International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 8 (2014), pp. 859-868

http://www. irphouse.com

Wireless Sensor Networks: Security Issues, Challenges and Solutions

Vikash Kumar[1], Anshu Jain[2] and P N Barwal[3]

[1, 2, 3]e-Governance, C-DAC,
C-56/1, GB NAGAR, NOIDA, INDIA

ABSTRACT

The emergence of wireless sensor networks (WSN) as one of the dominant technology trends in the coming decades has posed numerous unique challenges to researchers. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. The inclusion of wireless communication technology also incurs various types of security threats. The intent of this paper is to investigate the security related issues, the challenges and to propose some solutions to secure the WSN against these security threats. While the set of challenges in sensor networks are diverse, this paper focus only on the challenges related to the security of Wireless Sensor Network. This paper begins by introducing the concept of Wireless Sensor Network (WSN). The introductory section gives brief information on the WSN components and its architecture. Then it deals with some of the major security issues over wireless sensor networks (WSNs). This paper also proposes some of the security goal for Wireless Sensor Network. Further, as security being vital to the acceptance and use of sensor networks for many applications; I have made an in depth threat analysis of Wireless Sensor Network. Lastly it proposes some security mechanisms against these threats in Wireless Sensor Network.

Keywords- Challenges, Issues, Security, Wireless Sensor Network (WSN)

1. INTRODUCTION

ONE of fundamental goals for Wireless Sensor Networks (WSNs) is to collect information from the physical world. Comparing to existing infrastructure – based networks, wireless sensor networks can virtually work in any environment, especially those where wired connections are not possible. WSNs are often deployed to sense, process and disseminate information of targeted physical environments.

In general, WSNs consist of battery-operated sensor devices with computing, data processing, and communicating components. The ways the sensors are deployed can either be in a controlled environment where monitoring and surveillance are critical or in an uncontrolled environment. In the uncontrolled environments, security for sensor networks becomes extremely important. This paper is outlined as follows. Section I provides the introduction to WSN and also covers the basic components and architecture of WSN. Section II describes various security threats of WSN. Section III describes the security challenges in implementing WSN. Section IV provides goals of security in WSN. Section V describes some security mechanism against these security threats. Section VI provides the conclusion of highlighted issues.

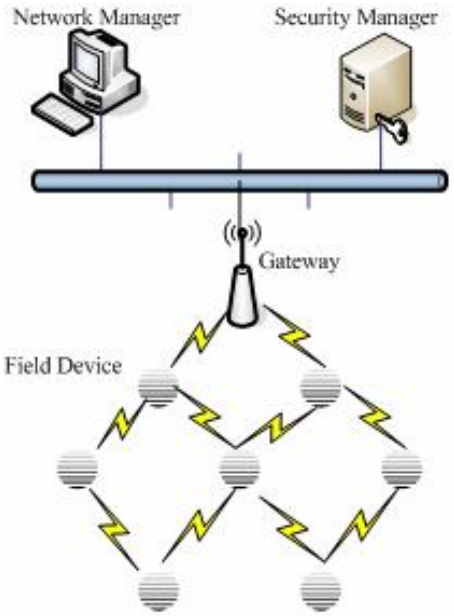
1.1 WSN Architecture

In a typical WSN we see following network components –

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

a) Interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.
b) Gateway or Access points – A Gateway enables communication between Host application and field devices.
c) Network manager – A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network.
d) Security manager – The Security Manager is responsible for the generation, storage, and management of keys.

The base stations are one or more distinguished components of the WSN with much more computational, energy and communication resources. They act as a gateway between sensor nodes and the end user as they typically forward data from the WSN on to a server. Other special components in routing based networks are routers, designed to compute, calculate and distribute the routing tables. Many techniques are used to connect to the outside world including mobile phone networks, satellite phones, radio modems, high power Wi-Fi links etc. Figure 1-1 shows the architecture of WSN.



2 Security Threats And Issues In WSN

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

2.1 Passive Attacks

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

2.1.1 Monitor and Eavesdropping:

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

2.1.2 Traffic Analysis:

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

2.1.3 Camouflage Adversaries:

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

2.2 Active Attacks

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

2.2.1 Routing Attacks in Sensor Networks:

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

2.2.1.1 Attacks on Information in transit:

In a sense or network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be altered, spoofed, replayed again or vanished. As wireless communication is vulnerable to eavesdropping, any attacker can monitor the traffic flow and get into action to Interrupt, intercept, modify or fabricate packets thus, provide wrong information to the base stations or sinks.

2.2.1.2 Selective Forwarding:

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

2.2.1.3 Black hole/Sinkhole Attack:

In this attack, a malicious node acts as a black hole to attract all the traffic in the sensor network. In fact, this attack can affect even the nodes those are considerably far from the base stations. Figure 2-1 shows the conceptual view of a black hole/sinkhole attack.

