attack can cause DoS in the network and thus could be considered as one type of DoS attack. Figure 2 shows a conceptual view of a blackhole/sinkhole attack. Some recent works addressing this attack and possible solutions to deal with it are [24], [25], [26], [27], [28], [29], [30], and [31].

3.5. Hello Flood Attack

Hello flood Attack was first detected and introduced by Karlof and Wagnor in [32]. This attack uses HELLO packets as a weapon to convince the sensors in the network. Many protocols require broadcasting of HELLO packets for neighbor discovery. In this case, a node receiving such a packet may assume that it is within (normal) radio range of the sender node. This assumption could be exploited by an attacker. An attacker with a large radio transmission range (termed as a laptop-class attacker in [32]) and enough processing power can send HELLO packets to a large

number of sensors in the network. Thus the sensors could be persuaded that the adversary is their neighbor. As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know it as their neighbor. In this way the attacker cheats the victims. A conceptual picture of hello flood attack is presented in Figure 3. Possible countermeasures to handle hello flood attack could be the use of bidirectional verification of links before using them, multipath routing, use of multiple base stations [33], or any kind of lightweight packet authentication scheme.

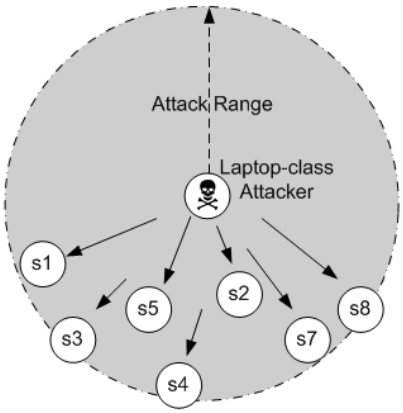

Figure 3: Hello flood Attack. A Laptop-class attacker (attacker with large radio range) is transmitting the HELLO packets and pretending to be a neighbor of all other legitimate nodes within its radio range

3.6. Wormhole Attack

Wormhole attack is a very critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location [34]. The tunneling or retransmission of bits could be done selectively. Wormhole attack is a significant threat to wireless sensor networks because this is possible even if the attacker has not compromised any node, and even if all communications provide authenticity and confidentiality. It could be performed even at the initial phase when the sensors start discovering the neighborhood information. In a nutshell, attacker's goal in wormhole attack is to disrupt routing information by creating shortcuts in the network.

Figure 4 shows a graphical representation of wormhole attack. In the figure, two adversaries are communicating with each other through a direct and dedicated channel by using wired link or additional RF (radio-frequency) transceivers with longer transmission range. The route via the wormhole looks like an attractive path to the legitimate sensor nodes because it generally offers less number of hops and less delay than other normal routing paths. While relaying packets, the

adversaries can arbitrarily drop the packets. Therefore data communications through the wormhole suffer from severe performance degradation. In a recently published work, Sharif and Leckie propose three new variants of wormhole attacks namely Energy Depleting Wormhole Attack (EDWA), Indirect Blackhole Attack (IBA), and Targeted Energy Depleting Wormhole Attack (TEDWA). Interested readers are suggested to read more in [35].

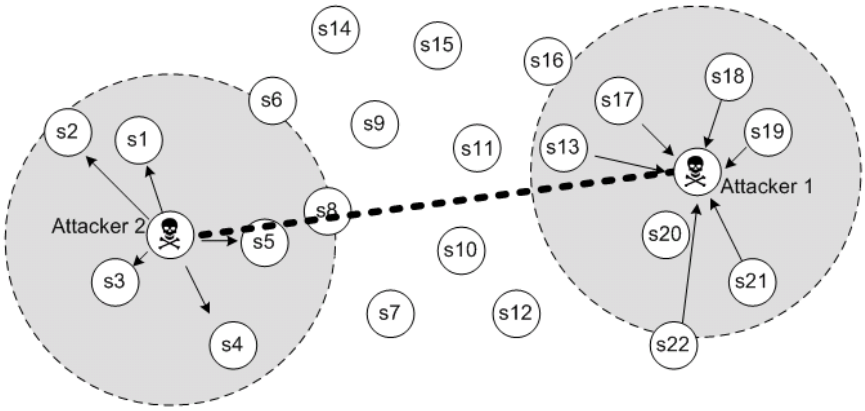

Figure 4: Wormhole attack. Two attackers have created a dedicated tunnel between them and are attracting traffic.

Several works tried to defend against this attack by detection of intruder nodes in the network. Some of them are [24], [29], [36], [37], [38], [39], [40], [41], [42], and [43]. Other than these works, [44] proposes an approach to deal with wormhole attacks using directional antennas, which is often not feasible for sensor networks.

So far, we have talked about various security threats and attacks in wireless sensor networks. Most of these attacks can be tackled by using proper cryptographic mechanisms. If the node authentication method is robust and messages in the network are made illegible to the outside entities, many security problems are eventually resolved or just need a little add-on with the defense mechanism. For utilizing any kind of cryptographic operation in the network, key management is a fundamental issue to deal with. Given the constrained resources of the sensors and the special characteristics of wireless sensor networks, key management in WSN is considered to be a very challenging topic and a hot research issue. Efficient mechanisms and management policies are needed to determine how the keys in such a network would be generated, stored, used, manipulated, renewed, or revoked. In the next section, we will try to get some insights on these issues.

