IJARIIT
INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
*(Volume3, Issue2)*
Available online at www.ijariit.com

# Wormhole Attack Prevention and Detection in MANETs Using HRL Method

**Neelima Singla**
*Student*
*Department of Electronics and Communication Engineering/LCET, Ludhiana, India.*

**Mr. Ramanjeet Singh**
*Assistant Professor*
*Department of Electronics and Communication Engineering/LCET, Ludhiana, India.*

***Abstract: In order to prevent MANET from wormhole attack a new method is proposed. In this, wormhole attack in MANET is detected and prevented by using Hop Count, Reverse Trip Time and Link Length method. According to the scheme, hop count specifies the actual reverse trip time from source to destination. To find the presence of tunnel, the source will compare calculated reverse trip time with actual reverse trip time and to verify the presence of tunnel, the source will compare calculated link length with actual link length of the links in paths. This scheme provides a security to mobile ad hoc networks from both short as well as long wormhole tunnels. Network simulator is used to evaluate the performance of mobile ad hoc network. The simulation results show that the proposed scheme outperformed in terms of throughput and packet delivery ratio.***

***Keywords: AODV; Packet Delivery Ratio; Routing Protocols; Throughput; Wormhole Attack.***

## I. INTRODUCTION

Mobile Ad-hoc Networks (MANET) are infrastructure fewer networks so security is the main issue. Different methods have been proposed so far to prevent MANETs from various kinds of attacks. Out of these attacks, wormhole attack is the main threat. Two intrusion detection techniques [1] are enhanced that will use clusters and show how clusters can be used in order to give the ability to detect wormhole attack and isolating them from routing process. After that two routing protocols are taken OLSR is Optimized Link State Routing Protocol (proactive) and AODV is Ad-hoc On-Demand Distance Vector Routing Protocol (reactive) in order to find which protocol is more vulnerable to wormhole attack [2]. The finding shows that AODV is more vulnerable to wormhole attack compared to OLSR. Further, a statistical analysis approach is used and it provides better security and performance as compared to conventional AODV [3], an improved clustering based approach in which the entire network is partitioned into different clusters and each cluster will have a Cluster Head, which controls all the nodes in the cluster and plays the role of a controlling authority in MANET and Out of band wormhole attacks that are launched by exploiting AODV routing protocol are eliminated effectively [4], a lightweight technique is able to detect and remove the wormhole attack to a greater extent and gives the lowest total packet loss rate compared with AODV under attack and the other techniques [5], an identity-based signature scheme does not require distribution of any certificate among nodes so it decreases computation overhead and the performance of the network is evaluated in terms of end-to-end delay, packet delivery ratio, packet loss rate [6]. Some other techniques [7]-[10] are also proposed in order to prevent wormhole attacks.

In this paper, wormhole attack is detected and prevented by using hop count, reverse trip time and link length between the nodes The proposed system firstly detects the presence of wormhole tunnel by using hop count and from the hop count actual reverse trip time is determined which is later on compared by the calculated reverse trip time and then detects the wormhole nodes using link length. The performance of the network is also analyzed which shows improved value of throughput and packet delivery ratio. The network's performance is simulated using NS2 simulator.

## II. PROPOSED METHODOLOGY

The objective of this research is to minimize the threat of wormhole attack in Mobile Ad-hoc Networks by preventing and detecting long as well as short wormhole tunnels in the network. In order to detect and prevent wormhole attack, H-R-L (Hop Count-Reverse Trip time-Link Length) method is used and the proposed technique works as represented through flow chart given below:

