Security of Wireless Sensor Network

Jinat Rehana
Helsinki University of Technology
jrehana@cc.hut.fi

Abstract

Wireless Sensor Networks (WSN) is an emerging technology and day by day it is attracting the attention of researchers with its challenging characteristics and diversified application domain. The more researchers try to develop further cost and energy efficient computing devices and algorithms for WSN, the more challenging it becomes to fit the security of WSN into that constrained environment. However, security is crucial to the success of applying WSN. So, familiarity with the security aspects of WSN is essential before designing WSN system. This paper studies the security problems of WSN based on its resource restricted design and deployment characteristics and the security requirements for designing a secure WSN. Also, this study documents the well known attacks at the different layers of WSN and some counter measures against those attacks. Finally, this paper discusses on some defensive measures of WSN giving focus on the key management, link layer and routing security.

KEYWORDS: Sensor, Security, Attack, Defense.

1 Introduction

With the advances in wireless communication and computing devices, Wireless Sensor Network has come into the spotlight. By utilizing these advances, WSN provides low cost solution to a variety of real world challenges. A Wireless Sensor Network is a combination of wireless networking and embedded system technology that monitors physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. Initially, Wireless Sensor Networks were mainly used for military surveillance. However, now its applicability is extended to civilian and commercial application areas, including environmental and medical monitoring, manufacturing machinery performance monitoring, home automation, traffic control etc.

Security is a common concern for any network system, but security in Wireless Sensor Network is of great importance to ensure its application success. For example, when sensor network is used for military purpose, it is very important to keep the sensed information confidential and authentic. Providing security for WSN represents a rich field of research problems as many existing security schemes for traditional networks are not applicable for WSN. For example, WSN requires lightweight security mechanisms so that the overhead caused by security purpose are minimized and cannot affect the performance of the network. This is because that WSN is limited in resources and networks than traditional networks. Also, deployment nature of WSN is different than usual networks. Typically, a sensor network consists of a large number of tiny sensor nodes and possibly a few powerful control nodes called base stations. Sensor nodes are supplied with limited battery power and they have small memory size and limited computational ability. A typical sensor node processor is of 4-8 MHz, having 4KB of RAM and 128KB flash [24]. Again, WSN is supported with low communication bandwidth. Very often, sensor nodes are scattered randomly in the inaccessible, hazardous environment without any infrastructure support and operate unattended. These characteristics of WSN make it vulnerable to lots of security problems and complicate the development of security mechanisms as well. Moreover, the unreliable communication channel makes the security defenses even harder. All these security challenges are encouraging new researches to properly address sensor network security from the start and develop security protocols and algorithms suitable for WSN.

The design limitations, communication and deployment patterns of WSN pose several security problems to it and make it vulnerable to different type attacks. Exploiting those security holes adversaries can perform different types of attacks in order to disrupt the network, hamper or misguide the communication flow of the network, or to intercept, fabricate or modify the confidential data. To combat against those attacks coming from different levels of WSN security vulnerabilities, firstly, it is very important to know about the security requirements of WSN. Moreover, analysis of security requirements gives right directions to develop or implement the proper safeguards against the security violations.

For fulfilling the basic security requirements of WSN and defending some potential attacks, the defensive measures discussed in this paper are categorized into cryptography, key distribution for supporting cryptographic security features, link layer security and secure routing. Defining these defensive measures for WSN with limited resource and network facilities is an open research and there has been a significant number of research works regarding this issue.

The rest of the sections of this paper explore the issues concerning the security of WSN one by one. The organization of this paper is as follows: Section 2 discusses about the security problems that arise in WSN because of its resource restrictions and deployment characteristics, Section 3 focuses on the essential requirements for ensuring WSN security, Section 4 briefly describes some attacks at different layers and some proposed countermeasures and Section 5 discusses about the defensive measures of WSN directing three important security aspects which are cryptography and key management, link layer and routing security with some related works in some detail.

2 Security Problems

Usually, sensor nodes are densely deployed and they interact with their surrounding environment very closely. They are operated unattended and also without the absence of any remote monitoring system. That is, the nodes are exposed to the hostile environment as well as to the attackers and at a risk of physically being tampered. So, there is always the possibility of capturing nodes physically by the attackers to attack the WSN. Also, there are lots of security problems in Wireless Sensor Network that can be logically exploited by the adversaries to attack the networks. According to [5][17][24] [1]the security problems in WSN as follows.

Sensor nodes themselves are points of attack for the Wireless Sensor Networks. Adversaries can compromise or subvert sensor nodes to gain full control of them and utilize them for disrupting the network. If sensor nodes are compromised, the attackers are able to know all the confidential information stored on them and may launch a variety of malicious actions against the network through these compromised nodes. For example, the compromised nodes may discard important data or report with wrong or modified data to mislead any decision which is taken based on this data. The subverted nodes may reveal the cryptographic key information and thus allow the attackers to compromise the whole network. False malicious nodes can be added to exhaust other sensor nodes, attract them to send data only to it preventing the passage of true data.

