www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 10 October, 2014 Page No. 8668-8672

Protecting AODV from Wormhole Attack in WSN

Harleen kaur [1] ***, Neetu Gupta*** [2]

Department of ECE, GIMET
Amritsar, Punjab, India
Harleen.kaur15@yahoo.com

Abstract- Wormhole attack is a severe threat against ubiquitous sensor networks. Due to variety of proactive protocols used in the network DSDV does not exploit the large network. AODV is an effective routing protocol for networks that doesn't maintain any routing tables at nodes which results in less overhead and more bandwidth. The connection setup delay is lower. MRT will work efficiently only when wormhole node will come in the path from source to destination. In this paper detection and isolation of the wormhole has been proposed. This approach is implemented using NS-2. The results and conclusions are shown in the paper.

***Keywords* – Wormhole, Ad-Hoc on Demand Distance Vector Protocol Vector (AODV), Mobile Ad-hoc Network.**

I. Introduction

Wireless sensor is small or large nodes called as sensor nodes and they are linked or connected with each other. WSN contains micro-controller, circuit for interface between sensor node and battery, a radio transceiver with antenna for generating the radio waves through which they can communicate and perform operations [1]. With the rapid development in wireless technology, ad hoc network have emerged to attract the attention from industrial and academic research projects. The wormhole attack is one of the major attack commonly involves two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out of bound channel available only to the attacker.

The paper is organized as follows: section I will talk about the simulation environment of this protocol, section II covers the wormhole attack and model, section III discusses the AODV model, section IV will discuss the design of the network needed by the protocol while section V shows the structure and discussions of technique, section VI will provide details on the protocol and how it provides the routing information and the final conclusion is described in section VII.

II.WORMHOLE

In the wormhole attack, an attacker tunnels messages received in one part of the network over a low latency link and replays them in a different part. The simplest instance of this attack is a single node situated between two other nodes forwarding messages between the two of them. An attacker situated close to a base station may be able to completely disrupt routing by creating a well placed wormhole. An attacker could convince nodes who would normally be multiple hops from a base station that they were only one or two hops away via the wormhole. This can create a sinkhole: since the attacker on the other side of the wormhole can artificially provide a high-quality route to the base station, potentially all traffic in the surrounding area will be drawn through if alternate routes were significantly less attractive. This will most likely always be the case when the end point of the wormhole was relatively far from a base station.

A Wormhole attack model

A particularly severe security attack, called the wormhole attack, has been introduced in ad-hoc networks [4], [5], [6]. During the attack [7] an adversary receives packets at one location in the network and tunnels them to another location in the network, where the packets were resent into the network, is illustrated in Fig 2. From an attacker's perspective, each of the attack's modes benefits is analysed.

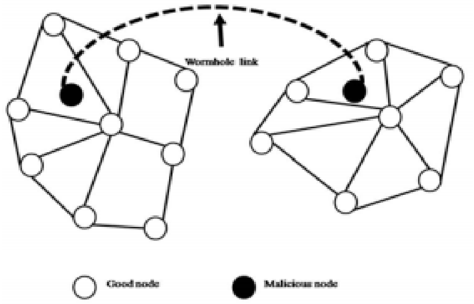

Fig.1The Wormhole Attack

III. AODV

AODV [8] is a reactive routing protocol developed for MANET which uses traditional routing table with one entry per destination. In this routing protocol, routes are established dynamically at intermediate nodes. Each node maintains sequence numbers to determine freshness of routing information and avoid routing loops. Another important feature is the maintenance of timer-based state, which is required to decide whether a routing table entry is expired or not. The route discovery process in AODV starts with the broadcast of route request (RREQ) packets by a source (S), who wants to send a packet to a destination (D) for which it does not have any route information. A recipient of RREQ first checks the sender ID and broadcast ID included in the RREQ packet to make sure whether it has already received the same RREQ. If not, it stores the sender ID as a reference for reverse path, increments the hop count field, and rebroadcasts the RREQ in its vicinity. This process is continued until a route to the destination (D) is found. Fig.2 shows the broadcast RREQ from the source (S) that is received by nodes A, E and G. Upon receiving the first RREQ, the destination (D) replies with RREP back to the source (S). In the given scenario, there are three ways to reach the destination (D) from the source (S): S-G-F-D, S-A-B-C-D, and S-E-B-C-D. Since S-G-F-D is the shortest path (3 hops), D first receives RREQ through this path. The RREP packet follows the reverse path where the RREQ arrived. So, RREP from D will reach node S through the path D-F-G-A, which is also selected as the route for exchanging packets between them [23].

