Chapter 6

Secure Routing Issues in Wireless Sensor Networks

6.1 Introduction
6.2 Key Issues for Achieving Security in Wireless Sensor Networks
6.3 Architecture of Wireless Sensor Networks
6.4 A Note on Active & Passive Attack
6.5 Protocol Stack of Wireless Sensor Networks
6.6 Threats at Different Layers in Wireless Sensor Network Protocol Stack
6.7 Solution at Different Layers in Wireless Sensor Networks
6.8 Conclusion
Wireless Sensor Network (WSN) as an emerging field has several application areas starting from civil life to sophisticated defense domain. These are normally designed to perform a set of high level information processing tasks, for example detection, tracking or classification. Different application areas of WSNs are Environmental Monitoring, Industrial Sensing and Diagnostics, Infrastructure Protection, Battle Field Awareness, Context Aware Computing etc. From different application areas of WSN, it has been observed that ensuring security and privacy is one of the highest priorities for Wireless Sensor Network Systems. Information in the network must be protected from the attackers. Attackers may device different types of security threats to make the WSN system unstable. In this chapter, different types of security threats possible for a sensor network setting are identified. Some existing solutions to different security threats are also discussed. Future scope of the work has also been outlined.


6.1 Introduction

Wireless sensor networks have emerged as a dominant technology in the current decade. Diversified application areas of wireless sensor networks indicate the bright future of this new paradigm. WSNs are becoming popular day by day. Already many companies have started developing commercial applications. At the same time they have posed numerous unique challenges to researchers. Wireless sensor networks are generally composed of hundreds or even thousands of tiny sensor nodes, which are constrained in many aspects like memory capacity, processing power and most importantly energy or battery power. Most of the time sensor nodes do not have access to renewable energy resources. The overall cost of a WSN is also required to be relatively lower.

Moreover when the applications of WSNs are observed, it is seen that there are many application areas, e.g., battlefield awareness, traffic monitoring system etc in which security of information remains as an important issue. Providing security to a WSN is a nontrivial problem. Security mechanisms which are applicable to wired or other ad-hoc networks are not suitable for WSN. There are many reasons behind it and those are discussed in the subsequent sections.

Though there are varieties of challenges in sensor networks, focus here is on different security issues and possible remedies of those. To make WSN feasible for all kinds of applications at lower cost, it is required to have simple protocols for communication, security, topology management, and medium access control which are supposed to be energy efficient. Though security is a very important issue in WSN, very little published work is available for securing a WSN. To understand the limitations of current security mechanisms it is necessary to realize the features of a wireless sensor network. Different features of WSN such as low memory, low energy, low bandwidth for communication and large scale nodes make most of the current security solutions available for other ad-hoc and wired networks, impractical for WSNs.

Author reports different challenges in providing security to a WSN deployment:

*The first challenge:* there is a conflict of interest between minimization of resource consumption and maximization of security level. A better solution actually gives a good compromise between these two. During the design of any security solution it is important to take care of the following resource constraints [16]:

- limited energy,
- limited memory,
- limited computing power,
- limited communication bandwidth, limited communication range.

*The second challenge:* The type of security mechanism that can be hosted on a sensor node platform is dependent on the capabilities and constraints of sensor node hardware.
The third challenge: Ad-hoc networking topology of WSN facilitates attackers for different types of link attacks ranging from passive eavesdropping to active interfering. Attacks on a WSN can come from all directions and target at any node leading to leaking of secret information, interfering message, impersonating nodes etc.

The fourth challenge: The communication in WSN is through wireless media, mainly radio. This characteristic of WSN makes wire based security schemes impractical for a WSN.

The fifth challenge: The topology of WSN is always dynamic. The sensor nodes can come and go in an arbitrary fashion. Node failures may be permanent or intermittent and this gives a higher level of system dynamics. Again very often large numbers of nodes are expected in sensor network deployments and the nature of this deployment is unpredictable.

The sixth challenge: The overall cost of the WSN should be as low as possible.

