International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 SJIF 2023: 8.176 ISSN: 2582-3930

SECURE ROUTING AGAINST WORMHOLE ATTACK IN MANETs

POOJA PATEL[1], MEGHA PAPEL[2]
[1]*Lecturer, Computer Department, MLIDS, MEHSANA, INDIA*
[21]*Lecturer, Computer Department, MLIDS, MEHSANA, INDIA*

***Abstract*: The abstract describes a secure routing algorithm designed to detect and prevent wormhole attacks in Mobile Ad hoc Networks (MANETs). The proposed algorithm utilizes a threshold-based approach to detect malicious links, where suspicious nodes are added to a suspicious list and their shortest paths to the destination are calculated. One-hop true neighbors are then queried for alternative paths to the suspicious node that are not direct, and if any path is less than the threshold value, the link is declared safe. Otherwise, the link is declared malicious and the presence of an attack is reported. The proposed algorithm is evaluated through simulations and compared with other existing algorithms, and results show that it effectively detects and prevents wormhole attacks in MANETs with high accuracy and low overhead.**

***Keywords*: Secure routing, Wormhole attack, Mobile Ad hoc Networks (MANETs), threshold-based approach, suspicious list, shortest path, one-hop neighbors, and alternative paths.**

Introduction

Mobile Ad hoc Networks (MANETs) are self-configuring networks of mobile nodes that communicate with each other without the need for a fixed infrastructure. Due to their decentralized nature, MANETs are vulnerable to a variety of security attacks, including wormhole attacks, which can seriously compromise the routing functionality of the network. Wormhole attacks involve an attacker creating a shortcut between two distant points in the network, causing traffic to be routed through the attacker's node. This can result in the attacker intercepting and modifying traffic, as well as launching other attacks.

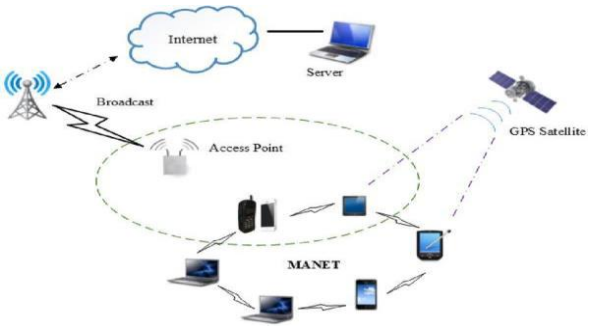

Figure 1: Architecture of MANET [17]

To address this problem, various secure routing algorithms have been proposed for MANETs. One such algorithm is a threshold-based approach, where a suspicious list is maintained, and nodes suspected of being part of a wormhole attack are added to the list. The shortest path from the source to the destination is then calculated, and one-hop true neighbors are queried for alternative paths to the suspicious node that are not direct. If any path is less than the threshold value, the link is declared safe; otherwise, it is declared malicious and the presence of an attack is reported.
In this way, the proposed algorithm effectively detects and prevents wormhole attacks in MANETs with high accuracy and low overhead.

Wormhole Attack

Wormhole attack is hard to detect because this attack does not inject abnormal volumes of traffic into the network. In a wormhole attack, attackers "tunnel" packets to another area of the network bypassing normal routes as shown in Figure1.7. In practice, attackers can use high power antennas or a wired link, or other methods. The resulting route through the wormhole may have a better metric, i.e., a lower hop-count than normal routes. With this leverage, attackers using wormholes can easily manipulate the routing priority in WSN to perform eavesdropping, packet modification or perform a DoS (Denial of Service) attack, and so on. The entire routing system in WSN can even be brought down using the wormhole attack.

The wormhole attack can strictly deteriorate the presentation and cooperation the safety of a sensor network through spoiling the routing protocols and weakening the security enhancements. What makes it even easier for attackers is the fact that routing protocols are not designed having security threats in mind. As a result, deployments of sensor networks not often include safety protection and small or no effort is frequently necessary from the side of the attacker to perform the attack [1].

