Scientific Journal of Impact Factor(SJIF): 3.134
e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2, Issue 6, June -2015

DETECTION OF WORMHOLE ATTACK AND MINTROUTE PROTOCOL

Nikita R. Patel

Assistant Professor Computer engineering department, Madhuben&Bhanubhai Patel Women's Institute of Engineering, New V.V.Nagar, Anand Gujarat-India

Abstract *–This Article present a detection of wormhole attack in wireless sensor network comes under network layer. Wormhole attack is a particularly devastating attack, where two or more malicious nodes create a higher level virtual tunnel in the network, which is employed to transport packets between the tunnel end points. Advantage of Wormhole attack is to hack any useful data packet and perform changes on those data packet. The aim of the work presented here is to introduce MintRoute which is one of the well-known network layer protocol which guarantees reliability by choosing the reliable link to the sink on a tree topology.*

Keywords*-component–Wormhole; Mint-route; Sinkhole;*

I. INTRODUCTION

A type of wireless networking which is comprised on number of numerous sensors and they are interlinked or connected with each other for performing the same function collectively or cooperatively for the sake of checking and balancing the environmental factors. This type of networking is called as Wireless sensor networking. Fig 1.1 is shown below.

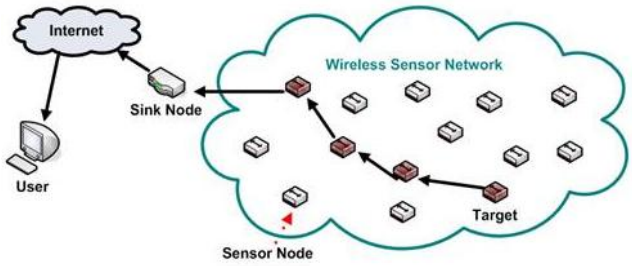

Fig-1.1 General wireless sensor network

Total working of wireless sensor networking is based on its construction. Sensor network initially consists of small or large nodes called as sensor nodes.Wireless sensor networking have such sensor nodes which are specially designed in such a typical way that they have a microcontroller which controls the monitoring, a radio transceiver for generating radio waves, and different type of wireless communicating devices and also equipped with an energy source such as battery.

II. RELATED RESEARCH

1) Detection of sinkhole attack

There are two rules to detect the attack:According to **first rule** the route update packet should be originated by one hop neighbor only. Route update packet consists of sender node ID and link estimates of the node. For example given in Figure 1.2 when rule 1 is triggered at node 1 it Overhears the rout update packet which is sent by attacker node 2 impersonating node 1[4]. Node 3, 4 and 7 will also realize that they are update packets from node 1 which is not a one hop neighbor.

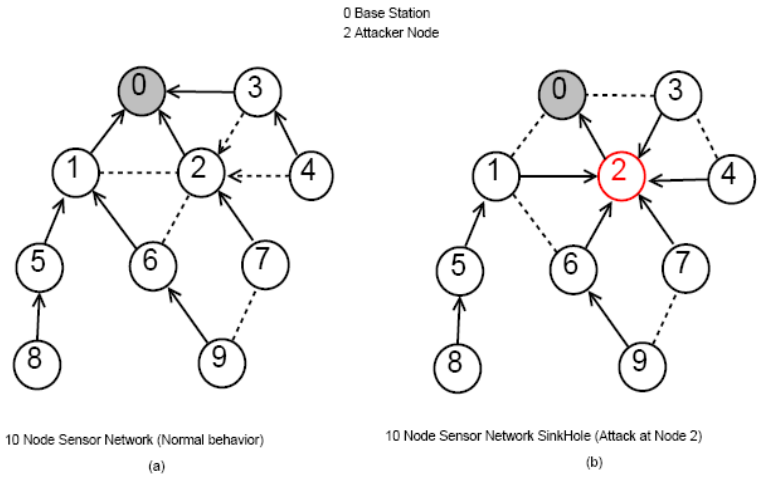

Fig-1.2 Detection of Sinkhole Attack

Second rule is based on the anomaly detection. In Mint-Route protocol [2], sensor nodes calculate the estimate for link quality for their neighbors. Nodes also receive link quality estimates from neighbor with the help of route update packets. There may not be a big difference in these two estimates of link quality. If the link quality estimate is showing a deviation of value more than 50, then it may be an impersonated value by applying both the rules together we can detect the sinkhole node.

2) Implementation of sinkhole attack using mint route protocol

Routing protocols, such as Mint-Route [2] make the use of estimated link quality to maintain the routing tree.Sinkhole attack can be launched using two steps on Mint-Route [4]first, the attacker node advertises a betterlink quality for itself, up to 255. Second step, it changes the link quality of current parent to worst value. Fig 1.3 is about Implementation of sinkhole attack.