Besides the sensor nodes, attackers can target the routing information which is used to maintain the communication between sensor nodes and the base station. The routing mechanisms used for WSN requires complete trust between all the participating nodes. The proper transport of data in the network depends on the integrity of the routing information given by other nodes. False routing information transmitted by a host may partition the network by misguiding the traffic to a small group of nodes and thus causes difficulty in communication. As WSN requires hop by hop routing to transport the packets to the destination, any intermediate node acting maliciously can drop, modify or misguide the traffic traversing through it. Adversaries can create these security problems in WSN by compromising nodes, or spoofing, altering, replaying the routing information.

Again, the unreliable wireless medium used as communication medium in WSN causes many security problems. The adversary just needs to be within the radio range of the nodes. Being there, he can easily intercept the transmission without causing any interruption in the network communication. Thus, an adversary can collect sensitive information if the transmission is not encrypted. Also, an attacker can easily inject malicious messages in the WSN. Moreover, by analyzing the traffic, an adversary can gather useful information to perform mischievous operations. However, for avoiding collision and providing cooperation among the nodes during the transmission, WSN uses medium access control protocols. But, a subverted node can change the behavior of this protocol in order to launch denial of service type attacks. Section 4 describes how an adversary can perform actual attacks on WSN exploiting these security threats.

3 Security Requirements

Wireless Sensor Network is vulnerable to various attacks like any other conventional network, but its limited resource characteristics and unique application features requires some extra security requirements including the typical network requirements. [10] [15] [23] discuss on several security properties that should be achieved when designing a secure WSN.

3.1 Data Confidentiality

Data confidentiality is one of the vital security requirements for WSN because of its application purpose (for example, military and key distribution applications). Sensor nodes communicate sensitive data, so it is necessary to ensure that any intruder or other neighboring network could not get confidential information intercepting the transmissions. One standard security method of providing data confidentiality is to encrypt data and use of shared key so that only intended receivers can get the sensitive data. Section 5 discusses more on this cryptography issues for WSN.

3.2 Authenticity and integrity

Only providing data confidentiality is not enough to ensure the data security in WSN. As an adversary can change messages on communication or inject malicious message, authentication of data as well as sender are also crucial security requirements. Source authentication provides the truthfulness of originality of the sender. Whereas, data authentication ensures the receiver that the data has not been modified during the transmission.

3.3 Availability

We can not ignore the importance of availability of nodes when they are needed. For example, when WSN is used for monitoring purpose in manufacturing system, unavailability of nodes may fail to detect possible accidents. Availability ensures that sensor nodes are active in the network to fulfill the functionality of the network. It should be ensured that security mechanisms imposed for data confidentiality and authentication are allowing the authorized nodes to participate in the processing of data or communication when their services are needed. As sensor nodes have limited battery power, unnecessary computations may exhaust them before their normal lifetime and make them unavailable. Sometimes, deployed security protocols or mechanisms in WSN are exploited by the adversaries to exhaust the sensor nodes by its resources and makes them unavailable for the network. So, security policies should be implied so that sensor nodes do not do extra computation or do not try to allocate extra resources for security purpose.

3.4 Requirements for Secure Sensor Network Protocols

The above mentioned security requirements are the basic security needs for WSN. However, sensor nodes are always at a risk of physically being captured. Only fulfilling those basic requirements can not totally solve the security problems created by node compromise. Tamper resistance hardware can protect the data stored on sensor node. But using such hardware exceeds the cost limit of WSN by increasing cost of individual sensor node. So, a better solution is to design secure sensor network protocols that are resilient to node comprise or node failure. Secure protocols can also be developed to achieve the basic security requirements.

Security protocols for WSN should have the capability of providing the following requirements besides the basic security requirements to ensure proper security functionality in WSN.

- *Data Freshness*

  Data Freshness implies that the data is recent. This is an important security requirement to ensure that no message has been replayed meaning that the messages are in an ordering and they cannot be reused. This prevents the adversaries from confusing the network by replaying the captured messages exchanged between sensor nodes. To achieve freshness, security protocols must be designed in such a way that they can identify duplicate packets and discard them preventing replay attack.

- *Robustness against Attacks*

  Security protocols should have robustness against attacks. If an attack is performed they should have the ability to minimize the impact. They also should have the ability to detect failed sensor nodes and work with the remaining nodes and updated topology.

- *Resilience*

  In practice, detection of compromised nodes and revocation of their cryptographic keys are not always possible. So, a security protocol should always consider WSN with compromised nodes. If a number of nodes are compromised, secure protocols should function in such a way that the performance of WSN degrades gracefully.

- *Broadcast Authentication*

  The base station broadcasts command and data to sensor nodes. An attacker can modify or forge the commands and sensor nodes perform incorrect operations accepting those commands. So, secure protocols should provide broadcast authentication functionality for the sensor nodes.

- *Self Organization*

  In WSN, there is no fixed network infrastructure as WSN is typically an ad hoc network. So, the sensor nodes must have the self organizing and self healing capability to support multi hop routing. But, secure communication among the sensor nodes is a precondition for providing security in WSN. So, security protocols should support efficient key management so that sensor nodes self organize themselves according to the key distribution and can build trust relations with the neighbor nodes and secure virtual infrastructure as well.

