An overview of Wireless Sensor Network Attacks and Security Technologies

B. Tamilarasi[1]
[1] Research Scholar (RM12CS44),
[1] SCSVMV University, Kanchipuram

Abstract- *Wireless sensor network (WSN) is a special type of wireless network for several industrial and quotidian applications to monitor physical or environmental conditions in real time. The development of wireless sensor network is motivated by military applications for battlefield surveillance. WSN consists of nodes from a few to several hundreds or even thousands, where each node communicates wirelessly to a central gateway, which provides connection to the wired and wireless world where the WSN date can be accessed by different types of external networks like internet, cellular networks or satellite. Wireless Sensor Network is affected by a number of network layer attacks. In this paper, we consider different types of network attacks and routing security in wireless sensor networks. The routing protocols of sensor networks are not designed with security, but security is important factor in the concept of wireless sensor networks.*

Keywords- attack, Routing, sink, security, Wireless Sensor Networks.

I. INTRODUCTION

Wireless sensor networks are usually deployed in unattended or hostile environment for gathering data. WSN networks handle low cost and small size devices in large number for data gathering purpose. Small size implies small battery, low cost and low power CPU, radio with minimum bandwidth and range [1], [2]. So, the development and deployment cost of WSN has fallen greatly and the applications of wireless sensor network are expanded from the military/surveillance areas to industrial and commercial fields [3], [4], [5]. Data gathering protocols and routing protocols are designed for configuring the wireless sensor network and collecting information from WSN sensors. Using these different protocols, data can be collected from sensors and transmitted to gateway where from the end user can access the data. But these protocols have not been designed with proper security capabilities. WSN uses traditional security methods, based on characteristic of node and application environment, but they are not sufficient for the special requirements of trust, security and privacy which are most essential things in data communication. So, it is the important task of WSN developers to secure the system and makes the system reliable from malicious attacks which can lead to malfunctioning systems and information data leakage. In this paper, we have analyzed possible attacks that arise on WSN in general as well as the security schemes of the entire major sensor network routing protocols.

II. OVERVIEW OF SECURITY ISSUES

Sensor networks routing protocols are usually not designed with security schemes, yet security techniques are difficult to add later on. If attackers or adversaries disrupt or interfere with routing of sensor data; the wireless sensor network becomes useless. This leads to need for the implementation of security schemes in wireless sensor networks.

1. Attack and Attacker

An attack can be defined as an unauthorized access to a resource or information or service of a particular system owned by private or public sectors. In the case of networking concept, attacks are caused by attackers, or the adversaries. The attacker eavesdrop data packets from the sensors of sensor networks using the weakness of the system security design, implementation, configuration. Any circumstance with the potential to adversely impact a system through a security breach and causing harm to a system.

2. Security Requirements

The security requirements of a wireless sensor network can be classified as follows:

- **Authentication:** As WSN nodes transmit sensitive data to the receiver, the receiver needs to ensure that the data originates from the correct source. So, authentication is necessary during exchange of sensitive information among the nodes of network.
- **Integrity:** Due to network attacks, data can be changed by the network attackers or adversaries. Data integrity is to ensure that the data is not changed or altered by malicious node or adversaries.

- **Data Confidentiality:** Data Confidentiality refers to maintaining data in secret manner. Encryption and key distribution are used rely on confidentiality.
- **Location Security:** In sensor network, all the information related to the location of the sensor nodes is important and it must be accurate. Attackers can easily attack the sensor nodes deployed in non secured location.

III. ROUTING ATTACKS OF WSN

Attacks on networks can be classified into four types.