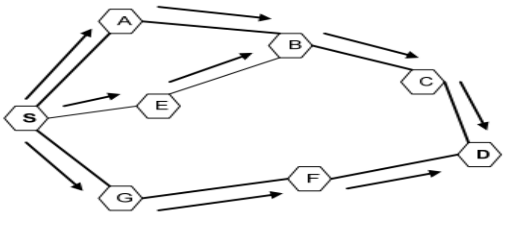

Fig 2.Propagation of RREQ packets

IV. METHODOLOGY

The methodology uses mobile node 1 as a source of the wormhole tunnel and mobile node 55 used as wormhole sink. Wireless attributes create the tunnel between source and sink. Initially simulation is carried out without malicious node. Then after two malicious nodes, node 27 and node 46 created a wormhole tunnel by increasing their transmission range. In this work, the nodes are used that exhibit wormhole behaviour in wireless network that uses the AODV protocol. CBR packet size is chosen to be 64; interval is set to 0.1sec; time interval is of 6.2 sec. and the simulations were run and results were obtained from different scenarios using NS2 simulator [16]. NS2 gives output in two different forms i.e. NAM and trace files, we used both to analyse the results.

Simulation of the wormhole attack is created with animated rate of 5ms and movement of the nodes are started at 0.1sec in the network. At 2.0 sec all the mobile nodes are placed in the area of 40m.Now divide the network into number of clusters. Each cluster has its own leader i.e. its own cluster head. The cluster head is elected on the basis of energy the node having the highest energy is elected as the leader. To each cluster data tracker is assigned. Data tracker contain all the information about the number of nodes in the cluster, number of packets forwarded and receive and communication path. When CBR is attached with UDP, communication between the nodes is started. After 14sec tunnel is created between the two nodes i.e. wormhole is present. Wormhole is detected if threshold value (number of forwarded packets – number of received packets) is more and to isolate the scheme two nodes are created in the path through which data packets are send.

V. PROPOSED WORK

The methodology is to discover wormhole in the route suggest by AODV protocol by using data trackers in which wormhole detection is performed between all the possible combination of nodes and decision will be taken on the basis of each and every possible combination If wormhole is detected in any of possible combination then whole suggested path is consider to be as wormhole effect path elsewhere if all the combination is wormhole free then path is consider to be as worm hole free path.

Proposed Algorithm

1. Divide the network in number of zones information of number of nodes and packet routing.
2. Select the leader for the respective zones giving the information of each node.
3. Assign the data tracker for each zone keeping the track of data send and received by the destination.
4. Mismatch between data sent by source and received by destination will lead to the detection of the wormhole in the network.
5. If the number of received packet - number of forwarded packets was more.
6. Isolate the wormhole nodes from the network by sending alert messages to the nodes.
7. Nodes after receiving the alert message will not communicate with the wormhole.

The flowchart of simulation is shown below in fig.3.

