Wireless Sensor Network: Threat Models and Security Issues

Reenkamal Kaur Gill[1], Priya Chawla[2] and Monika Sachdeva[3]
[1,2,3]*Department of Computer Science and Engineering,*
Shaheed Bhagat Singh State Technical Campus, Ferozepur–152004, Punjab, India
E-mail: [1]reenkamalgill@gmail.com, [2]piyachawla12@gmail.com, [3]monika.sal@rediffmail.com

***Abstract*—Wireless Sensor networks is new emerging technologies that involves the deployments of tiny devices which are equipped with sensors communicate with each other over a specific geographical area to provide a collaborative measurement. This sensor arrangement can be used for specific purposes such as smart cities, smart agriculture, etc. Wireless Sensor Networks are prone to various kinds of threats and attacks. In this paper, we analyze different threat models, security issues and attacks that should be resolved to make the sensor network secure and smooth going.**

Keywords: Sensor, Wireless Sensor Networks, Attacks, Threat Models, Security

I. INTRODUCTION

Wireless Sensor Network is composed of large number of sensor nodes and the basic idea of sensor network is to deploy the sensor nodes in some geographical area which are capable of monitoring and recording the physical conditions of environment like temperature, sound, pollution level, humidity, etc. and for several other purposes like target tracking, surveillance, etc.

Unstructured WSN: It is a network that contains a large number of sensor Wireless Sensor Network is categorized as: an Unstructured and Structured Wireless Sensor Networks.

Nodes and they can be automatically organized to form an ad-hoc network.

Structured WSN: It has a pre-planned criteria that how to deploy the sensor nodes in large geographical area.

Hence, on the whole we can say that Structured WSN has an advantage over Unstructured WSN that it has lower management and maintenance cost.

Various features of WSN that attracts researchers to pay attention towards various issues related to these networks. But if we analyze previous researches, we could observe that routing strategies of WSN have been given much more priority. But in this paper, we will discuss about the security issues of WSN as well as their challenges. In the second section we will discuss about the various elements of WSN and in the next section various threat models are discussed. In the third section we will emphasize on various dimensions of security like confidentiality, integrity, authentication and data freshness. In the last section various attacks on routing protocols will be presented.

II. ELEMENTS OF WSN

Typical elements of wireless sensor network are:

Node: It is an autonomous device equipped with sensors. Node includes a radio transceiver along with an antenna, a microcontroller, an interfacing electronic circuit, and an energy source usually a battery. e.g., WaspMote.

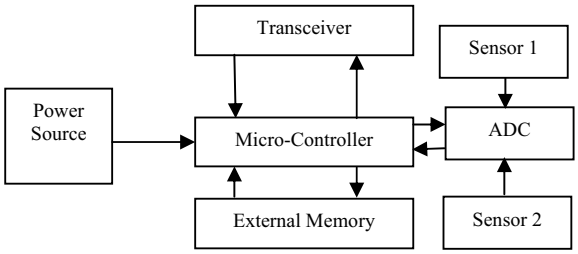

Fig. 1 Typical Architecture of the Sensor Node

Data Gatherer: This is a data capture device and it should be connected to external system in order to transmit sensor value.

e.g., Mashlium Xtreme.

External System: It is a data storing and managing centres. In case we want to store some data, we can use a non-volatile memory with some available space (e.g., EEPROM with 3 KB available) or maybe we can use the SD card (2 GB available) to store all the sensor values.

III. THREAT MODELS

Attacks on Wireless Sensor Network can be categorized into various categories on the basis of certain criteria. In the first category attack can be: Mote Class or Laptop Class [1].

In mote class attacker can interact with only few sensor nodes where the entire sensor nodes must have similar capabilities, whereas in case of a Laptop Class attacker can interact with more powerful devices like PDA's, Laptops etc.

A Laptop Class adversary can produce a huge amount of damage than Mote Class. Mote class adversary can effect only within small geographical area, but on the other hand Laptop Class adversary could have an effect on the entire network and even could block the entire sensor network.

Another classification of attack on Wireless Sensor Network can be: Insider or Outsider Attack.

In case of Insider attack the attacker has access to that node which has all the secret keys and is capable of participating in all the communications.

In Outsider attack attacker has no access to Wireless Sensor Network. It is done by the unauthorized node that eavesdrop the packets exchanged between the sensor nodes during their communication.

