International Journal of Scientific Research in Computer Science and Engineering
Research Paper
Vol.5, Issue.5, pp.35-40, October (2017)
**E-ISSN:** 2320-7639

# Detection and Elimination of Wormhole Attacks in a MANET

**A.Vani**

Dept. of ECE, Chaitanya Bharathi Institute of Technology (Autonomous), Hyderabad, India

**Corresponding Author: vanialamur@cbit.ac.in*

**Available online at: www.isroset.org**

Received 11th Sep 2017, Revised 14th Sep 2017Accepted 19th Oct 2017, Online 30th Oct 2017

***Abstract***—Wormhole attacks in Mobile ad hoc networks is impermeable to traditional security measures. The attack can be launched regardless of the MAC, routing, or security protocol used in the network. Two or more malicious nodes in conspiracy usually perform the wormhole attack. Two malicious nodes at different locations send received routing messages to each other via a secrete channel. In this way, although the two malicious nodes are located far from each other, they appear to be within one-hop communications range. Wormhole nodes can successfully execute such attacks without compromising any computer, and are inevitable even though some ad hoc wireless networks provide authenticity and confidentiality protection. Practically all widespread security extensions are proposed for popular routing protocols but they do not alleviate wormhole attacks. However, since wormhole attack such a severe thread to MANET security. In this situation wormhole attack methodology presented is motivated by WARP and the same procedure and terminology is used but slight modification In this work wormhole attack is detected and eliminated by simply modifying AODV routing protocol and its performance is measured.

***Keywords—*** MANET, Routing, AODV, Wormhole attack, WARP

## I.INTRODUCTION

Mobile ad hoc network formed temporarily for emergency needs and emerged with great popularity because the networks has no fixed infrastructure, dynamic and scalable. These networks mainly used for battlefield and emergency conditions and hence security is the main problem. In a MANET, a node can join a network automatically if the network is in the radio range of the node, thus it can communicate with other nodes in the network. MANET is more susceptible to attacks when no secure boundaries used. These networks exposed to attacks due to their security vulnerabilities. Wormhole attack is the one of the most serious attack that affects the availability and confidentiality security services.

Rest of the paper is organized as follows, Section I contains the introduction of Mobile ad hoc networks , Section II contain the related work of Wormhole attacks, Section III contain the methodology and procedure for proposed algorithm, Section IV describe the results and discussions and Section V presents conclusion and future scope.

## II.RELATED WORK

Several solutions have been proposed in the literature for wormhole attacks in MANET.

In [1, 2], who introduced wormhole attacks in ad hoc networks, suggested the use of geographical or temporal packet leashes to detect wormholes. A geographical leash (location-and time-based approach) requires each node to know its own location and all nodes to have loosely time synchronized clocks. The nodes need to securely exchange the information and have to authenticate the location and time information.

S.Capkun, L.Buttyain, and J.-P. Hubaux, SECTOR: secure tracking of node encounters in multi-hop wireless networks [3].Presented a protocol (distance bounding approach) that is based on distance bounding and does not require synchronization or location information to prevent wormhole attacks. However, they depend on a secure challenge request-response and require accurate time measurements. They assumed that the network operates with central authority that controls the network membership and assigns unique identity to each node.

In [4], using Directional antennas to prevent worm hole attack (special hardware approach). They assumed that the antennas on all nodes are aligned (which may be difficult in practice) and share a secret key with each other

Khalil et al have developed two protocols to defend against wormholes: LITEWORP [5] and MOBIWORP [49].

LITEWORP (time-based and neighbor information approach) works with a static network and assumes that there is a guard node within the transmission range of any two neighboring nodes.

In [6] (centralized and connectivity information approach) presented a scheme to detect wormhole attacks based on statistical analysis. A protocol that is employing connectivity information to detect wormholes is presented in [7]

In [8] (distance bounding approach) proposed a distributed technique to detect in-band wormhole attacks in mobile ad hoc networks. The protocol is based on the propagation speeds of requests and statistical profiling.

