Detection of Wormhole Attack In Wireless Sensor Network

Kashyap Patel (PG Scholar) , Mrs.T.Manoranjitham (Asst professor (S G))

Department of Computer science and Engineering/SRM University, Chennai, India

Abstract

Wireless sensor network consist several type of sensor nodes and many network layer attack can be perform on that network. Wormhole Attack is one of them which is most destructive routing attack for wireless sensor network. It can be implement using Mintroute protocol. In wormhole attack attacker node will attract the data packet while the data packet is transferring from one base station to another base station. In wormhole attack two or more node create a virtual tunnel in that network. Through that virtual tunnel two or more nodes can transfer data packet. This virtual tunnel imitate shorter link in wireless sensor network. This paper presents detection of wormhole attack, so using that simulation results we can provide higher level security in wireless sensor network.

1. INTRODUCTION

Wireless sensor network have number of sensor nodes and they are linked or connected with each other. This type of network called wireless sensor network. Fig.1 is shown below. Sensor network initially consists of small or large nodes called as sensor nodes. In wireless sensor network contain radio transceiver with antenna, it have microcontroller, circuit for interface between sensor nodes and battery.

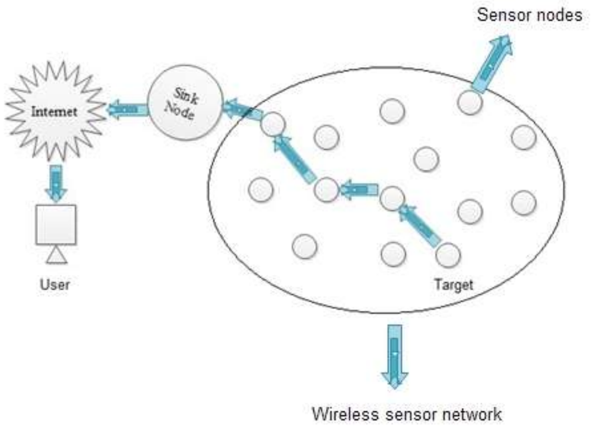

Fig.1 General Wireless Sensor Network

A radio transceiver for generating radio waves through that radio waves sensor nodes can communicate to each other and perform operations.

It have characteristic like mobility of nodes ,scalability of nodes, easy use and power consumption. Basically wireless sensor network is used for monitoring weather condition, temperature etc. It also used in military. Its main advantage is no use of cables. Its main disadvantage is too costly, data transfer is very slow and any one can hack easily.

1.1 Network Attacks

Network Attack means any Attacker can attack on wireless network and hack or spy any type of information from that network [4]. Fig.2 specifies the different types of Attacks in a different layers.

There are main two types of network attack:
1) Passive Attack
2) Active Attack

1.1.1 Types of Network Attack At Network Layer

1) Selective Forwarding

In such attack adversary node create own path, so attacker can drop the data packet and perform spy on those dropped data packet. This type of attack is harder to detect [1]. Solution of this attack is create multiple paths for data transferring. So using multiple paths at least one data packet can reach at destination.

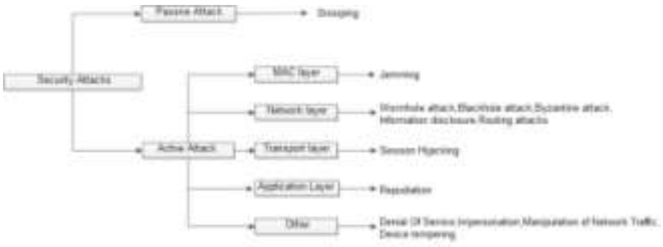
Passive Attack
Snooping
Security Attacks
MAC layer
Jamming
Network layer
Wormhole attack, Blackhole attack, Byzantine attack, Information disclosure, Routing attacks
Active Attack
Transport layer
Session Hijacking
Application Layer
Repudiation
Other
Denial Of Service, Impersonation, Manipulation of Network Traffic, Device tampering

Fig.2 Different Types Of Attacks

2) Sinkhole Attack

Sinkhole Attack work like advertising high link quality, like attacker node will advertise high link quality to other adjacent node. So all node then transfer data packet to that attacker node only [1].

3) Sybil Attack

In such type of attack adversary node create multiple identities of node, so attacker appears to be in multiple location. This is very confusing attack [5]. solution of this attack is provide unique key to each node so using that key nodes can transfer data packet.