- *Scalability*

  The number of sensor nodes in WSN can be of several orders of magnitudes and the nodes are densely deployed. Again, the network topology of WSN is dynamic in nature that is new nodes can be added extending the network size. So, scalability is an important issue and security protocols as well as key management should cope with the increasing network size. A security mechanism is not an efficient one if it performs well in a small size network but does not work well for large size network.

4 Attacks in Wireless Sensor Network

For securing the Wireless Sensor Networks, it is necessary to address the attacks and then take counter measures at the design time of WSN. This section lists and gives brief discussion about the major attacks against Wireless Sensor Network.

4.1 Physical Attack

This attack is also known as node capture. In this type of attack, attackers gain full control over some sensor nodes through direct physical access [3]. As the cost of sensor nodes must be kept as cheap as possible for WSN, sensor nodes with tamper proofing features are impractical. This is why sensor nodes are susceptible to be physically being accessed. Physical attacks have significant impacts on routing and access control mechanisms of WSN. For example, getting key information stored on sensor node's memory gives attacker the opportunity of unrestricted access to WSN.

For performing physical attack an adversary may require expert knowledge, costly equipments and other resources. Also, most of the time physical attack requires the victim node to be removed from the deployment area for a certain amount of time. The neighbor nodes can notice this removal. Still, some attacks can be performed without disrupting the normal node operations or without being noticed by other nodes. For example, an attacker can get control over the microcontroller of sensor node via JTAG or can gain the right of reading or writing the microcontroller's memory without affecting the current program stored in the microcontroller via Bootstrap Loader [3].Disabling the JTAG interface or protecting the Bootstrap Loader password can protest these types of attacks. Designing sensor nodes with hardware platform of up to date embedded system security can improve the physical level security. Moreover, monitoring sensor nodes for unusual length of inactivity period and revocation of suspicious node's authentication token are necessary steps those should be taken for securing WSN against Physical or node capture attacks.

4.2 Attacks at Different Layer

Besides physical attack, adversaries perform a large number of attacks remotely. These attacks take place affecting different networking layers of WSN. This subsection describes some of these well known attacks.

4.2.1 Physical Layer

Physical layer is responsible for actual data transmission and reception, frequency selection, carrier frequency generation, signaling function and data encryption. This layer also addresses the transmission media among the communicating nodes. WSN uses shared and radio based transmission medium which makes it susceptible to jamming or radio interference.

- *Jamming*

  In physical layer, jamming is a common attack that can be easily done by adversaries by only knowing the wireless transmission frequency used in the WSN. [10] Says the attacker transmits radio signal randomly with the same frequency as the sensor nodes are sending signals for communication. This radio signal interferes with other signal sent by a sensor node and the receivers within the range of the attacker cannot receive any message. Thus, affected nodes become completely isolated as long as the jamming signal continues and no messages can be exchanged between the affected nodes and other sender nodes.

  For preventing physical layer jamming [16] suggests frequency hopping as a countermeasure. In frequency hopping spread spectrum, nodes change frequency in a predetermined sequence. But, it is not suitable for WSN because every extra frequency requires extra processing and the range of possible frequencies for WSN is limited. [5] suggests Ultra Wide Band transmission technique as an anti jamming solution. UWB transmission is based on sending very short pulses in order of nanoseconds across a wide frequency band and is very difficult to detect. This technique is suitable for WSN because of its low energy consumption.

4.2.2 Link Layer

The data link layer is responsible for the multiplexing of data streams, data frame detection, medium access and error control. This layer is vulnerable to data collision when more than one sender tries to send data on a single transmission channel.

- *DoS Attack by Collision Generation*

  In link year, collision is generated to exhaust the sensor node's energy. In order to generate collision, the attacker listens to the transmissions in WSN. When he finds out the starting of a message, he sends his own radio signal for a small amount of time to interfere with the message [5] which causes CRC error at the receiving end. Because of this attack, the receivers can not receive the message correctly. Collision is more energy saving from the adversary part than radio jamming as according to the literature, collision in one byte is enough to cripple the message. So, we can say collision is energy efficient jamming. Sometimes, collision adversely exploits the used MAC layer protocol in WSN. Reception of incorrect message causes the sender node to retransmit the message. Thus, attackers are able to spoil the limited power of sender node by compelling the node to retransmit message continuously.

  Using error correcting codes is a typical way to defend against collision. But, error correcting codes can work up to a threshold level of collision for example, collision caused by environmental or probabilistic errors. However, error correcting codes add processing and communication overhead. So, they are not effective for WSN. Encrypting the packets at link layer may help to prevent the jamming actions based on the content of the packets. TinySec is a link layer security architecture that provides the facility of link layer packet encryption. Section 5 describes the functionality of TinySec in more details. Even when the packets are encrypted, the temporal arrangement of packets induced by the nature of the protocol may reveal the pattern and the adversary can take advantage of it for jamming [16]. Also, [16]suggests that in the absence of effective countermeasure TDM like protocol LMAC can be adopted as it has better anti jamming property than other protocols like SMAC and BMAC. In LMAC, each node is given only one time slot for collision free transmission. The slots are divided among the nodes according to a distributed algorithm.