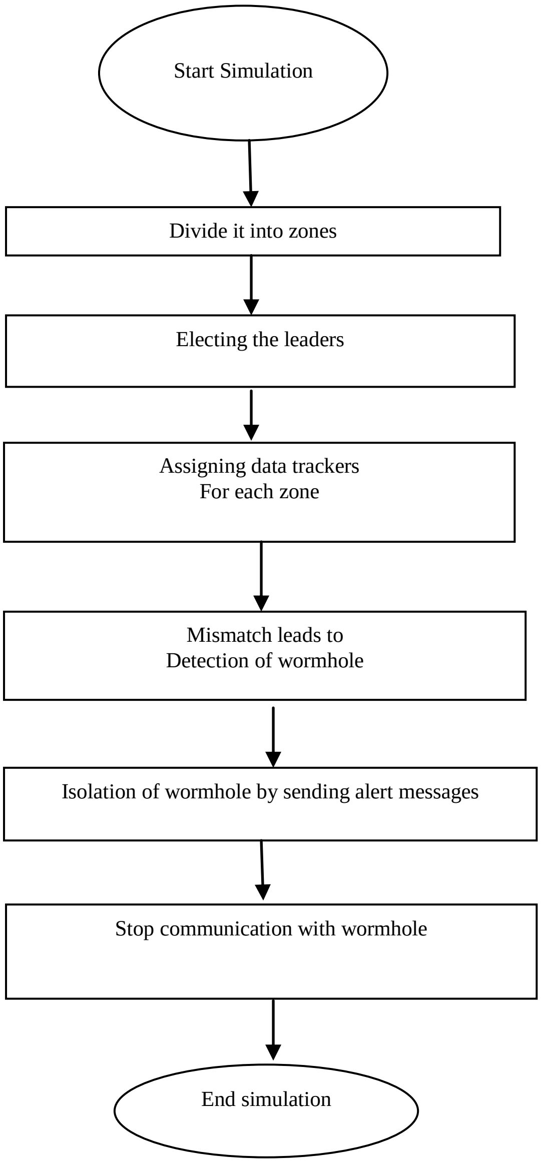

Fig. 3: Overall Processes

VI. RESULTS

The proposed algorithm is implemented using NS-2.The simulated NAM outputs of different scenarios are analysed. The network is developed based on X graphs and network animator using NS-2 Simulator. The metrics used to measure the performance of the network are PDR, throughput, average energy and overhead.

From Fig.4, an overhead of 1.75 is observed which signifies the amount of routing required to transmit the data in the network is 1.75 times the data packets.

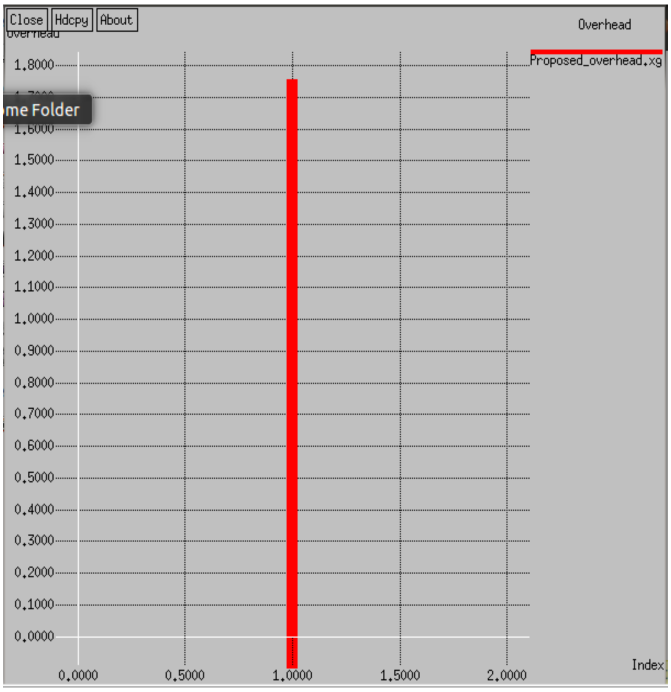

Fig.4: Overhead

Fig.5 depicts the network throughput. Network throughput is the amount of data that is received. In our study we have calculate the throughput on the node around which tunnel is formed. During the normal communication the throughput value was observed to be around 32 Kbps which drops to zero which signifies that tunnel has been made and the node is not receiving any data. The increase in the throughput is after preventing the wormholes and making a new path to resume the communication.