4) Wormhole Attack

In such type of attack two or more attacker node will create a higher level virtual tunnel(Wormhole Link) between those two attacker node, and advertise high link quality so all other nodes will transfer data packet through the virtual tunnel [5]. This attack is very hard to detect. Fig.3 specifies wormhole attack

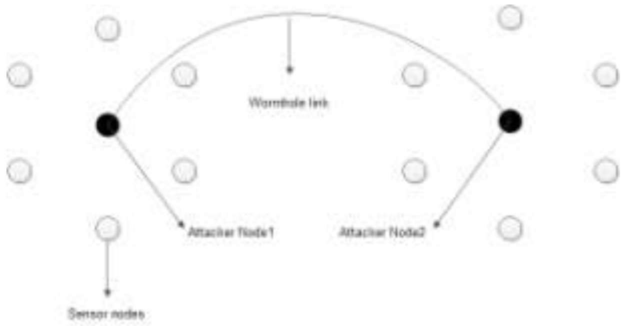

Fig. 3 Wormhole Attack

5) Hello Flood Attack

In such type of attack attacker node will inform its presence to neighbour node through broadcasting Hello message. so using that message neighbour node will assume that attacker have high link quality to send the data packet [5]. It is also known as broadcast wormhole attack.

2. RELATED WORK

There is a lot of work that has been done in order to curb the Wormhole attack [4]. Broadly there can be two categories of techniques/methods to curb a Wormhole attack that is detection method and prevention method [6]. Detection is nothing but detecting wormhole attack using any simulation process and prevention is nothing but methodology developed by organization to avoid wormhole attack. Wormhole Detection method can be developed using any language like c++, JAVA or developer can be use any networking simulator like ns2, tiny os etc.

Another solution for avoid Wormhole attack to provide tight time synchronization which is often not feasible and requires original protocol design by which to make these attack useless. There are many ways to solve wormhole attack like location and time based solution, key based solution, static based solution, graph based solution, neighbour based solution [4].

3. PRAPOSED TECHNIQUE

Wormhole attack is very hard to detect if its launch. So this paper represents detailed design of launching wormhole attack and detecting wormhole attack with its measurements [6].

3.1 Implementation of Wormhole Attack

Mintroute routing protocol use to estimated link quality [1], using this estimated link quality data packet is going to be delivered and reached to its destination. Here link quality will be estimated base on received packets and total no of generated packets. After an attacker node will launch wormhole attack in wireless sensor network. Wormhole attack can be launched using two steps [1]:

1) In first step attacker node will broadcast fake and better link quality to other nodes.

2) In second step sender node will change its current parent node to attacker node.

so after this two step attacker node will be active and it will work as a wormhole node, but same procedure will happen in same or another network and like that two attacker node will generate and both will create high level virtual tunnel. So all nodes in Network-A feel that it is near to all nodes in Network-B. Now both Attacker node is activated and both are connected. Fig.4 shows actual implementation of wormhole attack.

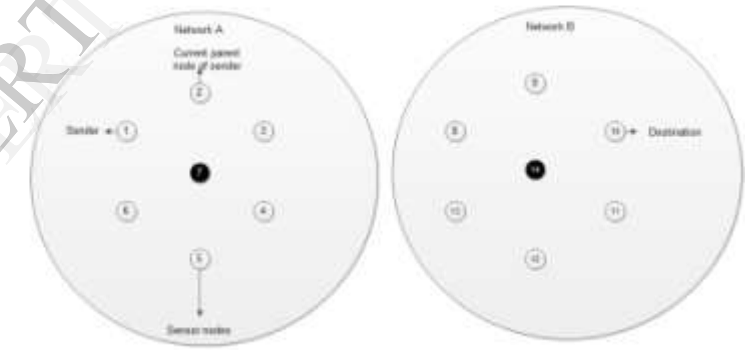

Fig.4 Implementation of Wormhole Attack

Here, in Fig.4 node 1 is a sender which is in network-A and node 10 is a destination which is in network-B. Currently node 2 is a parent node of node 1 so node 1 will send a data packet to node 2 and so on it reach to the destination in network-B.

