Various Security Threats in Wireless Sensor Networks and their Defense Schemes

Malhar Bhandari
M.E, A.G.P.C.E, Nagpur, Maharashtra, India
malhar9188@gmail.com

Abstract
Wireless sensor network (WSN) is a set of organized sensor nodes, typically deployed out in areas which have to be contacted wirelessly and are generally difficult to access. A sensor node is able to sense surroundings, communicate the information gathered to other nodes and also comprise computational power. These networks are by far open to many security threats, as once these networks are deployed, they are defenseless and neglected. Many intrinsic attributes like small memory and inadequate battery make sensor networks difficult to utilize usual security solutions. The applications of omnipresent wireless sensor networks have amplified the complication gradually to classify wireless sensor network attacks and shield against them. Various types of weakness related with WSN and their consequence as well as countermeasures are discussed in this paper.

Indexing terms
Attacks, Ad-hoc, Node, Security, Sensor

Academic Discipline and Sub-Disciplines
Wireless Communication and Computing

SUBJECT CLASSIFICATION
Wireless Sensor Networks

TYPE (METHOD/APPROACH)
Theory, Experimental Analysis

INTRODUCTION
Wireless sensor networks are comprised of several cheap micro sensor nodes employed in the observing/sensing the specific region/surroundings. In WSN, a multihop design can be created making use of three or more sensor nodes which can communicate wirelessly. Wireless sensor network is usually installed in open surroundings where they can be attacked easily. Since sensor nodes communicate via wireless communication link, the network could be easily attacked and hacked. WSN are not as safe as wired network, since they deal with several security related problems that are normal security threats plus encounters main attacks which includes the Denial of service (DOS) attack, selective forwarding-attack, etc. The sensor nodes possess very limited energy, storage ability and processing power. In wireless sensor networks the availability of low bandwidth comes up with a challenge for the security. There are also various unusual characteristics that make them very different from other networks for example wired network. Attention is needed to these additional features. Some characteristics are as following:

• Wireless sensor networks are self-managing and organizing in nature.
• Since number of sensor nodes may vary time to time in WSN, the topology of wireless sensor networks is not fixed.
• Sensor nodes have very limited resources like storage, processor's ability and battery life.
• Wireless sensor nodes are controlled centrally. In wireless sensor networks flow of data from one sensor node to another is determined as per the functional routing algorithm. According to security point of view, this paper shows a short but precise analysis of various attacks along with their effects and their defense schemes.

WIRELESS SENSOR NETWORKS CHALLENGES
As wireless sensor network is in demand today so much gradually, a lot of development is also going on. In comparison with conventional network, the WSN are still suffering from various challenges which are mentioned below in details:

Wireless Medium
The network is open various attacks due to wireless character of communication. These attacks are classified as active attacks and passive attacks. The active attacks are defined as the attacks in which attacker insert packets into the network and alter the content. On the other hand, in passive attacks attacker aims to snoop on communication within the network
and steal the valuable information. This factor is very important from point of view of security of WSN. The active and passive attacks are given in details in the following section.

**Ad-hoc Character**

An ad hoc network usually means any group of networks where every device has equal status on a network and is open to link with any additional ad hoc network device in link range. Because of high mobility nature of nodes network topology always gets changed. Therefore security system should be able to prevent malevolent attacks inside the ever changing dynamic network.

**Limited Memory Facility**

Sensor nodes are very small devices as a result they have inadequate storage or memory capacity. To make an effective security system, it is essential to write finite code because of limited memory.

**Less Battery Time**

As sensor nodes are small devices and for functioning they require a constant power supply which is slightly difficult to provide everywhere and consistently. If one of the sensor nodes fails it can result in the malfunction of whole network. As we can see, it is too a point of worry.

**Distant Surroundings**

As we know that wireless sensor nodes are installed in open unprotected surroundings. WSNs are vulnerable to a variety of security threats, because of broadcast character of the communication medium. Sensor nodes are usually deployed in hazardous vicinity or insecure areas where they can be stolen easily since they are not much physically protected from attackers. The intruder can take help of this weakness and can exploit the valuable information. For WSN such environment is the major challenge.

**Central Administration**

A sensor network is a distributed network lacking a central management point. This may raise the strength of the sensor network. If in the case where the network is designed faultily then it can cause problems and it will be really difficult to handle the network. So a central management can solve this problem.

**Extensibility**

Since every sensor node is of ad-hoc nature, it must be competent enough to take on dynamically varying topologies. Each node must be capable of communicating with other nodes of arbitrarily connected networks.