H.Vu, A.kulkarni, K. Sarac, and N.Mittal, A new framework to detect wormhole attacks in wireless ad hoc networks was proposed in [9] (time-based approach). The detection consists of two phases. The first phase is supposed to be inexpensive, referred to as “suspicion”, and must detect the wormhole. Two techniques are used in this phase to detect the wormhole RTT (round trip time) and topology information.

In [10] (location- based approach) an end-to-end wormhole attack detection is proposed. Based on geographic information exchanged between the source and the destination, the source node estimates the minimum hop count to the destination.

In [11] Proposed a modified dynamic source routing protocol for mobile ad–hoc networks (DSR) [11] proposed a modified DSR protocol to defend against wormhole nodes by adopting a multi-path routing method.

In [12] Wormhole detection mechanism for ad hoc wireless networks (proposed an AODV-based routing protocol) authors proposed a wormhole detection mechanism that relies on delay measurements.

In [14] an approach to mitigate wormhole attack in wireless ad hoc networks. In this, the authors proposed a scheme in which each node must broadcast messages that can be transmitted over two hops. Each node records the neighboring list of one hop and two hops, as well as the corresponding session keys.

In [15] Detecting and avoiding wormhole attacks in optimized link state routing protocol. In this the messages are exchanged to defend against wormhole attacks in the Optimized Link State Protocol (OLSR) based routing protocol, as wormhole nodes should process a large amount of packets, causing longer delays of packets than in normal nodes.

In [16], the author proposed a modified ad hoc on demand protocol for MANET to defend against wormhole attacks. The proposed solution uses a multi-path routing method.

## III.METHODOLOGY

In this, the principle used is to allow neighboring nodes of a wormhole node to notice that the wormhole node has an extreme capacity of competition in path discovery**.** In discovering the path, an intermediate node will attempt to make a route that does not go through a hot neighbor node, which has a route that builds route higher than the threshold. Thus, not only wormhole nodes are gradually identified and isolated by their normal neighboring nodes but traffic can also be avoided concentrating on nodes in order to achieve traffic load balance. Although a normal node may be located at a key position of connectivity in a work, and hence be isolated due to a high route-building rate, it would not be at the key position for long as the ad hoc wireless network topology is constantly changing. This is based a multi-path routing algorithm [17] it takes multiple paths for route discovery and only one path for data transmission. Wormhole node is detected using anomaly value of node after receiving route reply. The existing solution is good in terms of throughput or packet delivery ratio. However, the solution does not consider the tunneling property of wormhole node. In proposed solution, wormhole node is detected at the destination using hop count when it receives the route request and anomaly detection for route reply. Worm hole attack is detected using AODV protocol

## PROPOSED SOLUTION USING MODIFIED WARP

In this, same methodology is used as in WARP [16]. Wormhole attack is detected and eliminated by modifying the fields of AODV protocol format.

Wormhole attacks are avoided by considering two properties of wormhole

1. The nature of wormhole attack is to form a tunnel like channel between sources to destination that uses shortest route to destination. It uses minimum number of hop counts to reach the destination.
2. The wormhole node grabs the route from neighboring nodes to send the reply to source. Wormhole attack due to tunneling is detected by using hop count limit for RREQ at destination. This attack also exists due to second property. This can be detected using anomaly detection for secure neighbor discover for Route reply (RREP).

### Procedure for Receiving an RREQ

In this procedure, a node receiving RREQ first judges whether it is the destination node, if not, it is an intermediate node. For an intermediate node, if the hop count in the RREQ is larger than the hop count in the corresponding entry (having the same originator IP) of the routing table. The

RREQ is directly dropped; otherwise, the node creates a new entry in the routing table (multiple reverse entries, with the same originator IP but different first-hops), copies the data of the RREQ into this entry, and then drops the RREQ for a destination node receiving a RREQ. Then it checks whether the originators sequence number of the RREQ is smaller than that of an entry with the same destination IP in the routing table. If yes, the RREQ is dropped; otherwise the destination node replies to each RREQ with an RREP along the reverse route, in spite of the values in its hop count on first-hop fields.

