Review of different Attacks in Wireless Sensor Networks with Defense Techniques to handle attacks

Mr. Jaswinder Singh
Assistant Professor,
Dept. of Computer Applications,
Chandigarh Group of Colleges,
Landran,Mohali, India,
mca.jaswinder@gmail.com

Mr. Deepak Rattan
Assistant Professor,
Dept. of Computer Applications,
Chandigarh Group of Colleges,
Landran, Mohali, India,
mca.deepakrattan@gmail.com

Abstract
Wireless Sensor network is emerging research area composed of sensor nodes which is connected wirelessly with each other generally to sense the unfriendly, harsh environment. As these types of networks are generally deployed in unfriendly environment so there can be a number of security issues on different layers of these networks. In this paper we are going to discuss a wide range of network layer attacks and there defense techniques.
Keywords-Wireless Sensor Network, Security Objective, Network Layer Attacks, Defense techniques.

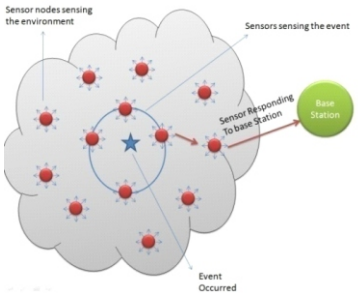
Introduction

Wireless Sensor network are composed of tiny sensor nodes connected with each other to sense the unfriendly environment. These nodes are running on limited battery power; have less memory and limited processing capabilities. These nodes sense a particular area on the basis of some parameters like pressure, temperature, sound etc and when a specific event occurs with high threshold value of required parameter (parameters are application dependent), the sensor node responds back to base station, as illustrated in Fig. I. A Single Sensor node has following **components:**

- Sensors
- Communication Device
- Processors
- Power Supply

Memory

Fig. I Wireless Sensor Network



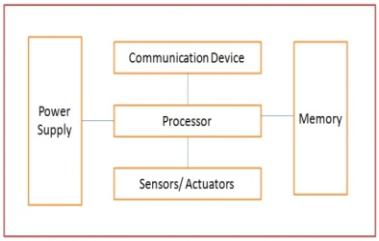


Fig. II Components of a Sensor Node

- **Sensor:** Sensor is an actual device which senses and records the physical parameters of the environment and responds back to base station.

- **Communication Device:** A device used for sending and receiving information over a wireless network.

- **Processors:** A Controller to process all the relevant data capable of executing arbitrary code.
- **Power Supply**: Batteries are used as a source of power supply in WSN.

- **Memory:** A Limited memory is used to store program and intermediate data.

The aim of this paper is to define various attacks on network layer in WSN, defense strategies and techniques, issues related to implementing those techniques. Section 2 of this paper provides information about the security objectives in Wireless Sensor Networks, Whereas Section 3 relates to different attacks on network layer in WSN, Section 4 discusses about the various defense techniques to secure the network followed by the conclusion section.

Security Objectives

Data Confidentiality

Data Confidentiality refers to protect the data so that it remains confidential within the network and is not revealed to unauthorized users.

Data Authentication

Identifying the identity of the sender or receiver is main concern in any network, Data flowing in the network may possibly altered by any malicious node which may leads to false conclusion in such area where data is utmost important. Secret key is used to compute message authentication code between sender and receiver to provide authentication.

Integrity

Data should not be tampered during transmission; Data received by the receiver should be in the form as is send by the sender node.

Availability
Data should be available to the user when it is required; Attacker can attack in different ways to threat availability by generating the radio inferences or by depleting the nodes.

Freshness
Data freshness refers that no old message should be replayed by attacker. Time based counter methods are generally used to avoid old message from being replayed.

Network Layer Attacks in WSN
Wireless Sensor networks are open to various security attacks due to the broadcast nature of the transmission medium; nodes are generally deployed in an unfriendly or dangerous environment where node capturing attacks can be one possibility. Basically attacks are classified as active attacks and passive attacks. In Active attacks, attacker temper with the data, May injects the fake data in the networks whereas in passive attack the attacker silently monitors the networks and steals the important information from the networks.

Attackers target on the different layers of network protocol in WSN, From Physical layer to application layer, In Physical Layer Node Capturing attack, Jamming attacks are the common ones whereas in Data Link Layer Attacks like Collision, Exhaustion and other similar attacks are generally used. Routing based attacks are used on network layer; attacks like Flooding, De-synchronization are used on Transport Layer.