**Physical Attacks Vulnerability**

According to requirement the sensors may be installed in an open environment, for gauging, temperature, weather and other parameters. Open unprotected surroundings always have a further threat issue that there is a probability of physical attacks like hacking by intruders or opponents or physical altering.

**Transmission Clashes**

Sensor networks follows packet based routing approach and wireless medium as a result it makes the transmission unpredictable. The wireless transmission is not trustworthy because there are no suitable protocols.

**SECURITY THREATS IN WIRELESS SENSOR NETWORKS**

Wireless sensor network’s key factor which makes the network prone to attacks is transmission’s broadcast nature. WSNs are prone to wide variety of security attacks due to wireless character of communication. Since the nature of communication is broadcast, here is always threat of attacks. Besides, as sensor nodes are regularly deployed in open surroundings, so there is additional threat of natural or physical attacks, since they are not protected physically.

Basically attacks can be classified in two types that are:

A) Active Attacks    B) Passive Attacks

**A. Active Attacks**

Every now and then when illegal users (attackers or intruders) eavesdrop the transmission (stream of data) and change the information during the transmission. Such attacks are identified as active attacks as in Table 1.
1) WSN Routing Attacks

Some of the routing attacks are mentioned in Table 2.

Table 2: WSN Routing Attacks

<table>
<thead>
<tr>
<th>Routing Attacks in WSN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sinkhole Attack</td>
</tr>
<tr>
<td>Selective forwarding</td>
</tr>
<tr>
<td>Wormhole Attack</td>
</tr>
<tr>
<td>Hello flood attack</td>
</tr>
<tr>
<td>Sybil Attack</td>
</tr>
</tbody>
</table>

a) Sinkhole Attack

Sinkhole attack is fundamentally the attack in which adversary tries to draw the entire traffic of the specific network. It happens when a negotiated node generates attraction centre for other nodes and attracts entire traffic (data passage). This happens only with the aid of a node which is compromised.

b) Selective Forwarding

In selective forwarding attack the negotiated node forwards merely chosen data packets and not all the packets to the receiver.

c) Wormhole Attack

In wormhole attack the invader records data packets in single location and then stores those data packets in a different location so as to resend them afterwards in the network.

d) Hello Flood Attack

In hello flood attack, a hello packet is sent to the receiver nodes by intruder, which is an effort to fool the sensor nodes that the base station has sent this hello message. This hello packet easily convinces other sensor nodes in the network.

e) Sybil Attack

In Sybil attack, attacker threatens the reputation system of a peer-to-peer network by creating a huge amount of false name identities. This attack principally aims to fault tolerant schemes for example topology maintenance, distributed storage and multipath routing.

2) Node Replication Attack

In node replication attack, as the name suggests a fake copy of a node is added in the network. By copying the node ID and additional information linked to their identity, an attacker inserts a replicated node in a sensor network. This malicious
node can be dangerous for the sensor network since using this node an attacker can control a particular network section or even demolish the network.

3) Message Corruption
In this attack, the intruder modifies the message during its transmission thus disturbing the reliability of the network.

4) Denial of Service Attack
Denial of service attack (DoS) is a obvious attempt to prevent the genuine user from using a service or data. The regular method of attack engages congesting the target system with requests, so as to prevent it from providing service to authentic traffic. This assault blocks services for authentic users. Some of the examples of DoS attacks are: collision, homing, flooding, jamming, tapering, etc.

5) Physical Attack
Sensor nodes are usually installed in unprotected surroundings, so risk of external attacks like physical alteration or changing of information is always present. They are likely to be replaced by malicious nodes in open surroundings. They can be damaged by the external intruders quite easily.

6) Node Outage
The condition where a node halts its working is recognized as node outage. It can be very much dangerous, if master node in the network is compromised.

7) Passive Information Gathering
If sensor node is not encrypted, then some adversary possessing dominant resources can collect information from the sensor networks easily. The trespasser with an appropriately dominant receiver and elegant antenna can merely draw the data stream. Interference of the communication containing the physical positions of sensor nodes allows an attacker to locate the nodes and damage them. An adversary can also learn the application explicit content of communication including timestamps, message IDs and other important information. It is essential to use superior encryption methods to reduce the threats of passive information gathering.

8) Node Malfunction
The reliability of sensor network is hampered, if a data collecting node as a cluster leader is a malfunction node thus generating the wrong data.