3.7. Key Management Issues in WSN

Primary goal of key management is to set up secure links among the neighboring nodes in the network at the formation phase. Some of the major challenges any kind of key management mechanism faces are:

(i) Unknown scalability of the network. It means that if there are *n* number of nodes initially in the network, *n´* more nodes could be added to it later. The key management scheme must consider the tactics to handle the addition of nodes in the network.

(ii) Unknown topological distribution of sensors in the network. As the topological information of the sensors are often very difficult to obtain and not known in prior in most of the cases, the key management scheme must distribute keys or keying information in such a way that the neighbor nodes could communicate securely with each other.

(iii) Limited available resources of the sensors. Like any other mechanism, this is a great hurdle that the key management scheme must confront with.

(iv) What if the nodes in the network are captured by adversaries? The key revocation mechanism should ensure that the captured keys cannot be used further in the network and still the network should be able to keep functioning with proper level of security.

(v) Re-keying. If there is any re-keying mechanism in the management scheme, how to generate or distribute the new keys among the already deployed sensors in the network?

There are mainly three kinds of approaches for key management in wireless sensor network:

- Key Pre-Distribution
- Key Management Based on Public Key
- Key Management Based on Online Server

3.7.1. Key Pre-Distribution

In case of key pre-distribution schemes, keys or the keying materials are delivered to all sensor nodes prior to their deployment. Keying materials are partial information of the keys that could be used by the nodes to derive keys for node-to-node secure communications. Among all the key management approaches, key pre-distribution seems to be the most feasible solution. This is because; most of the operations in this approach can be done prior to the deployment of the network.

For key pre-distribution, we mainly consider two phases of operations; initialization phase and network formation phase. In the initialization phase, most of the planning and computations are done so that the sensors could get relief of the heavy computational burdens. In the formation

phase, the sensors establish secure links among themselves based on the pre-stored information in their memories.

There are mainly three approaches of key pre-distribution:

- **System key pre-distribution** – Same key *k* is stored in each sensor. *k* could also be used for deriving other keys for secure communications among the sensors. The advantage of this approach is the use of little memory to store the key. The drawbacks are little resilience and weak authentication.
- **Trivial key pre-distribution** – Distinct pairwise keys $k_{i,j}$ are stored for each pair of nodes s_i and s_j. The two nodes contact with each other to derive the pairwise key for further secure communications. The advantage of this approach is greater resilience and strength of authentication. However, this approach is not scalable and in this case, it is hard to handle the addition of new sensors in the network.
- **Random key pre-distribution** – In this approach, a number of random keys (say *w* keys) from a key pool is stored in the sensors. Any two nodes in the network may share a key with probability *p*. The advantage of this type of scheme is the resiliency and support for addition of new sensors in the network. On the other hand, the drawbacks are the lose node authentication and possibility of not finding a common key even among the neighboring nodes. One of the legendary works on random key pre-distribution, known as the *basic scheme* was proposed by Eschenauer and Gligor [45]. The *basic scheme* is one of the early works which opened the door for further research on various aspects of key management in this type of network.

3.7.2. Key Management Based on Public-Key

Public key based schemes use asymmetric keys for encryption and decryption operations. There are some well-established public-key based schemes like Diffie-Hellman, Digital Signature Standard, ElGamal, Elliptic Curve Cryptography (ECC), RSA, etc. [46]. But the reality is, public key cryptography (PKC) based schemes are often not directly applicable for wireless sensor networks. As mentioned earlier, the limitation of resources of the sensors is the major hurdle for using these mechanisms. Also the need for a certificate authority or a trusted middle-man, unknown topology of the network, and random deployment of sensors often make their use more difficult. In spite of the existence of these barriers, the existing PKC schemes could somehow be modified for making them suitable for use in the sensors. Often the number of operations is

reduced to make the PKC schemes a bit lightweight. Though in the early days, the researchers thought that the PKC schemes are in all the ways inappropriate for WSN, some recent works have shown that some lightweight versions of these schemes might be very effective for high-security demanding applications. The works like [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], and [58] have presented some success stories and gains regarding using public key based security mechanisms and key management in WSN.

3.7.3. Key Management Based on Online Server

In this approach, an online server provides the necessary keys to the sensors for communications among themselves. The key could be provided by the base station or by the group leaders (sometimes called as cluster heads) in the network. However, this approach is not as efficient as the key pre-distribution approach as in this case, the special nodes must have relatively more memory, processing power, and energy than those of the ordinary sensors in the network. Also, the special nodes should be well-dispersed in the network so that they can cover the whole network for providing the keys with minimum effort. Maintaining security during the transmission of keys also requires some other supporting mechanisms or some trust-based approach. Overall, most of the researchers agree that this approach in most of the scenarios, not a good solution for managing keys in this type of network.

Some of the recent and notable works on key management in sensor networks are [59], [60], [61], [62], [63], [64], [65], [66], [67], [68], [69], [70], [71], [72], [73], [74], [75], [87], and [89]. Readers are encouraged to go through these for gaining in-depth knowledge on key management in wireless sensor networks. Other than these works, a recent survey on the key management schemes in WSN is presented in [76].