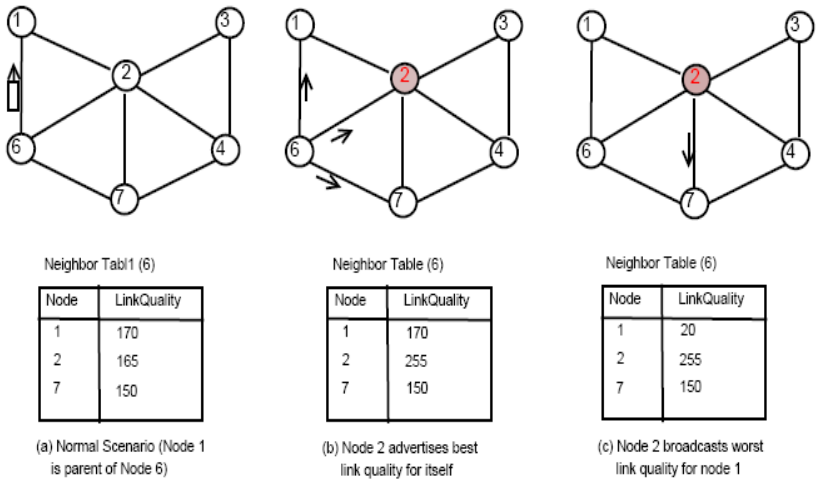

Fig-1.3 Implementation of Sinkhole Attack

Here, sensor node 2 is an adversary node. Current parent of node 6 is sensor node 1 in this scenario.Adversary node 2 advertises a false link quality estimate (255) to itself in the network. So, whenever attacker receives the route update packet of node 6, it changes the link quality of node 1 to a low value (i.e. 20) and sends it back to 6 as a unicast packet, impersonating 1.

Here node 6 thinks that the route update packet is sent by node 1. Node 6 estimates the link quality and refreshes own neighbor table with the new entry.

This way node 6 triggers the parent changing mechanism and chooses node 2 as new parent. Hence the node 2 becomes the new parent of the node 6.

III. PROPOSED WORK

1) WORMHOLE ATTACK

For launching a wormhole attack, an adversary connects two distant points in the network using a direct low-latency communication link called as the **wormhole link**[1].The wormhole link can be established by a variety of means, e.g., by using an Ethernet cable, a long-range wireless transmission, or an optical link. Once the wormhole link is established, the adversary captures wireless transmissions on one end, sends them through the wormhole link and replays them at the other end. Fig 1.4 is about Wormhole Attack.

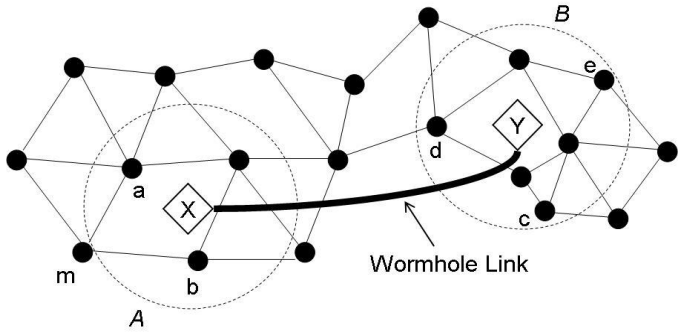

Fig-1.4 Wormhole Attack

An example is shown in the above figure. Here X and Y are the two end-points of the wormhole link (called as wormholes). X replays in its neighbourhood (in area A) everything that Y hears in its own neighbourhood (area B) and vice versa. The net effect of such an attack is that all the nodes in area A assume that nodes in area B are their neighbours and vice versa. This, as a result, affects routing and other connectivity based protocols in the network. Once the new routes are established and the traffic in the network starts using the X-Y shortcut, the wormhole nodes can start dropping packets and cause network disruption. They can also spy on the packets going through and use the large amount of collected information to break any network security. The wormhole attack [3]will also affect connectivity-based localization algorithms and protocols based on localization, like geographic routing, will find many inconsistencies resulting in further network disruption.