- Interruption
- Modification
- Fabrication
- Interception

IV. NETWORK LAYER ATTACKS

Routing protocols designed for wireless sensor networks are very simple. So, network layer attacks are possible in general ad-hoc routing protocols implemented in wireless sensor networks [6]. Sensor networks are affected by different types of network layer attacks which are described below:

1. Spoofed, altered, or replayed routing information

This is the common attack against networks routing protocol. In this type of attack, the actual route between the real sensor nodes is partitioned by adversary node and new path is created among actual sensor nodes and adversary node. Adversaries may be able to create new routing loops between the source sensor nodes, change the network traffic, extend or shorten actual routes, partition the network, and inject false error message into the sensor nodes and increase end-to-end latency.

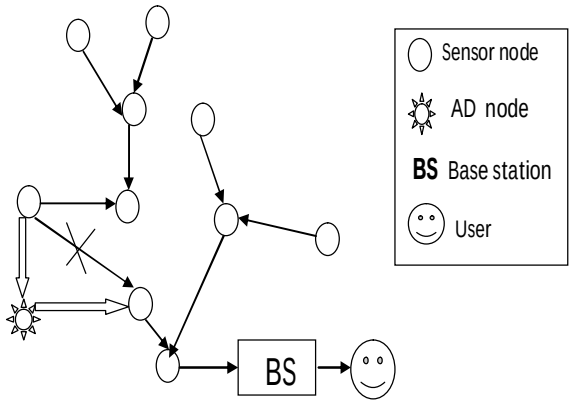

Figure 1. Spoofed, altered, or replayed routing information

2. Selective forwarding attack

Routing protocols of wireless sensor network are designed to follow multi-hop mode of communication. By using multi-hop communication technique, deployed sensor nodes of wireless sensor network senses the environmental data and forward the sensed data to the nearby sensor nodes and at the same time it also receives the sensed data from other sensor nodes. In the case of selective forwarding attack, the false adversary node takes a place between any two original nodes of wireless sensor network. This newly placed false adversary node act as original node and receives all the data packets from a sensor node, but forwards only a few packets to the next adjacent sensor node by dropping the remaining packets. Now, this adjacent node sends the few received packets from the adversary nodes to the next node or the base station. Because of this reason, the base station cannot receive all the data packets sent by sensor nodes and it is difficult for the base station to detect missing of packets [7], [8]. For this problem, the packet sequence numbers must be added in packet header, when the packets are forwarded from one sensor node to other. Using the packet sequence numbers, the base station can detect the missing number of packets and the inclusion of adversary node.

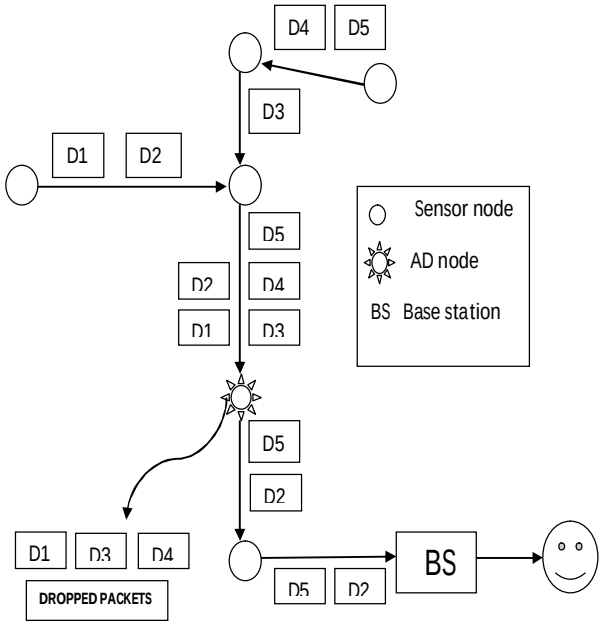

Figure 2. Selective forwarding attack

3. 3.Sinkhole attack

In sinkhole attack, the attacker selects a central area where most of the sensor data are accumulated. In that central area, the attacker creates a malicious compromised node called sinkhole. Using this compromised node, the attacker attracts most of the traffic close to the base station so that the

malicious node could be perceived as a base station. By performing this routing process, the attacker launches severe attacks like selective forwarding, modifying the original packets, dropping some packets [9]. To reduce this attack, the neighboring nodes must establish unique key identification before initializing multi-hop communication.