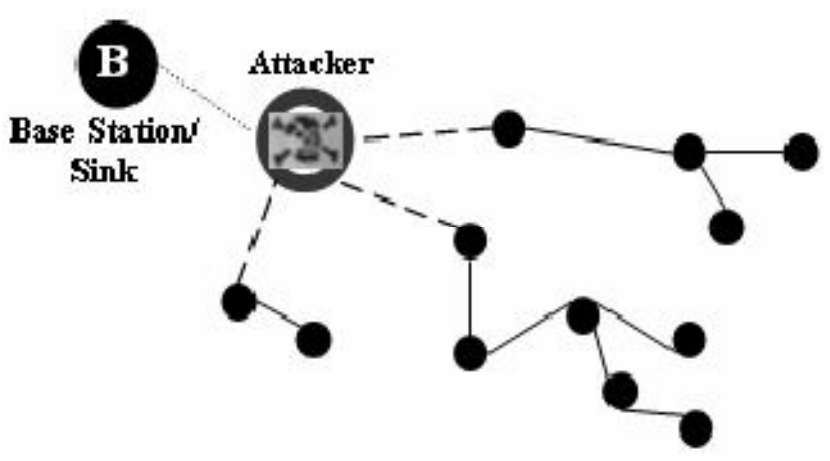
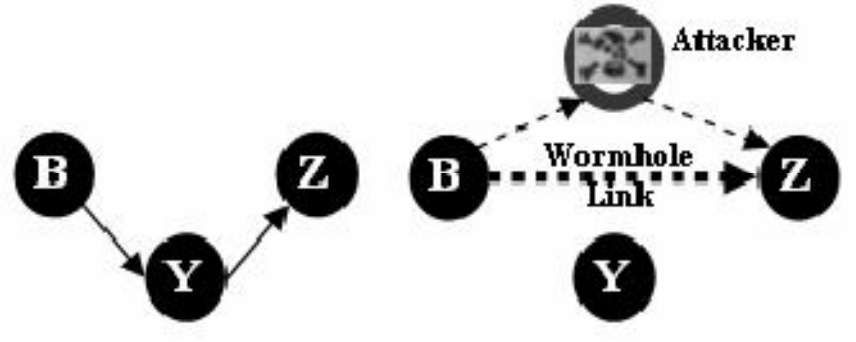


Figure 2-1: Conceptual view of Black hole Attack

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



(a) (b)

Figure 2-2: Wormhole Attack

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

2.2.1.4 HELLO flood attacks:
An attacker sends or replays a routing protocol's HELLO packets from one node to another with more energy. This attack uses HELLO packets as a weapon to convince the sensors in WSN.

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

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

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

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

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

2.2.7 Message Corruption:
Any modification of the content of a message by an attacker compromises its integrity.

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

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

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

3 Security Challenges In Wsn
The nature of large, ad-hoc, wireless sensor networks presents significant challenges in designing security schemes. A wireless sensor network is a special network which has many constraint compared to a traditional computer network.

3.1 Wireless Medium
The wireless medium is inherently less secure because its broadcast nature makes eavesdropping simple. Any transmission can easily be intercepted, altered, or replayed by an adversary. The wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones. Although this problem is not unique to sensor networks, traditional solutions must be adapted to efficiently execute on sensor networks.

3.2 Ad-Hoc Deployment:
The ad-hoc nature of sensor networks means no structure can be statically defined. Nodes may be deployed by airdrop, so nothing is known of the topology prior to deployment. Since nodes may fail or be replaced the network must support self-configuration. Security schemes must be able to operate within this dynamic environment.

3.3 Hostile Environment
The next challenging factor is the hostile environment in which sensor nodes function. Motes face the possibility of destruction or capture by attackers. The highly hostile environment represents a serious challenge for security researchers.

3.4 Immense Scale
The proposed scale of sensor networks poses a significant challenge for security mechanisms. Simply networking tens to hundreds of thousands of nodes has proven to be a substantial task.

4 Security Goals For Sensor Networks
The security goals are classified as primary and secondary. The primary goals are known as Standard security goals such as Confidentiality, Integrity, authentication and Availability (CIAA). The secondary goals are Data Freshness, Self Organization, Time Synchronization and Secure Localization.

4.1 Primary Goals
4.1.1 Data Confidentiality:
Confidentiality is the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential. This is the most important issue in network security. A sensor node should not reveal its data to the neighbors.

4.1.2 Data Authentication:
Authentication ensures the reliability of the message by identifying its origin.

4.1.3 Data Integrity:
Data Integrity in sensor networks is needed to ensure the reliability of data and refers to the ability to confirm that the message has not been tempered with, altered or changed. Even if the network has confidentiality measures there is still a possibility that the data integrity has been compromised by alterations. The integrity of the network will be in trouble when:

- A malicious node present in the network injects false data.
- Unstable conditions due to wireless channel cause damage or loss of data.

