Grenze International Journal of Engineering and Technology, Special issue

A Trusted Framework for MANET to Mitigate WORMHOLE Attack

J. Gautam[1], V.J. Susmitha[2], A. Sivadharshini[3] and B.Vijayalaxmi[4]
[1]Assi. prof, Department of Information Technology, K.L.N college of Engineering, Pottapalayam
gautamjprakash@gmail.com
[2-4]Department of Information Technology, K.L.N. college of Engineering, Pottapalayam
susmivj@gmail.com, dharshini1992015@gmail.com, viji06bala@gmail.com

***Abstract*—A Mobile Ad-hoc Network (MANET) is an accumulation of nodes where these nodes are connected through the radio signals i.e., Wireless link. These nodes form a dynamic infrastructure i.e., portable and it can easily come and get out from the network. There is no central administrator for coordinating these devices. Each node of MANET acts as a router that finds out a suitable path for forward a packet from source to destination. On process of routing, the nodes may affect by security threats. In wormhole attack, two or more malicious nodes produce a virtual tunnel to record a transmitted packets from one location and tunnels all the packet to the another location. In this paper, the problem of mitigating wormhole attack that refuse to forward the packets has been addressed. The simulated result shown to be detrimental to network performance, lowering the packet delivery ratio and increasing end-to-end delay. A new technique has been proposed to provide secure routing in MANET using a trusted framework that ensures all the nodes that participate in the routing process have optimal efficiency and better packet transfer rate. This research is based on mitigating the wormhole attack using Trusted AODV. This is simulated using NS-3 and its performance is compared with normal AODV protocol. This analysis shows that Trusted AODV protocol mitigates the wormhole attack efficiently and provide secure path for routing.**

***Index Terms*— Mobile Ad-hoc Network, AODV, Wormhole Attack, Trust.**

I. INTRODUCTION

Network is the spine for telecommunication, Wi- Fi networks like cellular network. As aftermath of the remarkable exploit of hand held gadgets Mobile Ad-Hoc Network (MANET)is a thriving technology in today's scenario. Over the past few years, Mobile Ad-hoc Networks (MANETs) have emerged in many forms thanks to the unprecedented development within the wireless communication technology. The primary features of MANETs include no infrastructure, shared broadcast channel, insecure wireless environment, no central administration, dynamic topology, and limited resources. It is also an independent, autonomous system, where nodes are connected with each other through wireless links. In MANETs, each node communicate neighboring nodes that are in its transmission vary and works each as a number furthermore as a router. In order to communicate with non- neighbors, a node establishes indirect connection with the help of other nodes in its neighborhood in a hop- by-hop manner. MANET is Open access network so any node can join or leave at any time freely. Mobile Ad-Hoc network can change rapidly because the nodes move freely. This property of the

Grenze ID: 01.GIJET.5.1.25

nodes makes the MANET unpredictable from topology and scalability. The communication path between pairs of nodes may have multiple links. The security in such networks is major concern. A MANET is a multi-hop temporary proclamation network of cell nodes that operates with Wi-Fi transmitters and receivers without the assistance of any pre-existing network infrastructure. The nodes are equipped to move freely. Every node can participate in the venture of transferring the packets. The nodes keep up a correspondence through sending packets to distinct nodes within its radio range. Routing meet specified standards with a chief function in the safety of the entire network. Thus, these operations bring several security issues in MANET. In nature by default wireless affiliation characteristics vary in time: The area unit transmission impediments like weakening, path loss, blockage and interference that adds to the prone behavior of wireless channels. The responsibility of wireless transmission is resisted by various factors. Packet losses attributable to errors in transmission MANETs expertise higher packet loss attributable to factors like hidden terminals that ends up in collisions, wireless channel problems (high bit error rate (BER)), interference, frequent breakage in ways caused.