3.8. Secure Routing in WSN

Basically, secure routing is not a separate issue than that we have discussed so far. If we have an efficient key management scheme with a supporting security infrastructure, this issue is easily solved. In that case, the whole thing reduces to the task of verifying who is communicating with whom and through whom. A number of routing protocols are proposed for wireless sensor networks (for further reading, [77] and [78] are suggested to the interested readers). However, the key point is that most of the routing protocols have overlooked the issue of security at their design phase. Sometimes it is quite impossible to fit a good security mechanism with a good routing protocol.

If the operational method of a routing protocol does not support a particular security mechanism, we need to choose any other suitable security approach for that one. In such a case, often the suitable security solution might not be the best solution or might not at all help for secure routing using that particular protocol. A routing protocol may focus on saving energy resources of the sensors, but if a security mechanism is added to it, it might not hold its major point of advantage or could even turn into an energy-consuming routing protocol. Therefore, it is better to consider the security issues at the design phase of any routing protocol. If the structural design and communication methods of the routing protocol allow the security solutions to run side-by-side or on top of it, then it could be beneficial for secure routing as well as for handling almost all types of threats and attacks in WSN. Nonetheless, it should be noted that a single solution cannot solve all the problems at the same time. Instead, based on the application requirements and network settings, the strategy of routing and security should be set. Often we need to consider some trade offs among some parameters like security, QoS (Quality of Service), latency, packet loss, etc.

In one of the prominent works on secure routing in wireless sensor networks, Karlof and Wagner [32] noted that:

> "*One aspect of sensor networks that complicates the design of a secure routing protocol is in-network aggregation. In more conventional networks, a secure routing protocol is typically only required to guarantee message availability. Message integrity, authenticity, and confidentiality are handled at a higher layer by an end-to-end security mechanism such as SSH or SSL. End-to-end security is possible in more conventional networks because it is neither necessary nor desirable for intermediate routers to have access to the content of messages. However, in sensor networks, in-network processing makes end-to-end security mechanisms harder to deploy because intermediate nodes need direct access to the content of the messages. Link layer security mechanisms can help mediate some of the resulting vulnerabilities, but it is not enough: we will now require much more from our routing protocols, and they must be designed with this in mind.*"

In general, for secure routing in wireless sensor networks, the following points could be considered:

- Multipath routing can help for introducing some sort of security.
- Use of symmetric key cryptography can reduce the processing overhead.

- The routing protocols should be intrusion tolerant and should be able to keep on functioning at least up to a certain level so that the overall network operations are not hampered in case of the presence of intruders.
- As involvement of security mechanisms can increase the overheads of the protocol, the overall design should be kept as simple as possible.
- Any broken routing path should not hamper the functions of the associated security mechanisms. The working method of the protocol should allow finding an alternate path to the destination within a minimum interval.

3.9. Physical Security Issues

Earlier we have introduced the types of physical attacks in WSN in brief. In this section, we will have a closer look at the physical security issues in wireless sensor networks. We know that the sensors in the network could be physically reached by adversaries because of the network's unattended nature. There are several ways to protect a sensor network from the physical attacks.

- The most suitable way to tackle this is the concept of *self-destruction*. In this case, a sensor detects a physical attack and quickly deletes all of its hidden information to become non-functional. For a large-scale sensor network, this could be a feasible solution as their might be several backups of the sensors' data, cryptographic keys, codes, and other secret information. Also if a part of the network is attacked, the sensors in other parts can be ready to destroy themselves before getting captured. Though this sort of *self-destruction* mechanism is expensive to incorporate with the sensor's physical package, it is not impossible.
- An alternate solution could be using a mechanism where each sensor monitors the status of its neighboring sensors. Any suspicious behavior or lack of response of a neighbor for a certain period of time might trigger a warning. Consequently, the other neighbors can get ready for hiding all of their secret information.
- Analyzing the deployment policy and detailed mapping of the network could also be effective for reducing the probability of physical attacks. However, in many applications, such kind of thorough study of the deployment area might not be possible.
- Camouflaging of sensors could be efficient in some deployment scenarios. Say for example, a wireless sensor network is to be deployed over a rocky hilly area. In that case, the sensors could be colored like rocks or could be given the shapes of rocks (with some outer coverings!), which can make the task of physically locating them more difficult.

- Sensors might have some sort of protective shields that can save the internal hardware from external pressure or from other environmental conditions.

However, applying any of these approaches depends on the deployment budget and requirements of the application. Some of the recent works on physical security issues in wireless sensor networks can be found in [5], [6], [79], and [80].

4. CHALLENGES FOR FUTURE RESEARCH

With the sophistication of various communication protocols and rapid advancements of Micro-Electro-Mechanical Systems (MEMS) technologies [81], sensors are gaining more resources and capabilities with which many barriers of security could be surmounted. In spite of the previous advancements and those that are coming in the near future, some issues regarding security in WSN could still pose great challenges. In this section, we will talk about those issues and will try to visualize the future so that the research works on security in WSN may get a proper direction towards devising realistic solutions.

4.1. Holistic Approach to Security in WSN

A holistic approach aims at improving the performance of wireless sensor networks with respect to security, longevity, and connectivity under changing environmental conditions. This approach of security concerns about involving all the operational layers for ensuring total security in the network. When talking about layering concepts, it should be mentioned that the security in network layer is mainly concerned about authentication, availability of routing information, and integrity of information, the data link layer is concerned mainly about data confidentiality and data freshness, and the physical layer is concerned about tamper-resistance. Holistic approach tries to lead to a single architecture so that different security mechanisms can work in tandem for different layers. Some key principles of holistic approach are:

- In a given network, 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.
- The security measures should be developed to work in a decentralized fashion.