### Procedure for Forwarding of RREP

In WARP [16], only the destination node can send RREP regardless of how many RREQs it received. The destination will reply until the sequence number or an RREQ is smaller than existing sequence number in the routing table.

### Procedure for receiving an RREP-DEC

In this, an intermediate node is prohibited to reply to the RREQ with an RREP and only the destination node can send RREPs back to the originator because each node has the responsibility to monitor the anomaly values of its neighboring nodes. If one intermediate node replies to the RREQ with an RREP, none of the following nodes on the path would be able to properly accumulate the anomaly value of its next neighboring node along the route.

After receiving the RREQs, the destination node will reply to them with RREPs one by one. Unless the sequence number of an RREQ is smaller than the existing sequence number in the routing table (i.e. the RREQ is expired). Finally, the originator would use the only forward entry to transmit the RREP-DEC packet to the destination along the route. This packet has three purposes:

1. Inform the nodes on the route that they are winners in the route competitors.
2. Inform the nodes on the route (including the originator) to update the anomaly value of its neighboring node (next hop to the destination) on the forward entry, and
3. Inform the destination node to delete useless reverse route entries.

In AODV routing protocol, intermediate nodes send route reply(RREP) when it receives route request(RREQ) but in proposed solution, destination only send the RREP after receiving RREQ from its one hop neighbors. Source node generates RREP-Dec-Pkt after receiving RREP.

### ALGORITHM

```
1.  Source node sends RREQ Packet for route discovery.
2.  Destination checks the minimum hop count on RREQ
    If minimum hop count < 3, Suspect’s wormhole
3.  Destination sends reject RREQ to route containing
    minimum hop count.
    In addition, send RREPs and MAL-ID to one-hop
    neighbors having
       minimum hop count >3
4.  Each intermediate node receives multiple RREPS.
5.  Check for anomaly value
6.  Based on anomaly value detect wormhole
   Anomaly value=RREP-Dec-Pkt/ [RREP count+1]
8.  If, Anomaly value > threshold    value
9.  Declare previous second hop node and previous nodes as
    wormhole node
10. Wormhole node ID is announced.
11. Then
    Source initiate new path discovery
12. If     Further packet from wormhole node
13. Drop the packet
```

In this, an additional property of wormhole has introduced, i.e. even though this is based on multipath link disjointness wormhole uses the shortest path to reach the destination with minimum hop count. If more number of one hop neighbors are present at the destination more delay will be required to find out the reverse route to source by using anomaly value. The destination itself avoids to sends the RREP to those having minimum hop count below threshold. To do this, in RREQ route discovery each node adds hop count and node ID. In this solution, delay decreases at the cost of increased overhead. This is the one of the important requirement in real time applications such as emergency, disaster condition where fast delivery is important.

## IV. Results and Discussion

### Simulation Scenario

Several scenarios have been considered to evaluate the performance evaluation. In this scenario, number of nodes, node mobility and number of malicious nodes are variable parameters. The performance metrics in each scenario and all the simulation scenarios are configured according to the table 1. In this scenario, 50 normal mobile nodes were randomly distributed in a 1200m x1200m space, with transmission range of about 250m.

| Parameter | Value |
|---|---|
| Simulator | NS-2 [ver2-32] |
| Simulation time | 600S |
| Number of nodes | 100 |
| Pause time | 2s |
| Routing protocol | AODV |
| Traffic model | CBR |
| Mobility model | Random way point |
| Terrain area | 1200m x 1200m |
| Transmission range | 250m |
| Maximum mobility | 70m/s |
| Number of malicious nodes | 1-6 |

| | |
|---|---|
| Threshold value | 2 |

Table 1: Simulation parameters

## Simulation Results

Simulation results are evaluated by varying number of nodes, Node mobility, and number of malicious nodes.