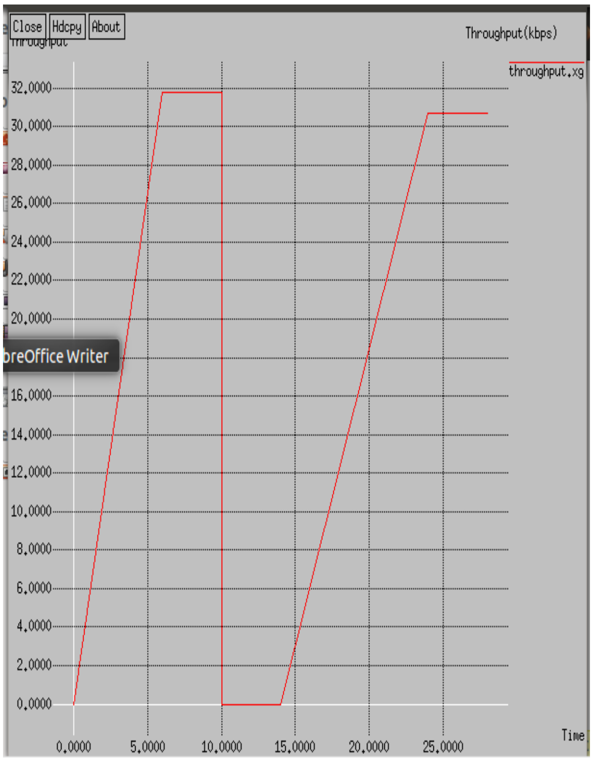

Fig.5: Throughput

Fig.6 shows energy consumption. The percent energy consumed by a node is calculated as the energy consumed to the initial energy. And finally the percent energy consumed by all the nodes in a scenario is calculated as the average of their individual energy consumption of the nodes.

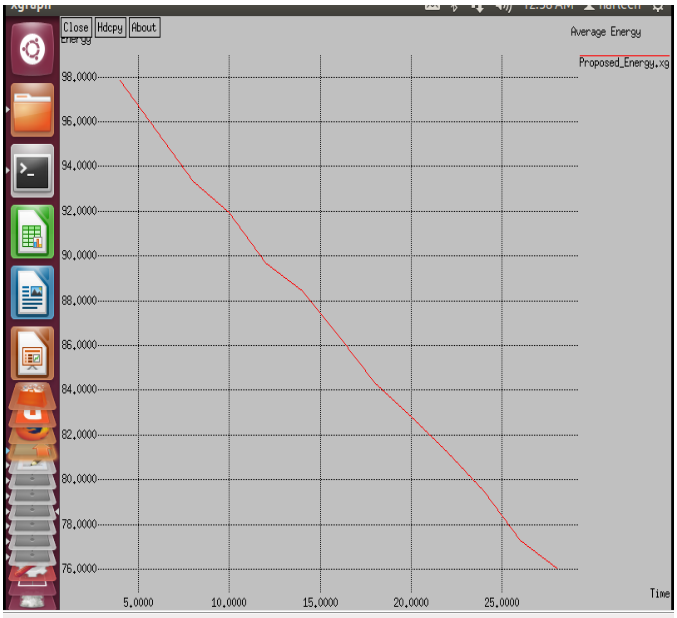

Fig.6: Average Energy

Packet delivery ratio is the ratio of number of packets received at destination node to that of number of packets sent by source node. PDR decreases drastically indicating the formation of tunnel and increase afterwards depicts formation of new path to resume the communication as show in Fig.7.

