Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 3, Issue 4; April-June, 2016, pp. 226-229

http://www.krishisanskriti.org/Publication.html

Detection of Attacks and Malicious Node in Wireless Sensor Networks

Priyanka[1] and Harish Mittal[2]

[1]Computer Science and Engineering Department, Sat Priya Group of Institutions, Rohtak, Haryana, India
[2]Sat Priya Group of Institutions, Rohtak, Haryana, India
E-mail: [1]mathur. priyanka92@gmail. com, [2]mittalberi@gmail. com

Abstract—*Wireless Sensor networks have gained worldwide attention particularly in the recent years particularly with the proliferation in Micro-Elecrtro-Mechnical system (MEMS) technology which have facilitated the development of smart sensors. These sensors are small having limited memory, limited battery and inexpensive compared to traditional sensors. Wireless sensors are inherently broadcast in nature, this makes them vulnerable to attacks. These Attacks can degrade the performance and even can defeat the purpose of deployement. Any node under attack in wireless sensor networks exhibits an anomalous behavior called the malicious behavior. So detect these behaviours becomes necessary. In this paper we perform the AODV Simulation to detect Malicious node.*

Keywords*: Wireless Sensor Network, Security, Attacks, Malicious node.*

1. INTRODUCTION

A Wireless Sensor network is a wireless network consisting autonomous devices using sensors to monitor physical or environmental conditions. A Wireless system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes. The wireless protocol you select depends upon your application requirements. WSN gain popularity due to its operating nature from few last years i. e it is used in environmental monitoring of air, water, and soil, military and also in structural monitoring. Security is the main concern of the WSNs. In Contrast to traditional wireless networks, special security and performance issues have to be carefully considered for sensor networks[1]. e. g, Due to the unattended nature of sensor networks, an attacker could launch various attacks and even compromise sensor devices without being detected. An attacker can launch a number of attacks in the wireless sensor networks, these attacks leads many anomaliesthat can be detectable and these anomalies are called as malicious node. Another concern is about energy efficiency. So, for well-performed WSNs we need robust sensor networks against attacks and if any attack succeeds then the attack should be minimized. WSNs are easily prone to more attacks than wired networks[2].

Fig. 1: WSN Components, Gateway, and Distributed Nodes

The rest of paper is structured as follows. In section II represents the Related Work of WSN. In Section III represents the proposed work. In Section IV represent Result. Section V represents conclusion.

2. RELATED WORK

According to Manisha, Gaurav Gupta[1], 2013 Wireless sensor networks are less expensive and more powerful devices called sensor nodes. This paper describes the security requirements as WSNs are easily prone to more Attacks than wired networks. This paper studies about the Security attacks in WSNs like Wormhole attacks and their countermeasures in the network layer.

According to S. Rajasegarar[3], 2008: According to this paper Anomaly detection in wireless sensor networks is an important challenge for fault diagnosis, intrusion detection and monitoring applications. The algorithm developed for anomaly detection have a inherent limitation of sensor networks in their design so that the energy consumption in sensor node is minimized and the lifetime of the network is maximized. In this paper we analyze the state of the art in anomaly detection techniques for wireless sensor networks.

According to Idris M. Atakli, Hongbing Hu, Yu Chen[1], 2008: Deployed in a hostile environment, individual nodes of a wirelesssensor networks (WSN) could be easily compromised by the adversary due to the constraints such as

limited battery, memory space and computing capability. In this Paper Researchers find that Through intensive Simulation, We verified the correctness and efficiency of their detection scheme.

3. PROPOSED WORK

Any node under attack in wireless sensor networks exhibits an anomalous behavior called the malicious behavior[4]. The most likely threats to public safety wireless deployments, especially those using 802. 15. 4 technologies, are passive eavesdropping, masquerading, and denial-of-serviceattacks. All of these are supported by widely available tools and can be difficult to detect. In addition, passive eavesdropping and denial-of-service can never be completely prevented.

1. Eavesdropping attacks are designed to expose protected information. Passive eavesdropping the most likely eavesdropping threat, can be best prevented through the use of strong encryption against these attacks and are becoming widely available.

2. Masquerading attacks involve attacksers inserting themselves into the wireless network. In most of these attacks, the attacker simulates the wireless access point itself. Fortunately, the Wireless Protected Access(WAP) and 802. 1 li technologies are effective defenses.