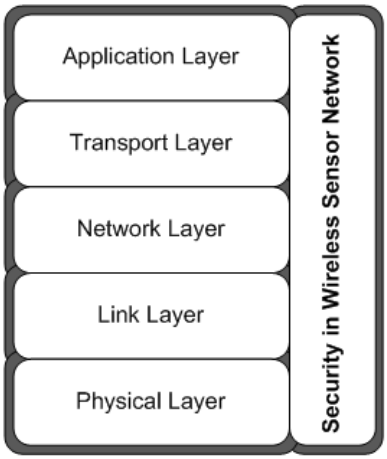

Figure 5: Holistic view of security in WSN

Considering all types of security threats and attacks in WSN, we can understand that for this type of network, a single security solution for a single layer cannot be considered as a reasonable solution. It is better to employ a holistic approach so that all facets of the network could be made secure at the same time. As an example, if a WSN has very good security solutions for almost all the layers but physically the network is vulnerable, we cannot guarantee that the total security of the network is ensured. In such a case, any adversary can go and pick up the sensors from the field, extract the cryptographic keys, can use jamming for causing physical layer DoS attacks, destroy the sensors, and so on. Though physical security is often not possible to ensure for WSNs, at least the overall system must allow a graceful degradation of the network's operation when it is attacked. However, designing and developing such type of efficient security architecture and management policy remain as an open challenge. At least we can hope that with the advancements of technological capabilities of sensors, this task will become a bit easier in the future.

4.2. What to Expect Next?

Today, the limitation of resources of the sensors is considered as the primary obstacle for applying robust security mechanisms. In future, this barrier might totally be vanished or might be reduced by significant extent. We might see sensors capable of handling even the heavy computations associated with public key cryptography schemes (like RSA, SHA-1, etc.) without any reduced operation. Say for example, one of the latest advanced wireless sensor platforms, Imote2 [82] is built with the low power PXA271 XScale processor at 13-416MHz and it integrates an 802.15.4 radio (CC2420) with a built-in 2.4GHz antenna. Imote2 has 256kB SRAM, 32MB FLASH, and 32MB SDRAM. It is a modular stackable platform and can be expanded with

extension boards to customize the system to a specific application. Through the extension board connectors, sensor boards can provide specific analog or digital interfaces. A battery board is provided to supply system power, or even it can be powered via the integrated USB interface. All these features make it a very powerful sensor node compared to its predecessors. The rechargeable feature of the sensor's battery opens the door to overcome the problem of constrained and non-renewable energy. Considering today's achievements, it is reasonable to assume that some years later we could even see sensors with much higher configurations with the same tiny size! If it becomes true, some interesting questions may arise. What will be the case if these tiny devices get the capabilities like high configuration computers? Will we be able to run classic security schemes that require heavy computations? If so, will all the works done so far be meaningless? The answer to all of these questions is; "No work will be thrown away even if the sensors achieve very high configurations". Basically the researchers have been working on the fact that, given such low-configuration devices, how best level of security can be provided for the network. Yes, in future the sensors might get more capabilities keeping even today's physical size, but even then the devices with current specifications could remain as low-cost alternatives. Also, some other tiny devices might have such limited resources. It is also reasonable to think that the sensors with current specifications might become much smaller in physical size. If it becomes true, in that case, reduction of physical size would ultimately increase the level of physical security of these devices. In fact, reduced size of sensors would make them more *physically secure* in the hostile deployment areas as a relatively smaller object is harder to notice! Hence, the major point is, no matter how much capabilities a sensor node attains in future, the research works done with today's given limitations (like MICA2's specifications) will still be useful for use for the devices with such capabilities. As a whole, the research area will still remain challenging.

In future we might also see wide-spread use of wireless multimedia sensor networks [83], [91] for various security applications like; distributed vision, tracking, and monitoring applications. At that time, processing multimedia data might become a little bit easier. However, when issues like QoS (Quality of Service) and latency are involved with this, the challenge is likely to remain for finding efficient solutions. In fact, ensuring a good level of QoS and a good level of security at the same time is always very difficult and often *contradictory*! Not only for sensor networks but also for other types of networks this statement is true. This is because, any sort of security operation requires some processing time. If the level of security is increased, the processing delay

also increases causing degradation of quality of service. For real-time multimedia applications (if at all possible using WSNs or if at all required!), this challenge will remain for a long time.

Some of the recent works show that, in future some applications might need to handle multiple types of data within the same network [84]. The development of sensors like ExScal motes [85], [86] has already opened the door for further research on heterogeneous applications using homogenous multi-purpose nodes. The heterogeneous data generated from such multipurpose nodes might have different levels of security based on their priorities. Handling these heterogeneous data with different security levels could also be an interesting topic for research in the near future.

5. CONCLUSIONS

In this chapter, we have learnt about security in wireless sensor networks considering five major aspects; (i) security approaches for sensor networks, (ii) threats and attacks against sensor networks, (iii) key management issues, (iv) secure routing issues, and (v) future possibilities and challenges. We have learnt that most of the attacks against security mechanisms in wireless sensor network are launched by injecting false information either by compromised nodes residing in the network or by attackers. Most of the attacks could be resisted by employing efficient schemes to detect the attackers or the compromised nodes. Distributed detection and prevention mechanisms can really help to resist lots of attacks. But it is not desired to give the sensors some extra tasks than what is necessary. Hence, developing distributed detection and prevention schemes still remains as a challenging research issue.