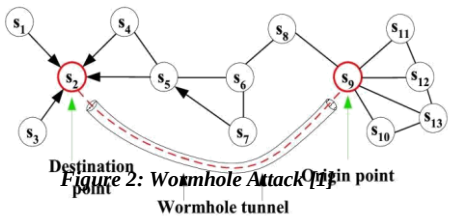

Figure 2: Wormhole Attack [1]

Proposed Work

Aim: Secure Routing against Wormhole Attack in Mobile Ad hoc Network

Protocol Used: Ad-hoc on-demand distance vector (AODV)

Ad-hoc On-demand Distance Vector (AODV)

AODV Routing Protocol: AODV (Ad-hoc on Demand Distance Vector) is a reactive protocol [12].The reactive routing protocols do not periodically update the routing table like table driven proactive protocols. It is the modification of DSDV (Destination Sequence Distance Vector). It provides uncast, multicast broadcast. It works on, on demand algorithm. It searches for route between nodes only as decide by source nodes. These routes are maintained as long as they are needed by source. AODV builds route using route request and route reply query cycle. It is the loop free, self starting scale to large number of nodes. AODV is a well known distance vector routing protocol [9] and it works as follows. Whenever a node wants to communicate with another node, it looks for an available path to the destination node, in its local routing table. If there is no path exists, then it broadcasts a route request (RREQ) message to its neighborhood nodes. Any node that receives this message for route discovery looks for a path leading to the respective destination node. The important feature of AODV is the maintenance of time based states. This means that routing entry which is not used recently is expired. The intermediate nodes store the route information in the form of route table. Control messages used for the discovery and breakage of route are as follows:

- Route request message (Rreq)
- Route reply message (Rrep)
- Route error message (Rerr)

Proposed Approach

Mostly Algorithm stands for throughput improvement and increase detection accuracy. Algorithm only works on to detect the wormhole attack. Like if we try to detect wormhole attack then it is possibility that it may increase detection accuracy and it's improving throughput. WSN have centralized approach in term of network control. Data flows from sender nodes towards a few aggregation points which further forward the data to base station. The AODV is a routing protocol that creates a route to the destination on demand. The source node does not have a direct connection to the destination. The source node generates a route request that it broadcast to its neighboring nodes.
Here in our Proposed Work we try to detect three of wormhole attack to improve throughput and increase accuracy by applying AODV Protocol. Our Algorithm checks the RTT and Route length to detect wormhole attack. Our proposed Algorithm is given below:

Proposed Algorithm

Step 1: Start
Step 2: Sender Broadcast route request and Record Time.
Step 3: Receiver Receive RREQ and send back RREP.
Step 4: check the RREP arrive before time Out?
If the RREP arrive before timeout than go to step (13) otherwise go to next step.
Step 5: Add node into suspicious list.
Step 6: calculate the shortest path to the suspicious node.
Step 7: Shortest path does not include node as one hop neighbors. The direct path also not considers.
Step 8: Ask all the 1 hop true neighbors to find alternative path to the suspicious node which is not direct and report the number of hops.
Step 8: If the length of any path is less than the value of threshold then go to next step otherwise go to step (11).
Step 9: Delete node from suspicious List and Declare as safe link.
Step 10: Stop.
Step 11: The Link is announced as malicious link and presence of an attack is found.
Step 12: stop.
Step 13: No Wormhole.

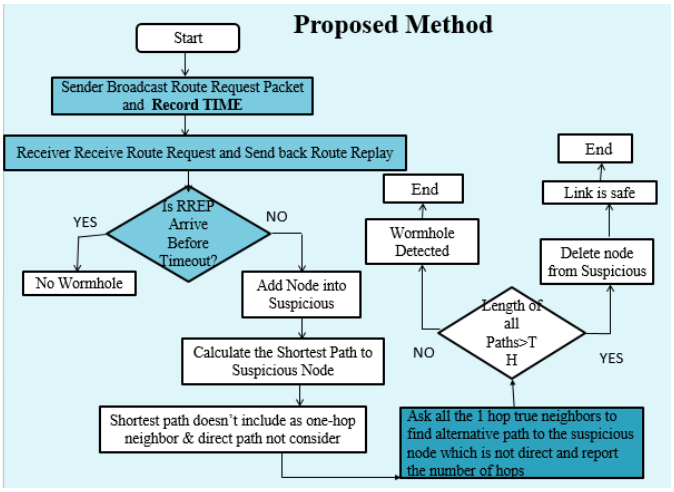

Figure 3: Proposed Method

Implementation and Result

For implementation we have used NS2. The simulation parameters are as follow:

Simulation area	500m x 500m
Routing protocol	AODV
Size of packet	512 bytes
Traffic rate	CBR
Number of nodes	10, 25, 35,45
Range of transmission	150m
Simulation time	200s
Mobility model	Random way point