Any malicious node in the network can disturb the whole process or can even stop it. To stop such malicious behavior several detection and prevention solutions have been discovered.

Algorithm

1. If link layer reports a link failure, try to repair the link locally using buffer information.

2.. Remove the lost neighbor from all the precursor lists.

3. For each unreachable destination if precursor list non-empty add to RERR(route error) and delete the precursor list.

4. If a packet is forwarded where no route exist, drop the packet and send error upstream.

5. If a valid route has expired, purge all packets from send buffer and invalidate the route.

6. Check the TTL on every node, if it is zero, and then discard to prevent from routing loop.

7. Sequence numbers is used to determine an up-to-date path to a destination.

8. Set an expiry time to the route by adding active route time to current time.

In our research we are using AODV (Adhoc Ondemand Distance Vector)protocol. Because, When we compare two protocols AODV performances effectively than DSDV simulation[5]. AODV is a reactive protocol that uses an on-demand approach to find and establish routes. AODV maintains routes as long as they needed by the source nodes and it is considered one of the best routing protocols in terms of power consumptionand establishing the shortest path.

4. RESULT

The analysis is being done on the basis of the result of *. tcl, *. nam and the *. tr file with the help of Network Animator(NAM) and trace graph by plotting the graph.

Detection Technique: To detect malicious node timers are used with AODV protocol. AODV uses the following fields with each route table entry:

Destination IP Address

Destination Sequence Number

Valid Destination Sequence Number flag

Other state and routing flags (e. g, valid, invalid, repairable, being reparied)

Network Interface

Hop Count (number of hops needed to reach destination)

Next Hop

List of Precursors

Lifetime (expiration or deletion time of the route)

A link can break between two nodes. If the broken link is closer to the destination than source, attempt a local repair. For local repair buffer the packets in interface queue.

//mark the route as under repair rt-> rt flags=RTF_IN_REPAIR

If time out in local repair attempt, route can yet to be repaired, bring down the route and send route errors upstream. This routine is invoked when the link-layer reports a route failed. This is link failure management function. In this condition, try to build route from the source. Non-data packets and Broadcast packets can be dropped. For each valid route maintained by a node(containing a finite Hop CountMetric) as a routing table entry, the node also maintains a list of precursors that may be forwarding packets on this route[4]. These precursors will receive notifications from the node in the event of detection of the loss of the next hop link. The list of precursors in a routing table entry contains those neighbouring node to which a route reply was generated or forwarded. Remove the lost neighbor from all the precursor lists.

If the route is up, forward the packet. If it is the source of the packet then do a Route Request Alocal repairs is in progress. Buffer the Packet. If a packet is forwarded for someone else to which it don’t have a route, drop the packet and send error upstream[4]. Now the route errors are broadcast to upstream neighbours.

If a valid route has expired, purge all packets from send buffer and invalidate the route. If the route is not expired and there are packets in the send buffer waiting, forward them. If the route is down and if there is a packet for this destination waiting in the sendbuffer, then send out route request. SendRequest will check whether it is time to really send out request or not.

In order to track direction of packet flow, direction_in_hdr_cmn is used instead of incoming flag. For Packet originating

*Add the IPHeader ch->size()+=IP_HDR_LEN;

It can happen that a node received a packet that it sent. Probably it is a routing loop. Check the TTL, If it is zero, then discard. Time-to-live(TTL) is a value in an Internet protocol(IP) packet that tells a network router whether or not the packet has been in the network too long and should be discarded. For a number of reasons, packet may not get delivered to their destination in a reasonable length of time.

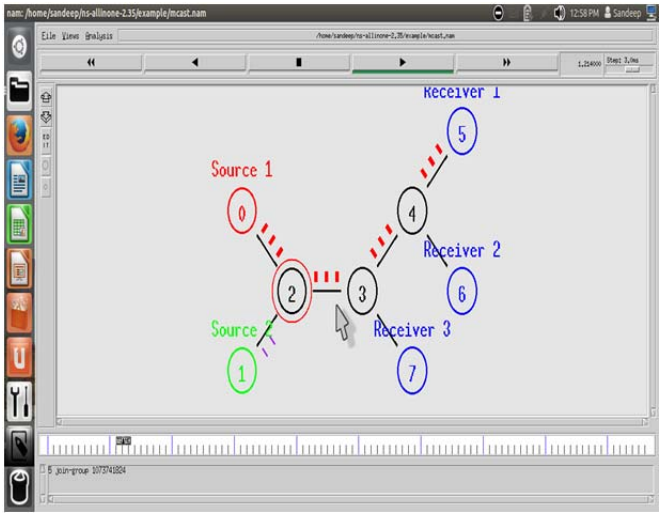

Fig. 2: Data reaches from sender to receiver

In ns2. 35 tcl file is created with the. tcl extension. Nam file represents the Result. Here source nodes creates link with the receiver node with the help of Simplex mode of data transmission. They can use as an agent either tcp or udp.