Considering current direction of research and advancements of the methodologies, we can expect that in the coming days, ensuring holistic security in wireless sensor network will become a major research issue. Many of today's proposed security mechanisms are based on specific applications, network models, or application specific assumptions. Till today there is a lack of proper effort to make the security mechanisms operable with one another. If the efficient and lightweight security mechanisms for different layers could be made compatible for providing holistic security, it would be a great achievement for this research area.

With the increase of innovative applications of wireless sensor networks, the security issue is expected to get more emphasis. There is a well-known adage, "*An ounce of prevention is worth a pound of cure*". If the solutions of other issues are developed keeping security in mind or at least

they are made operable with the available security mechanisms, we can expect wide-spread use of wireless sensor networks for many security-demanding data extraction applications in the coming days.

6. REFERENCES

[1] Pathan, A.-S. K., Lee, H.-W., and Hong, C. S., "Security in Wireless Sensor Networks: Issues and Challenges", Proceedings of the 8th IEEE ICACT, Volume II, February 20-22, 2006, Phoenix Park, Korea, pp. 1043-1048.

[2] Hämäläinen, P., Kuorilehto, M., Alho, T., Hännikäinen, M., and Hämäläinen, T. D., "Security in Wireless Sensor Networks: Considerations and Experiments", SAMOS 2006, LNCS 4017, Springer-Verlag 2006, pp. 167-177.

[3] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., and Cayirci, E., "Wireless Sensor Networks: A Survey", Computer Communications, Volume 38, 2002, pp. 393-422.

[4] http://www.xbow.com/Products/productsdetails.aspx?sid=72

[5] Gu, W., Wang, X., Chellappan, S., Xuan, D., Lai, T.H. , "Defending Against Search-Based Physical Attacks in Sensor Networks", 2005 IEEE International Mobile Adhoc and Sensor Systems Conference, 7-10 Nov. 2005.

[6] Becher A., Benenson Z., and Dornseif, M., "Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks", SPC 2006, LNCS 3934, Springer-Verlag 2006, pp. 104-118.

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

[8] 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.

[9] 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.

[10] 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, 2003, Japan.

[11] Römer, K., Blum, P., Meier, L., "Time Synchronization and Calibration in Wireless Sensor Networks", Handbook of Sensor Networks: Algorithms and Architectures (Ivan Stojmenovic Ed.), John Wiley & Sons, ISBN 0-471-68472-4, September 2005, pp. 199-237.

[12] Wood, A. D. and Stankovic, J. A., "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks", in Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems (edited by Ilyas, M. and Mahgoub, I.), CRC Press, 2004.

[13] Čagalj, M., Čapkun, S., and Hubaux, J.-P., "Wormhole-Based Antijamming Techniques in Sensor Networks", IEEE Transactions on Mobile Computing, Vol. 6, No. 1, January 2007, pp. 100-114.

[14] Wood, A. D., Stankovic, J. A., and Son, S. H., "Jam: A Jammed-Area Mapping Service for Sensor Networks", Proceedings of the 24th IEEE Real-time Systems Symposium, 2003, pp. 54-62.

[15] Alnifie, G. and Simon, R., "A Multi-Channel Defense Against Jamming Attacks in Wireless Sensor Networks", Proceedings of ACM Q2SWinet'07, 22 October, Crete Island, Greece, 2007, pp. 95-104.

[16] Chen, H., Han, P., Zhou, X., and Gao, C., "Lightweight Anomaly Intrusion Detection in Wireless Sensor Networks", PAISI 2007, LNCS 4430, Springer-Verlag 2007, pp. 105-116.

[17] Douceur, J. R., "The Sybil Attack", IPTPS 2002, LNCS 2429, Springer-Verlag 2002, pp. 251-260.

[18] Newsome, J., Shi, E., Song, D., and Perrig, A., "The Sybil Attack in Sensor Networks: Analysis & Defense", Proceedings of ACM IPSN'04, April 26-17, 2004, California, USA, pp. 259-268.

[19] Zhang, Q., Wang, P., Reeves, D.S., Ning, P. "Defending against Sybil attacks in sensor networks", Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshops, 2005, 6-10 June 2005, pp. 185 – 191.

[20] Mukhopadhyay, D. and Saha, I., "Location Verification Based Defense Against Sybil Attack in Sensor Networks", ICDCN 2006, LNCS 4308, Springer-Verlag 2006, pp. 509-521.

[21] Yu, H., Kaminsky, M., Gibbons, P. B., and Flaxman, A., "SybilGuard: Defending Against Sybil Attacks via Social Networks", Proceedings of ACM SIGCOMM, September 11-15, 2006, Pisa, Italy, pp. 267-278.

[22] Jiangtao, W., Geng, Y., Yuan, S., and Shengshou, C., "Sybil Attack Detection Based on RSSI for Wireless Sensor Network", Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing (WiCom 2007), 21-25 September, 2007, pp. 2684 – 2687.

[23] Ahmed, N., Kanhere, S., and Jha, S., "The Holes Problem in Wireless Sensor Networks: A survey", ACM SIGMOBILE Mobile Computing and Communications Review (MC2R), Vol. 9 No 2, April 2005, pp. 4-18.