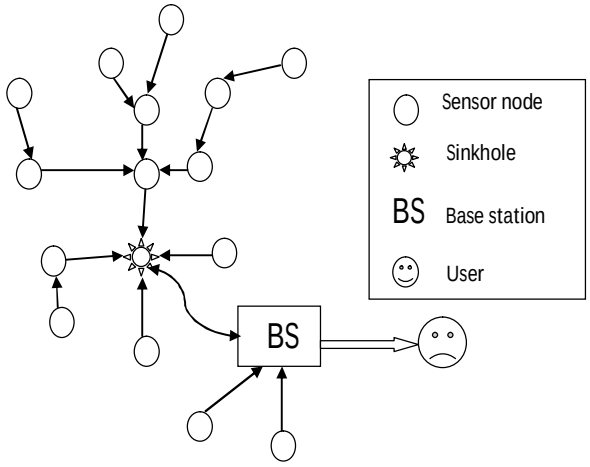

Figure 3. Sinkhole attack

4. Sybil attack

Sybil attack is defined as a "malicious node illegitimately taking on multiple identities". Using the Sybil attack, an adversary can "be in more than one place at once" as a single node presents multiple identities to other nodes in the network which can significantly reduce the effectiveness of fault tolerant schemes such as distributed storage, dispersity [10] and multipath. It may be extremely difficult for an adversary to launch such an attack in a network where every pair of neighboring nodes uses a unique key to initialize frequency hopping or spread spectrum communication. Sybil attacks also pose a significant threat to geographic routing protocols. In a Sybil attack, an attacker can appear to be in multiple places at the same time. This can be convincing by creating fake identities of nodes located at the edge of communication range. Multiple identities can be occupied within the sensor network either by fabricating or stealing the identities of legitimate nodes. Sybil attacks can pose a significant threat to geographic routing protocols. Location aware routing often requires nodes to exchange coordinate information with their neighbors to construct the network. So it expects nodes to be present with a single set of coordinates, but by using the Sybil attack an adversary can ‘‘be in more than one place at once’’. Since identity fraud leads to the Sybil attack, proper authentication can defend it.

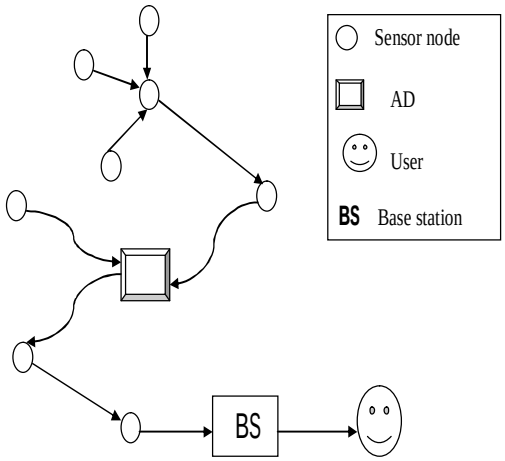

Figure 4. Sybil attack

5. Wormhole attack

To launch a wormhole attack, an adversary establishes a direct link referred as wormhole link between any two sensor node points in the network. A direct link can be established via a wired line, a long-range wireless transmission, or an optical link. Once the wormhole link is operational, the adversary eavesdrop messages at one end, referred as the origin point, tunnels them through the wormhole link and replays them in a timely fashion at the other end, referred as the destination point. In the wormhole model, it is assumed that the adversary does not compromise the integrity and authenticity of the communication, and any cryptographic quantity remains secret. When wormhole attack happens in sensor networks, the sensor nodes get wrong information about their neighbors [11]. We must use probabilistic techniques for dealing with wormhole.