4.1.4 Data Availability:
Availability determines whether a node has the ability to use the resources and

whether the network is available for the messages to communicate. However, failure of the base station or cluster leader's availability will eventually threaten the entire sensor network. Thus availability is of primary importance for maintaining an operational network.

4.2 Secondary Goals

4.2.1 Data Freshness:

Even if Data Confidentiality and Data Integrity are assured, there is a need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. To solve this problem a nonce or another time-related counter, can be added into the packet to ensure data freshness.

4.2.2 Self Organization:

A wireless sensor network is typically an ad-hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infra-structure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security. If self-organization is lacking in a sensor network, the damage resulting from an attack or even the risky environment may be devastating.

4.2.3 Time Synchronization:

Most sensor network applications rely on some form of time synchronization. Sensors may wish to compute the end to end delay of a packet as it travels between two pair wise sensors. A more collaborative sensor network may require group synchronization for tracking applications.

4.2.4 Secure Localization

Often, the utility of a sensor network will rely on its ability to accurately automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pin point the location of a fault. Unfortunately, an attacker can easily manipulate non-secured location information by reporting false signal strengths, replaying signals.

5 Security Mechanisms In Wsn

The security mechanisms are actually used to detect, prevent and recover from the security attacks. A wide variety of security schemes can be invented to counter malicious attacks and these can be categorized as high-level and low-level.

5.1 Low-Level Mechanism

Low-level security primitives for securing sensor networks include:

5.1.1 Key Establishment and Trust Setup:

The primary requirement of setting up the sensor network is the establishment of cryptographic keys. Generally the sensor devices have limited computational power and the public key cryptographic primitives are too expensive to follow. Key-establishment techniques need to scale to networks with hundreds or thousands of nodes.

5.1.2 Secrecy and Authentication:

Most of the sensor network applications require protection against eavesdropping, injection, and modification of packets. The earliest sensor networks are likely to use link layer cryptography, because this approach provides the greatest ease of deployment among currently available network cryptographic approaches.

5.1.3 Privacy:

Like other traditional networks, the sensor networks have also force privacy concerns. Initially the sensor networks are deployed for legitimate purpose might subsequently be used in unanticipated ways. Providing awareness of the presence of sensor nodes and data acquisition is particularly important.

5.1.4 Robustness to Communication Denial of Service:

An adversary attempts to disrupt the network's operation

5.1.5 Secure routing:

Routing and data forwarding is a crucial service for enabling communication in sensor networks. Unfortunately, current routing protocols suffer from many security vulnerabilities.

6 Conclusion

Security in Wireless Sensor Network is vital to the acceptance and use of sensor networks. In particular, Wireless Sensor Network product in industry will not get acceptance unless there is a full proof security to the network. This paper summarizes the attacks and their classifications in wireless sensor networks and also an attempt has been made to explore the security mechanism widely used to handle those attacks. The challenges of Wireless Sensor Networks are also briefly discussed.

References

[1] Römer and Mattern, The Design Space of Wireless Sensor Networks. IEEE Wireless Communications, 2004.

[2] B. Krishnamashari, D. Estrin and S. Wicker, "Impact of Data Aggregation in Wireless Sensor Networks", Proc. 22nd International Conference Distrib. Comp. Systems, Jul. 2002.

[3] X. Du, and H-H. Chen, "Security in Wireless Sensor Networks", IEEE Wireless Communications, vol. 15, no. 4, Aug. 2008, pp.60-66.
[4] H. Luo, Y. Lin and S. K. Das, "Routing Correlated Data in Wireless Sensor Networks: A Survey", IEEE Network, vol. 21, no.6, Nov/Dec. 2007, pp. 40-47.
[5] R. Ramen, J. Lopez, S. Gritzalis, "Situation awareness mechanisms for wireless sensor networks ", IEEE Communication Magazine, vol. 46, no. 4, pp. 102-107, Apr. 2008.
[6] S. Rajasegarar, C. Leckie, and M. Palansiwami, "Anomaly detection in wireless sensor networks", IEEE Wireless Communications, vol. 15, no. 4, Aug. 2008, pp. 34-40.
[7] Yun Zhou, Yuguang Fang, Yanchao Zhang, Securing Wireless Sensor Networks: A Survey, IEEE Communications Surveys & Tutorials, year 2008
[8] Y. Wang, G. Attebury, and B. Ramamurthy, “A Survey of Security Issues in Wireless Sensor Networks, ” IEEE Commun. Surveys Tutorials, vol. 8, pp. 2–23, year 2006.