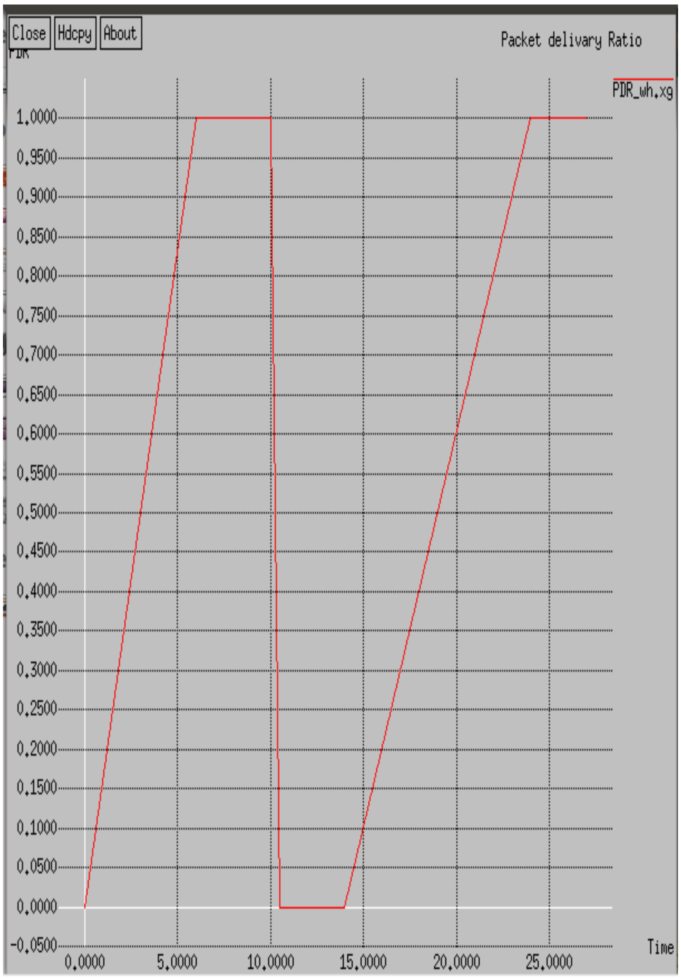

Fig.7: Packet Ratio

VII. CONCLUSIONS

The deployment of mobile nodes in an attended environment makes the network vulnerable. This thesis gives a bird eye over WSN and their security threat mainly Wormhole attack. Wormhole is a very serious threat over WSN that present an illusion of shortest path and try to attack all the traffic over the network.

REFERENCES

[1] Issa Khalil, Saurabh Bagchi, Ness B. Shroff, “LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks”, International Conference on Dependable Systems and Networks, pp. 0-7695, 2005.

[2] Yih-Chun Hu,Adrian Perrig ,David B.Johnson, “Wormhole attacks in wireless networks” IEEE Journal on Selected Areas in Communications, vol. 24, pp. 0733-8716,February2006,.

[3] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures”, IEEE International Workshop on Sensor Network Protocols and Applications (WSNA), pp. 113-127, 2003.

[4] Y. C. Hu, A. Per rig, and D. B. Johnson, "Packet Leashes: A Defence Against Wormhole Attacks in Wireless Networks," Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), pp. 1976-1986, 2003.

[5] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," Network and Distributed System Security Symposium (NDSS), San Diego, 2004.

[6] K. Lee, H. Jeon, and D. Kim, "Wormhole Detection Method based on Location in Wireless Ad-Hoc Networks," New Technologies, Mobility and Security: Springer Netherlands, pp. 361-372, 2007.

[7] Bintu Kadhiwala and Harsh Shah, "Exploration of Wormhole Attack with its Detection and Prevention Techniques in Wireless Ad-hoc Networks", International Conference in Recent Trends in Information Technology and Computer Science, 2012.

[8] Devendra Singh, Kushwaha Ashish Khare, J. L .Rana, " Improved Trustful Routing Protocol to Detect Wormhole Attack in MANET" International Journal of Computer Applications,vol.62, January 2013.

[9] Saurabh Gupta,Subrat Kar ,S Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet", IEEE International Conference on Innovations in Information Technology,2011.

[10] Nish ant Sharma et al., "Various Approaches to Detect Wormhole Attack in Wireless Sensor Networks”, International Journal of Computer Science and Mobile Computing, vol.3, issue.2, pp. 29-33 February 2014.

[11] C.E. Perkins & P. Bhagwat, "Highly Dynamic Destination Sequence-Vector Routing (DSDV) for Mobile Computers", Computer Communication Review, vol. 24, pp. 234-244, 1994.

[12] Vijayalaskhmi M."QoS Parameter Analysis on AODV and DSDV Protocols in a Wireless Network", International Journal of Communication Network & Security, vol.1, 2011.