[24] Pirzada, A. A. and McDonald, C., "Circumventing Sinkholes and Wormholes in Wireless Sensor Networks", Proceedings of International Workshop on Wireless Ad Hoc Networks, May 23-26, 2005.

[25] Karakehayov, Z., “Using REWARD to Detect Team Black-Hole Attacks in Wireless Sensor Networks”, Proceedings of the Workshop on Real-World Wireless Sensor Networks (REALWSN'05), Stockholm, Sweden, June 2005.

[26] Yin, J. and Madria, S.K., "A Hierarchical Secure Routing Protocol against Black Hole Attacks in Sensor Networks", Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006, Volume 1,June 05-07, 2006, pp. 376 - 383.

[27] Ramaswami, S. S. and Upadhyaya, S., "Smart Handling of Colluding Black Hole Attacks in MANETs and Wireless Sensor Networks using Multipath Routing", Proceedings of the 2006 IEEE Workshop on Information Assurance, 2006, NY, USA, pp. 253-260.

[28] Ngai, E. C. H., Liu, J., and Lyu, M. R., "An Efficient Intruder Detection Algorithm Against Sinkhole Attacks in Wireless Sensor Networks", Computer Communications, Vol. 30, 2007, pp. 2353-2364.

[29] Nahas, H. A., Deogun, J. S., and Manley, E. D., "Proactive Mitigation of Impact of Wormholes and Sinkholes on Routing Security in Energy-Efficient Wireless Sensor Networks", Wireless Networks, Springer Netherlands, DOI 10.1007/s11276-007-0060-7, 2007.

[30] Demirbas, M. and Song, Y., "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks", Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks (IEEE WoWMoM 06), 2006, pp. 564-570.

[31] Krontiris, I., Dimitriou, T., Giannetsos, T., and Mpasoukos, M., “Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks”, 3rd International Workshop on Algorithmic Aspects of Wireless Sensor Networks (AlgoSensors‘07), Wroclaw, Poland, July 2007.

[32] Karlof, C. and Wagner, D., "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Ad Hoc Networks, Vol. 1, 2003, pp. 293-315.

[33] Hamid, M. A., Mamun-Or-Rashid, M., and Hong, C. S., "Routing Security in Sensor Network: HELLO Flood Attack and Defense", Proceedings of IEEE ICNEWS, January 2-4, 2006, Dhaka, Bangladesh, pp. 77-81.

[34] Hu, Y. C., Perrig, A., and Johnson, D. B., "Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, February 2006, pp. 370-380.

[35] Sharif, W. and Leckie, C., "New Variants of Wormhole Attacks for Sensor Networks", Proceedings of the Australian Telecommunication Networks and Applications Conference, December 4-6, 2006, Melbourne, Australia, pp. 26-30.

[36] Hu, Y.-C., Perrig, A., and Johnson, D. B., "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks", Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), vol. 3, April 2003, San Francisco, CA, pp. 1976-1986.

[37] Buttyán, L., Dóra, L., and Vajda, I., "Statistical Wormhole Detection in Sensor Networks", ESAS 2005, LNCS 3813, Springer-Verlag 2005, pp. 128-141.

[38] Alzaid, H., Abanmi, S., Kanhere, S., and Chou, C. T., "Detecting Wormhole Attacks in Wireless Sensor Networks", Technical Report, Computer Science and Engineering School, The Network Research Laboratory, University of New South Wales, 2006.

[39] Maheshwari, R., Gao, J., and Das, S. R., "Detecting Wormhole Attacks in Wireless Sensor Networks Using Connectivity Information", Proceedings of the 26th Annual IEEE Conference on Computer Communications (INFOCOM'07), May, 2007, pp. 107-115.

[40] Khalil, I., Bagchi, S., and Shroff, N. B., "MOBIWORP: Mitigation of the Wormhole Attack in Mobile Multihop Wireless Networks", Ad Hoc Networks, 2007.

[41] Yun, J.-H., Kim, I.-H., Lim, J.-H., and Seo, S.-W., "WODEM: Wormhole Attack Defense Mechanism in Wireless Sensor Networks", ICUCT 2006, LNCS 4412, Springer-Verlag 2007, pp. 200-209.

[42] Poovendran, R. and Lazos, L., "A Graph Theoretic Framework for Preventing the Wormhole Attack in wireless Ad Hoc Networks", Wireless Network, Vol. 13, Springer, 2007, pp. 27-59.

[43] Xu, Y., Chen, G., Ford, J., and Makedon, F. S., "Distributed Wormhole Detection in Wireless Sensor Networks", Critical Infrastructure Protection (E. Goetz and S. Shenoi eds.), Springer, Boston, 2008 (to appear).

[44] Hu, L. and Evans, D., "Using Directional Antennas to Prevent Wormhole Attacks", Proceedings of the 11th Network and Distributed System Security Symposium, February 2003, pp. 131–141.

[45] Eschenauer, L. and Gligor, V. D., "A Key-Management Scheme for Distributed Sensor Networks", Proceedings of the 9th ACM conference on Computer and Communications, Washington, DC, USA, 18-22 Nov. 2002, pp. 41 – 47.

[46] Rhee, M. Y., Internet Security: Cryptographic Principles, Algorithms and Protocols, WILEY, 2003.