### 1 Impact of Number of Nodes

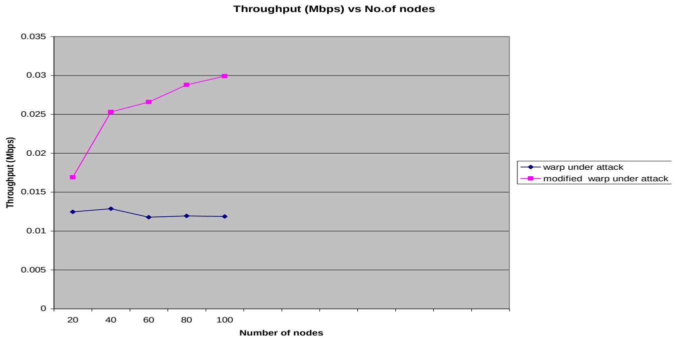


Fig (a)

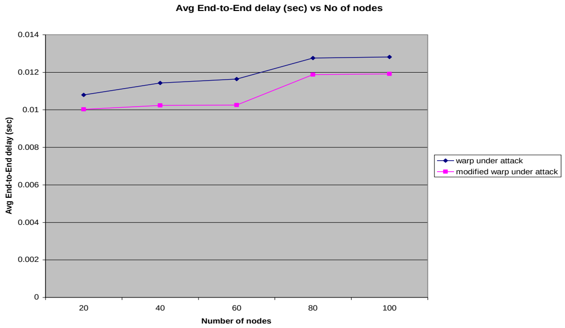


Fig (b)

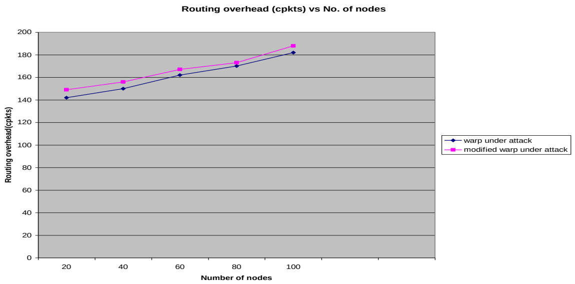


Fig (c)

Fig 1. Simulation results for Number of Nodes

Fig 1 (a) shows, as the number nodes increases throughput of modifying WARP solution increases compared to WARP solution.

Fig4.1 (b) shows the increase in delay for both as the number of nodes increases. However, delay in modifying WARP is less compared to WARP.

Routing overhead is 7cpkts more in proposed solution (modified WARP) compared to WARP as shown in fig 1 (c)

### 2. Impact of Node Mobility

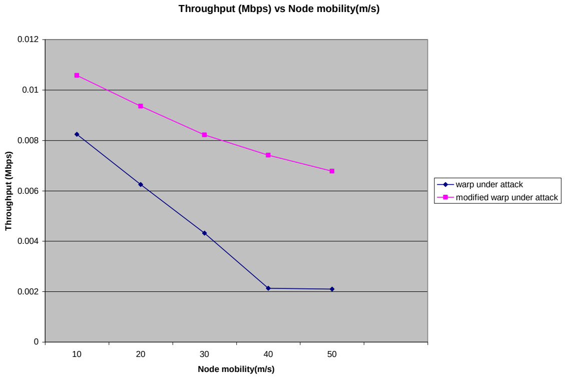


Fig (a)

