



## Performance Evaluation of Reactive Wormhole Detection Mechanism for Mobile Ad Hoc Network

Ashish M. Mishra

PG Scholar,

Dept. of CSE, SKSITS, Indore, India

Dr. G. D. Gidwani

Executive Director & Professor

SKSITS, Indore, India

*Abstract - Mobile Ad-Hoc Network (MANET) is a wireless network having infrastructure less group of nodes communicating with each other using themselves only. Here each node is responsible for getting all the functionalities of the routing performed by the mobile nodes. Such network is affected by different attacked situations because of their dynamic nature and movable environment. Wormhole attack is the most vulnerable to the network because in heavy movement based network identifying or detecting the authenticity and behaviour of the node is very difficult. Thus some of the nodes perform malicious operations by dropping the packets routed through them. If the nodes cooperatively provides a tunneled path to destination with smallest distance might be wormhole node. This work aims towards detecting and removing the wormhole node effectively in terms of routing load, throughput and the energy of the network. The detection here is based on the hop count, time to live filed of the packet and the delay per hop for the network. At the evaluation point of view the approach is giving better results than the existing wormhole detection mechanism.*

*Index Word: MANET, Wormhole, Delay per hop, TTL, Hop Count, Routing load, Throughput, Energy;*

### I. INTRODUCTION

In today's world the wireless communicating medium and devices are getting popularity due to their mobility based services. Such networks are mainly classified in to two domain based on their supportive requirements: infrastructure oriented and infrastructure less. In the formal one, the communication takes place between the movable wireless host or nodes using the access points (AP). Here the wireless nodes cannot communicate directly. The access points are work as routing medium between them. In infrastructure less network, the fix devices and access points are not presents. Here the communication can only takes place using the mobile nodes or device itself. Each node here will works as router which can move freely in a random zone. They are not having any larger devices and hence their setup requirements and time is very less.

The network holds some of the characteristics while forming a connection. If the connection is made for limited communication or temporary transmission then it is called as ad-hoc in nature. Mobile ad-hoc network (MANET) is one of them which provide short range communication without any routing devices. Here each mobile node will work as router which supports the radio waves based communications. Here the devices are mobile nodes and hence the configuration for them must have the minimized resource constraints. The MANET is not control via some centralized authority and the topology is also continuously changing. The routing mechanism must also be of lower complexity and consumptions. Thus the routing protocol in MANET is classified in three major areas:

➤ **Proactive Routing Protocol**

In Proactive routing protocols each node maintains one or more tables containing routing information about all other node in the network. All nodes keep on updating these tables to maintain latest view of the network. Some popular proactive protocols are: DSDV, WRP and ZRP

➤ **Reactive Routing Protocols**

In these protocols, the nodes don't maintain a routing table. Instead, they maintain a route cache. Routes are created only when a node want to communicate with another node. For this purpose source invokes the route discovery procedure. Some reactive routing protocols are: DSR, AODV and TORA

➤ **Hybrid Routing Protocols**

This type of protocols contains the best features of proactive and reactive routing protocols. In case of the intra-domain routing, these protocols uses the proactive approach, while in case of inter-domain routing these protocols uses the reactive approach For example, Zone Routing Protocol (ZRP) etc.

In MANET the nodes are continuously changing their topology from one zone to other making the distant communication feasible with the help of intermediate nodes. Now here the change in the nodes position and behaviour are getting very abrupt in some cases. There are some cases where the data transmission is operated on the untrusted wireless environment. Such environment is vulnerable to high attack situations and the security breaches are associated here through malicious behaviour or operations like Black Hole, White Hole, Gray Hole, Wormhole etc. Out of these the wormhole is the most vanishing attacks. In wormhole attack, two or more malicious nodes together makes a tunnel in the

network, in which the traffic is enter from one end and passes through the tunnel and leaves from the other end. Wormhole link or tunnel can be created by means of a high quality wireless link or a logical link. After building a wormhole link, one attacker is able to receive all the messages which travel from this route. This attacker node then copies packets from its neighbors, and forwards them to the other malicious attacker through the wormhole link. Then another malicious node which receives these packets, replays them into the network in its vicinity. There are two types of wormhole attacks have been identified: Hidden attack and Exposed attack.