Next classification of attacks is based on Network Layer which are: Attacks at Physical Layer, at Data Link Layer and at Network Layer.

At Physical Layer attacker mainly exhaust the resources available by transmitting the radio signals on a Wireless Channel.

At Data Link Layer the attacker violate the predefined protocols of the Link Layer. This kind of attack also leads to Denial of Service attack.

At Network Layer attacker threatens the sensor applications and services. In this Localization and Aggregation are used to prevent from this attack.

TABLE 1: WSN THREATS IN LAYERS [2]

Layers	Attacks
Physical	1. Denial of Service (DoS) 2. Tempering
Data Link	1. Jamming 2. Collision
Network	1. Sybil Attack 2. Wormhole Attack 3. Sinkhole Attack 4. Flooding
Application	1. Desynchronization 2. Aggregation based attacks

IV. SECURITY REQUIREMENTS IN WSN

The different security concerns of Wireless Sensor Network are as follows:

1. *Data Confidentiality:* It means the content of the message when transmitted across the network must remain confidential i.e. only the intended receiver and no one else should be able to read the message. Hence encryption is used for effective and secure communication in which data is encrypted into secret words.
2. *Data Integrity:* It means data must reach the destination without being changed by the adversaries or Attackers. Data Integrity ensures that the data has not been changed during the transmission, neither accidentally or intentionally. Checksum is used for data integrity.
3. *Data Authentication:* It is the fundamental requirement for security in WSN. Attacks in the sensor networks do not just involve the alteration of packets; adversaries can also inject additional false packets [3]. In message authentication, receiver needs to be sure of the sender's identity as an adversary can change the entire data. So the receiver needs to be assured that whatever data used in Decision making process comes from an authorized source or not.
4. *Data Freshness:* Data freshness [4] ensures that data should be recent and no old messages have been replayed. This requirement is essential when shared key strategies are used. So there is a great need to get renew the shared keys time to time. As it takes a little bit time to propagate the shared keys over the entire network during that time adversary can perform a replay attack. To tackle the problem of the replay attack timestamp is added to the message.

V. MAJOR ATTACKS IN WSN

As most of the routing protocols for WSN are very simple, so they are more vulnerable to attacks [5]. Attacks on Network Layer protocol fall into one of the following categories:

1. *Denial of Service (DoS):* Denial of Service (DoS) [6] attack is produced by malicious nodes or users. The main intention behind this attack is that it is an attempt to make network resources unavailable to its legitimate users. As the network is flooded with huge requests by an adversary so that legitimate user cannot access the services of the network. In wireless sensor network several types of DoS attacks might be performed at different layers. At Physical Layer, DoS attack can be known as Jamming. In this, adversaries continuously transmit radio signals

TABLE 2: DENIAL OF SERVICE ATTACKS AND DEFENSES TO COMBAT AT DIFFERENT PROTOCOL LAYERS [7]

Protocol Layer	Attacks	Defenses
Physical	Jamming	Sleep
	Node Destruction	Hide nodes or tamper proof packaging
MAC (Medium Access Control)	Denial of Sleep	Sleep, authentication and anti-replay
Network	Spoofing, replaying	Authentication, anti-replay
	Hello floods	Geographic routing
	Homing	Header Encryption
Transport	SYN flood	SYN cookies
	De synchronization attack	Packet authentication
Application	Path based DoS	Authentication and anti-replay protection
	Reprogramming attacks	

as well as high energy signals so that wireless medium could be blocked. Jamming is further of two types: Constant Jamming and Intermittent Jamming. In case of Constant Jamming, there is a complete jamming of the entire network, whereas in case of intermittent jamming, sensor nodes are capable of communicating data periodically but not consistently.