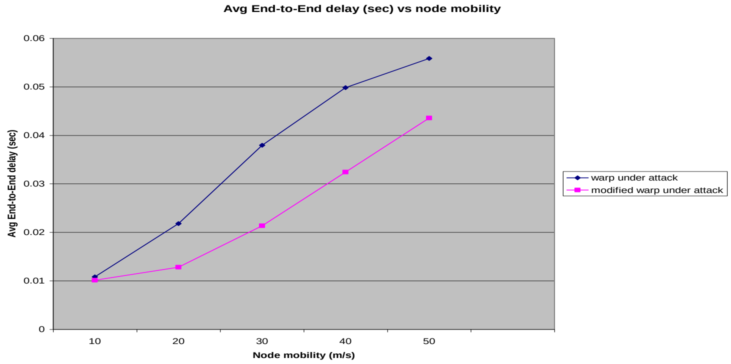
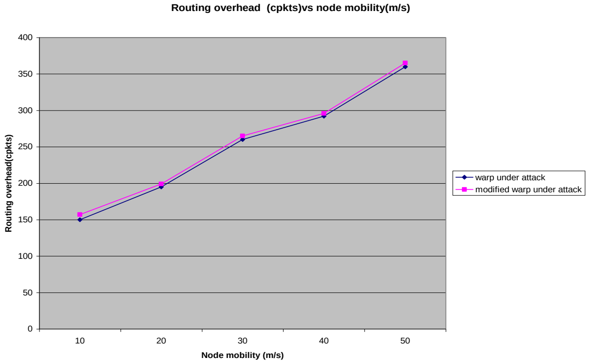


Fig (b)



Fig(c)

Fig 2. Simulation results for Node Mobility

Fig 2 (a) shows, the throughput decreases in WARP and modified WARP as node mobility increases due to change in topology. However, in modified WARP throughput is improved compared to WARP.

Fig 2 (b) shows that initially both solution requires same delay to send packets. As the node mobility increase the existing solution (WARP) requires more delay compared to proposed (modified WARP). This is due to change in topology changes the position of hot neighboring nodes.

### 3 Impact of Number of Malicious Nodes

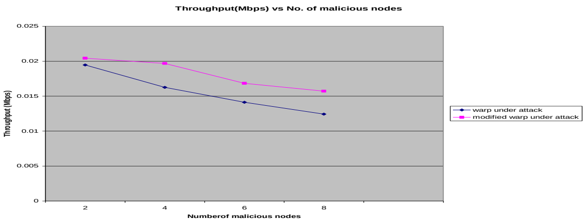


Fig (a)

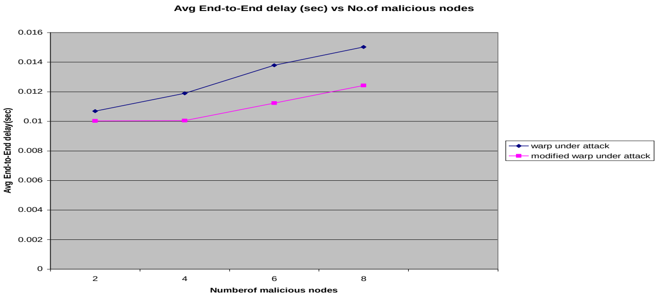
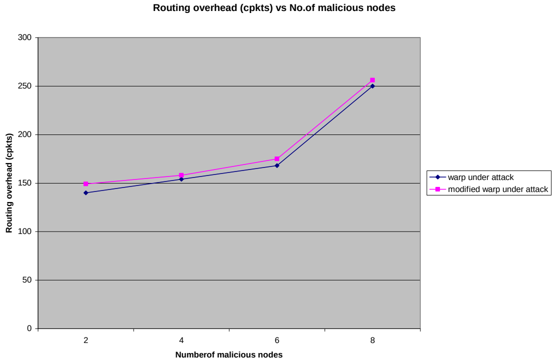


Fig (b)



Fig(c)

Fig 3. Simulation results for Number of Malicious Nodes

Fig 3 (a) shows, as the number of malicious nodes increases throughput is improved.Fig3 (b) shows that avg end-to-end delay is more in WARP compared to proposed solution (modified WARP). And routing overhead required for modified WARP is a few more control packets compared to WARP as shown in fig 3 ( c) .

## V.CONCLUSION AND FUTURE SCOPE

In this study, the effects of wormhole attack in Mobile adhoc networks are analyzed. The proposed solution is implementation using an AODV protocol and the behavior of wormhole attack is simulated in NS-2.In this work security against wormhole attack provided which causes the interception and confidentiality of the ad hoc wireless networks. Proposed work is based on WARP and compared the modified WARP with WARP. Modified WARP detects and eliminates the wormhole attack. In modified WARP throughput is more, average end-to-end delay is less and. routing overhead increases slightly compared to the WARP.