2) MINTROUTE PROTOCOL

Mint-Route [2]builds tree based topology toward the sink. As compared to the shortest hop routing protocol, each node measures the link quality toward the sink. Among multiple links, a neighbor node having the highest value over the link is assigned as parent node. In order to estimate link quality in Mint-Route, periodical beacon message and packet reception ratio are employed. In addition, for smoothing computed value, exponential moving average method is also introduced. For parent selection, Mint-Route follows three major steps. First, it discovers neighbors and estimates the link quality through broadcasting beacon messages periodically. This packet carries sequence number to detect if any packet is lost, when the time period is over. PRi,j (packet reception ratio) for the link between nodei and j is given in equation (1.1). In equation (1.1), Packets_Rcv represents the number of packets received correctly. Also, Packets_Exp represents the number of packets expected that means the number of packets actually sent. The time interval for beacon is set to t.
Thus, parent selection procedure is accomplished every t seconds.

$$PR_{i,j}(t-1,t) = \frac{\text{Packets\_Rcv in t}}{\text{MAX(packets\_Exp in t,packets\_rcv in t)}} \quad \text{... (1.1)}$$

By applying exponential moving average method, link cost is computed in equation (1.2), where α is ranged from 0 to 1. Based on the value from equation (1.2), a node with the largest LRi,j(t) is selected as parent of node i as shown in equation (1.3), where NS represents set of neighbors within the transmission range

$$L_{i,j}(t)=\alpha*PR_{i,j}(0,t-1)+(1-\alpha)*PR_{i,j}(t-1,t) \quad \text{....(1.2)}$$

$$P_i=MAX(\arg\max\{L_{i,j}(t)\},L_{i,pi}(t)) \quad \text{.....(1.3)}$$

When a node finishes computing, the resulting value is compared with cost on a parent in equation (3.3). If a new cost is greater than parent node's cost, a new parent is chosen and then packets are transmitted along this new link. Otherwise, current node serves parent continuously.

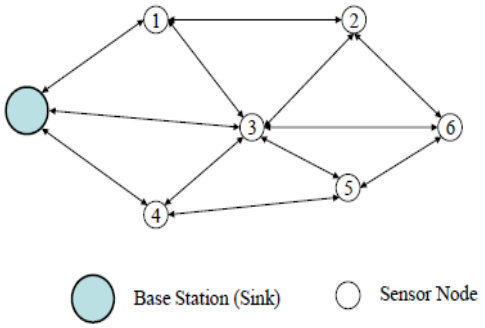

Fig-1.5Neighbour discovery: step 1

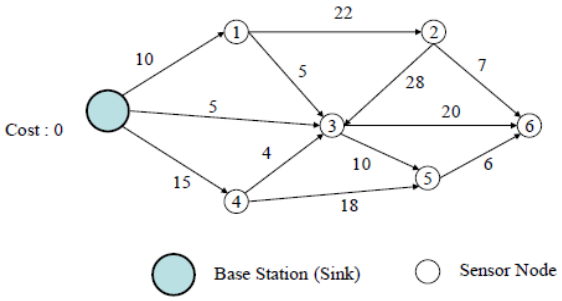

Fig-1.6Cost estimation: step 2

Based on above procedure, Figure 3.3 and Figure 3.4 show how Mint-Route estimates cost for each link. In Figure 3.3, each node uses beacon message to discover the neighbor and collect the link quality information. After finding neighbors, the link cost is set as shown in Figure 3.4 In next step, parent selection algorithm is accomplished with this computed value. Furthermore, Table 3.1 shows the cost of each node when parent selection phase is completely done. For example, a node 6 sends the packet to the sink along the path 6-5-3-0, because the parent of node 5 is set to node 3. Through this procedure, each link maintains a reliable link toward the sink periodically

Node ID	Cost	Parent
1	10	0
2	32	1
3	5	0
4	9	3
5	15	3
6	21	5

Table-1.1 Cost for Parent selection table

Causes of Instability. Based on basic operation of Mint-Route[2], instability is mostly caused by link selection procedure and data collection for measurement over the link. Current Mint-Route takes a long time to get stable value from the initial network time. At the starting time, since each node has little information for the link, parent changes are made frequently. Another reason as explained before, if a new computed value is greater than the previous one, then a new parent is selected.

Even though exponential moving average method makes the smooth value, this procedure is also potential cause of instability in Mint-Route. The last reason is backward parent selection problem. Unlike the initial operation, a node can select the backward parent towards the sink according to the computed value in equation (1.2). This backward forwarding decreases the reliability as well as makes the network unstable. These three main procedures make the Mint-Route unstable.

IV. IMPLEMENTATION RESULTS

Mintroute routing protocol [2] use to estimated link quality, using this estimated link quality data packet is going to be delivered and reached to its destination. Here link quality (4.1) will be estimated base on received packets and total no of generated packets.

Link quality = (Received no of packets) / (Total no of generated packets) (1.7)

After an attacker node will launch wormhole attack in wireless sensor network. Wormhole attack can be launched using two steps:

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[1]. Now both Attacker node is activated and both are connected. Fig 1.7 shows actual implementation of wormhole attack.