1. *Selective Forwarding:* It is also a network Layer attack. In this, an adversary usually forwards some of the packets and drops rest of the packets containing vital information. This degrades the quality of service in WSN. If somehow attacker discards all the packets, then the receiver node becomes conscious that there must be some obstacle in between, so neighboring nodes decide to take another route. But to overcome this doubt adversary forwards a selective packets to the node rather than dropping all the packets.
2. *Blackhole/Sinkhole Attack:* In this attack the major intention of the malicious node (Blackhole [8]) is to attract the maximum traffic towards itself. An adversary makes assures to all the sensor nodes that it is also a compromised node and it will provide them the best quality route and even the shortest path to the base station. Then all the neighboring nodes of the adversary will start transmitting the packets to the adversary and when the whole of the traffic reaches the adversary, it can do anything with that information. Even it can perform selective forwarding attack i.e., to drop the crucial data and forwards the rest of the irrelevant packets to the base station.
3. Sensor networks are much more prone to sinkhole attacks as they have the common destination and a compromised node needs only to assure that it will provide high quality routes to the base station just to attract the maximum traffic towards itself.
4. *Hello Attack:* In this attack, malicious node having high radio transmission range broadcasts HELLO message to the neighboring sensor nodes to make them assure that it is also a legitimate node as well as it will provide shortest route to the base station. As a result, while sending the packets to the base station sensors nodes packets pass through the malicious node because it has made them an illusion that it is their legitimate neighboring node and hence get all the relevant data and attack the sensor network.
5. *Sybil Attack:* This type of attack mainly occurs in peer to peer network and detection of it is very difficult. We define Sybil attack as a malicious node which forges the false identity of many legitimate nodes [9], [10]. Whenever there is a communication between the two legitimate nodes adversary node occurs in between the interaction and proves the sender node that it is the one that the sender wants to exchange the data with by using the identity of receiver node. Adversary node takes all the information and hence can use selective forwarding, degrading of the data, etc. Newsome *et al.* [10] used radio resource testing to detect the presence of Sybil node in the sensor network and showed the probability to detect the existence of Sybil attack.
6. *Wormhole Attack:* Wormhole [11] is a critical attack in which attacker connects two distant points in the network using a low latency communication link called wormhole link [12]. Once the link is established the adversary records the packet at one location in the network and replays them at the other end. This type of attack is a significant threat to the sensor network as it could even be performed at the initial phase when sensors discover their neighboring information.

VI. Conclusion

Wireless Sensor Networks would be widely deployed in future mission critical applications. So security related issues in wireless sensor networks have become an important part of research in present scenario. In this paper we have described various security requirements in wireless sensor networks and also emphasized on various attacks related to wireless sensor networks.

As most of the attacks against security in this network are caused by the insertion of false information by the adversary node, so there is a great need of detecting the false reports and to develop such a mechanism that detects this is a great research challenge.

References

[1] Chris Karlof and David Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” University of California, Berkeley.

[2] Abhishek Jain, Kamal Kant and M.R. Tripathy, “Security Solutions for Wireless Sensor Networks,” Amity University, India, In Second International Conference on Advanced Computing and Communication Technologies.

[3] 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.

[4] Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci,“A Survey on Sensor Networks”, IEEE Communication Magazine, year 2002.

[5] Al-Sakib Khan Pathan, Hyung-Woo Lee, and Choong Seon Hong, “Security in Wireless Sensor Network: Issues and Challenges,” *Kyung Hee University Korea*, Feb. 2006.

[6] Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M., “Analyzing interaction between distributed denial of service attacks and mitigation technologies”, Proc. DARPA Information Survivability Conference and Exposition, Volume 1, 22-24 April, 2003, pp. 26 – 36.

[7] Doddapaneni, Krishna Chaitanya and Ghosh Arindam “Analysis of DoS attack on WSN using Simulation.”

[8] Culpepper, B.J. and Tseng, H.C., “Sinkhole intrusion indicators in DSR MANETs”, Proc. First International Conference on Broad band Networks, 2004, pp. 681 – 688.

[9] Douceur, J. “The Sybil Attack”, 1st International Workshop on Peer-to-Peer Systems (2002).

[10] Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensor networks: analysis & defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004,pp. 259 – 268.

[11] Hu, Y.-C., Perrig, A., and Johnson, D.B., "Packet leashes: a defense against wormhole attacks in wireless networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies.IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 – 1986.

[12] Ritesh Maheshwari, Jie Gao, Samir R Das, "Detecting Wormhole Attacks in Wireless Sensor Networks using Connectivity Information," In IEEE INFOCOM 2007, Alaska.

[13] Mohammad Sadeghi, Farshad Khosravi, Kayvan Atefi and Mehdi Barati, "Security Analysis of Routing Protocols in WSN," Jan. 2012.