Volume: 07 Issue: 05 Pages: 2887-2892 (2016) ISSN: 0975-0290

Review of Security Issues in Mobile Wireless Sensor Networks

Aarti Singh[1]
Associate Professor, Maharishi Markandeshwar University, Mullana
Email: singh2208@gmail.com
Kavita Gupta[2]
Research Scholar, Maharishi Markandeshwar University, Mullana
Email: kavita_mittal25@yahoo.co.in

ABSTRACT

MWSNs are finding applicability in wide range of applications. Applications spread from day to day utilities to military and surveillance, where they may sense information about vehicular movements around border. Considering the importance of data being sent by these nodes, threat of compromising them has also increased. This paper aims to explore various types of attacks and tries to classify them based on some common parameter. Better understanding of various attacks, their style of functioning and point of penetration can help researchers devise better preventive measures.

Keywords: **Attacker, MWSN, security attacks, security prerequisites**

Date of submission: March 02, 2016 Date of Acceptance: March 28, 2016

1. Introduction

Mobile Wireless Sensor Network is a collection of tiny sensor nodes having mobile nature [1]. These sensor nodes have limited amount of memory and limited energy source associated with them. Being cheap and easily deployable they are finding utility in military applications and also surveillance in public sectors. Sensors can sense and report change is values of various parameters such as temperature, pressure, vehicular movement and presence or absence of light or some other objects. They are generally deployed in hostile environments to sense sensitive information, which can't be collected otherwise. Like other wireless adhoc networks, MWSNs are also prone to security risks, however existence of a base station makes it feasible to apply security measures in this case. Although limited computational ability associated with these mobile wireless sensor nodes makes it difficult to deploy strong security systems inside them.

MWSNs are prone to two types of attacks in terms of security, first can be attack on the communicated data which takes place through routing process and second can be attack on security mechanism being adopted. Sensor nodes sense and transmit information to base station which may be captured by some intruder in the medium and may be modified or deleted. Considering the importance of data being sensed it becomes essential to develop robust security measures for communication in MWSNs. Thus, security in sensor networks is defined as protecting sensed data from unauthorized access in order to modify or delete it before being received by the intended recipient. This paper aims to explore various dimensions of security in MWSNs such as need of security, various types of attacks possible on these networks and preventive measures existing in literature.

This paper gives the overview of various security attacks; section 2 presents need of security in MWSN, section 3 describes the threat model and its assumptions, Section 4provides overview of security attacks at various layers of routing protocols, Section 5 concludes the paper.

2. Security Prerequisites

Considering the applicability of MWSNs in sensitive applications, security of data being sensed becomes very important. Following are the reasons for having strong security in MWSNs: Figure 1. given below presents the various security perquisites.

2.1 Data Confidentiality: Confidentiality of data is the major concern in case of wireless transmission. Data encryption is the widely accepted technique for maintaining confidentiality. Data should be encrypted in such a way that it should be read or understood by intended recipients [5].

2.2 Data Integration: Data integration aims to ensure that there is no change in data being sent by the sender and contents reach unaltered and with any loss to its destination. Various methods may be applied at MAC layer for ensuring the reliability of data [5].