4.2.3 Network Layer

Network layer is responsible for routing messages from one to another node which are neighbors or may be multi hops away for example, node to base station or node to cluster leader. The network layer for WSN is usually designed considering the power efficiency and data centric characteristics of WSN. There are several attacks exploiting routing mechanisms in WSN. Some familiar attacks are listed here.

- *Selective Forwarding*

  Selective forwarding is an attack where compromised or malicious node just drops packets of its interest and selectively forwards packets to minimize the suspicion to the neighbor nodes. The impact becomes worse when these malicious nodes are at closer to the base station [24]. Then many sensor nodes route messages through these malicious nodes. As a consequence of this attack, a WSN may give wrong observation about the environment which affects badly the purpose of mission critical applications such as, military surveillance and forest fire monitoring. This attack can be extended to forward messages to wrong nodes and thus misdirecting the traffic.

  Two different countermeasures have been proposed against selective forwarding attack. One defense is to send data using multi path routing [8]. Another one is detection of compromised nodes which are misbehaving in terms of selective forwarding and route the data seeking an alternative path. [27]proposes CHEMAS (CHEckpoint-based Multi-hop Acknowledgement Scheme), a lightweight security scheme for detecting selective forwarding attacks. This scheme randomly selects a number of intermediate nodes as checkpoints which are responsible for generating acknowledgement. According to this scheme, along a forwarding path, if a checkpoint node does not receive enough acknowledgements from the downstream checkpoint nodes it can detect abnormal packet loss and identify suspect nodes.

- *Sinkhole Attack*

  In sinkhole attack, a compromised node attracts a large number of traffic of surrounding neighbors by spoofing or replaying an advertisement of high quality route to the base station [17]. The attacker can do any malicious activity with the packets passing through the compromised node.

- *Wormhole Attack*

  Wormhole is a critical attack, where the attacker receives packets at one point in the network, tunnels them through a less latency link than the network links to another point in the network and replay packets there locally [13]. This convinces the neighbor nodes of these two end points that these two distant points at either end of the tunnel are very close to each other. If one end point of the tunnel is at near to the base station, the wormhole tunnel can attract significant amount of data traffic to disrupt the routing and operational functionality of WSN. In this case, the attack is similar to sinkhole as the adversary at the other side of the tunnel advertises a better route to the base station.

  Both the sinkhole and wormhole attacks are difficult to detect especially in WSNs those use routing protocols in which routes are decided based on information advertisements such as remaining energy or minimum hop count to base station. [16] suggests to use geographic routing protocol which has better resilience against these attacks. GPSR [12] and GEAR [25] are such geographic based routing protocols. In geographic routing protocol, the traffic is always directed to the base station along a geographically shortest path. These protocols do not rely on adversaries' advertisement and is able to find out the actual location of adversary nodes. [26] proposes a secure routing protocol named SERWA that fights against wormhole attacks. This protocol can detect wormhole attack without using any special hardware and can provide a real secure route against the wormhole attack.

- *Hello Flood Attack*

  In Hello flood attack, the attacker broadcasts hello message with a very powerful radio transmission to the network to convince all nodes to choose the attacker to route their messages. The affected nodes waste their energy by sending messages to the node which is out of their radio range.

  The key solution against Hello Flood attack is authentication. Authenticated broadcast protocols for example, μTESLA is an efficient one for this purpose. This protocol is based on symmetric key cryptography with minimum packet overheads. Section 5 gives further description on μTESLA. [14] proposed a countermeasure against Hello Flood attack adopting a probabilistic secret sharing protocol and using bidirectional verification. Here, according to the probabilistic secret sharing, secrets shared between two sensor nodes are not exposed to any other nodes. For defending against attack, each request (REQ) message forwarded by a node is encrypted with a key which is generated on the fly (during communication). Sender node's reachable neighbors can decrypt and verify the REQ message but the attacker will be prevented from launching the attack without knowing that key.

- *Sybil Attack*

  In Sybil attack, a malicious or subverted node forges the identities of more than one node or fabricates identity. This attack has significant effect in geographic routing protocols [17]. In the location based routing protocols, nodes need to exchange location information with their neighbors to route the geographically addressed packets efficiently. Sybil attack disrupts this protocol functionality simultaneously being at more than one place.

  Identity verification is the key requirement for countering against Sybil attack. Unlike traditional networks, verification of identity in WSN cannot be done with a single shared symmetric key and public key algorithm because of computational limitation of WSN. Newsome et al. in [19]shows with quantitative analysis that random key pre distribution scheme can be used to defend against Sybil attack. For this purpose, they associated sensor node's identity with its assigned key using one way hash function. According to their mechanism, the network is able to verify part or all of the keys that an identity claims to have and thus counters against Sybil attack.

4.2.4 Transport Layer

In network layer end to end connections are managed.

- *Flooding Attack*

  According to [26] and [22], at this layer, adversaries exploit the protocols that maintain state at either end of the connection. For example, adversary sends many connection establishment requests to the victim node to exhaust its resources causing the Flooding attack.