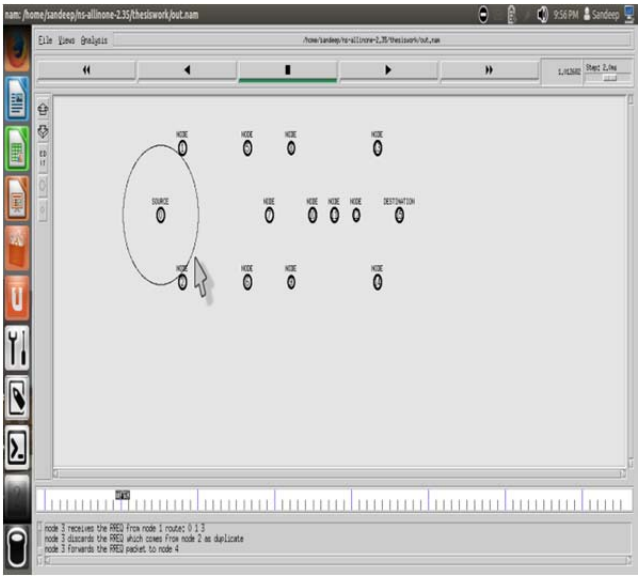

Fig. 3: AODV Simulation

NAM helps us to see the flow of route request(RREQ) and route reply(RREP). It also shows the packets are dropping or reaching to the destination properly. When the TCL file is written, NAM is invoked inside that file. All nodes will receive the message and forward it to its neighbor, except the malicious node, which drop the packets.

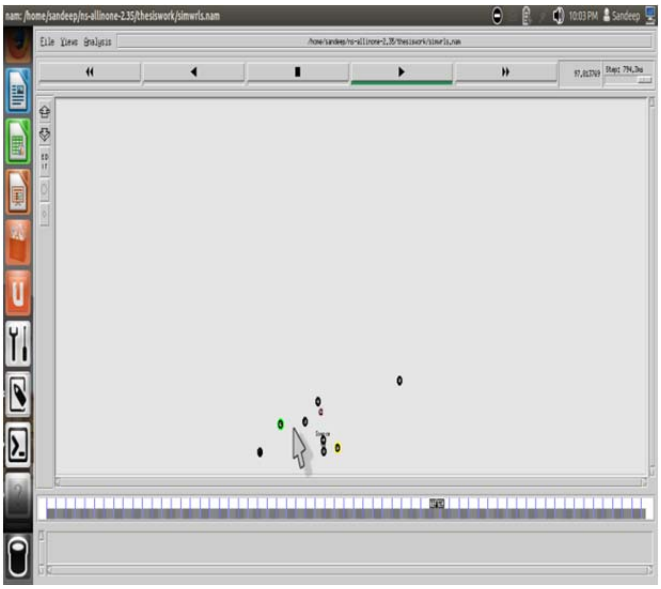

Fig. 4: Detect Malicious node

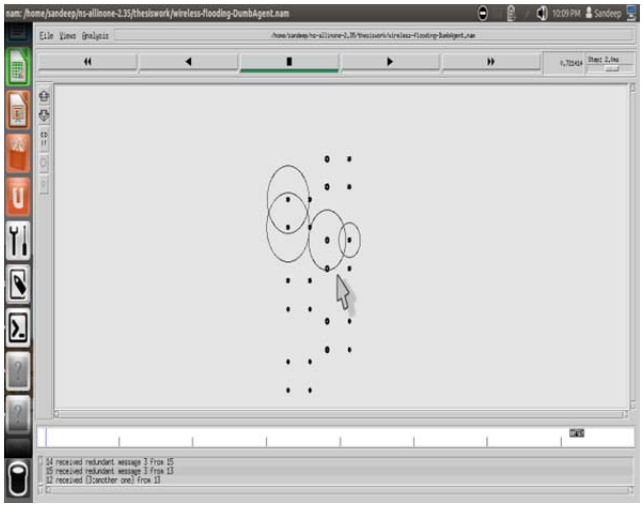

Fig. 5: Flooding(malicious node)

When a receiver wants low amount of data but suddenly receiver seems that there is forwarded a lot of data, this is the reason that data is not safe or we can say that data is suffered from flooding. Flooding provides very attractive false route.