[47] Malan, D.J., Welsh, M., and Smith, M.D., "A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography", Proceedings of the First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON'04), October 4-7, 2004, pp. 71-80.

[48] Watro, R., Kong, D., Cuti, S.-f., Gardiner, C., Lynn, C. and Kruus, P., "TinyPK: Securing Sensor Networks with Public Key Technology," ACM SASN'04, Washington, DC, USA, 2004, pp. 59-64.

[49] Du, W., Wang, R., and Ning, P., "An Efficient Scheme for Authenticating Public Keys in Sensor Networks", Proceedings of ACM MobiHoc'05, May 25-27, Illinois, USA, pp. 58-67.

[50] Gaubatz, G., Kaps, J., and Sunar, B., "Public Keys Cryptography in Sensor Networks -- Revisited", ESAS 2004, LNCS 3313, Springer-Verlag 2005, pp. 2-18.

[51] Gaubatz, G., Kaps, J.-P., Öztürk, E., and Sunar, B., "State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks", Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom 2005), March 8-12, 2005, pp. 146-150.

[52] Blaß, E.-O. and Zitterbart, M., "Towards Acceptable Public-Key Encryption in Sensor Networks", Proceedings of ACM 2nd International Workshop on Ubiquitous Computing, INSTICC Press, Miami, USA, May 2005, pp. 88--93.

[53] Jing, Q., Hu, J., and Chen, Z., “C4W: An Energy Efficient Public Key Cryptosystem for Large-Scale Wireless Sensor Networks”, IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), Oct. 2006, pp. 827-832.

[54] Nyang D. and Mohaisen A., “Cooperative Public Key Authentication Protocol in Wireless Sensor Network”, UIC 2006, LNCS 4159, Springer-Verlag, pp. 864-873, 2006.

[55] Mykletun, E., Girao, J., and Westhoff, D., " Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks", Proceedings of IEEE International Conference on Communications (ICC'06), Volume 5, June 2006, pp. 2288-2295.

[56] Arazi, O., Elhanany, I., Rose, D., Qi, H., and Arazi, B., "Self-certified public key generation on the intel mote 2 sensor network platform", 2nd IEEE Workshop on Wireless Mesh Networks, 2006. WiMesh 2006, pp. 118 - 120.

[57] Arazi, O., Qi, H., and Rose, D., "Public Key Cryptographic Method for Denial of Service Mitigation in Wireless Sensor Networks", 4th Annual IEEE Communications Society Conference

on Sensor, Mesh and Ad Hoc Communications and Networks (SECON'07), June 18-21, 2007, pp. 51-59.

[58] Pathan, A.-S. K., Ryu, J. H., Haque, M. M., and Hong, C. S., "Security Management in Wireless Sensor Networks with a Public Key Based Scheme", APNOMS 2007, LNCS 4773, Springer-Verlag 2007, pp. 503-506.

[59] Pathan, A.-S. K., Dai, T. T., and Hong, C. S., "A Key Management Scheme with Encoding and Improved Security for Wireless Sensor Networks", ICDCIT 2006, LNCS 4317, Springer-Verlag 2006, pp. 102-115.

[60] Jolly, G., Kuşçu, M. C., Kokate, P., and Younis, M., "A Low-Energy Key Management Protocol for Wireless Sensor Networks", Proceedings of the Eighth IEEE International Symposium on Computers and Communication, 2003 (ISCC 2003), pp. 335-340.

[61] Huang, D., Mehta, M., Medhi, D., and Harn, L., "Location-aware Key Management Scheme for Wireless Sensor Networks", Proceedings of ACM SASN'04, October 25, 2004, Washington, DC, USA, pp. 29-42.

[62] Dutertre, B., Cheung, S., and Levy, J., "Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust", SDL Technical Report SRI-SDL-04-02, SRI International, April 6, 2004.

[63] Lee, Y.-H., Phadke, V., Deshmukh, A., and Lee, J. W., "Key Management in Wireless Sensor Networks", ESAS 2004, LNCS 3313, Springer-Verlag 2005, pp. 190-204.

[64] Liu, D., Ning, P., and Li, R., "Establishing Pairwise Keys in Distributed Sensor Networks", ACM Transactions on Information and System Security, Vol. 8, No. 1, February 2005, pp. 41-77.

[65] An, F., Cheng, X., Rivera, J. M., Li, J., and Cheng, Z., "PKM: A Pairwise Key Management Scheme for Wireless Sensor networks", ICCNMC 2005, LNCS 3619, Springer-Verlag 2005, pp. 992-1001.

[66] Du, W., Deng, J., Han, Y. S., Varshney, P. K., Katz, J., and Khalili, A., "A Pairwise Key Predistribution Scheme for Wireless Sensor Networks", ACM Transactions on Information and System Security, Vol. 8, No. 2, May 2005, pp. 228–258.

[67] Du, W., Deng, J., Han, Y. S., and Varshney, P. K., "A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge", IEEE Transactions on Dependable and Secure Computing, Volume 3, Number 2, January-March 2006, pp. 62-77.

[68] Yang, C., Zhou, J., Zhang, W., and Wong, J., "Pairwise Key Establishment for Large-Scale Sensor Networks: from Identifier-based to Location-based", Proceedings of the First International Conference on Scalable Information Systems, May 29-June 1 2006, Hong Kong.