The seventh challenge: Although the sensor nodes are static in nature in the case of a WSN, in some applications of WSN the sensor nodes are mobile having low or moderate mobility. In this scenario all solutions to different security issues of WSN become more complex. Again in the event of high mobility of the sensor nodes this becomes extremely difficult.

6.2 Key Issues for Achieving Security in Wireless Sensor Networks

The ad-hoc networks such as wireless sensor networks suffer from different security attacks. Different security issues in this context are reported in [81][82][84]. Based on the analysis on security challenges and potential attacks on wireless sensor networks, four key issues have been identified for providing security to the WSNs. Those are mentioned below:

A) Key Management in WSN: Confidentiality, integrity and authentication services are critical factors for maintaining the security of a WSN. Key management is a highly important issue for this kind of protection in WSN. However, providing key management service in WSN is extremely difficult due to various constraints in the WSN environment, e.g., ad-hoc nature of the network, intermittent connectivity, resource limitation, limited communication bandwidth etc.

B) Encryption and Decryption Mechanism: Since the WSN environment is resource constrained, this encryption procedure as well as the decryption mechanism has to be very simple and energy efficient. Due to memory and energy constraint in a WSN environment it is not feasible to go for traditional asymmetric cryptographic approach.

C) Secure Routing in WSN: The major two types of threats in routing protocols of wireless sensor networks are:
a) External attackers: External attackers may become successful in partitioning a network or in introducing excessive traffic load into the network. Various attacks include – injection of erroneous routing information, replaying old routing information, distorting routing information etc. Use of cryptographic schemes can defend against the external attacks.

b) Internal compromised nodes: It is difficult to put defense against such attacks. These nodes may send malicious information to other nodes in the network.

D) Prevention of Denial-of-Service: A Denial of Service attack is any event that diminishes or eliminates a network’s capacity to perform its expected function. Hardware failures, software bugs, resource exhaustion, environmental conditions, or any complicated interaction between these factors can cause a Denial of Service.

6.3 Architecture of Wireless Sensor Networks

Based on the design parameters like scalability, power consumption, fault-tolerance and robustness there are two types of sensor network architecture available, e.g., layered architecture and clustered architecture.

A) Layered Architecture

In layered architecture, a powerful Base Station is surrounded by the different layers of sensor nodes. Each layer contains sensor nodes that have same hop-count to the Base Station (BS). The main advantage of the layered architecture is that each node in the sensor network is involved in only short distance and low-energy transmissions to the nodes of the neighboring layers. [19]

B) Clustered Architecture

In clustered architecture, sensor nodes are logically organized into clusters and each cluster remains under the control of a relatively powerful node called as Cluster Head (CH). Each node in a cluster is involved in message exchanges with their respective Cluster Heads. And finally the Cluster Heads send the aggregated data to the BS. The sensor networks are inherently suitable for data fusion and therefore, all data gathered by the sensor nodes can be fused at the CH. After the fusion of data at the CH, the amount of data to be transmitted to the BS gets reduced significantly. [19]

6.4 A Note on Active & Passive Attack

One way of classifying security attacks is in the form of active attack and passive attack. A passive attack tries to learn information from the system without affecting the system resources. On the other hand active attack tries to affect the system resources.
Chapter 6

Passive attack tries to learn the information in a system by eavesdropping or by monitoring the transmissions. Two major types of passive attacks are release of message content and traffic analysis. Passive attacks are difficult to detect as they don’t try to alter the data in question. It is feasible to protect data against these types of attacks by encrypting the data with a strong mechanism.

Active attack involves the alteration of data or introduction of some false data. This type of attack can be divided into four main categories: masquerade, replay, modification of messages, and denial of service. It is very difficult to prevent active attacks absolutely. Therefore, emphasis is on to detect any active attack and then to recover from any disruption or delays caused by those.