II. RELATED WORKS

[1]RTT and buffer length based approach:
Richa Mudgal and Rohit Gupta [1]in the year 2016 proposed an efficient method and secure routing using the concept of RTT and buffer length against wormhole routing. Using this approach, the routing overhead minimizes and the packet send at the time of routing increase. The malicious node is identified by comparing RTT value of each node hop count and buffer length the time based threshold value is derived for locating malicious node. This method produced maximum security and minimize the routing overhead.
[2]AODV protocol:
Gulzar Ahmad Wani and Sanjay Jamwal [2] in the year 2016 proposed a method of consequences of wormhole attack using AODV protocol. This method uses the AODV protocol it is a reactive protocol that the node that initiated the request uses the route containing the least number of hops through other nodes. The routing table contain the source, destination and sequence number.to find neighbor hello message is used. Hello message is used to find active of route.
[3]Trust routing:
Shabina Parbin and Leeladhar Mahor [3] in the year 2016 proposed a method of trusted mechanism and reputation method for trusted location in the MANET by applying base station.it provide the estimate of the trust worthiness. the calculation of the RREQ routing trustiness is still a major problem calculate the trust value and finding the trusted location and send the trusted message during the routing.
Detection of wormhole attack:
[4]H.Ghayvat, S.Pandya, S.Shah, S.C.Mukhopadhyay, M.H.Yap and K.H.Wandra in the year 2016 used the digital signature method to mitigate wormhole attack it analyze the overall time taken to tunnel the packet and set the static threshold value based on the tunneling and threshold value it decide whether the given node is malicious node or the trusted node. afterward using digital signature and hashing algorithm to detect the malicious node.
[5]Throughput based approach:
Roshani Verma,Roopesh Sharma and Upendra Singh in the year 2017 uses the approach to prevent the wormhole attack based on the maximum throughput utility and also hop based approach it start the route discovery and broadcast the route request.by identify the route it verify the destination node. this process is repeated until destination is reached during routing packet deliveryratio and round trip time is calculated if the PDR is less than 1 then the node is said to be the wormhole node and announced it to other node it is wormhole node and send the RERR to that path.
[6]Absolute based approach:
Sayan Majumder and Dr. Debika Bhattacharyya in the year 2018 using the approach of the absolute deviation statistical method it first set the route request after finding the route it send route replay from destination to the source the time delay is calculated and mean absolute is obtained for all variable and divided by the statistical deviation and then calculated the covariance after calculating the value it check it is in the range or discard otherwise.

III. PROPOSED METHOD

The dynamic nature of MANET makes it vulnerable to variety of security threats like Wormhole attack, Eavesdropping, Blackhole attack etc. Due to the Self-Configuring nature & lack of Central Administrator, MANET needs a secured protocol to ensure its Quality of Service. MANET being an network with an instant set up feature it is recommended to design a framework to overcome all the limitations of MANET and improve a reliable packet transfer. Based on the Trustworthy framework, mitigation of wormhole attack has been done to provide a secure routing in a network. The different modules are discussed as follows.

A. Network Simulation

Simulation is processed in NS-3. In our simulation, no route overhead was considered due to link stability and route lifetime. To increase average hop length of a route with relatively small nodes, 650 X 650 square area used and nodes are existing among these areas. 50 nodes are created. The transmission range is fixed at 100 meters. Maximum speed of node is set to 30 m/sec. The nodes are assigned with an initial position. All nodes are moving and the simulation second is 500 seconds. The yellow node represents source and destination, the intermediate nodes are red in color and pink node indicates wormhole node [Fig.1].