Here, in Fig.5 node 7 will become an attacker node and it will send fake & better link quality signal to each and every node in network-A similarly node 14 will become an attacker node and it will send fake and better link quality signal to each and every node in network-B. So both node 7 and 14 will create a virtual tunnel, which is called wormhole link also. So now if node 1 wants to send a data packet to node 10 which is in network-B then data packet will transfer through node 7 and 14 node only which is attacker node. Fig.5 shows fully implementation of wormhole attack and wormhole link.

This same process can be applied to all other nodes in the wireless sensor network and perform wormhole attack [4].

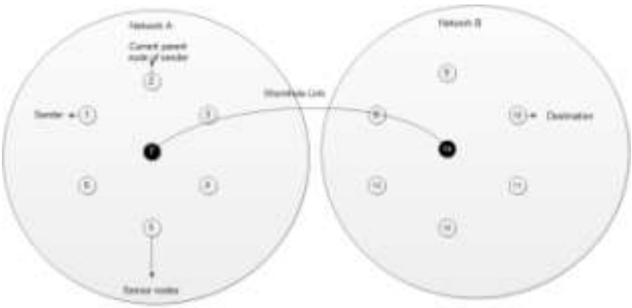

Fig.5 Implementation of Wormhole Attack

3.2 Detection of Wormhole Attack Using Simulation

Data packet transferring in wireless sensor network take place in wireless medium. Hence each node can receive or analyze data packet from their neighbour nodes. So detection of wormhole attack can be done on basis of data packet flow. Simulation

Wormhole attack detection is implement using network simulator called NS2 and code is written as tcl script. Wormhole attack is implemented on NS2 using 14 sensor nodes and their communication range is 250 m. So after performing simulation countermeasures will be generate based on those measurements or graph we can say that wormhole attack is detected. Using received packets and total generated packets analysis this graph like no of dropped packets, packet reception ratio, throughput, delay etc will generate [6].

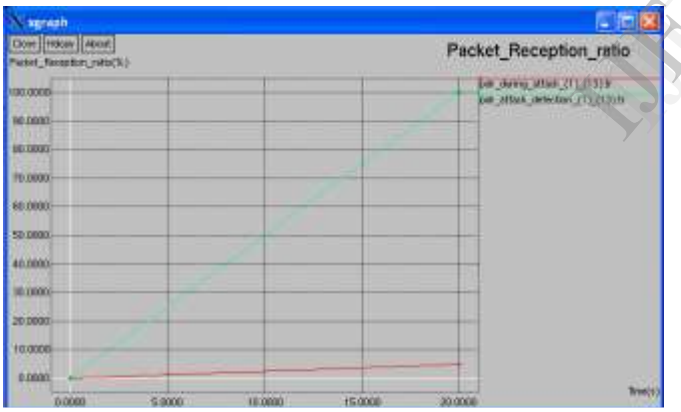

Fig.6 Generated Graph of Packet Reception Ratio

Fig.6 shows no of packet reception ratio before wormhole attack and after wormhole attack. In Fig.6 green line shows packet received before wormhole attack and red line shows packet received after wormhole attack. Here no of packet reception ratio is decreasing so based on that analysis wormhole attack is detected.

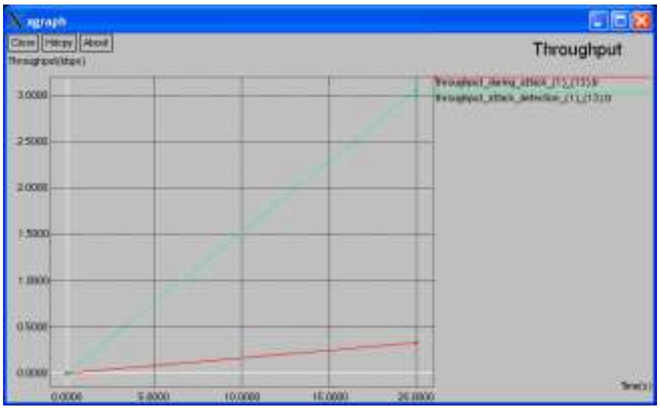

Fig.7 Generated Graph of Throughput

Fig.7 shows throughput before wormhole attack and after wormhole attack. Here green line shows throughput before wormhole attack and red line shows throughput after wormhole attack, so based on this graph wormhole attack is detected because throughput is decreasing.

