Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 11, November -2017

Security Analysis of Wormhole Attack in WSN

Vishal Makwana

Computer Engineering, Marwadi Education Foundation, Rajkot

Abstract —*With the tremendous growth of mobile devices, the deployment of wireless sensor networks in the unfavorable environment makes it very popular for research field. Wireless sensor networks (WSN) is widely used in various fields, like Military, Health (Scanning), Space Exploration, Vehicular Movement, Mechanical stress levels on attached objects, Environment monitoring, Weather forecasting, Traffic control, Natural disaster prevention etc. WSN is made of by significant number of nodes deployed in an unfavorable area in which not all nodes are directly connected. The data exchange carried by multihop communications. Routing protocols are responsible for discovering and maintaining the routes in the network. Now a day, Security is prime concern for wireless sensor network. Wireless sensor networks are very weak and susceptible to many types of security attacks, like Sybil attack, Blackhole attack, Flooding attack, Wormhole attack etc. The wormhole attack creates serious issues in WSN, such as routing error, a reduction in sensor lifetime and broken network topology. Several wormhole detection approaches have been proposed, but most of them need special hardware devices and consume a lot of system resources. The main aim for this research to detect wormhole attack in wireless sensor Network (WSN) and at the same time perform rescue task to defend against attack. All the simulation will be performed in NS2.*

Keywords-*WSN; Wormhole Attack; RTT; AOMDV; Malicious Node*

I. INTRODUCTION

Wireless Sensor Networks (WSNs) is self-configured and infrastructure-less wireless networks. WSN consists of a large number of sensor nodes which have sensing, communication, computing and mobile capabilities. These sensor nodes are distributed in a certain area which is hard to access or in an unfavorable environment, to collect the information. Sensors communicate with each other to transmit information to the base station by multi-hop, so we can analyze the information received by various sensor node to carry out some applications like environment monitoring, weather forecasting, traffic control, natural disaster prevention (like earthquakes, hurricanes and tsunamis), etc. There are few components in WSN like Sensor Field, Sensor Node, Base Station and Task Manager. Sensor Field is an area where the deployment of sensor nodes takes place. Sensor Nodes are smart nodes which interact with environment and routes the information collected to the base node. Base station is responsible for data storage and processing data received from other sensor nodes. Task Manager is defined as the centralized controller of the network, dealing with collection of information and then propagating the information to the network and takes appropriate action based on analysis. Sensor nodes are small devices having limited amount of energy resource. When Sensor Nodes energy starved, nodes are dying by environment factors. Structure of Wireless Sensor network is continuous changing in nature. Every node has different computational power and storage capacity. Due to unbound delays, there is chance to communication failure.

In WSN, based on the sensing range and environment, the sensor nodes are classified into four groups, specialized sensing node, generic sensing node, high bandwidth sensing node and gateway node. The radio bandwidth for the sensor nodes are <50 Kbps, <100 Kbps, ≈ 500 Kbps and >500 Kbps respectively. These nodes are used for various purposes. Specialized sensing nodes are preferred for special purpose devices, intelligent generic sensing node preferred for generic functions. For interconnectivity functions high end smart bandwidth sensing node and gateway nodes are preferred. There are many different kinds of attacks in WSN, like Sybil attack, Blackhole attack, Flooding attack, Wormhole attack etc. These attacks may lead to data loss, the entire network topology might be broken.

The wormhole attack creates serious issues in WSN, such as routing error, a reduction in sensor lifetime and broken network topology. The wormhole launches an attack by creating a tunnel between one or more pairs of malicious nodes, as shown in Figure 1. There are no differences between malicious nodes and sensing nodes in the behaviors of mobility and communication. Nodes within the wormhole transmission range will receive the information about neighbors from another wormhole through the tunnel which is wireless or physical. Therefore, those nodes which are affected by the wormhole attack will route in the error path. This may lead to rapid battery consumption of nodes and unstable topology.

In Figure 1. shows there is wormhole link between W1 and W2. There is a Base station for collecting information from the various sensor nodes.