  One solution against this attack is to limit the number of connections that a node can make. But, this can prevent legitimate nodes to connect to the victim node. Another solution is based on the client puzzles idea described in [2]. According to this idea, if a node wants to connect with other node, it at first must solve a puzzle. An attacker does not likely have infinite resources and it is not possible for him to make connections fast enough to exhaust a serving node. Though solving puzzle includes processing overhead, it is more desirable than excessive communication.

- *desynchronization attack*

  In desynchronization attack, an attacker repeatedly forges messages to one or both end points of an active connection with fake sequence number or control flag. Thus attackers desynchronize the end points so that sensor nodes retransmit messages and waste their energy.

  One countermeasure against this attack is to authenticate all the packets exchanged between sensor nodes along with all the control fields in transport header. The adversary cannot spoof the packets and header and thus this attack can be prevented.

4.2.5 Application Layer

In application layer, data is collected and manages. Here, sensor nodes can be subverted to reveal its information including disclosure of cryptographic keys hence compromising the whole sensor network. Moreover, a node can be compromised to malfunction and generate inaccurate data and this effect can be worse enough when the node is a cluster leader in WSN [24].

If a node is compromised, detection and exclusion of that node from the sensor network is a probable solution. LEAP [28] can verify whether a node has been compromised or not and can revoke compromised nodes with efficient re keying mechanism.

5 WSN Defenses and Related Works

It is very hard to accumulate all the security requirements in a single security mechanism as the WSN has severe resource constraints and it has no predefined infrastructure. Lots of research have been done and are on going to privilege the WSN with crucial security support. WSN needs effective, energy and resource efficient key management scheme for providing confidentiality, integrity and authentication security services. Link layer security mechanism in WSN can provide important security support by guaranteeing integrity, authenticity, and confidentiality of messages because they deny an outsider access to the network. Secure routing is another essential requirement for protecting WSN against external and insider attack. Proper security solution for preventing DoS attacks at different layers is also a dire need for protecting the WSN from disruption. This section discusses on cryptography and key establishment for WSN and then some security mechanisms regarding link layer and routing security of WSN are explored in some detail.

5.1 Cryptography

Cryptography is essential for ensuring security services. Public key cryptography such as Diffie-Hellman key agreement protocol or RSA signature is not suitable for WSN because of its limitation in memory, computation and power. For example, to perform a single security operation RSA executes thousands or even millions of multiplication instructions. In wireless devices with limited facilities, for encryption and decryption RSA requires on the order of tens of seconds and up to minutes [4]. Whereas, symmetric cryptography and hash functions are faster and more computationally efficient than public key algorithms. That is why, most security schemes and security researches for WSN are based on symmetric key cryptography.

5.2 Key Distribution / Management

One major problem of symmetric cryptography is how to distribute shared key to communicating nodes. Another problem is to keep shared key secret only between the communicating hosts so that adversary's can not get reach of it. This is why, besides light weight cipher, efficient key distribution and key management are fundamental security requirements for WSN. Self organization is an important aspect of WSN as the sensor nodes are deployed without following any pre established structure. For example, some times sensor nodes are just airdropped in enemies' arena. In such situations, sensor nodes organize themselves to form a wireless network. Key pre-distribution is a key management scheme where before deployment each sensor node is provided with some keys and after reaching the target position the sensor nodes builds up a secure network among them based on those keys. Another important aspect of WSN is in network processing as it provides energy efficiency to WSN. In this case, WSN is divided into number of clusters, data is collected and processed by an aggregator node of each cluster and then transmitted to another aggregator forming a hierarchy and this data fusion saves energy of WSN. Here passive participation is another aspect, in which sensor nodes take actions based on messages from other nodes. In such cases, hierarchical key management is required to provide security in different level of communication in WSN. The following discussion is on some works based on these two types of key management protocol.

5.2.1 Key Pre-distribution Key Management

Eschenauer and Gligor in [7] introduced a random key pre-distribution scheme where the key distribution is divided into three phases which are key pre-distribution, shared-key discovery, and path-key establishment. In key pre-distribution stage, a large pool of S keys and associated identifiers for each key are generated. Then from that key pool a number of key rings are generated by randomly drawing k keys along with their identifiers for each key ring and then each sensor node is given a key ring. The base station stores the key rings of each node and the associated node identifiers. Also, each sensor node shares a pair wise key with the base station. In shared key discovery phase, after the deployment, each node broadcasts a list α, $\mathrm{E}_{Ki}(\alpha)$; i= 1,...,k where α is a challenge. In the communication range of the broadcasting node if a receiving node can decrypt $\mathrm{E}_{Ki}(\alpha)$ with the proper key from its key chain then the broadcasting node and that receiver node establish a secure link between them with that shared key. If two sensor nodes which do not share a common key but want to communicate and are at two or more links away, then they can get a path-key in path establishment phase. If a node is compromised, the base station sends a message containing the identifier list of the keys of the compromised node's key chain to all the nodes encrypting with the pair wise keys shared with them. The nodes in the network can then delete the corresponding key from their key chain. This scheme is also known as basic scheme.