Table 1: Simulation parameters

Fig 4: NAM File for 10 Nodes Wormhole Affected AODV Protocol

Fig 5: NAM File for 25 Nodes Wormhole Affected AODV Protocol

Fig 6: NAM file for 35 nodes wormhole affected AODV protocol

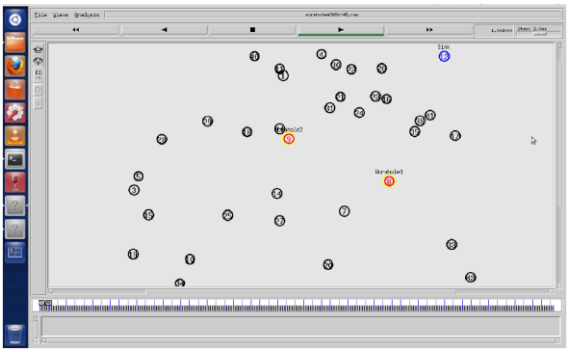

Fig 7: NAM File for 45 Nodes Wormhole Affected AODV Protocol

We have measured Packet delivery ratio, throughput and End-to-End Delay for normal scenario, attacking scenario.

1. Packet Delivery Ratio:

The ratio between the total number of packets received by destination nodes and the total number of packets generated by source nodes.

Packet Delivery Ratio = Received packets / Sent packets

 For 10 Nodes in normal scenario the packet delivery ratio is 94.67 percentages while in attacking scenario it decreases to 51.24 percentages and after applying proposed method its increase to 90.19 percentages

 For 25 Nodes in normal scenario the packet delivery ratio is 87.99 percentages while in attacking scenario it decreases to 72.25 percentages and after applying proposed method its increase to 78.25 percentages.

 For 35 Nodes in normal scenario the packet delivery ratio is 96 percentages while in attacking scenario it decreases to 73.66 percentages and after applying proposed method its increase to 87.88 percentages.

 For 45 Nodes in normal scenario the packet delivery ratio is 98.45 percentages while in attacking scenario it decreases to 76.14 percentages and after applying proposed method its increase to 95.34 percentages

2. Throughput:

Throughput is the no. of data packets delivered from source to the destination per unit time. As packet may get lost during transmission, it is one of the parameter which measures the efficiency of the protocol.

Throughput = Total received packets at destination / Total simulation time (bytes/sec)

 For 10 Nodes in normal scenario the throughput is 83.63 kbps while in attacking scenario it decreases to 48.09 kbps and after applying proposed method its increase to 80.81 kbps.

 For 25 Nodes in normal scenario the throughput is 79.24 kbps while in attacking scenario it decreases to 66.67 kbps and after applying proposed method its increase to 73.96 kbps.

 For 35 Nodes in normal scenario the throughput is 86.41 kbps while in attacking scenario it decreases to 67.24 kbps after applying proposed method its increase to 82.14 kbps

 For 45 Nodes in normal scenario the throughput is 88.67 kbps while in attacking scenario it decreases to 69.52 kbps and after applying proposed method its increase to 85.47 kbps.

Experimental Result

Here we have shown the Comparison table for normal scenario and with attacking scenario for packet delivery ratio, throughput and comparison of proposed method and base method for 10 nodes, 25 nodes, 35 nodes and 45 nodes.

1. Packet Delivery Ratio Result

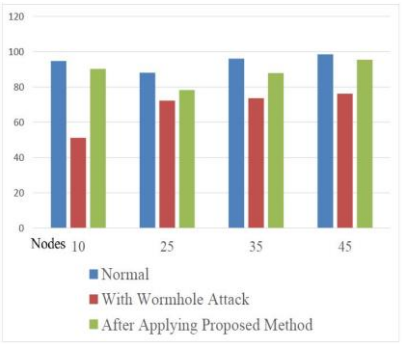

Fig 8 Packet Delivery Ratio (%) v/s No. of Nodes

2. Throughput Result

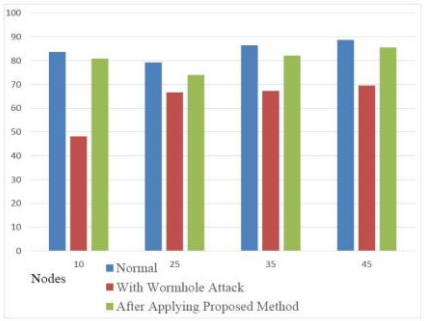

Fig 9 Throughput (Kbps) v/s No. of Nodes

3. Comparisons between proposed method and base method for PDR

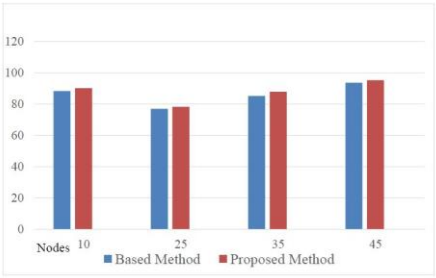

Fig 10 Comparison of Based Method and Proposed Method for Packet Delivery Ratio (%)