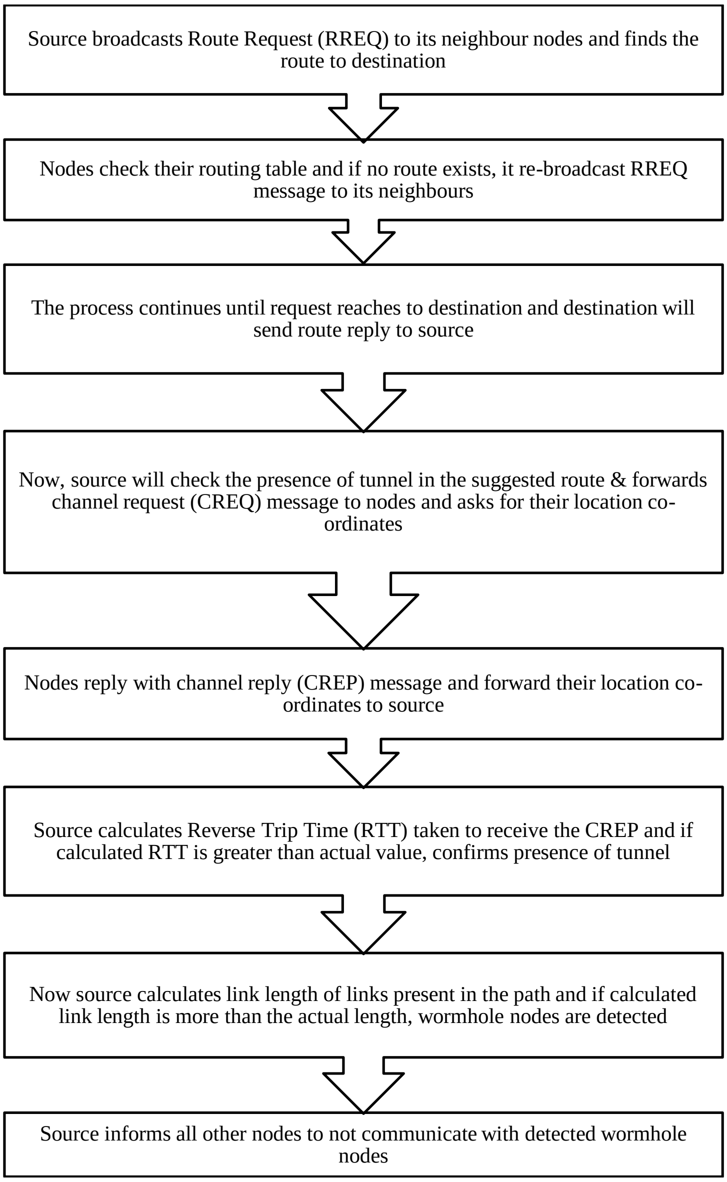
Source broadcasts Route Request (RREQ) to its neighbour nodes and finds the route to destination
Nodes check their routing table and if no route exists, it re-broadcast RREQ message to its neighbours
The process continues until request reaches to destination and destination will send route reply to source
Now, source will check the presence of tunnel in the suggested route & forwards channel request (CREQ) message to nodes and asks for their location co-ordinates
Nodes reply with channel reply (CREP) message and forward their location co-ordinates to source
Source calculates Reverse Trip Time (RTT) taken to receive the CREP and if calculated RTT is greater than actual value, confirms presence of tunnel
Now source calculates link length of links present in the path and if calculated link length is more than the actual length, wormhole nodes are detected
Source informs all other nodes to not communicate with detected wormhole nodes

**Fig1.Flowchart shows working of proposed scheme**

## III. Implementation

In the proposed methodology number of nodes is 50 which are deployed in the network using Random Way Point mobility model. Next step starts with the broadcasting of the Route Request messages by the source node in the network. The source node will find one-hop neighbor nodes in its radio communication range. In network simulator 2.35 the nodes have a radio range of 250 meters. The source node will then forward the Route Request to them and these neighbor nodes are at one hop distance from the source. If the nodes have a fresh route to the destination node, they will reply back to the source node else they will re-broadcast the Route Request message to their own neighbors.

The destination node received the route request messages from the four hop nodes which would mean that the destination node is at five hop distance from the source node. The destination node will now send the Route reply messages to the source node via the nodes from which route request messages were received. Next step in the proposed work is to detect the formation of the tunnel and then to detect the nodes between which the tunnel is created.

In order to detect whether the link contains a tunnel or not between the nodes, the reverse trip time will be calculated. Then it will be compared with the theoretical value. If the calculated value is more than the theoretical value then the formation of the tunnel is detected since the reverse trip having more value indicates that the more time is taken for the message to come back to the source node. For this, the source node will send the control message to the nodes in the path from where the route reply was received. The source node will also ask for the location coordinates of the nodes consisting of the path. The nodes also respond with the location coordinates of the source node same as Node 49 replying to source node along with location coordinates 643, 469, Node 48 replying to source node along with location coordinates 320, 294, Node 2 replying to source node along with location coordinates 162, 144. The location coordinates will be used to detect the nodes which formed the tunnel if the condition is true that calculated reverse trip time is more than the theoretical value.