## II. BACKGROUND

Mobile ad-hoc network (MANET) is a dynamic wireless network which support mobility based communication in which the nodes are regularly changing their topology. Due to node mobility nature of nodes, the nodes have limited battery power & limited bandwidth. In absence of centralized access point or administrator the source & destination communicate through multiple hops. In such network the devices are frequently coming and moving from the range. Thus, to verify the nodes authenticity in such network is quite complicated. Thus some of the attackers keep in track of such activity to affect the formal communication of the network. Thus MANET is vulnerable to the various attacks whose primary objective is to affect the normal transmissions by dropping or changing the routing through some malicious operations. These operations are performed by non trusted nodes.

Among the various attack types this work concentrates its exploration towards getting in depth knowledge of Worm Hole attack by which some feasible and effective solution is given. In way to do that, this paper puts an approach and its analysis which works towards making the things more effective for the detection process. Wormhole attack performs various malicious tasks by misdealing the routing information, scanning the confidential data behind it or dropping the complete message. Its variants work in several directions which eventually drop the packets and misguide the route formations. It is the most serious threat for the MANET and can't be detected easily.

In a wormhole attack two or more node can jointly work for making a virtual private tunnel from which the packets are forced to transmit. This tunnel provides wrong shortest path to the destination and when the packet starts routed from here then they are scanned, dropped or changed maliciously. It causes repeated transmission which at the last occupies unnecessary resources.

### Routing Protocol: AODV

AODV is ad-hoc on demand distance vector routing with capacity to accommodate thousands of the nodes. Here the protocol is demand driven means when the demand or request came then only the protocol starts operating, thus it will also be known as reactive. The protocol is having a message instruction sets on the basis of which various routing operations are performed based on the connected hops. This saves memory and lowers computational overhead for route maintenance. It also contains information enabling the host to share information with other nodes when link states change. The sequence number, unique to each destination route, is the key to maintaining up to date routing information. Protocol messages that contain routing information also include a sequence number. By observing the value of the sequence number, an intermediate node can determine the "freshness" of the routing information. The basic message set consists of RREQ (Route Request), RREP (Route reply), RERR (Route error) and HELLO message.

### Behaviour of Wormhole Attack

- (i) The attackers can tunnel each route request packets to another attacker that is near to destination node. When the neighbors of the destination hear this RREQ, they will rebroadcast this RREQ and then discard all other received RREQs in the same route discovery process.
- (ii) It must attract a large amount of network traffic which is done by giving a shortest route to destination in the network. Therefore, the routes going through the wormhole must be shorter than alternate routes through valid network nodes.
- (iii) Its attack the traffic of network and either scan, change or drops the entire confidential message inside the packet in the time of journey of packet over the wormhole tunnel.
- (iv) Apart from the above behaviour the performance drops and overhead measurements is one of the major issues with wormhole attacks. Here the source generating such attack must be detected or predicted with alert for others for avoiding the communication with the attacker node.

## III. PROPOSED SOLUTION

After analyzing the complete behaviour of worm hole its protecting mechanism can be developed by considering the above factors in concern. Worm hole mainly creates the tunnel between the two nodes by which the data losses can be initiated by dropping or misleading the packets. Here the proposed solution works towards detecting these conditions using some of the packet monitoring and route measuring parameters. The solution primarily finds the time to live (TTL) values along with the hop count between the source node and the destination node for each and every route. On the basis on the two factors the Delay per hop (DPH) is calculated for each route. Later on the energy is calculated which detects the presence of the worm hole in the network. Below is the procedure to check how these values are compared and evaluated.

- (i) **TTL Values:** For generating the TTL values for the source to every other node a RREQ packet is marked with the r flag, sending time and the hop count initially set to the zero value. The RREQ packets are transmitted and travelled to route after which the destination replies the packets with the RREP packet. The route reply packet

traversed through the same route in backward direction. Thus the time to leave is the difference between the receiving time of RREP and the sending time of the RREQ.