Volume: 07 Issue: 05 Pages: 2887-2892 (2016) ISSN: 0975-0290

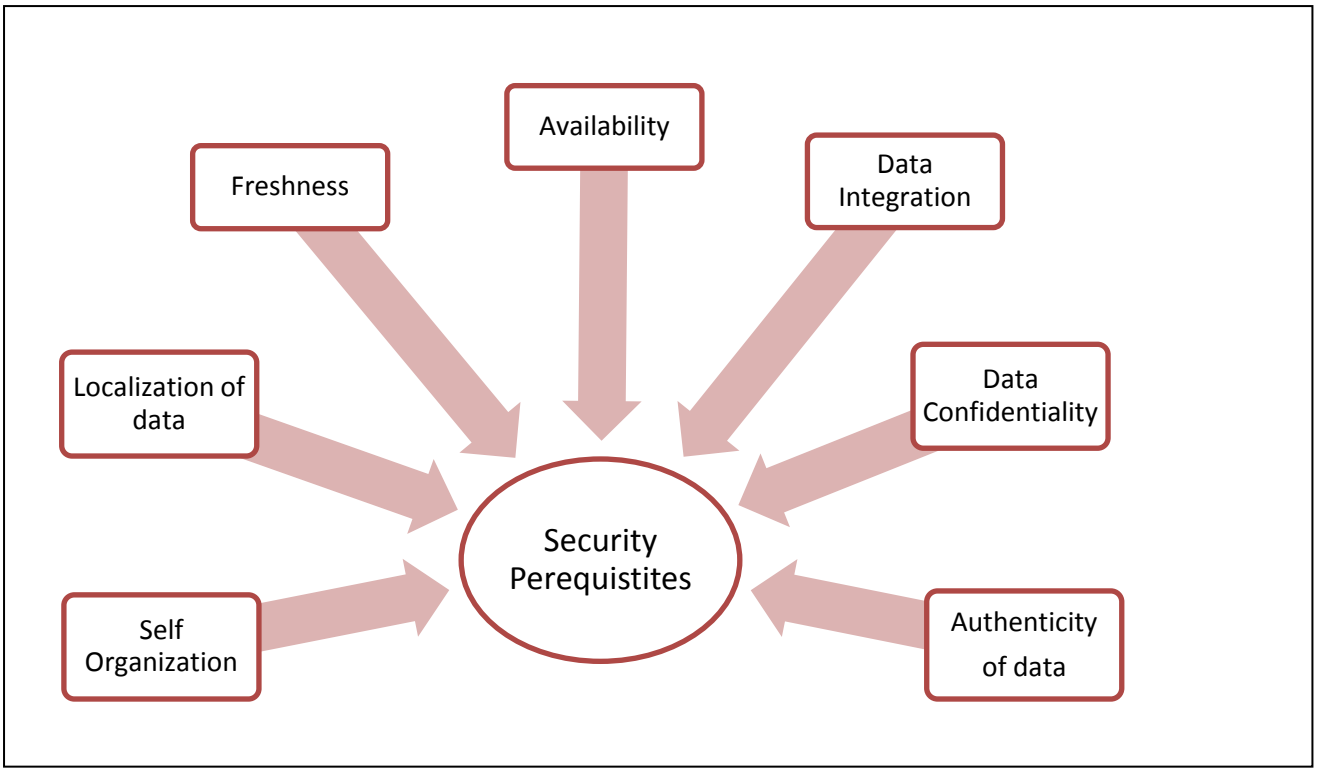

Fig. 1 Security Prerequisites

2.3 Authenticity of Nodes: Authenticity helps to ensure the receiver that information being received has originated from intended sender. Authentications in sensor networks ensure the origin of data packets and also prevent the alteration of data packets by the attackers [6].Node authentication is required in hierarchical networks where nodes are organized in form of clusters. In clustered networks nodes join the respective clusters as per their sensing capabilities or many other attributes.

2.4 Availability: Availability ensures that all the resources are available for all the nodes and network enables the transmission of data. It also ensures that all the resources can be used at any time as per requirements even if any internal or external attack is there. In the field of MWSN there exist various types of risk that can results in loss of availability of resources and they also effect the real time applications [5].

2.5 Self-Organization: As nodes in sensor network are of mobile nature, thus they may organize themselves to form a network. This self-organizing capability helps MWSNs to survive and work in hostile environments; however it raises security [18] challenges. Since dynamic change in network topology and introduction of new participants in networks dilutes security [19] measures to some extent.

2.6 Freshness: Freshness of data implies that fresh copy of data is forwarded. It also ensures that data is not copied and no duplicate data packet is there in the network that prevent the data from various types of attacks like replay attack, select & forwarding attack.

Next section elaborates the threat model for MWSNs, which covers all possible types of attacks in these networks.

3. Threat Model

Threat model classifies attacks based on location, damage level, style of attack or devices used for attack. Following is the description for these classifications.