In this key management scheme if the size of the network grows, each node in the network needs to store only a few keys, which is memory efficient and provides scalability. Again, when a node is compromised, the probability of an attacker to successfully attack a node is k/S where k«S. So, in key revocation process much communication overhead is not introduced as a small number of nodes are affected. But, this scheme is not able to provide node to node authentication which is a requirement to protect node replication attack (i.e, sybil attack).

Chan et al. in [6] proposed Q-Composite Scheme, which was introduced to increase the resilience of the network against node capture than basic scheme. Here in this scheme, in shared key discovery phase, to establish a secure link two nodes require at least q common keys in their key rings instead of a single common key as in basic scheme. According to the authors' observation this property increases the resilience to node capture when a small number of nodes are compromised. However, this scheme performs badly when more nodes are compromised as same keys are used repeatedly in a network. But, usually adversaries first try to attack in small scale and if they succeed then they proceed for large scale attack. So, this scheme is reasonable to protect small scale attack and thus preventing large scale one. This scheme also cannot provide node to node authentication and if an attacker performs large scale attack the security of the network breaks down under this scheme.

Chan et al. in [6] also proposed a multipath keyreinforcement scheme for WSN where security is more important than bandwidth or power drain. The problem in basic scheme is that the common key which establishes a security link between two nodes A and B, may reside in the memory of other nodes in the network and by capturing those nodes an adversary can attack that secure link between A and B. So, Chan et al. introduced a key update phase in multipath keyreinforcement scheme. In this case, A generates random j random values (v1, v2,. . . ,vj) where j is the number of disjoint paths available from A to B. Then A sends each random value along a different disjoint path. After receiving all the random values, B generates a new key by doing XOR the original key with all the random values. If an adversary wants to reconstruct the communication key he needs to eavesdrop all the j disjoint paths. The disadvantage of this scheme is that it introduces communication overhead which may exhaust nodes battery life and may give chance adversaries to launch DOS attack. Chan et al. further extended their research by proposing random pairwise key scheme to provide node to node authentication.

5.2.2 Hierarchical Key Management

Zhu et al. [28] proposed Localized Encryption and Authentication Protocol (LEAP) for WSN which is a key management protocol. LEAP provides different security requirements for different types of messages exchanged between sensor nodes. For this purpose, LEAP introduces 4 types of keys for each sensor node which are individual key, pairwise shared key, group key and cluster key.

Each sensor node has a unique key named individual key which is shared with the base station to secure the messages between a sensor node and the base station. Example of such messages are alert message of abnormal observation about neighboring node from a sensor node to base station, keying material or special instruction for a node from the base station and so on.

Pairwise shared key is a unique key which is shared between each node and its neighboring node. This key provides security when a node wants to share cluster key with its neighbor or a node sends data to the aggregator node. This key is also used to provide efficient node to node authentication.

Group key is shared among all the nodes in the network and the base station uses this key to provide security of broadcast message sent to the whole group. For example, the base station encrypts the missions, queries and interests with this key and broadcasts the encrypted message. As this key is shared among all the nodes, there is a chance that an adversary can get the key by compromising a node. So, LEAP also provides efficient rekeying mechanism for updating group key to solve this problem.

Cluster key is a key shared by a node and all its neighbors. This key secures locally broadcast message and supports in network processing and passive participation. For example, when a node locally broadcast the sensor message by securing with this key, the neighbor nodes can take decision whether to send the same message or not by decrypting or authenticating that message.

LEAP can minimize the effect of selective forwarding attack as it uses local broadcast, thereby the effect of this attack cannot be transferred more than 2 hops away. LEAP can prevent HELLO Flood attack as the node accepts packets only from its authenticated neighbor. LEAP can also prevent Sybil attack by providing unique ID authentication for each node. Again, after key establishment as each node has the knowledge about its neighbors, it is not easy for and adviser to convince a node that it is near to a particular compromised node, thereby Worm Whole attack is discouraged. The disadvantage of this scheme is that memory for each node to store 4 types of keys as well as computation and communication overhead increase if the density of WSN increases.

5.3 Link Layer Security

TinySec [11] works at link layer and provides access control, message authencity, integrity and message confidentiality. TinySec provides message security using cryptographic primitives- encryption and MAC. TinySec supports two different security options: authenticated encryption (TinySec-AE) and authentication only (TinySec-Auth). In TinySec-AE, TinySec encrypts the data payload and authenticates the packet with a MAC. With TinySec-Auth, the packet authentication is performed with a MAC without encrypting the data payload.

For encryption, TinySec uses an 8 byte IV and cipher block chaining (CBC). One problem here is that if IV repeats it can introduce security leakage. This is why CBC mode is used here as with the same IV under CBC mode the cipher text will leak only the length (in blocks) of the longest shared prefix of the two plaintexts. For providing message integrity, TinySec uses a cipher block chaining construction, CBC-MAC with 4 byte output for computing and verifying MACs. With a 4 byte MAC if an adversary tries to inject a malicious packet into the network, he will succeed after 2^{31} tries. Even If an adversary tries to do so, implementing a simple mechanism that nodes will signal the base station when the rate of MAC failures exceeds some predetermined threshold can prevent such attempts. TinySec also provides the flexibility of using any keying mechanism. The drawback for implementing TinySec is that TinySec packets are one to five bytes longer than normal WSN packets which may reduce bandwidth and increase latency and energy consumption.