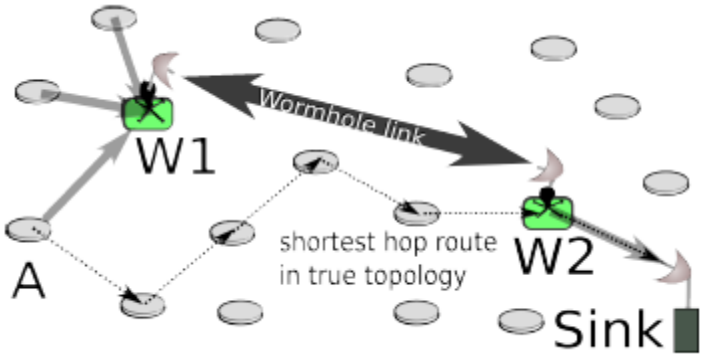

Figure 1.[1] The wormhole attack in operation

There are two different modes of Wormhole attack [3]:

1. **Hidden attacks:** Before forwarding a packet by a node, it updated the packet by putting their identity or MAC address in packet's header that allows receiver to know packet directly comes from.
2. **Exposed attacks:** Wormhole nodes don't modify the content of packet but they add their identities in packet header as legitimate nodes do.

II. CHALLENGES AND ISSUES

The process of determining the best path to forward the data from source to destination is known as routing. Routing mechanisms are very different in wireless sensor networks as compared to traditional approaches. Because, it is infrastructure less networks, unreliable and energy constrained networks. There are different routing protocols including proactive, reactive, hybrid, location based and hierarchal. There are following issue to design routing protocol in WSN [2]:

i. Energy Considerations
ii. Data Aggregation
iii. Node capabilities
iv. Data Delivery Models
v. Node Deployment
vi. Network Dynamics

Due to various resource and physical limitations including unreliable communication, collisions, latency and unattended after deployment and management by remote user, makes WSN vulnerable to attacks[2].

III. ROUTING PROTOCOL

Routing is a process of sending data packets from source node to destination node. Routing in wireless sensor networks differs from conventional routing in fixed networks in various ways. There is no infrastructure, wireless links are unreliable, sensor nodes may fail and routing protocols have to meet strict energy saving requirements [5]. Therefore, routing in wireless networks is a critical issue. There are a number of routing protocols existing in various networks such as AODV (Ad-hoc On Demand Distance Vector routing), DSR (Dynamic Source Routing), DSDV (Destination Sequenced Distance Vector routing) and many more routing protocols. In this research we will work and check the performance of AOMDV protocol which is Proactive and table driven protocol.

IV. LITERATURE REVIEW

J. Harbin, P. Mitchell and D. Pearce [1] analyzed that disturbance based routing schemes provides a considerable improvement in wormhole avoidance over shortest path schemes. And use AODV protocol as routing protocol. R. Mudgal and R. Gupta [3] they analyzed various techniques to detect wormhole attack. They proposed routing technique is based on a secure route discovery technique using Routes Redundancy and Time-based Hop Calculation and also use CPR routing for load aware routing technique. As a result, it is able to produce maximum security, maximum progress ratio and minimizing the router overhead. H. Ghayvat, S. Pandya, S. Shah, S. C. Mukhopadhyay, M. H. Yap and K. H. Wandra[4] they proposed security approach is to detect and prevent wormhole attack. They used AODV as routing protocol. This method is based on a calculation of tunneling time to analyze the behavior of wormhole. They used digital signature and hash chain algorithm is applied to remove the malicious node. This method helps to increases throughput and minimizes network delay compared to the existing system.

V. PROPOSED ALGORITHM TO DEFEND AGAINST WORMHOLE ATTACK

We proposed method for detect wormhole node and at the same time prevent the network in WSN. This algorithm use AOMDV protocol as a routing protocol. This algorithm works in two phases: In first phase, calculate threshold RTT with the help of normal network conditions. In second phase, use this calculated threshold RTT to defend against wormhole attack.