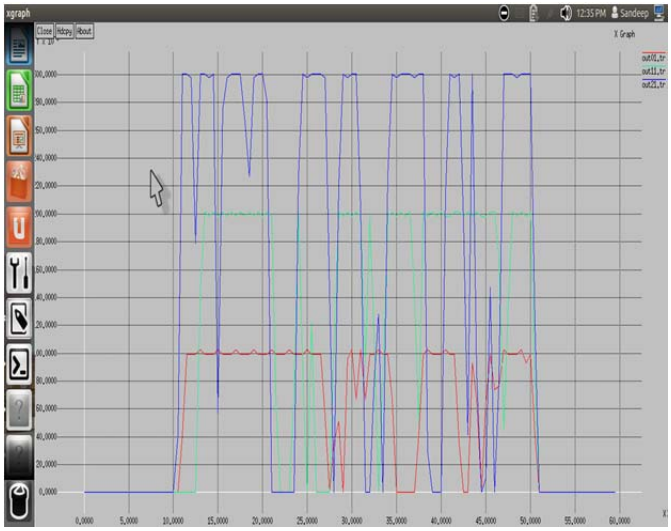

Fig. 6 Data Bit Rate.

When the Data flow is going on progress then due to more links want data the change in topology arises, due to which change in data bit rate, variations in data transmission and packet losses may be arises. Both of these graphs represent the effect of the Traffic and packet loss.

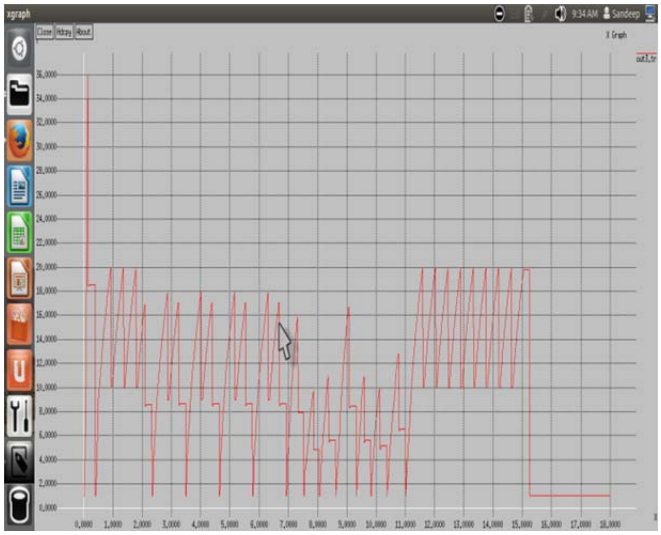

Fig. 7: Data transmission with variations.

5. CONCLUSION

Security is the significant issue in the Wireless Sensor networks. Intrusion of malicious nodes may cause serious impairements to the security. Through this paper we know that AODV protocol performs better than DSDV protocol. In this paper we represents the AODV Mode(Simple mode, malicious mode). This work can help in the area of security based system. An important contribution of this dissertation is the AODV with and without the malicious node. As the malicious node enter into the network, it tries to capture the network. Due to malicious node the performance of the network affected badly. In Future other parameters can be considered like energy consumption, overload, throughput etc.

REFRENCES

[1] Idris M. Atakli, Hongbing Hu, Yu Chen, Wei-Shinn Ku, Zhou Su, ” Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation” Spring sim, 2008, pp. no – 836.

[2] Manisha, Gaurav Gupta, ” Attacks on Wireless Sensor Networks: A Survey”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, October 2013

[3] S. Rajasegarar” Anomaly detection in wireless sensor networks ”IEEE wireless Communication, Volume 15, Issue 4, 2008

[4] Sonu Kumar, Anshul Anand, ” Saving Wireless Networks By Detecting, And Designing Efficient From Masquerade Attacks” INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 3, ISSUE 8, August 2014

[5] Adel. S. El ashheb1, ” Performance Evaluation of AODV and DSDV Routing Protocol in wireless sensor network Environment”