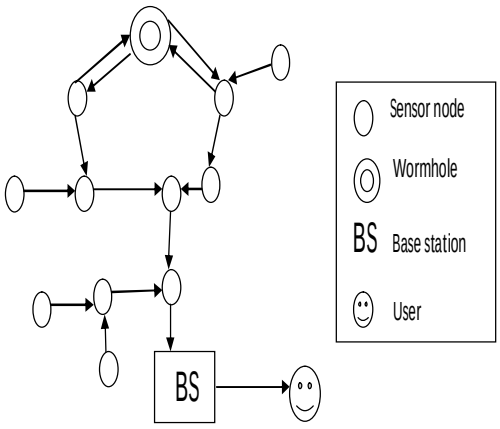

Figure 5. Wormhole attack

6. HELLO flood attack

Many protocols require nodes to broadcast HELLO packets for neighbor’s discovery, and a node receiving such a packet may assume that it is within (normal) radio range of the

sender. A laptop-class attacker with large transmission power could actuate every node in the network that the adversary is its neighbor, so that all the nodes of the sensor network will respond to the HELLO message and waste their energy. Hence the sensor nodes are left in the situation of confusion state [12], [13]. Hello flood attack can be prevented by cryptographic techniques and signal strength based mechanisms.

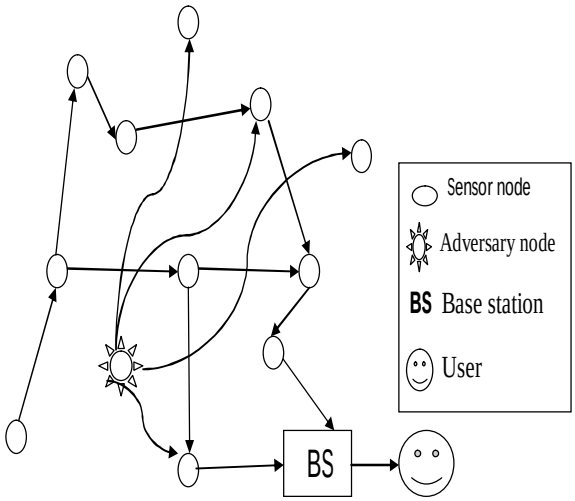

Figure 6. HELLO flood attack

7. Acknowledgement spoofing

Several sensor network routing algorithms acknowledgements, due to the inherent broadcast medium, an adversary can spoof link layer acknowledgments for "overheard" packets addressed to neighboring nodes. Protocols that choose the next hop based on reliability issues are susceptible to acknowledgments spoofing. This results in packets being lost when traveling along such links. The goal includes convincing the sender that a weak link is strong or that a dead or disabled node is alive. Since packets sent along weak or dead links are lost, an adversary can effectively mount a selective forwarding attack using acknowledgement spoofing by encouraging the target node to transmit packets on those links. Acknowledgement spoofing attacks can be prevented by using good encryption techniques and proper authentication for communication.

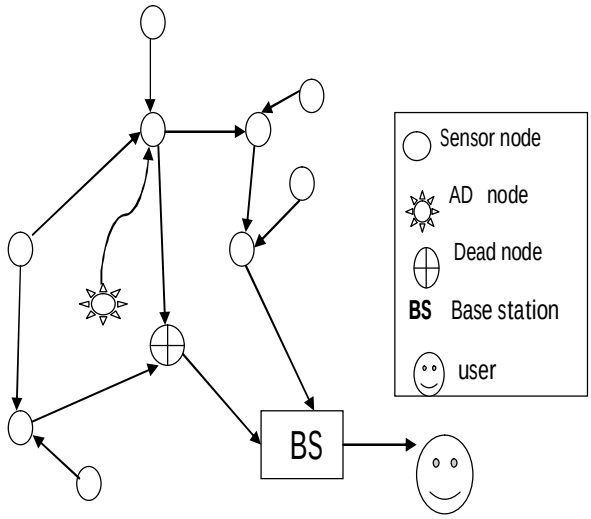

Figure 7. Acknowledgement spoofing

8. IP spoofing

IP spoofing is the method of attack used by network attackers to gain unauthorized access to a computer. In IP spoofing, the network attacker sends messages to a distant computer indicating that the message has come from a trusted system. After getting successful connection with that distant system, the attacker determines the IP address of a trusted system. Using this forged IP address of the trusted system, the attacker forwards duplicate packets to all other members of the trusted system.