3.1 Classification of attacks based on location of attacker

Attacker may attack the sensor nodes by entering into the network or staying out of the network. Based on its location, attacks may be classified as either insider or outsider attacks.

3.1.1 Insider or Internal attack Handling insider attack is really difficult in MWSNs. Attacker may steal the identity of other nodes and may change routes of data transmission. While inside the network, attacker may cause following harms:

- Consumes the energy of other sensor nodes: it may get energy of other nodes wasted by sending them false data requests.

Volume: 07 Issue: 05 Pages: 2887-2892 (2016) ISSN: 0975-0290

- Causes Topology change: attacker may pretend like the neighboring node for the victim and may persuade others to change their data transmission paths.

- Accessing of nodes is easy [8,9]: being inside the network it is really easy for the attacker to pretend like a participating node or more than one participating nodes. It may easily access data transfers taking place and may behave like sink node to get all data directed to it.

3.1.2 Outsider or External attack

In outsider attack, attacker may be sitting anywhere outside the MWSN. It is also a major threat since it is difficult to locate the attacker, while it may keep on damaging the network [8,9,10].

3.2 Classification of attacks based on damage level

This classification focuses attacks based on the extent of damage caused by them to the network and extent of penetration in the network. On this basis attacks can be categorized as active and passive attacks:

3.2.1 Active Attacks

The attacks which perform some type of operation in the network such as

- Faulty data intrusion
- Packet Modification
- Radio frequency Overlapping
- Data alteration

3.2.2 Passive Attacks

This type of attack includes the following

- Attacker looks like a normal node
- Access the encrypted information
- Degrade the network performance
- Avoids cooperation

3.3 Classification of attacks based on their functionality

Based on their functionality attacks may be classified into three types, attacks on secrecy of data, attacks on availability of nodes, attacks on the network:

3.3.1 Attacks on secrecy of data

- Packet spoofing,
- Eavesdropping
- False Data Intrusion

3.3.2 Attack on availability of nodes

Denial of service attacks [15,16] fall in this category which degrades the network's performance and disrupts the mobile wireless sensor network's services.

3.3.3 Attack on the network

These type of attacks affect the routing communication channel and partially degrades the mobile wireless sensor network's services and functionality.

3.4 Classification of attacks based on attacking device

Different types of devices are used by attackers for degrading the MWSNs performance and these devices have different types of radio antenna, power source and performance capabilities. Based on type of devices used, attacks are of two types:

3.4.1 Mote Class Attacker

In this type of attack, attacker use internal nodes for attacking the network and these nodes may or may not have properties as that of ordinary sensor nodes. [11,12].

3.4.2 Laptop Class Attacker

In this type of attack, attacker use external powerful source for attacking. That external source can be a laptop or any other communication device. It can disturb or even corrupt the entire network and also affects the radio frequency and bandwidth of communication channel.

Not only there are various types of attacks, but also the attacks focus on different layer of communication protocols for their propagation. Next section summarizes attacks on different layers of communication protocols.

4. Security Attacks at Various Layers of Routing Protocol

Sensor network architecture usually adopts OSI reference model for communication. But out of seven layer following five layers are used by sensor network [20].

4.1 Attacks at Physical Layer

At physical layer, encryption of transmitted data takes place. Thus attacks working on this layer focus on unauthorized decryption of data or try to damage it. Some such attacks are described below

Data Integrity& Confidentiality

Data is transferred in the form of bits and fixed no of bits are integrated to form data packet. These attacks access the encrypted information and may degrade the network performance.

4.1.1 Eavesdropping attack

In this process an attacker may gather the information from network in unauthorized way i.e. secretly snooping the information and encrypted data such as node ids and password information for further use.

4.1.2 Jamming

In this attack multiple data packets are sent over the same frequency range to exhaust the frequency. It may also reduce the inter arrival time between the data packets to flood the recipients. Such attacks will lead to

Volume: 07 Issue: 05 Pages: 2887-2892 (2016) ISSN: 0975-0290

confusion in data packets and wastage of resources of sensor nodes.

4.1.3 Tampering

Physical access of node by attacker is known as tampering. By tempering a node attacker can extract the cryptographic key or other data from the node.