Fig.8 shows packet drop before wormhole attack and after wormhole attack. Here green line shows packet drop before wormhole attack and red line shows packet drop after wormhole attack. Here packet drop ratio is increasing so based on that analysis wormhole attack is detected.

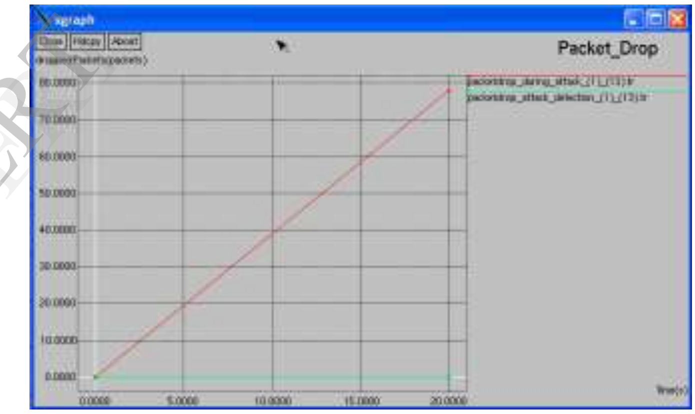

Fig.8 Generated Graph of Packet Drop

4. CONCLUSION

This paper is about implementation and detection of wormhole attack in wireless sensor network. Advantage of Wormhole attack is to hack any useful data packet and perform changes on those data packet. So based on simulation results shows that wormhole attack is detected based on packet reception ratio, packet dropped ratio, and throughput. Here number of packets are decreasing exponentially. so wireless sensor network can be secure using these results and wormhole attack can be prevent. In future by creating multi wormhole link between different nodes on the basis of link estimation, wormhole attack may be implemented.

5. References

[1] Meenakshi Tripathi, M S Gaur, Vijay Laxmi, Vinod Kumar Jatav,(2012),"Wireless sensor networks: Attack Models and Detection",IACSIT Hong Kong Conferences IPCSIT vol30,IACSIT Press,Singapore,PP144-149.

[2] Ki-Il Kim and Min-Jing Baek (2012),"Improving MintRoute Protocol at Different Scenarios", Applied Mathematics & Information Science An International Journal,Appl.Math.Inf.Sci.6, No.2Spp., NSP, PP619-625.

[3] Dhara Buch and Devesh Jinwala(2011),"Prevention of Wormhole Attack in Wireless Sensor Network", Journal of Network Security & its Application, Vol.3, No.5,PP85-98.

[4] Marianne Azer, Magdy, El-Soudani, Sherif El-Kassas(2009)," A Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole Attacks in Wireless AdHoc Networks",International journal of Computer Science and Information Security, Vol.1,No.1,PP 41-52.

[5] Dr.Harsh Kumar Verma, Saurabh Singh(2011),"Security For Wireless Sensor Network", International Journal on Computer Science and Engineering, Vol.3,No.6,PP2393-2399.

[6] A.Vani and D.Sreenivasa Rao(2011),"A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In AdHoc Wireless Networks", International Journal on Computer Science and Engineering, Vol.3,No.6,PP2377-2384.

[7] Revathi Venkataraman, M.Pushalatha, T.Rama and Rishav Khemka(2009),"A Graph-Theoretic Algorithm for Detection of Multiple Wormhole Attacks in Mobile Ad Hoc Networks", International Journal of Recent Trends in Engineering, Vol.1, No.2,PP220-222.

[8] Ms.N.S.Raote and Mr.K.N.Hande(2011),"Approaches towards Mitigating Wormhole Attack in Wireless Ad-hocNetwork", International Journal of Advanced Engineeringsciences and technologies,Vol.2,No.2,PP172-175.

[9] Mohammad Rafiqual Alam ,"Detecting Wormhole and Byzantine Attacks in Mobile ad hoc Networks", Curtin University of Technology, May 2011.

[10] Majid Meghdadi, Suat Ozdemir and Inan Giiler(2011),"A Survey of Wormhole-based Attacks and theirCountermeasures in Wireless Sensor Network",IETE Technical review, Vol.28, Issue.2,PP89-102.

[11] Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki(2009), "A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-hoc Networks", International Journal of Network Security and itsApplication, Vol.1, No.1,PP44-52.

[12] ns-2, "http://www.isi.edu/nsnam/ns/."