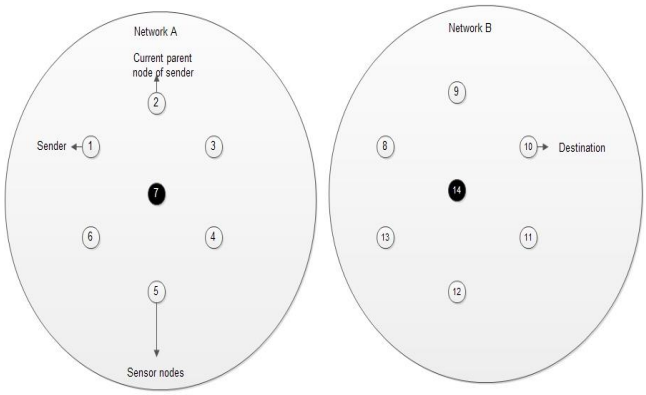

Fig-1.7 Implementation of wormhole attack

Here, in Fig 1.7 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 1.8 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 1.8 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.

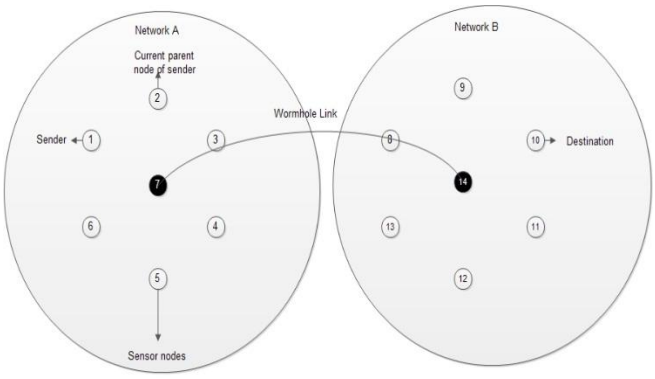

Fig-1.8 Implementation of wormhole attack

V. CONCLUSION & FUTURE WORK

A particularly devastating attack is known as the wormhole attack, where two or more malicious nodes create a higher level virtual tunnel in the network, which is employed to transport packets between the tunnel end points. In this paper we conclude that wormhole attack can be implement and detect using mintroute protocol. Mint-Route is one of well-known network layer protocol which guarantees reliability by choosing the reliable link to the sink on a tree topology. So wireless sensor network can be secure using these results and wormhole attack can be prevent.

Using Mint-route Protocol we can do simulations on different topology,number of nodes, and other factors such as beacon interval will continue to evaluate performance. At network layer Protocols like hello Flood attacks Selective Forwarding, Sinkhole Attackscan be detect using Mint-route Protocol.

REFERENCES

[1] Marianne Azer, Magdy, El-Soudani, Sherif El-Kassas,"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,May 2009, 41-52.

[2] Ki-Il Kim and Min-Jing Baek,"Improving MintRoute Protocol at Different Scenarios", Applied Mathematics & Information Science An International Journal,Appl.Math.Inf.Sci.6, No.2S pp.,2012 NSP,619-625.

[3] DharaBuch and DeveshJinwala," Prevention of Wormhole Attack in Wireless Sensor Network, Journal of Network Security & its Application", Vol.3, No.5, Sep 2011,85-98.

[4] MeenakshiTripathi, M S Gaur, Vijay Laxmi, Vinod Kumar Jatav,"Wireless sensor networks: Attack Models and Detection", IACSIT Hong Kong Conferences IPCSIT vol30, IACSIT Press, Singapore, 2012,144-149.

[5] Dr.Harsh Kumar Verma, SaurabhSingh,"Security For Wireless Sensor Network", International Journal on Computer Science and Engineering, Vol.3,No.6, June 2011,2393-2399.

[6] A.Vani and D.SreenivasaRao,"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,June 2011,2377-2384.

[7] RevathiVenkataraman, M.Pushalatha, T.Rama and RishavKhemka,"A Graph- Theoretic Algorithm for Detection of Multiple Wormhole Attacks in Mobile AdHocNetworks", International Journal of Recent Trends in Engineering, Vol.1, No.2, May 2009,220-222.

[8] Ms.N.S.Raote and Mr.K.N.Hande, "Approaches towards Mitigating Wormhole Attack in Wireless Ad-hoc Network", International Journal of Advanced Engineeringsciences and technologies, Vol.2, No.2, 2011, 172-175.

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

[10] Majid Meghdadi, SuatOzdemir and InanGiiler,"A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Network", IETE Technical review, Vol.28, Issue.2, Mar-Apr 2011,89-102.

[11] Debdutta Barman Roy, RituparnaChaki, NabenduChaki, "A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-hoc Networks" ,International Journal of Network Security and its Application, Vol.1, No.1, April 2009,44-52.