6.5 Protocol Stack of Wireless Sensor Networks

The most popular protocol stack so far for wireless sensor networks has been described in [16]. This protocol stack is used by the Sink as well as the sensor nodes. It consists of the Physical Layer, Data Link Layer, Network Layer, Transport Layer and Application Layer along with the planes namely Power Management Plane, Mobility Management Plane and Task Management Plane. Main responsibilities of different entities in the protocol stack are as follows:

<table>
<thead>
<tr>
<th>Entity</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Layer</td>
<td>Robust yet simple Modulation, Transmission and Receiving Technique</td>
</tr>
<tr>
<td>Data Link Layer</td>
<td>Power Aware MAC Protocol</td>
</tr>
<tr>
<td>Network Layer</td>
<td>Routing of data</td>
</tr>
<tr>
<td>Transport Layer</td>
<td>Maintain the flow of data</td>
</tr>
<tr>
<td>Application Layer</td>
<td>Different application software can be built in this layer</td>
</tr>
<tr>
<td>Power Management Plane</td>
<td>Manages power in each sensor node</td>
</tr>
<tr>
<td>Mobility Management Plane</td>
<td>Detects and registers the movement of sensor nodes</td>
</tr>
<tr>
<td>Task Management Plane</td>
<td>Balances and schedules (among the sensor nodes) the sensing tasks given to a region.</td>
</tr>
</tbody>
</table>

Table 6.1 Protocol Stack Entities of Wireless Sensor Network
6.6 Threats at Different Layers in Wireless Sensor Network Protocol Stack

In this section, different types of security threats present in different layers in the protocol stack of a wireless sensor network are discussed. There are some types of security threats which span even over more than one layer. In the work reported in [83][85] authors enlisted different security threats present in different layers of the protocol stack along with their respective countermeasures which are possible to adapt.

**A) Physical Layer**

The communication media among the sensors is normally radio. Since the media is open, high amount of risk is present there. Some of those security threats are mentioned below.

JAMMING: In this type of attack, adversaries interfere with the communication frequencies (radio frequencies) of the sensor nodes present in the network. For this purpose the adversary may select a few jamming nodes from within the whole network and then she may apply jamming simultaneously from these selected nodes. In this case, the number of nodes the adversary needs is a small fraction of the total number of nodes present in the network. Jamming is a popular Denial of Service (DoS) attack.

SYBIL ATTACK: The base of Sybil Attack is actually at the Physical Layer but it becomes more prompt in the higher layers like Link Layer and Network Layer. In this class of attack the adversary introduces a malicious node into the network. This can be done by compromising any legitimate sensor node or by fabricating a new node. This malicious node acquires identity through one of the two ways- by fabricating new identities or by stealing some identities. The malicious node behaves as if it were of different identities from different places in the network. It is a famous Classical Attack.

TAMPERING: In most of the applications the number of sensor nodes deployed is very high and the geographic area over which those nodes are distributed is also very large. Therefore, it becomes impossible to control the access to all nodes from others. Again the fabrication of the sensor nodes is simple and this is done mainly to reduce the cost. Normally tamper resistant hardware is not provided as it adds more cost to the sensor nodes. Due to these factors any body can get access to the sensor nodes physically and even adversaries may introduce some identical sensor nodes into the sensor network field from their own side. Again adversaries may become successful in compromising some of the legitimate nodes in the network. After compromising a node, she may carry out lots of misleading activities inside the network.

**B) Data Link Layer**

Following are some of the security threats in link layer:

COLLISION: In this type of Denial of Service attack, adversary can induce collision in only one small portion of the entire packet transmitted by a node. A small change in the
data portion of the packet leads to an error in the checksum of the whole packet and asks for retransmission of the same packet.

SYBIL ATTACK: This type of attack is very much prominent in Link Layer. Different variations of Sybil Attacks are as follows:

*Data Aggregation:* Data aggregation is an important part in wireless sensor networks as it reduces the power consumption as well as the bandwidth requirements for individual message transmission. In this situation, a Sybil Attack can be used to induce negative reinforcements. A single malicious node is sufficient to act as different Sybil Nodes and then this may give many negative reinforcements to make the aggregate message a false one.