4. Comparisons between proposed method and base method for throughput

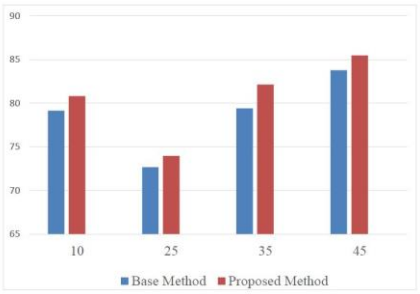

Fig 11 Comparison for Based method and Proposed Method for Throughput (Kbps)

Conclusion

We have proposed a new robust wormhole detection algorithm based on traversal time and hop count analysis without using any hardware and also network cost is low. The detection process is dependent on accurate packet processing time measurements on intermediate nodes. We compare the simulation results of various parameters like average end to end delay, packet delivery fraction and average throughput of basic AODV and wormhole attack and proposed algorithm.

References

[1] J Muhammad Imran, Farrukh Aslam Khan, Tauseef Jamal, Muhammad Hanif Durad,"Analysis Of Detection Features For Wormhole Attacks In Manets ", Elsevier, Procedia Computer Science 56(2015) 384-390.

[2] Hon Sun Chiu And King-Shan Lui ,"Delphi: Wormhole Detection Mechanism For Ad Hoc Wireless Networks " IEEE- 2006.

[3] Soo-Young Shin, Eddy Hartono Halim," Wormhole Attacks Detection In Manets Using Routes Redundancy And Time- Based Hop Calculation" IEEE 2012.

[4] Sun Choi, Doo-Young Kim, Do-Hyeon Lee, Jae-Il Jung , "Wap: Wormhole Attack

[5] Prevention Algorithm In Mobile Ad Hoc Networks, "2008 IEEE International Conference On Sensor Networks.

[6] Saurabh Gupta, Subrat Kar, S Dharmaraja, "Whop: Wormhole Attack Detection Protocol Using Hound Packet" IEEE -2011 International Conference On Innovation In Information Technology.

[7] Parmar Amish, V.B.Vaghela , "Detection And Prevention Of Wormhole Attack In

[8] Wireless Sensor Network Using Aomdv Protocol" Elsevier, Procedia Computer Science 79(2016) 700-707.

[9] Mohanmmand Rafiqul Alam, King Sun Chan,"RTT-Tc :A Topological Comparison Based Method To Detect Wormhole Attacks In MANET" IEEE- 2010.

[10] Umesh Kumar Chaurasia, Mrs. Varsha Singh,"Maodv: Modified Wormhole Detection AODV Protocol" IEEE-2013.

[11] Neha Agrawal, Nitin Mishra," RTT Based Wormhole Detection Using Ns-3" IEEE 2014 Sixth International Conference On Computer Intelligence And Computer Networks.

[12] Y. C. Hu, A. Perrig, And D. B. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks In Wireless Networks," Proc. IEEE Conf.Infocom, April 2003.

[13] X. Hu And D. Evans, "Using Directional Antennas To Prevent Wormhole Attacks," Proc.IEEE Symp. Network And Distributed System, Security (Ndss 04), San Diego; February 2004.

[14] D. Djenouri, L. Khelladi And A.N. Badache. "A Survey Of Security Issues In Mobile Ad Hoc And Sensor Networks", Communications Surveys & Tutorials, IEEE, Vol. 7, Issue 4, Pp. 2--28, Fourth Quarter 2005

[15] Hoang Lan Nguyen, Uyen Trang Nguyen," A Study Of Different Types Of Attacks In Mobile Ad Hoc Networks", Department Of Computer Science And Engineering, 2012, IEEE.

[16] Yih-Chun Hu , Adrian Perrig, "A Survey Of Secure Wireless Ad Hoc Routing", IEEE Security And Privacy, V.2 N.3, P.28-39, May 2004.

[17] H Yang, H Y. Luo, F Ye, S W. Lu, And L Zhang, "Security In Mobile Ad Hoc Networks: Challenges And Solutions" (2004). IEEE Wireless Communications. 11 (1), Pp. 38-47.

[18] H.D.Trung, W.Benjapolakul, P.M.Duc, "Performance Evaluation And Comparison Of Different Ad Hoc Routing Protocols", Department Of Electrical Engineering, Chulalongkorn University, Bangkok, Thailand, May 2007.

[19] Asma Tuteja, Rajneesh Gujral, Sunil Thalia, "Comparative Performance Analysis Of DSDV, AODV And DSR Routing Protocols In MANET Using Ns2", International Conference