- (ii) **Hop Count:** The approach also uses hop count as its one of the factors for detecting the wormhole tunnel. Whenever there are two routes for same destination then the hop count comes in to the role. The odes with minimum hop count will be served as shortest path and selected for transmitting the data.
- (iii) **Delay per Hop (DPH):** When source node gets the value of TTL & Hop Count it calculates the DPH(Delay Per Hop) value of each & every route by given formula
  - a.  $DPH = TTL/2 * \text{Total Hop Count}$
- (iv) **Energy checking of nodes previous to destination:** Now source node sends energy check packet through every route towards destination node & calculate the energy of every nodes previous to destination node.

**Algorithm**

1. Initialize the network
2. Declaration:
3. S=Source Node; D=Destination Node; Wormhole Node=W1, W2; DSN=Destination Sequence Number;
4. Hop Count=HC; Node ID=NID;
5. Send RREQ to every Node;
6. Intermediate Node Check Destination Address
7. If Matches Generates RREP;
8. Else Forward to its Neighbour;
9. Destination Receives RREP;
10. Match Found Then reply with RREP;
11. Store all Information in Routing table;
12. Calculate the  $TTL = Tr - Ts$ ;
13. Calculate Hop Count;
14. Calculate DPH;
15. Calculate Energy of Each node;
16. Check Routing Table and Sort it in order of Destination Sequence Number;
17. If  $DSN \gg SSN$  & The Hop Count is Minimum;
18. Mark Node ID1= W1 & NodeID2=W2 as Worm Hole;
19. Measure Energy consumption and PDR is if Max;
20. Node is Worm Hole;
21. Inform Other Node by a Alarm Message; Update to Routing Table;
22. Exit;

Thus by using above mechanism the worm hole is successfully detected and removed form the system. Approach easures all the factors on the basis of which the detection of wormhole is authentically measured and removed without any extra burden to the limited capacity ad-hoc network.

**IV. EXPERIMENTAL EVALUATION**

For showing the practical feasibility of the proposed approach the work is implemented on well known simulation tool NS2. To prepare simulation for desired network utility the following given network setup is provided. Using TCL script the network scenario is created then Simulation is executed. And by using AWK file RREQ packets send, received is captured and also used for the remaining energy of the nodes. When the simulation starts then trace file and nam file generated. fig shown below is the scenario of the Wireless mobile ad-hoc network with thirty nodes.

Table 1 Network Setup

No of nodes	30
Radio-propagation	Propagation/TwoRayGround
Antenna model	Antenna/OmniAntenna
Routing protocol	AODV
Simulation dimension	750 X 550
Initial energy in Joules	1000
Simulation time	150 seconds
Traffic	TCP
Channel type	Channel/WirelessChannel

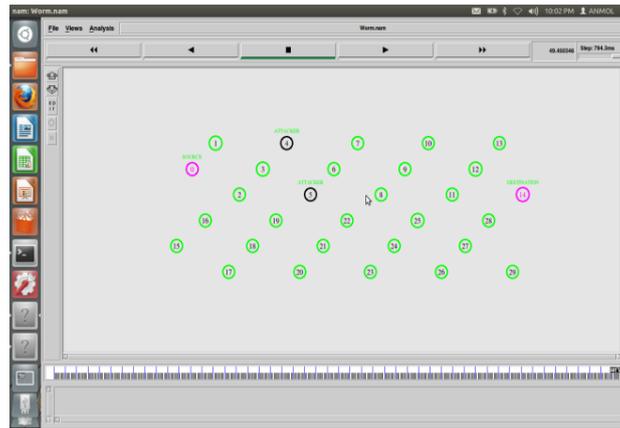


Figure 1: nam file of the network simulation.

To calculate the better topology control we need to add some of the quality measures which analyze various factors for improved bandwidth utilization, power saving & strong connections. For these performance evaluations, metrics includes the following QoS parameters such as PDR (Packet Delivery Ratio), Throughput, End to End Delay, Routing overhead and Jitter.