TABLE I. SIMULATION PARAMETERS

Parameter	Values
Coverage area	650m X 650m
Simulation Time	1000s
No of nodes	50
Traffic type	UDP-CBR
Packet Size	512 bytes
Maximum Speed	30 m/s
Routing Protocol	AODV
Mobility Model	Random Walk 2D

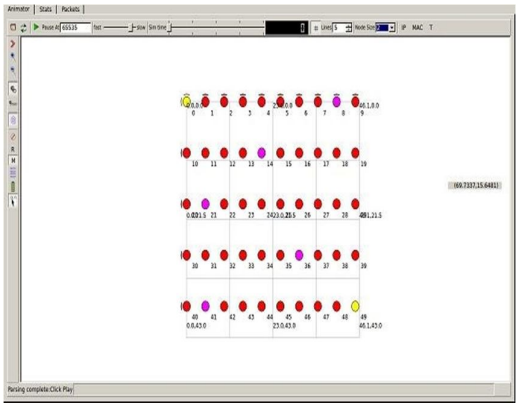

Fig.1 -Network Formation

B. Trust Framework

In this proposed approach we compute a trust value for each node present in the network. These trust values are based on the packet drop

i.e. The total number of packet dropped compared with the total number of packets sent by the source will generate the packet drop ratio. If the packet drop is very large irrespective of traffic and congestion it is considered as a malicious node, otherwise it should be a trusted node or it is highly trusted node. The trust value lies in the range of the 0-1. Comparing with malicious node the packet drop does not highly affect because of the traffic.

TABLE II. THRESHOLD COMPARISON

Value	Category
0-0.4	Selfish node
0.4-0.7	Trusted node
0.7-1.0	Highly trusted node

Selfish node: It acts as a malicious node which does not forward the packet to another node. In these nodes, the trust value would be minimum and it may drop the packet or modify the packet and may have a third party access. Such nodes are considered to be wormhole nodes and are to be isolated from the routing process

Trusted node: This category of nodes are trusted for a routing but has to be monitored periodically since their trust values are not at a satisfactory level. These nodes may lose its trustworthiness and converted into selfish nodes at any time. So these nodes are to be investigated periodically and routing is performed.

Highly trusted node: These category nodes will obtain a maximum trust value where every node has a guaranteed packet transfer feature. A route established with Highly trusted nodes are considered to be the best optimal route.

B. Trusted Routing Using Taodv:

- When a source node wants to send a packet to destination it starts route discovery process. During route discovery it broadcasts the route request (RREQ) to the neighboring node. Route request packet contains the destination address, hop count, source address, gateway. This Process iterates until it reaches the destination.
- The destination node send the RREP to the destination node the routing table is updated.
- Compute Packet Drop for each node by computing.

PACKET DROP = TOTAL NUMBER OF PACKET SEND --- NO OF PACKET SEND BY EACH NODE

$$\text{AVERAGE PACKET DROP} = \frac{\textit{TOTAL NUMBER OF PACKETS DROP}}{\textit{TOTAL NUMBER OF PACKETS}}$$

TRUSTED VALUE = 1 – AVERAGE PACKET DROP

- The calculated trust value of each node compared with threshold value. If all the n nodes in the established route are highly trusted then the path is fixed for routing and if any one node in the route is a selfish node then the path is ignored and new route discovery process in initiated.
- If a path consists of both Trusted and Highly Trusted nodes, the occupancy of highly trusted nodes is considered. When a path has more number of highly trusted nodes than trusted nodes then the path is chosen, ignored otherwise.
- This algorithm provides the secure and optimal path for the routing

C. Performance Analysis

Trusted AODV provides trusted path for routing and provide secure path to transmit the packet based on the packet drop ratio and throughput.