ALGORITHM : Calculate Threshold RTT

Step1	Deploy sensor nodes and create a network with ideal conditions
Step2	Sender send RREQ (Route Request) message to destination
Step3	Wait for acknowledgement RREP (Route Reply) from the receiver, if RREP received
Step4	Calculate RTT, **Round Trip Time (RTT) = Traveling Time Taken by Packet / No. of Hop**
Step5	Estimate the threshold RTT denoted as **Threshold RTT**, by repeating the RTT calculation for N different scenarios using formula, **Threshold RTT = 1/N (Σ RTT (i))** Where i = 1 to N
Step6	Broadcast the estimated RTT, Threshold RTT to entire network

Figure 2. Phase-I Algorithm

ALGORITHM : Defend Against Wormhole attack

Step1	Sender sends RREQ message for the route discovery
Step2	Receiver acknowledged with RREP message to sender
Step3	when packet send, Each sender put the transmission time (Tt).
Step4	When receiver receive the packet record the receiving time (Tr).
Step5	Calculate time difference (Td), Td = Tr - Tt
Step6	if (Td ≤ Threshold RTT) then Previous node as genuine node.
Step7	if (Td > Threshold RTT) then Last hop is malicious.

Figure 3. Phase-II Algorithm

In first phase, estimate threshold RTT. For that, deploy wireless Sensor Network with N nodes. This algorithm works for ideal conditions for finding the estimate threshold. After that, we want to send data from source S to destination D. So, Source broadcast the RREQ message and receive by the all node in the network. There are multiple paths to send data from S to D. So, destination D receives the RREQ message and acknowledged with RREP message. If RREP received by sender then calculate the RTT by using given formula in step-4 in Fig 2. Repeat the above procedure

for N scenarios and after that estimate the threshold RTT by using given formula in step-5 Fig. 2. This estimated threshold RTT is used in next phase to detect and prevent against wormhole.

In second phase, the malicious link is discovered. So, the entire process can be understood by the route discovery phase. First the sender transmits the RREQ to the receiver node. During this process each node maintains a table for one hop neighbor. That contains the average time to travel and the time for hop last hop information. When the sender receives the acknowledgment from the different sources then the table is compared with the obtained threshold and decided is route malicious or not. If the last hop RTT is less than Threshold RTT, then the route is genuine else that can be involved with the malicious nodes or route. Additionally the table entry is labeled as the malicious. Above algorithm will implement using AOMDV as routing protocol.

VI. SIMULATION ENVIRONMENT AND RESULTS

In this section the simulation results are shown for parameters like average throughput, end to end delay and packet delivery function by comparing AODV and proposed AOMDV protocol in a network. Initially, we collect reading for above mention parameters for 10,20,30,40 and 50 nodes respectively. The wireless environment is formed using network simulator 2.35. The following table indicates the simulation parameters.

Table 1 Simulation parameters

Simulation Area	1000m × 1000m
Routing Protocol	AODV, AOMDV
Number of Nodes	10,20,30,40,50
Traffic	CBR
Mobility Model	Fixed
Simulation Time	100s

In all figures below on x-axis shows number of nodes and on y-axis shows the parameter. Figure 4. shows the values of avg. throughput against numbers of nodes for both AODV and proposed AOMDV routing protocol. Clearly shows increase avg. throughput in proposed AOMDV protocol.

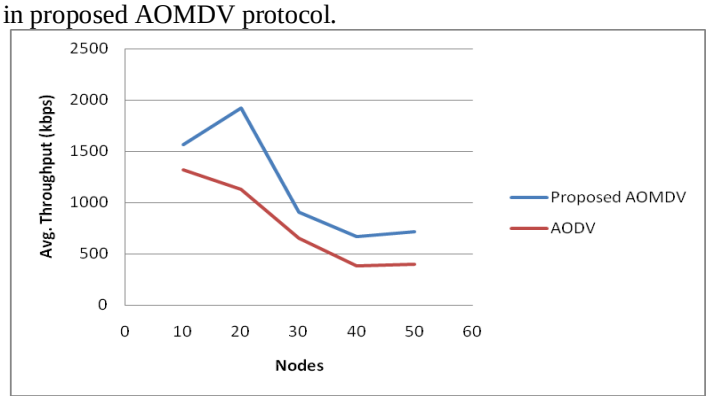

Figure 4. Avg. Throughput Comparison

In Figure 5. shows the values of end to end delay against numbers of nodes for both AODV and proposed AOMDV routing protocol. Clearly shows decrease end to end delay in proposed AOMDV protocol.