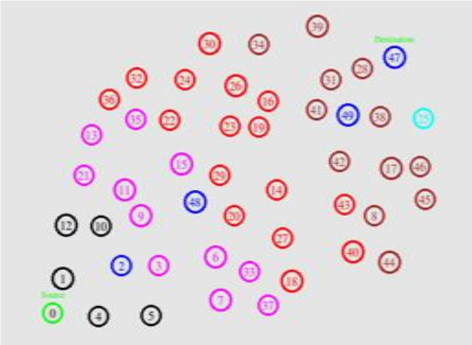

**Fig 1.Detection of wormhole tunnel through network simulator 2.35**

Fig.2 shows detection of wormhole tunnel in a network simulator. After comparing the theoretical value of the reverse trip time with the calculated value we found that the theoretical value of the reverse trip time for the four hop length path should be 0.02184 but calculated value was found to be 0.0279921. This means that it took more time for the message to come back over the round trip. The packet must have taken a long distance to travel indicating the presence of the tunnel in the link. Now the location coordinates received in the control message will be used to detect the nodes which formed the tunnel. The nodes have a radio range of communication 250 meters that would mean the link between the nodes should not have a length greater than 250 meters. After receiving the location coordinates the source node finds out the length of each link that constitute the path to the destination node. The link length between nodes 48 and 49 was found to be 367.361 meters which are more than the average link length. This means that these nodes are wormhole nodes.

Link Length of link 2 calculated is more than the average link length which means nodes 48 and 49 are wormhole nodes. After finding out the wormhole nodes, the source node will inform the nodes in all other paths to not communicate with the wormhole nodes. The nodes in the orange color are those constitute the other paths from source to destination node. Now source will use these paths to send information to the destination.

The source sends data through the other path shown: 0 - 5 - 33 - 43 - 46 - 47. So our proposed technique first detects the presence of the tunnel in the path from source to destination node using the reverse trip time and the hop count values. After the detection of the tunnel, the source node detects the wormhole nodes by checking the link length of the nodes.

## IV. SIMULATION RESULTS

### *A. Simulation Setup*

The simulation parameters used in the work are defined below:

**TABLE I. SIMULATION PARAMETERS**

| **Parameter** | **Value** |
|---|---|
| Channel | Wireless |
| Propagation Model | Two Ray Ground |
| Mobility Model | Random Way Point |
| Routing Protocol | AODV |
| Number of nodes | 50 |
| Mac | 802.11 |
| Antenna | Omni Directional |
| Initial Energy | 50 Joules |
| Network Area | 1300m * 1300m |
| Queue | Drop Tail |

The channel used is wireless and propagation model is two ray ground because when the signal received consists of a line of sight and multi-hop components, it predicts path loss. The number of nodes used is 50 and antenna used is omnidirectional. The queue used is drop tail. In this queue, when the queue is filled with maximum capacity then the newly incoming packets are dropped until queue have sufficient space to accept more packets.

### *B. Packet Delivery Ratio*

Fig. 3 shows the comparison of PDR (packet delivery ratio) of the network achieved after using proposed scheme and the existing scheme. The proposed scheme showed the better value of packet delivery ratio at 0.95 whereas the value of packet delivery for the existing scheme is 0.64. This means less number of data packets was dropped after application of proposed scheme which also means the data transmission was more efficient and secure.