[69] Dai, T. T., Pathan, A.-S. K., and Hong, C. S., “A Resource-Optimal Key Pre-distribution Scheme with Improved Security for Wireless Sensor Networks”, APNOMS 2006, LNCS 4238, Springer-Verlag 2006, pp. 546-549.

[70] Çamtepe, S. A. and Yener, B., “Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks”, IEEE/ACM Transactions on Networking, Vol.15 No.2, April 2007, pp. 346-358.

[71] Chorzempa, M., Park, J.-M., and Eltoweissy, M., "Key Management for Long-Lived Sensor Networks in Hostile Environments", Computer Communications, Vol. 30, 2007, pp. 1964-1979.

[72] Großschädl, J., Szekely, A., and Tillich, S., "The Energy Cost of Cryptographic Key Establishment in Wireless Sensor Networks", Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security (ASIACCS'07), 2007, pp. 380–382.

[73] Huang, D., Mehta, M., Liefvoort, A.V.D., and Medhi, D., "Modeling Pairwise Key Establishment for Random Key Predistribution in Large-Scale Sensor Networks", IEEE/ACM Transactions on Networking, Vol. 15, No. 5, October 2007, pp. 1204–1215.

[74] Huang, D. and Medhi, D., "Secure Pairwise Key Establishment in Large-Scale Sensor Networks: An Area Partitioning and Multigroup Key Predistribution Approach", ACM Transactions on Sensor Networks, Vol. 3, No. 3, Article 16, August 2007.

[75] Zhang, W., Tran, M., Zhu, S., and Cao, G., "A Random Perturbation-Based Scheme for Pairwise Key Establishment in Sensor Networks", Proceedings of ACM MobiHoc'07, Montreal, Canada, September 9-14, 2007, pp. 90-99.

[76] Xiao, Y., Rayi, V. K., Sun, B., Du, X., Hu, F., and Galloway, M., "A Survey of Key Management Schemes in Wireless Sensor Networks", Computer Communications, Vol. 30, 2007, pp. 2314–2341.

[77] Younis, M. and Akkaya, K., "A Survey on Routing Protocols for Wireless Sensor Networks", Ad Hoc Networks, Vol. 3, 2005, pp. 325-349.

[78] Karl, H. and Willig, A., Protocols and Architectures for Wireless Sensor Networks, Wiley, January 2006.

[79] Wang, X., Gu, W., Chellappan, S., Schosek, K., and Xuan, D., "Lifetime Optimization of Sensor Networks Under Physical Attacks", Proceedings of 2005 IEEE International Conference on Commmunications (ICC 2005), Volume 5, May 16-20, 2005, pp. 3295-3301.

[80] Wang, X., Gu, W., Schosek, K., Chellappan, S., and Xuan, D., "Sensor Network Configuration Under Physical Attacks", ICCNMC 2005, LNCS 3619, Springer-Verlag 2005, pp. 23-32.

[81] Warneke, B. A. and Pister, K. S. J., "MEMS for Distributed Wireless Sensor Networks", Proceedings of the 9th IEEE International Conference on Electronics, Circuits and Systems, Volume 1, Dubrovnik, Croatia, 15-18 September 2002, pp. 291-294.

[82] http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/Imote2_Datasheet.pdf

[83] Akyildiz, I. F., Melodia, T., and Chowdhury, K. R., "A Survey on Wireless Multimedia Sensor Networks", Computer Networks, Vol. 51, 2007, pp. 921-260.

[84] Pathan, A.-S. K., Heo, G. and Hong, C. S., "A Secure Lightweight Approach of Node Membership Verification in Dense HDSN", Proceedings of the IEEE Military Communications Conference (IEEE MILCOM 2007), October 29-31, Orlando, Florida, USA.

[85] Gu, L., Jia, D., Vicaire, P., Yan, T., Luo, L., Tirumala, A., Cao, Q., He, T., Stankovic, J. A., Abdelzaher, T., and Krogh, B. H., "Lightweight detection and classification for wireless sensor networks in realistic environments", Proceedings of ACM SenSys 2005, 2-4 November, San Diego, California, USA, 2005, pp. 205-217.

[86] Dutta, P., Grimmer, M., Arora, A., Bibyk, S., and Culler, D., "Design of a Wireless Sensor Network Platform for Detecting Rare, Random, and Ephemeral Events", Proceedings of the 3rd symposium on Information Processing in Sensor Networks (IPSN'05), LA, California, 2005, pp. 497-502.

[87] Chan, S.-P., Poovendran, R., and Sun, M.-T., "A Key Management Scheme in Distributed Sensor Networks Using Attacks Probabilities", Proceedings of IEEE GLOBECOM 2005, Volume 2.

[88] 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, Vol. 23, No. 4, April 2005, pp. 839-850.

[89] Chan, H., Perrig, A., and Song, D., "Random Key Predistribution Schemes for Sensor Networks", Proceedings of Security and Privacy Symposium 2003, May 11-14, 2003, pp. 197 - 213.

[90] Tanachaiwiwat, S. and Helmy, A., "Correlation Analysis for Alleviating Effects of Inserted Data in Wireless Sensor Networks", Proceedings of MobiQuitous'05, July 17-21, 2005, pp. 97-108.

[91] Gurses, E. and Akan, O. B., "Multimedia Communication in Wireless Sensor Networks", Annals of Telecommunications, Vol. 60, No. 7-8, July-August 2005, pp. 799-827.