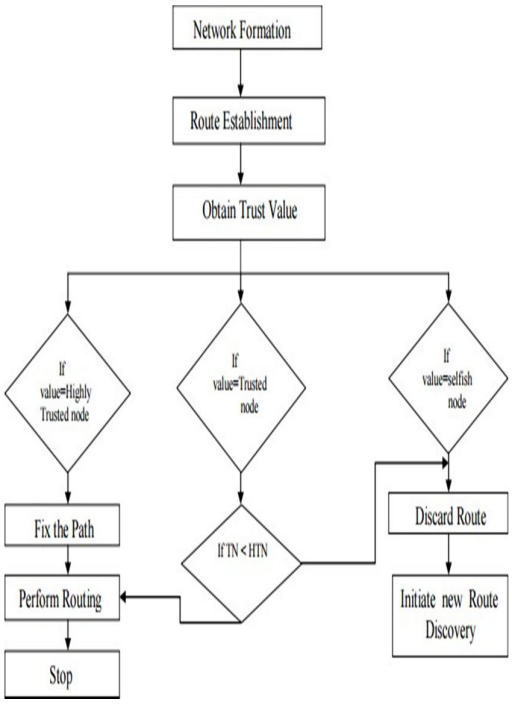

Fig.2 Trust based routing

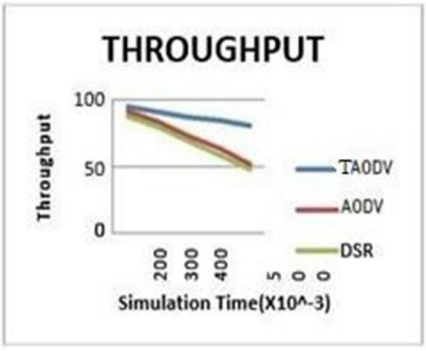

Fig. 3 Variation of throughput with time

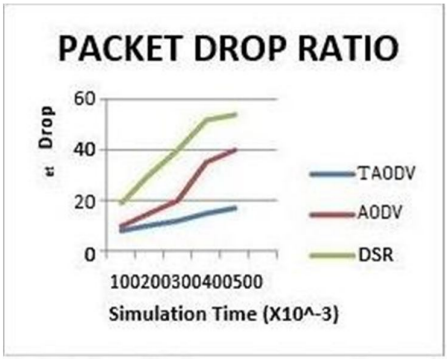

Fig .4packet delivery rate in TAODV

IV. Conclusion

In this paper, the malicious nodes which highly influence the performance of the network has been identified and isolated. A trusted framework has been designed and implemented for efficient service of the network. Using this trusted framework the Quality of Service of the network has been enhanced by focusing on major parameters such as Packet drop ratio, throughput and reliability. TAODV provides the secured optimal path for routing by ignoring the assumed wormhole nodes from the network. Our future work is to implement the trusted framework for various kinds of attack in network that degrades the quality of service.

References

[1] Richa Mudgal, Rohit Gupta "An Efficient Approach for Wormhole detection in MANET" ICTCS '16, March 04-05,2016, Udaipur, India.

[2] Gulzar Ahmad Wani, Sanjay Jamwal "Examination of AODV Routing Protocol with Wormhole Attack", International Journal of Computer Applications(0975 - 8887), Vol: 135-No. 5,February 2016.

[3] Shabina Parbin, Leeladhar Mahor "Analysis and Prevention of Wormhole Attack Using Trust And Reputation Management Scheme in MANET", International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT),2016.

[4] H.Ghayvat,S.Pandya,S.Shah,S.C.Mukhop adhyay,M.H.Yap and K.H.Wandra, " An Advanced AODV approach for efficient detection and mitigation of wormhole attack in MANET", International Conference on Sensing Technology (ICST), 2016.

[5] Roshani Verma,Roopesh Sharma and Upendra Singh," New approach through detection and prevention of wormhole attack in MANET ", International Conference of Electronics, Communication and Aerospace Technology (ICECA), 2017.

[6] Sayan Majumder and Dr. Debika Bhattacharyya " Mitigating Wormhole Attack in MANET using Absolute Deviation Statistical Approach"

[7] Muhammad Imran, Farrukh Aslam Khan, Tauseef Jamal, Muhammad Hanif Durad, "Analysis of Detection Features for Wormhole Attacks in MANETs", International Workshop on Cyber Security and Digital Investigation(CSDI 2015).