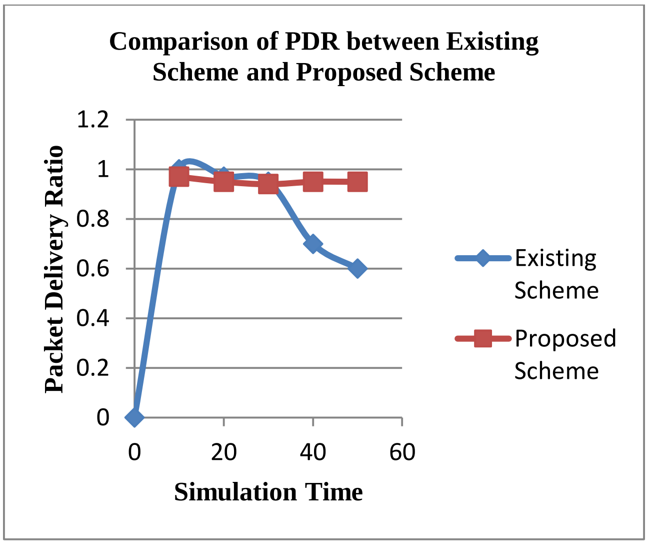

**Fig 1. Comparison of Packet Delivery Ratio between Proposed Scheme and Existing Scheme**

### *C. Throughput*

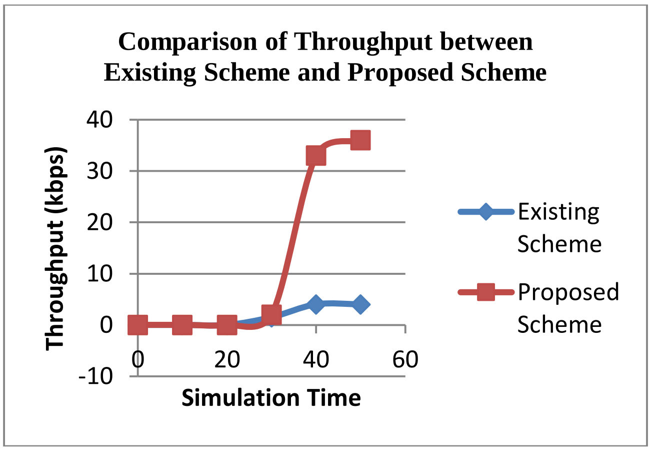

**Fig.4 Comparison of Throughput of Network between Proposed Scheme and Existing Scheme**

Fig. 4 shows the comparison of the throughput of network achieved after applying the existing scheme and the proposed scheme. The graphs have been plotted against simulation time which is time taken to simulate the network. The value of throughput achieved with our proposed scheme is 36 kbps and that with the existing scheme is approx 5 Kbps. This shows that our proposed scheme outperforms the existing scheme.

## CONCLUSION

Wormhole attack is a very dangerous attack and many researchers have proposed many techniques in order to detect and prevent MANETs from wormhole attacks. In the proposed work, the technique successfully detects and prevents the wormhole attack for both tunnels short and long tunnels. The performance of the network was analyzed using parameters: packet delivery ratio and throughput. Both these factors tend to show an improved performance of the network. This shows that the proposed scheme has performed effectively.

In future, the proposed technique can be used to detect rushing attack in which the nodes rush the route request messages to the destination earlier than other nodes using the tunnel.

## REFERENCES

[1] Mahdi Nouri, Somayeh Abazari Aghdam, Sajjad Abazari Aghdam, "Collaborative Techniques for Detecting Wormhole Attack in MANETs", International Conference on Research and Innovation in Information Systems (ICRIIS), IEEE, November 2011.

[2] Mohammad Sadeghi, Saadiah Yahya, "Analysis of Wormhole attack on MANETs using different MANET routing protocols", Fourth International Conference on Ubiquitous and Future Networks (ICUFN), IEEE, July 2012.

[3] Saurabh Upadhyay, Brijesh Kumar Chaurasia, "Detecting and Avoiding Wormhole Attack in MANET Using Statistical Analysis Approach", Advances in Computer Science and Information Technology Networks and Communications, Springer, Vol. 84, pp. 402-408, 2012.

[4] J. Anju, C. N. Sminesh, "An Improved Clustering-Based Approach for Wormhole Attack Detection in MANET", 3rd International Conference on Eco-friendly Computing and Communication Systems, IEEE, pp. 149-154, 2014.

[5] Hosny M. Ibrahim, Nagwa M. Omar, Ebram K. William, "A Lightweight Technique to Prevent Wormhole Attacks in AODV", International Journal of Computer Applications, Vol. 104, October 2014.

[6] Dhruvi Sharma, Vimal Kumar, Rakesh Kumar, "Prevention of Wormhole Attack Using Identity-Based Signature Scheme in MANET", Computational Intelligence in Data Mining, Vol. 2, pp. 475-485, 2015.

[7] Juhi Biswas, Ajay Gupta, Dayashankar Singh, "WADP: A wormhole attack detection and prevention technique in MANET using modified AODV routing protocol", 9th International Conference on Industrial and Information Systems (ICIIS), IEEE, December 2014.

[8] Rajan Patel, Anal Patel, Nimisha Patel, "Defending Against Wormhole Attack in MANET", Fifth International Conference on Communication Systems and Network Technologies, IEEE, 2015.

[9] S. B. Geetha, Venkanagouda C Patil, "Evaluating the Research Trends and Techniques for Addressing Wormhole Attack in MANET", International Journal of Computer Applications, Vol. 110, No. 6, January 2015.

[10] Amit Kumar, Sayar Singh Shekhawat, "A Parameter Estimation Based Model for Worm Hole Preventive Route Optimization", International Journal of Computer Science and Mobile Computing, Vol. 4, Issue 8, pp. 80 – 85, August 2015.