*Voting:* It is observed that voting may be a good choice for number of tasks in a wireless sensor network system. Many MAC protocols may go for voting for finding the better link for transmission from a pool of available links. Here, the Sybil Attack could be used to stuff the ballot box. An attacker may be able to determine the outcome of any voting and off course it depends on the number of identities the attacker owns.

INTERROGATION ATTACK: Some Medium Access Control layer implementations use RTS (Request To Send) and CTS (Control To Send) packets to reserve channel access to transmit data. A malicious node can send RTS packets continuously to a targeted node by ignoring CTS reply packets. Then this can flood the network link of the targeted node. Normally this type of attack is done by either a malicious node or by a self sacrificing node.

EXHAUSTION: Some Link Layer protocols attempt retransmission repeatedly, in the event of the transmission getting triggered by a collision. Adversaries may exploit it for doing exhaustive Denial of Service attack in which she continuously disturbs the communication between two nodes and forces the source node retransmit continuously. This leads to the quick decay in the energy level of the sensor nodes.
Chapter 6

Layer | Attacks
--- | ---
Physical Layer | Jamming, Sybil Attack, Tampering
Data Link Layer | Collision, Sybil Attack, Interrogation Attack, Exhaustion
Transport Layer | Flooding Attack, De-synchronization

Table 6.2 Summary of Security Attacks in Wireless Sensor Networks

C) Network Layer

Major security goals of Network Layer are as mentioned below.

i) Every eligible receiver should receive all messages intended for it. Every receiving node should also be able to verify the integrity of every message as well as the identity of the sensor.

ii) Routing protocol should also be responsible for preventing eavesdropping caused by misuse or abuse of the protocol itself.

In a wireless sensor network, every node behaves as a router and routing issue is a complicated one from security point of view also. Designers of routing protocols didn’t consider security aspects during the design of the routing protocols and that is why wireless sensor networks routing protocols are vulnerable to different types of attacks.

Here is a list of different types of attacks on the Network Layer:

SYBIL ATTACK: All multi-path routing protocols are vulnerable to Sybil Attacks. The malicious node present in the network may advertise different identities. Then all paths in the multi-path protocol may pass through the malicious node. And the protocol may have a picture of existence of different paths. But actually it is the same path through the
malicious node. Sybil Attack actually can fool the protocol giving a picture of existence of different routing paths to the destination but it is the same path through the Sybil node. On top of that even geographic routing protocols are also vulnerable to Sybil attack. It is because of the fact that the same Sybil Identity or different Sybil nodes may give an illusion of their presence at different geographic locations.

NEGLECT AND GREED: In this type of attack, a node that is present in the routing path can drop the message by participating in the lower level protocols. What the node does is, it sends the ‘ACK’ message of the Link Layer and drops the Network Layer message. The node can also give arbitrary priorities to the messages that pass through it.

BLACK HOLE ATTACK: In this type of attack, some of the malicious nodes in the WSN intentionally advertise zero-cost routes through them. Then some routing protocols (e.g., distance vector routing) establish a route to a destination by selecting this malicious node as an intermediate node into the routing path; (as they look for low cost link). Also the neighbors of this malicious node select this route and compete for the bandwidth. In this process the neighbors of this malicious node waste their energy and create a hole or partition in the network called black hole.

MISDIRECTION: This is a more active attack in which a malicious node present in the routing path can send the packets in wrong direction through which the destination is unreachable. In place of sending the packets in correct direction the attacker misdirects those and that too towards one node and thus this node may be victimized.

SPOOFING AND ALTERING THE ROUTING INFORMATION: This is the most direct attack on a routing protocol; because, it targets the routing information which are supposed to be exchanged between the nodes. By spoofing, altering or replaying routing information, adversaries may be successful to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end to end latency etc.

INTERNET SMURF ATTACK: In this type of attack, the adversary can flood the victim node’s network link. The attacker forges the victim’s address and broadcasts echoes in the network and also routes all the replies to the victim node. This way the attacker can flood the network link of the victim.