## REFERENCES

[1] Hu Y. C. Hu, A. Perrig, and D. B. Johnson, "*Packet leashes: a defense against wormhole attacks in wireless networks*," in In Proce. of IEEE INFOCOM, 2003.

[2] H. Yih-Chun, A. Perrig, and D. B. Johnson, "*Wormhole attacks in wireless networks,"* Selected Areas in Communications, IEEE Journal on, vol. 24, no. 2, pp. 370-380, 2006.

[3] S. Capkun, L. Buttya'n, and J.-P. Hubaux, "*Sector: secure tracking of node encounters in multi-hop wireless networks*," in Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks. Fairfax, Virginia: ACM, 2003, 986862 21-32.

[4] L. Hu and D. Evans, "*Using directional antennas to prevent wormhole attacks,*" in Network and Distributed System Security Symposium (NDSS), San Diego, 2004.

[5] I. Khalil, S. Bagchi, and N. B. Shroff, "*Liteworp: Detection and isolation of the wormhole attack in static multihop wireless networks,*" Comput. Netw., vol. 16. 51, no. 13, pp.3750-3772, 2007, 1276793.

[6] I. Khalil, S. Bagchi, and N. B. Shroff, "*Mobiworp: Mitigation of the wormhole attack in mobile multihop wireless networks*," Ad Hoc Netw., vol. 6, no. 3, pp. 344-362, 2008, 1328997.

[7] L. Qian, N. Song, and X. Li, "*Detection of wormhole attacks in multi-path routed wireless ad hoc networks: a statistical analysis approach*," J. Netw. Comput. Appl.,vol. 30, no. 1, pp. 308-330, 2007.

[8] R. Maheshwari, J. Gao, and S. R. Das, "*Detecting wormhole attacks in wireless networks using connectivity information*," in INFOCOM 2007. 26th IEEE Internation2.4.1.1al Conference on Computer Communications. IEEE, J. Gao, Ed., 2007, pp.107-115 .

[9] X. Su and R. V. Boppana, "*On mitigating in-band wormhole attacks in mobile ad hoc networks,"* in Communications, 2007. ICC '07. IEEE International Conference on, R. V. Boppana, Ed., 2007, pp. 1136-1141.

[10] H. Vu, A. Kulkarni, K. Sarac, and N. Mittal, "*Wormeros: A new framework for defending against wormhole attacks on wireless ad hoc networks,"* in In Proc. of the Third International Conference on Wireless Algorithms, Systems, and Applications, 2008.

[11] X. Wang and J. Wong, "*An end-to-end detection of wormhole attack in wireless ad-hoc networks,"* in In Proc. of International Conference on Computer Software and Applications, 2007.

[12] Ning Song, Lijun Qian, and Xiangfang Li. *Wormhole attacks detection in wireless* IEEE international parallel and distributed processing symposium (IPDPS'05); 2005.

[13] Hon Sun Chiu, King-Shan Lui. *DelPHI: wormhole detection mechanism for ad hoc wireless networks.* In the proceedings of the 1st international symposium on wireless pervasive computing; 2006.

[14] P. Dhivya and S. Meenakshi, "*A Review of Congestion Control Techniques in Mobile Ad-hoc Network*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.9, pp.44-49, 2015.

[15] G.Kalpana and S.Archana, "*Performance Analysis of Threshold Based Algorithms under Wormhole Attack in MANET*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.7, pp.133-138, 2015.

[16] Ming-Yang Su "*WARP: A Wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks*", COMPUTERS & SECURITY 29 (2010) 208-224.

[17] Mahesh K.Marina and Samir R.Das., "*On-demand multipath distance vector routing in ad hoc networks"*, In the proceedings of the IEEE international conference on network protocols(ICNP);2001.pp.14-23.