4.2 Attacks at Data Link layer Attack

4.2.1 Collision Attack

In this attack multiple data packets are transmitted over the same frequency that can cause change in data within packets and checksum error at receiving end [5]. This attack occurs due to environmental effects and due to probabilistic collision.

4.2.2 Unfairness

In this attack data is not equally distributed among all data frames i.e. data packets doesn't contain same no of bits, leading to non-cooperation among sensor nodes.

4.3 Attacks at Network Layer

4.3.1 Replay Attack

In this attack data packets are retransmitted either by source or by intruder [17] on the route. There intruder/attacker captures a data packet and resend it to destination or to host in repeated manner so as to waste its resources like energy and buffer capacity.

4.3.2 Select & Forwarding Attack

In this attack some data packets are stopped in between and few of data packets are forwarded to base station. This may cause the loss of data packets and reduce the efficiency of the network.

4.3.3 Spoofing Attack

In this attack, attacker creates the routing loops and gives wrong routing information.

4.3.4 Wormhole Attack

In this attack, attacker collects all packets at one point and then start sending the copy of same packet with high speed so that duplicate packets may reach to destination before the original packets and drains the energy of sink node unnecessarily [7].

4.4 Attacks at Transport Layer

4.4.1 Flooding Attack

In this attack attacker send large number of data packets over the network towards base station or to access point to increase confusion at receiving end. Wrong routing information is also floated by the attacker.

4.4.2 De-Synchronization

In this attack attacker affects the end to end delivery of data packets by flashing a forges message between terminals.

4.4.3 Sybil Attack

In this attack a node claims multiple identities under the influence of attacker and that results in miscommunication about address of node. Thus packets meant for some other node are delivered to dummy node.

4.5 Attacks at Application Layer

4.5.1 Sinkhole Attack

As this attack works on the top layer of the routing protocol [12], in this attack, attacker placed itself in between data packets and base station, attract all the data packets traffic towards it. Attacker gives the perception that it is the shortest route for data transmission and in turn may corrupt the data packets.

Volume: 07 Issue: 05 Pages: 2887-2892 (2016) ISSN: 0975-0290

Table 1 given below provides summery of various attacks at each layer of communication protocol along with their possible effects.

Table 1 Attack at Various Layers of Communication Protocol

Layer	Attack	Effects of attack
Physical Layer	• Denial of Service(DoS) • Jamming • Tampering • Data Integration • Data Confidentiality	• False Data Intrusion • Change of Data in Packets • Multiple data packets sent on same radio frequency create congestion
Data Link Layer	• Collision attack • Unfairness	• Data loss • Data may be delivered at wrong address
Network Layer	• Replay Attack • Select & Forwarding • Wormhole Attack • Spoofing Attack	• Increased Network traffic • Looping in rou1111ting can increase time of packet delivery • Duplication of data packets • Wrong routing information
Transport Layer	• De synchronization Attack • Flooding Attack • Sybil Attack	• Data delivery is not reliable • Destination may have multiple copy of data • Creates Confusion on routing path
Application Layer	• Sinkhole Attack	• Unreliable communication

5 Conclusion

Security is crucial for MWSNs. Since these networks operate in hostile unattended environments they are easy targets for intruders. Deployment of these networks in hostile environments is due to importance of data available there. Thus security of sensor nodes and sensor networks becomes essential for maintaining the integrity of information captured through them. This work has explored various types of attacks possible for MWSNs along with essentials of security mechanisms. Mobility feature in sensor nodes further increases security threats and requires still better mechanisms to be developed for these networks. Future work aims to present a security mechanism for MWSNs.

References

[1] Javad Rezazadeh, MarjanMoradi, Abdul Samad Ismail, Mobile Wireless Sensor Networks Overview, Published in *International Journal of Computer Communications and Networks, Vol. 2*, issue 1, 2012, pp.17-22.

[2] Kavita Gupta, Aarti Singh, Saurabh Mukherjee, An Improved Cluster Head Selection Algorithm for Mobile Wireless Sensor Network, Published in *JNCET, Volume 5*, Special Issue 2, December 2015.

