An Attack Monitoring Framework Design for Clustered WSN using OMNet++

Abdul Rahaman Sardar  
Department of CSE  
NITMAS, West Bengal, India

Jamuna Kanta Sing  
Dept. of Computer Science & Enng  
Jadavpur University, Kolkata, India

Subir Kumar Sarkar  
Dept. of ETCE  
Jadavpur University Kolkata, India  
Email: su_sarkar@hotmail.com

Abstract – Wireless Sensor Networks (WSN) are becoming an important research paradigm because of its low cost and wide area of applications particularly in military, healthcare and environmental applications. Most of the cases Sensor nodes are also deployed in open and hostile environment which are very attractive to security threats. Therefore, some attack monitoring framework for wireless sensor network becomes essential and must be addressed in order to protect the network and its data. In this paper an attack monitoring framework for WSN using OMNet++ simulator is designed. We have also simulated the network under normal scenario i.e without any attack and also simulated the network with some transport layer DOS and Black hole attacks.

Keywords – Wireless Sensor Network, Attack Monitoring, Sensor Network Attacks

I. INTRODUCTION

WSNs are normally resource constrained. Sensor nodes are usually low-cost, low-power, small devices equipped with limited data processing capability, transmission rate, energy, and memory [1]. Due to the limitation in transmission power, the available bandwidth and the radio range of the wireless channel are also limited. WSNs are typically used for information gathering in applications like habitat monitoring, military surveillance, agriculture and environmental sensing, and health monitoring. The primary functionality of a WSN is to sense and monitor the state of the physical world.

Sensor networks are particularly vulnerable to several key types of attacks [2]. Attacks can be performed in a variety of ways, most notably as denial of service attacks, but also through traffic analysis, privacy violation, physical attacks, and so on [3,4]. In section 2 attacks in WSN is described. Section 3 described the network implementation. Simulation and result is shown in section 4. Finally we provide conclusion and future work in section 5.

II. ATTACKS IN WSN

Due to random deployment of sensor nodes in an unattended and hostile environment and also for wireless nature of communication sensor networks are susceptible to various types of attacks. Some of the common attacks are discussed below:

Denial of Service Attack: The main aim of this type of attack is to flood the network with useless traffic such that it causes sleep deprivation of sensor nodes and wastes their energy to process the useless traffic. This can be combined with other attacks such as altering of routing information in order to maximize its effect.

The Sybil attack: The Sybil attack is defined as a “malicious device illegitimately taking on multiple identities”. For instance, in a sensor network voting scheme, the Sybil attack might utilize multiple identities to generate additional “votes.” Similarly, to attack the routing protocol, the Sybil attack would rely on a malicious node taking on the identity of multiple nodes, and thus routing multiple paths through a single malicious node.

Traffic Analysis Attacks: In this type of attack, an attacker need only monitor which nodes are sending packets and follow those nodes that are sending the most packets. After that it launches various attacks such as black hole, worm-hole etc.

Node Replication Attacks: A node replication attack is quite simple: an attacker seeks to add a node to an existing sensor network by copying (replicating) the node ID of an existing sensor node. A node replicated in this fashion can be corrupted or even misrouted. This can result in a disconnected network, false sensor readings, etc.

Black holes: In this type of attack an attacker drops all packets when it passes through those malicious nodes.

Wormholes: In a wormhole attack[3], a malicious node tunnels messages between two different parts of the network via a high speed link. This can make distant nodes appear “closer” in the network. Moreover, if the attacker is appropriately positioned, it can disrupt the entire network by diverting traffic from the base station.

Selective Forwarding: In a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. A simple form of this attack is when a malicious node behaves like a black hole and refuses to forward every packet it sees.

III. NETWORK IMPLEMENTATION

In our network implementation we have consider three types of nodes:- Sensor ,Monitor and Head of nodes:-
Sensor, Monitor and Head (Base Station). A common scenario is shown in Fig. 1.

Sensor Node: Sensor node consist of sensor equipments for measuring environmental data, radio resources for transmitting data to the base station and receiving packets. Every sensor node in the network has a unique id with which each sensor node will be identified. Every sensor node has a message processing queue with limited storage length. On receiving multiple packets at a time, messages are first inserted into the queue and then processed one by one.

Monitoring Node: Each monitoring node monitors or overhears the transmission from or to the sensor nodes assigned to it. Monitoring node further reports the information to base station for making intrusion related decision. Besides this, monitoring node also delivers the routing packet to the sensor nodes under its supervision. Every monitor node has a message processing queue with limited storage length. On receiving multiple packets at a time, messages are first inserted into the queue and then processed one by one.

Head Node: It is the main node of the network which collects all the network information, make decisions related to intrusion.

Routing packets are formed only in the base station based on the information collected from the network. The packet structure is given below:

a) Source (2 byte) – Node id of the base station.
b) Destination (2 byte) – node id of that node whose routing table is stored in the packet.
c) Hop count (2 byte) – The number of nodes traversed by the packet between source and destination.
d) Payload (Variable length) – Routing table for destination node.
e) Monitor id (2 byte) – for sensor node routing packet this field indicates through which monitor the routing packet must deliver.

Monitoring Packet: The packet which the monitoring node sends to the base station consisting of monitoring information collected by overhearing the sensor nodes. The packet structure is

a) Source (2 byte) – Node id of the sensor nodes whose data is collected by the monitor node.
b) Destination (2 byte) – monitor id of the base station.
c) Hop Count (2 byte) - The number of nodes traversed by the packet between source and destination.
d) Monitor id (2 byte) – monitor id of the monitor node which has collected the data by overhearing the sensor node transmission.
e) Drop (2 byte) – amount of the dropped message by the sensor node calculated by the monitor on the basis of received and sent message count.
f) Gen (2 byte) – amount of the generated message by the sensor node calculated by the monitor on the basis of received and sent message count.

**IV. SIMULATION AND RESULT**

A simulator model based on OMNet++ [5] is designed here. First we have simulated our network with normal sensor nodes and after that we have also simulated the network with some Black hole node and transport layer DOS is also simulated by generating useless packets. The simulation scenario is shown in Fig 2. The observation at monitoring node is shown in Fig. 3.

![Network with 30 nodes, 6 Monitor and a Base Station](image)

**Network Packets:** We have used three different kind of packet structure to store and transmit information within network.

**Data Packet:** The sensor nodes collect the general sensor data and transmit them through this packet to the base station. The packet structure is as follows:

a) Source (2 byte) – Node id of the sensor which has collected the data.
b) Destination (2 byte) – It is always the node id of the base station.
c) Hop count (2 byte) – The number of nodes traversed by the packet between source and destination.
d) Payload (2 byte) – Sensor information

**Routing Packet:** It consists of the routing table for sensor and monitoring nodes in its payload field.
Fig. 3. Generated message count recorded at sensor nodes.

V. CONCLUSION AND FUTURE WORK

In this work we have developed a simulation framework for monitoring the behaviour of sensor nodes. In our future work we want to implement some intelligent intrusion detection method using this framework.

REFERENCES


http://www.omnetpp.org/.