5.4 Secure Routing

In conventional networks the routing protocols mainly concern about the reliable delivery of messages. Message security (i.e. confidentiality, integration and authentication) and protection against DOS attacks are performed by end to end mechanisms such as SSL or SSH. As end to end communication is the main concern, there is no need for the intermediate routers to know the content of the message except the necessary headers. But, the scenario is different in WSN where in many cases intermediate nodes need to communicate with each other for providing in network processing or data aggregation before sending the message to the base station. In this case, intermediate nodes have the ability to modify, suppress or eavesdrop the message content and compromised node can exploit the features of routing protocol to cause potential damage of working functionality of the network. So, for WSN, routing protocols must be designed taking security also as a goal. For facilitating routing protocols with security mechanisms key management for each sensor node is an essential part which has been discussed in the previous text. The following text is on some secure routing mechanisms for WSN.

[9] proposed a routing protocol directed diffusion for WSN which is energy, bandwidth and memory efficient highly desirable for WSN. But this protocol is not able to afford secure group communication that is the communication between sink and sources. Pietro et al. in [21] extended this directed diffusion protocol to incorporate security in it. They extended the Logical Key Hierarchy (LKH) for facilitating secure multicast and merged this extension with directed diffusion and named their scheme as LKHW. LKHW gives robustness in communication and enforces both backward and forward secrecy. But, it cannot provide data authentication.

Nasser et al in [18] proposed SEER: Secure and Energy-Efficient multipath Routing protocol in which base station performs the route discovery, maintenance and route selection. Instead of using a single path, base station periodically select a new path from multipath based on current energy level of nodes along each path. Attacks on routing protocols that attract traffic by advertising high quality route to the base station such as, Wormhole and Sinkhole can be defended by SEER as the routing path is selected by the base station. If in the routing path a node is compromised, the attack lasts for limited time as the base station periodically reselects new path. SEER can also defend selective forwarding attack as the attacker cannot include itself in the routing path to launch the selective forwarding attack. Again if any compromised node selectively drops packet it can be detected by the next hop as SEER uses sequence number that uniquely identify each packet. But, if adversaries can breach the security of base station they can disrupt the whole network.

Perrig et al. [20] present SPINS which comprises two security building blocks optimized to use in WSN which are SNEP and μTESLA. SNEP provides semantic security, data authentication, replay protection and weak freshness by implementing symmetric cryptographic primitives such as MAC, and encryption with RC5. Before encrypting the message sender attaches a random bit string with the message and this property provides semantic security, replay protection and weak freshness. For excluding extra communication overhead of sending this extra random bit with each message, SNEP shares a counter between the communicating nodes for the block cipher in counter mode (CTR). The communicating parties increment the shared counter after each block. Data authentication is achieved by verifying the MAC value of the message.

μTESLA provides authenticated broadcast for WSN from symmetric primitives, but introduces asymmetry with delayed key disclosure and one-way function key chains. μTESLA uses a loosely synchronized timer on both the base station and other nodes to authenticate the MAC key. The base station computes a MAC on a packet with a key which is secret at that certain time to send the packet as authenticated. When a node receives a packet it can verify that the base station has not yet disclosed the corresponding MAC key. So, it stores the packet in its buffer until for the next key disclosure of the base station. After having the disclosed key, the node verifies the correctness of the key and authenticates the packet which it stored in buffer for authentication before key disclosure. As μTESLA incorporates the mechanism to verify the MAC key of base station by sensor nodes, sensor nodes are assured that no adversary could alter the packet in transit. But, the broadcast here is limited to the base station. If any node wants to broadcast it has to do that via base station.

6 Conclusion

With super small sensor nodes, super low power consumption and alluring low cost, Wireless Sensor Network is attracting uncountable application domains to sense and collect data. But, these attractive features made Wireless Sensor Network challenging to integrate security mechanism into it. This paper gives an idea of a major subset of security problems that Wireless Sensor Network faces because of its exceptional design characteristics, communication and deployment pattern. At the same time, this paper includes brief discussion on the important security aspects that are required to design a secure Wire Sensor Network. Some Well known attacks and their proposed counter measures are also discussed in this paper in order to give an idea about how the adversaries can actually attack the WSN exploiting its vulnerabilities and what kind of security awareness should be taken into account when incorporating security mechanisms in WSN. Finally, this paper explores some works on three crucial security aspects of WSN which are key management, link layer security and secure routing. There are also many security aspects of WSN such as secure data aggregation, intrusion detection, secure localization, etc. which are not covered in this paper.

There are many security solutions or mechanisms that have been proposed for Wireless Sensor Network; some of which are concerned about specific security attacks whereas some are concerned about specific security aspect. There is no standard security mechanism that can provide overall security for WSN. Providing such mechanism is not possible also as WSNs are implemented in various application domains with different level of security requirements. Designing a secure WSN needs proper mapping of security solutions or mechanisms with different security aspects. This also imposes a research challenge for WSN security.

References

[1] F. Anjum and P. Mouchtaris. *SECURITY FOR WIRELESS AD HOC NETWORKS*. Wiley, 2007.