WORMHOLE ATTACK: An adversary situated close to the Base Station may be able to completely disrupt routing by creating a well placed wormhole. An adversary could also convince nodes who would normally be multiple hops from a Base Station that they are only one or two hops away via the wormhole. All existing routing protocols are vulnerable to this type of attack and there is no solid defense available against the Wormhole Attack.

HELLO FLOOD ATTACK: Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors. A node receiving such a packet may assume that it is within radio range of the sender. And this assumption may be false.
SELECTIVE FORWARDING ATTACK: Normally it is believed that in a multi-hop network, participating nodes will faithfully forward the received messages. But sometimes this does not happen. This is what exactly happens in a selective forwarding attack. The malicious nodes may refuse to forward certain messages and they drop these messages to ensure that the messages do not get propagated any further. A simple form of this attack is - a malicious node behaves like a black hole and does not forward every packet she sees. But such an attacker may fail because the neighboring nodes may conclude that she has failed and decide to seek another route.

Another form of this attack is when an adversary may selectively forward packets. Here, the adversary may be interested in suppressing or modifying packets originating from a few selected nodes. In this situation, the adversary reliably forwards the remaining traffic to limit the suspicion of her wrong doing.

RUSHING ATTACKS: In this type of attack, an adversary node which receives a route-request packet from any source node, floods the packet throughout the network so quickly that the other nodes which also receive the same route-request packet, hardly find any time to react. Now, when the nodes in the network receive the legitimate route-request packet assume that these are duplicate packets of the packet already received through the adversary node and so they discard those. Now the scenario is like this- any route discovered by the source node will contain the adversary node as one of the intermediate nodes. Therefore, the source node will not be able to find out any secure route which will not include the adversary node as one of the intermediate nodes. This type of attack is always possible in the case of on-demand routing protocols that use duplicate suppression during the route discovery process.

D) Transport Layer

Different types of threats present in the Transport Layer are as mentioned below.

FLOODING ATTACK: Protocols that maintain state information at either end of the communication are vulnerable to Flooding Attack. One well-known attack is TCP SYN flood attack in which the adversary continuously sends the connection requests and floods the network link at the targeted node.

DE SYNCHRONIZATION: By disrupting some of the packets transmitting in between the nodes and by maintaining proper timings an adversary can make a pair of nodes stuck in synchronization recovery protocol. This compels the nodes to waste their energy.
Chapter 6

6.7 Solutions at Different Layers in Wireless Sensor Networks

In this section, various security solutions available at different layers of the protocol stack of WSN are discussed.

A) Physical Layer

JAMMING: Various forms of spread-spectrum communication are used as defense against Jamming. Frequency hoping is one form of spread-spectrum approach and this has been widely used as a defense against Jamming. In this approach, all communication nodes maintain a hopping sequence. Here the tricky point is, a jammer can get the hoping sequence if he observes the transmission and therefore, hoping should be done very fast. In that case the jammer can not interfere with the communication. The cost involved against frequency hoping is higher as the sensor nodes are power constrained as well as they have low computational capability.

SYBIL ATTACK: Normally this class of attacks is tackled efficiently in the higher layers of the protocol stack in a WSN, though they originate in the Physical Layer only. Some preventive measures like fixing of the number of nodes in a WSN (which may depend on the type of application, the WSN is intended for) can be taken which will prevent the adversary from fabricating new identities.

TAMPERING: The defense mechanism designed against tempering should prevent the attackers (adversaries) from getting any information about cryptographic keys or about the network even though she is successful in compromising some of the nodes. Here is a list of few defenses:

First: Self Destruction – whenever somebody accesses the sensor nodes physically the nodes vaporize their memory contents and this prevents any leakage of information.

Second: Fault Tolerant Protocols – the protocols designed for a WSN should be resilient to this type of attacks. This means even if some nodes are removed from the network setting or they are compromised, still the network should function properly.

B) Link Layer

Good encryption mechanism, authentication mechanism and error correcting techniques are required to put defense against most of the Link Layer threats. Since the sensor nodes are resource constrained, the above mentioned techniques should not be computation intensive and they should not put much overhead to the sensor nodes and also communication overhead should be minimum.