[8] Aakanksha Kadam, Niravkumar Patel, Vaishali Gaikwad "Detection and Prevention of Wormhole attack in MANET ",IRJET ,Vol: 03 Issue: 03 | March-2016.

[9] Amit Rawat, Radhika Manjusha "The Effects of Various Wormhole Detection Techniques",IRJET ,Vol: 03 Issue: 12 | December-2016.

[10] Sunil Kumar Jangir and Naveen Hemrajani, "A Comprehensive Review On Detection Of Wormhole Attack in MANET", IEEE 2016.

[11] Ashka Shastri and Jignesh Joshi, "A Wormhole Attack in Mobile Ad-hoc Network:Detection and Prevention", ICTCS '16, March 04-05,2016, Udaipur, India.

[12] Weichao Wang, Bharat Bhargava, Yi Lu and Xiaoxin Wu, "Defending against wormhole attacks in mobile ad-hoc networks", January 2006 in Wiley Interscience.

[13] Niki Tsitsiroudi; Panagiotis Sarigiannidis; Eirini Karapistoli; Anasta- sios A. Economides, EyeSim: A mobile application for visual-assisted wormhole attack detection in IoT-enabled WSNs at 9th IFIP Wireless and Mobile Networking Conference (WMNC) (2016).

[14] Megha Sharma; Ajay Khunteta; Deepak Sharma : Fuzzy integrated HMM model for communication optimization under wormhole attack in mobile network 2015 International Conference on Applied and Theoret- ical Computing and Communication Technology (iCATccT).

[15] Mostefa Bendjima, Mohammed Feham : Wormhole attack detection in wireless sensor networks, at SAI Computing Conference (SAI) 2016.

[16] Rakhil R; Rani Koshy : An efficient algorithm for Neighbor Discovery and wormhole attack detection in WANET, In International Conference on Control Communication & Computing India (ICCC), 2015.

[17] Meng-Hsiu Jao; Ming-Hsuan Hsieh; Kuan-Hsien He; Dai-Hua Liu; Shu- Yu Kuo;Ting-Hui Chu; Yao-Hsin Chou : A Wormhole Attacks Detection Using a QTS Algorithm with MA in WSN, In Systems, Man, and Cybernetics (SMC), 2015 IEEE International Conference.

[18] Akansha Shrivastava and Rajni Dubey, Wormhole Attack in Mobile Ad- hoc Network: A Survey, International Journal of Security and Its Applications Vol.9, No.7 (2015).

[19] Chitra Gupta; Priya Pathak. Movement based or neighbor based tehnique for preventing wormhole attack in MANET, In Symposium on Colossal Data Analysis and Networking (CDAN)(2016).

[20] Tapodhir Acharjee; Pinky Borah; Sudipta Roy, A New Hybrid Algorithm to Eliminate Wormhole Attack in Wireless Mesh Networks, International Conference on Computational Intelligence and Communication Networks (CICN)(2015).

[21] Jiu-hu Zheng; Huan-yan Qian; Lei Wang, Defense Technology of Wormhole Attacks Based on Node Connectivity, at IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)(2015).

[22] Aarfa Khan, Prof. Shweta Shrivastava and Prof. Vineet, Normalized Worm-hole Local Intrusion Detection Algorithm (NWLIDA), 2014 In- ternational Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 05, 2014.
[23] Juhi Biswas, Ajay Gupta, Dayashankar Singh, WADP: A wormhole attack detection and prevention technique in MANET using modified AODV routing protocol in 9th International Conference on Industrial and Information Systems (ICIIS)(2014).
[24] J. Anju, C. N. Sminesh: An Improved Clustering-Based Approach for Wormhole Attack Detection in MANET at Eco-friendly Computing and Communication Systems (ICECCS), 2014 3rd International Conference
[25] Khan, M. S., Jadoon, Q. K., & Khan, M. I. (2015). A Comparative Performance Analysis of MANET Routing Protocols under Security Attacks. In Mobile and Wireless Technology 2015.