[3] Dimple Juneja, Kavita Gupta, Aarti Singh, Exploiting Mobility of Mobile Agents for data aggregation and result sharing in Mobile Wireless Sensor Networks, Published in *JNCET, Volume 5*, Special Issue 2, December 2015.

[4] Dimple Juneja, Aartisingh, Kavita Gupta, Reassessing Mobile Wireless Sensor Networks, Published *in International Journal of Computing Academic Research, Volume 4*, Number 1,February 2015, pp. 12-18.

[5] Mohammad Masdari, Sadegh Mohammadzadeh Bazarchi, Moazam Bidaki, Analysis of SecureLEACH-Based Clustering Protocols in Wireless Sensor Networks, *Published in journal of network and computer application, Elsevier*, 2013,pp. 1243-1260.

[6] F. Akyildiz et al., A Survey on Sensor Networks, *IEEE Comm. Mag., vol. 40*, no. 8, Aug. 2002, pp. 102–114.

[7] M. Saxena, Security in Wireless Sensor Networks: A Layer-Based Classification, 2011. https://www.cerias.purdue.edu/apps/reports_and_papers/view/3106/

[8] A. Dimitrievski, V. Pejovska and D. Davcev, Security Issues and Approaches in WSN, 2011.

[9] K. Sharma and M. K. Ghose, Wireless Sensor Networks: An Overview on Its Security Threats, *International Journal of Computers and Their Applications, Special Issue on*

Volume: 07 Issue: 05 Pages: 2887-2892 (2016) ISSN: 0975-0290

"Mobile Ad-hoc Networks", *Vol. 1*, 2010, pp. 42-45.

[10] A. Dimitrievski, V. Pejovska and D. Davcev, Security Issues and Approaches in WSN, 2011.

[11] J. Yick, B. Mukherjee and D. Ghosal, Wireless Sensor Network Survey, *Computer Networks*, *Vol. 52*, No. 12, 2008, pp. 2292-2330.

[12] K.Venkatraman, J.Vijay Daniel, G.Murugaboopathi, Various Attacks Wireless Sensor Network: Survey, Published in *International Journal of Soft Computing and Engineering (IJSCE), Vol-3*, Issue-1, March 2013.

[13] Walters P.J. and Liang Z., Wireless Sensor Network Security: A Survey. Published in Book titled '*Security in Distributed, Grid and Pervasive Computing'*, Published by CRC Press, USA, April 2007, pp. 367.

[14] Pathan K. Al-Sakib, Lee W. H. and Hone S. C., Security in Wireless Sensor Networks: Issues and Challenges, Published in *IEEE Eighth International Advanced Communication Technology Conference (ICACT 2006),* pp. 1043-1048, February 2006.

[15] Singh A. and Juneja D., Agent Based Preventive Measure for UDP Flood Attack in DDoS Attacks, Published in *International Journal of Engineering Science & Technology, Vol. 2* , Issue 8, August 2010, pp. 3405-3411.

[16] Juneja D., Bedi R. and Singh A., An Agent Based Framework to counterattack DDoS Attacks, Published in *International Journal of Wireless Networks and Communications (IJWNC), Volume 1*, No. 2 , pp. 193-200, 2009.

[17] Singh A. and Sharma G., Intrusion Detection using Neural Network techniques, *International Journal of IT & Knowledge Management, Volume I,* June-2008, pp 79-84.

[18] Singh A. and Ahuja P., Robust Algorithm for Securing an Agent Hosting Platform. Published in *International Journal of Advancements in Technology, Vol. 3*, Issue 2, pp.84-91, April 2012.

[19] Singh A. and Malhotra M., Security Concerns at Various Levels of Cloud Computing Paradigm: A Review, Published in *International Journal of Computer Networks and Applications , Volume 2*, Issue 2, March – April (2015), pp. 41-45.

[20] Alkhatib A, Baicher G. S., Wireless Sensor Network Architecture, Published in *IPCSIT, Vol. 35*, 2012, pp. 11-15.