COLLISION: Providing error correcting codes – error correcting codes can be incorporated in the data packets to defend against collision. But, this solution comes at a higher cost in terms of computational complexity and energy consumption.
SYBIL ATTACKS: Radio Resource Testing – It is a popular defense against Sybil Attack. If one node is interested in verifying whether its neighbors are valid or Sybil identities then this node can assign each of its ‘n’ neighbors a different channel to broadcast some test messages. After this, the node can listen to any channel and find out whether the neighbor that was assigned that channel is legitimate or not. Apart from this some secret information may be shared by a node with its neighbors and Sybil identities may be detected. But this may put some extra communication overhead.

INTERROGATION ATTACK: To put a defense against such type of attacks a node can limit itself in accepting connections from same identity. During implementation it may be decided that a particular node will not accept more than a fixed number connections from same identity. A careful selection has to be made in fixing this threshold value.

EXHAUSTION: The defense against exhaustive Denial of Service Attack is very simple and still effective. If a node retransmits a message for more than a threshold number of times, then the node identifies itself as under attack and goes to sleep mode. Latter it may wake up and resume its normal operation.

C) Network Layer

The problem of securing the Network Layer reduces to the problem of securing route discovery of a routing protocol.

SYBIL ATTACK: There is no effective defense mechanism available against Sybil Attack in the Network Layer. But it is important to note that this attack cannot survive only in routing layer. First of all, the attacker interested in Sybil Attack must attack the Link Layer and also she needs to get Sybil Identities. And very good defense mechanisms for Sybil Attack in Link Layer are available through which this type of attack can be defended in the Link Layer itself.

NEGLECT AND GREED AND SELECTIVE FORWARDING ATTACK: One simple defense against this type of attack is – to use multiple routing paths or send redundant messages (which is off course not a power efficient scheme), through which the probability of selecting a vulnerable route can be reduced. This can also force the adversary to compromise more number of nodes to succeed.

BLACKHOLE ATTACK: This type of attack can be defended by accepting routing replies only from authorized nodes. Unauthorized nodes can easily be identified by just checking if some node is behaving abnormally.

MISDIRECTION AND INTERNET SMURF ATTACK: This kind of attack can be handled easily as follows – if it gets observed that a node’s network link is getting flooded without any useful information then the victim node can be scheduled into sleep mode for some time.
SPOOFING, ALTERING MESSAGES: Efficient encryption and authentication techniques can defend Spoofing Attacks. Encryption may be applied to some required fields in the header of the message. And this may save some energy from computing and communicating some extra bits. TESLA can be adopted for authentication.

WORMHOLE ATTACK AND HELLO FLOOD ATTACK: One defense against these types of attack is by checking the bi-directional link whenever selecting a path. Again location based routing protocols can avoid Wormhole Attacks since in these protocols each node knows approximately how many hops it is away from Sink. Here, Wormholes can not fool the nodes since they know their location.

RUSHING ATTACK: One defense against Rushing Attack is by detecting secure neighbor. And this may be done by bidirectional checking of the link while electing the route.

D) Transport Layer

The security issues in the transport layer are mainly due to the existence of the flaws in the Transport Layer protocols. Efficient design of Transport Layer protocols can avoid Transport Layer threats.

FLOODING ATTACKS: As a defense against this class of attack, a limit can be put on the number of connections from a particular node. Again a careful selection has to be made in determining this upper limit on the number of connections. A study of the topology of the network may be helpful in this regard.

DESYNCHRONIZATION: A solid authentication mechanism can be deployed to authenticate all packets exchanged, including all control fields in the transport packet header. It is assumed that the authentication mechanism is robust and adversaries also can not forge this mechanism. In this situation, the end nodes can detect malicious packets and ignore those.

6.8 Conclusion

Providing security in wireless sensor network is a non trivial task. In this chapter author studied different key issues in achieving security in WSN. Author has also studied different security threats those exist in different layers of the protocol stack of WSN. Possible solutions against different threats have also been outlined.