In this paper we focus on different network Layer attacks:

a) Altered and replayed routing information

In this attack the attacker can alter the routing information shared between nodes, by doing so attacker is able to control the network traffic, can attract or repel the network traffic, can partition the network, generate false error messages etc.

b) Selective Forwarding

In Multi hop networks message will travel though multiple nodes before reaching the destination, it is assumed that intermediate nodes will faithfully forward the received messages. In this selective forwarding attack malicious node may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further.

c) Sinkhole Attack

In sinkhole attack the malicious node looks attractive to surrounding nodes, as malicious node advertises to have the extremely optimum and high quality route to the base station. Adversary's goal is to attract nearly all the traffic from a particular area. Some protocols may try to check the

quality of the route by end-to-end acknowledgements, but a malicious node uses either wormhole attack or laptop class adversary to ensure high quality route. Once all the nodes in a particular area start sending the traffic to the malicious node, it creates a metaphorical sinkhole with the malicious node at the center.

d) Sybil Attacks

In a Sybil attack, a single node presents multiple identities to other nodes in the network. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network.

e) Wormholes Attacks

Attacker in wormhole attack tunnels messages at one location and retransmits them on another location.

f) HELLO flood attacks

In many protocols node sends HELLO message to announce itself as neighboring node. An attacker sends a routing protocol's HELLO packets from one node to another. This malicious node by using high radio transmission range will convince the other nodes that adversary is their neighbor. The victim nodes then start transmitting the data to base station through attacker.

Defense Techniques

Defense Mechanism for Selective Forwarding

Distributed detection scheme that uses multi hop acknowledgements

In this approach Yu and Xiao [1] suggested a distributed detection scheme that uses multi hop acknowledgements of intermediary nodes to trigger alarms in the network. Their emphasis of the solution is on selective forwarding attack in which detection occurs in both the base station and source nodes. In this scheme, each intermediary node along the forwarding path is in charge of detecting malicious nodes. If an intermediate node detects the misbehavior of its downstream (upstream) nodes, it will generate an alarm packet and deliver it to the source node (the base station) through multiple hops.

A Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks

This is approach presented in [2] trace maliciously packet-dropping nodes using Neighbor Watch System (NWS). This scheme uses a single-path data forwarding, which consumes less power than multi-path forwarding. Single-path is used to send the data towards base station; whereas multi-

path data forwarding is used at the location where NWS detects relaying nodes‟ misbehavior. The watch node around a malicious node can find that after receiving, the malicious node do not transmit to other nodes or transmit to a node that does not exist in its neighbor list, and then the watch node must retransmit the package.

Defense Mechanism for Sinkhole Attack
Data Consistency & Network Flow Information Approach

In this approach presented in [3] has base station involved in detecting the malicious node. The base station floods message in the network containing the id of the affected node, the affected node reply backs to the base station with a message containing their IDs, ID of the next hop and the associated cost. Based on that information, base station constructs a network flow graph and will help in detecting sink-hole.

RSSI Based Scheme
In this approach sinkhole attack is detected using Received Signal Strength Indicator (RSSI) readings of message [4]. The proposed solution needs collaboration of some Extra Monitor (EM) nodes apart from the ordinary nodes. It uses values of RSSI from four EM nodes to determine the position of all sensor nodes where the Base Station (BS) is located at origin position (0, 0). This information is used as weight from the BS in order to detect Sinkhole attack.

Monitoring node's CPU usage
In this approach presented in [5] for detecting Sinkhole attacks the consistency for CPU usage of the each sensor node is monitored. The base station calculates the difference of CPU usage of each node by monitoring and analyzing the CPU usage in fixed interval of time, after comparing the difference with a threshold, the base station is able to trace the node is malicious or legitimate.

Conclusion
The sensor nodes are vulnerable to different attacks as sensor nodes are deployed in an unattended environment. Security is the critical factor for the deployment of Wireless Sensor Networks. This paper provides the abstract view on different attacks and their classifications with an attempt to traverse through the various defense techniques used to handle the attacks. The challenges of Wireless Sensor Networks are also briefly discussed. This

References

[1] A Hamid, S Hong, (2006) Defense against Lap-top Class Attacker in Wireless Sensor Network, ICACT, 2006.

[2] B. Yu and B. Xiao, "Detecting selective forwarding attacks in wireless sensor networks," in Proc. of the 2nd International Workshop on Security in Systems and Networks, April 2006, pp. 1-8.

[3] Chanatip Tumrongwittayapak and Ruttikorn Varakulsiripunth; "Detecting Sinkhole Attacks in Wireless Sensor Networks" ICROS-SICE International Joint Conference 2009, pp. 1966-1971.

[4] Changlong Chen, Min Song, and George Hsieh; "Intrusion Detection of Sinkhole Attacks In Large-scale Wireless Sensor Networks" IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS), 2010, pp. 711-716.

[5] Edith C. H. Ngai, Jiangchuan Liu and Michael R. Lyu; "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks" IEEE International Conference on Communications, 2006, Volume 8, pp. 3383- 3389.

[6] S.-B. Lee and Y.-H. Choi, A Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks, In Proceedings of the Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks(SASN‟06), pp. 59-70, 2006.