V. CONCLUSION

This paper outlined different security issues in wireless sensor network in general and made an extensive study of different threats associated with routing protocols. Secure routing protocols should guarantee the integrity, authenticity, and availability of messages in the presence of adversaries of arbitrary power. As these protocols are not designed taking security issues into account, most of them are prone to different types of attacks. Even some of the protocols are seems to be vulnerable to most of the attacks. Similarly some attacks like HELLO flood, Acknowledgement spoofing and sniffing can be used by the adversaries to affect most of the protocols. Link layer encryption and authentication mechanisms may be a reasonable first approximation for defense against mote-class outsiders, but cryptography is not enough to defend against laptop-class adversaries and insiders: careful protocol design is needed for wireless sensor networks.

REFERENCES

[1] Ian F. Akyildiz, Weilian Su, Yogesh Sankaraubramaniam, and Erdal Cayirci: " A Survey on

sensor networks", IEEE Communications Magazine (2002).

[2] Buratti, C., Dardari, D., Verdone, R., and Conti, A.," An Overview on Wireless Sensor Networks Technology and Evolution. Sensors", vol, 9: p., 6869-6896, 2009.

[3] Chien-Chung hen,Chavalit Srisathapornphat,Chaiporn Jaikaeo:" Sensor Information Networking Architecture and Applications, IEEE Personal Communications", pp.52-59(August 2001).

[4] Al-Karaki,J.N,Al-Mashagbeh: "Energy-CentricRouting in Wireless Sensor Networks Computers and Communications", ISCC 06 Proceedings, 11th IEEE Symposium (2006).

[5] Mohd Fauzi Othmana , Khairunnisa Shazalib , "Wireless Sensor Network Applications: A Study in Environment Monitoring System", International S symposium on Robotics and Intelligent Sensors 2012 (IR IS 2012).

[6] Sachin LalarȦ, "Security in Wireless Sensor Networks: Issues and Security Mechanisms", International Journal of Current Engineering and Technology E-ISSN 2277 – 4106, P-ISSN 2347 – 5161, February 2014, Vol.4, No.1.

[7] H. Sun, C. Chen and Y. Hsiao, "An efficient countermeasure to the selective forwarding attack in wireless sensor networks," in Proc. Of IEEE TENCON 2007, Oct.2007, pp. 1-4.

[8] Youngho Cho and Gang Qu, "Detection and Prevention of Selective Forwarding-Based Denial-of-Service Attacks in WSNs", Hindawi, Publishing Corporation International Journal of Distributed Sensor Networks", Volume 2013, Article ID 205920.

[9] D. Dallas, C. Leckie, and K. Ramamohanarao, "Hop-count monitoring: Detecting sinkhole attacks in wireless sensor networks," in ICON '07: Proceedings of the 15th IEEE International Conference on Networks, Adelaide, SA, 2007, pp. 176–181.

[10] Kuan Zhang, and Rongxing Lu,"Sybil Attacks and Their Defenses in the Internet of Things", IEEE internet of things journal, vol. 1, no. 5, October 2014.

[11] Dhara Buch and Devesh Jinwala,"Prevention of wormhole attack in Wireless sensor network", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011.

[12] Virendra Pal Singh, Sweta Jain and Jyoti Singhai, "Hello Flood Attack and its Countermeasures in Wireless Sensor Networks",IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, May 2010.

[13] Virendra Pal Singh, Aishwarya S., Anand Ukey andSweta Jain, "Signal Strength based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887) Volume 62– No.15, January 2013.