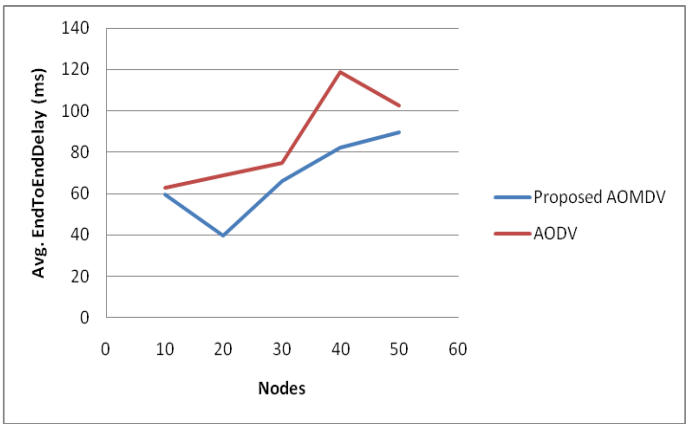

Figure 5. end to end delay Comparison

In Figure 6. shows the values of packet delivery function against numbers of nodes for both AODV and proposed AOMDV routing protocol. Clearly shows increase packet delivery function in proposed AOMDV protocol.

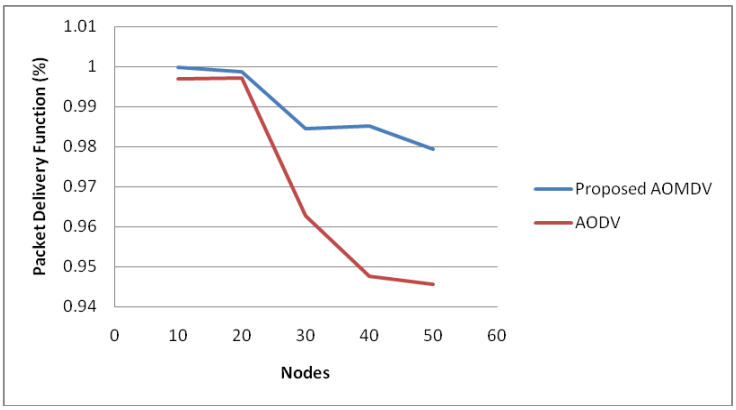

Figure 6. Packet Delivery Function comparison

VII. CONCLUSION

We notice different performance metrics like average throughput, packet delivery function and average end-to-end delay of network with and without wormhole attack in network using different numbers of nodes using AOMDV protocol. The simulation result and graphs clearly suggest that performance of proposed algorithm using AOMDV protocol gives quite better performance for various performance metrics.

REFERENCES

[1] J. Harbin, P. Mitchell and D. Pearce, "Wireless sensor network wormhole avoidance using disturbance-based routing schemes," *2009 6th International Symposium on Wireless Communication Systems*, Tuscany, 2009, pp. 76-80.

[2] S. Goyal, T. Bhatia and A. K. Verma, "Wormhole and Sybil attack in WSN: A review," *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2015, pp. 1463-1468.

[3] R. Mudgal and R. Gupta, "Study of various wormhole attack detection techniques in mobile ad hoc network," *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, Chennai, 2016, pp. 3748-3754.

[4] H. Ghayvat, S. Pandya, S. Shah, S. C. Mukhopadhyay, M. H. Yap and K. H. Wandra, "Advanced AODV approach for efficient detection and mitigation of wormhole attack in MANET," *2016 10th International Conference on Sensing Technology (ICST)*, Nanjing, 2016, pp. 1-6.

[5] D. Goyal and M. R. Tripathy, "Routing Protocols in Wireless Sensor Networks: A Survey," *2012 Second International Conference on Advanced Computing & Communication Technologies*, Rohtak, Haryana, 2012, pp. 474-480.