9) Node Subversion
If the attacker captures a node, then there is danger of revelation of secret data like cryptographic keys and so compromise the entire sensor network. An attacker can obtain secret information (key) stored on a node by hacking it.

10) False Node
False node attack is said to occur, when an intruder adds an additional node in any network so as to insert malevolent data. By means of this false node a trespasser can insert some fake data which can upset the communication. This malicious code inserted in the network through a false node could extend to all nodes, which can damage complete network.

B. Passive Attacks
At times when illegal users (attackers or intruders) eavesdrop or monitor the transmission (stream of data) are known as passive attacks. Passive attacks are also called attacks against privacy. Some of the general attacks against privacy of sensor nodes are:

1) Traffic Analysis
There is danger of malevolent harm even if the message which is being transmitted is encrypted. This can be possible only when the adversary constantly studies the pattern of communication. This study can provide sufficient information to adversary to damage the network.

2) Camouflage Adversaries
Any attacker can place in a malevolent node in the network or even it can negotiate a node so as to draw the data packets of the network to alter or misroute them.

3) Eavesdropping & Monitoring
This is probably the most regular attack on node’s privacy. The opponent can simply acquire the message contents by snooping. Eavesdropping is very harmful when sometimes nodes are communicating information regarding controls.
WIRELESS SENSOR NETWORKS SECURITY SOLUTIONS

In the modern era, wireless sensor network security has fascinated number of researchers around the globe. The key spotlight of this research is to evaluate and widen a variety of security solutions for wireless sensor networks.

A. Shared Keys

One of the security aspects that receive plenty of attention in wireless sensor networks is key management area. Due to their mobility, size and power limitation wireless sensor networks are distinctive in this feature. Conventionally, public-key protocols are used to complete the key establishment. A common technique of protecting any network against foreigner attacks is to apply a straightforward key infrastructure. Though it is identified that a global key offers no network flexibility, but pair wise keys cannot be a scalable solution.

B. Protected Grouping

Wireless sensor network comprises of a huge number of tiny nodes. Nodes are compressed and programmed devices. As sensor nodes need to connect themselves so as to complete a specific task, it is essential that the group elements communicate securing among each other's; regardless of the fact that overall security may be in use as well. However, secure grouping is not yet an exact solution. Situations where more powerful nodes are in control of defending the member of static groups are exceptions.

C. Encryption

Sensor network usually operate in open or wild regions over naturally insecure wireless channels. It is therefore trivial for a device to snoop or even inject messages in the network. The conventional solution to this threat has been to adopt methods such as symmetric key encryption schemes, (MAC) message authentication codes and public key cryptography.

D. Secure Data Aggregation

Data aggregation techniques and Sensor networks are prone to a variety of attacks which includes denial of service (DOS) attacks. As the transfer of data increases, data traffic is the most key problem in networks. So to facilitate reduction of network traffic and overhead cost, sensor node cumulate measurements prior to sending to the base station. Such data is mainly attractive to an attacker. An opponent with command over an aggregating node can prefer to ignore the report or produce a fake report, thus disturbing the credibility of the data generated and hence the network must be considered as a whole. The key intend in this area is to utilize resilient functions that will be able to determine and report counterfeit reports by representing the validity of data by one way or another.

E. SPINS: Security Protocols for Sensor Networks

SPINS is a collection of security building blocks estimated by Perig et al. It is specially made for resource controlled environments and wireless communication. SPINS has quite a few building blocks because of which it presents a lot of security properties like replay protection, data freshness, semantic security, data authentication, and low communication overhead.

F. TinySec: Link Layer Security Architecture

TinySec is a trivial and general security package that may be incorporated into sensor network applications. It is integrated in the official TinyOS release. Two particular security options are supported by TinySec: authentication only (TinySecAuth) and authenticated encryption (TinySecAE). In authentication only mode, TinySec validates the whole packet with a MAC, but the data payload lacks encryption [9]. While in authenticated encryption, TinySec encrypts the entire data payload and validates the packet with a MAC.

CONCLUSION

This paper provides concrete information about the security attacks. This comprises of the description of attacks as well as their categorization with good examples. In current state issues related to security in wireless sensor network has become a significant piece of research. This research paper illustrates the variety of requirements of security in wireless sensor networks. The variety of security issues and attacks has been examined and summarized. Different types of security susceptible solutions were projected to accomplish the improvement of power efficient and fault tolerant wireless sensor network model. The researchers will be certainly encouraged by this paper for research on wireless sensor networks and inspire them to come up with good innovative ideas for future work.

REFERENCES