[2] T. Aura, P. Nikander, and J. Leiwo. Dos-resistant authentication with client puzzles. pages 170–177. 2001.

[3] E. Becher, Z. Benenson, and M. Dornseif. Tampering with motes: Real-world physical attacks on wireless sensor networks. In *Proceeding of the 3rd International Conference on Security in Pervasive Computing (SPC*, pages 104–118, 2006.

[4] M. Brown, D. Cheung, D. Hankerson, J. L. Hern, M. Kirkup, and A. Menezes. Pgp in constrained wireless devices. In *in Proceedings of the 9th USENIX Security Symposium*, pages 247–261, 2000.

[5] S. Datema. A Case Study of Wireless Sensor Network Attacks. Master's thesis, Delft University of Technology, September 2005.

[6] W. Du, J. Deng, Y. S. Han, and P. K. Varshney. A key predistribution scheme for sensor networks using deployment knowledge. *IEEE Transactions on Dependable and Secure Computing*, 3(1):62–77, 2006.

[7] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In *CCS '02: Proceedings of the 9th ACM conference on Computer and communications security*, pages 41–47, New York, NY, USA, 2002. ACM Press.

[8] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin. Highly-resilient, energy-efficient multipath routing in wireless sensor networks. *SIGMOBILE Mob. Comput. Commun. Rev.*, 5(4):11–25, October 2001.

[9] C. Intanagonwiwat, R. Govindan, and D. Estrin. Directed diusion: a scalable and robust communication paradigm for sensor networks. In *ACM International Conference on Mobile Computing and Networking (MOBICOM'00*, pages 56–67, 2000.

[10] John Paul Walters, Zhengqiang Liang, Weisong Shi and Vipin Chaudhary. Wireless sensor network security: A survey. *Security in Distributed, Grid, and Pervasive Computing*, 2006.

[11] C. Karlof, N. Sastry, and D. Wagner. Tinysec: a link layer security architecture for wireless sensor networks. In *SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 162–175, New York, NY, USA, 2004. ACM Press.

[12] B. Karp and H. T. Kung. Gpsr: greedy perimeter stateless routing for wireless networks. In *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 243–254, New York, NY, USA, 2000. ACM Press.

[13] I. Khalil, S. Bagchi, and N. B. Shroff. Liteworp: Detection and isolation of the wormhole attack in static multihop wireless networks. *Comput. Netw.*, 51(13):3750–3772, 2007.

[14] M. A. R. K.Hamid and H. C. S. Routing security in sensor network: Hello flood attack and defense. In *to appear in IEEE ICNEWS*, Dhaka, January 2006.

[15] C. W. L. Weimin, Y. Zongkai and T. Ymmen. Research on the security in wireless sensor network. *ŤAsian Journal of Information Technology*, 2006.

[16] Y. W. Law and P. Havinga. How to secure a wireless sensor network. pages 89–95, Dec. 2005.

[17] Mayank Saraogi . Security in Wireless Sensor Networks. In *ACM SenSys*, 2004.

[18] N. Nasser and Y. Chen. Secure multipath routing protocol for wireless sensor networks. pages 12–12, June 2007.

[19] J. Newsome, C. Mellon, and E. Shi. The sybil attack in sensor networks: Analysis and defenses. pages 259–268. ACM Press, 2004.

[20] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar. Spins: Security protocols for sensor networks. In *Wireless Networks*, pages 189–199, 2001.

[21] R. D. Pietro, L. V. Mancini, Y. W. Law, S. Etalle, and P. Havinga. Lkhw: A directed diffusion-based secure multicast scheme for wireless sensor networks. *Parallel Processing Workshops, International Conference on*, 0:397, 2003.

[22] D. R. Raymond and S. F. Midkiff. Denial-of-service in wireless sensor networks: Attacks and defenses. In *IEEE Pervasive Computing*, volume 7, pages 74–81, 2008.

[23] E. Shi and A. Perrig. Designing secure sensor networks. In *Wireless Communications, IEE*, volume 11, December 2004.

[24] Z. Tanveer and Z. Albert. Security issues in wireless sensor networks. In *ICSNC '06: Proceedings of the International Conference on Systems and Networks Communication*, page 40, Washington, DC, USA, 2006. IEEE Computer Society.

[25] N.-C. Wang, P.-C. Yeh, and Y.-F. Huang. An energy-aware data aggregation scheme for grid-based wireless sensor networks. In *IWCMC '07: Proceedings of the 2007 international conference on Wireless communications and mobile computing*, pages 487–492, New York, NY, USA, 2007. ACM.

[26] A. Wood and J. Stankovic. Denial of service in sensor networks. In *Computer*, volume 35, page 54Ű62, 2002.

[27] B. Xiao, B. Yu, and C. Gao. Chemas: Identify suspect nodes in selective forwarding attacks. *Journal of Parallel and Distributed Computing*, 67(11):1218 – 1230, 2007.

[28] S. Zhu, S. Setia, and S. Jajodia. Leap: efficient security mechanisms for large-scale distributed sensor networks. In *CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*, pages 62–72, New York, NY, USA, 2003. ACM Press.