- 1) **Packet Delivery Ratio (PDR):** also known as the ratio of the data packets delivered to the destinations to those generated by the CBR sources. This metric characterizes both the completeness and correctness of the routing protocol also reliability of routing protocol.
- 2) **Throughput:** Throughput is the ratio of total number of delivered or received data packets to the total duration of simulation time.
- 3) **Normalized Protocol Overhead/ Routing Load:** Routing Load is the ratio of total number of the routing packets to the total number of received data packets at destination.

In future the results will show the effectiveness of proposed scheme. For network simulation, there are several performance metrics which is used to evaluate the performance. In future simulation purpose this work will use different performance metrics for showing the expected results. Results are plotted using Xgraph utility of NS2

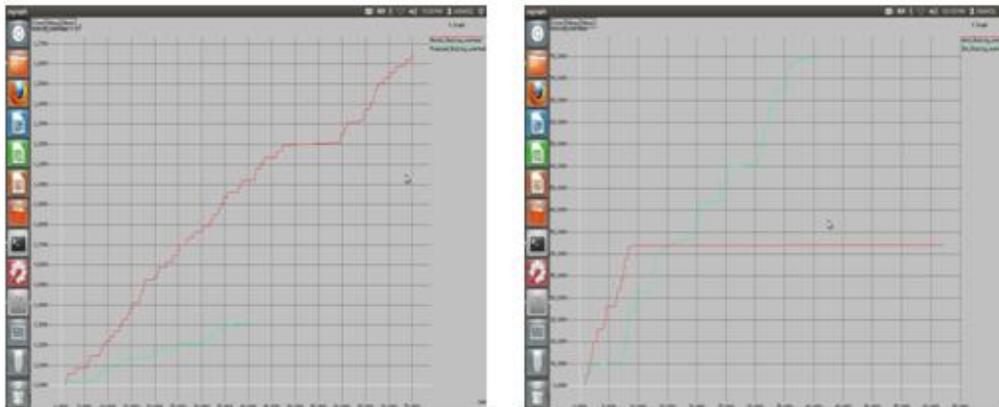


Figure 2: Comparative Routing Load Graph for Normal, Wormhole and Proposed

**Graph Summary:** The above graph verifies its results by minimum routing overhead associated with the suggested approach. It also shows that the complexity of using the proposed method is quite less in comparison with the existing.



Figure 3: Comparative PDR Graph for Normal, Wormhole and Proposed

**Graph Summary:** As the PDR ratio is used to identify the performance of the approaches using the packet delivery ratio. It is the ration of number of packet sent to the number of packet received. In ideal condition it should be high as possible. For comparing the suggested work, the above graph interprets the result as an improved PDR ration than the existing approaches.

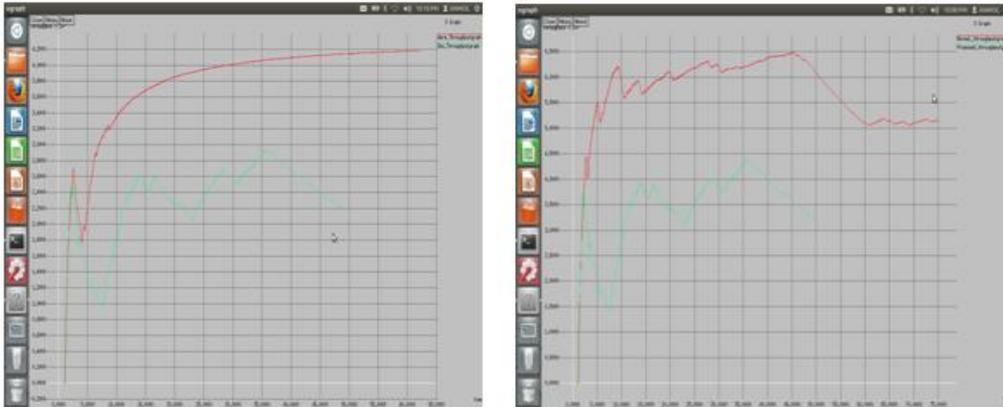


Figure 4: Comparative Throughput Graph for Normal, Wormhole and Proposed

**Graph Summary:** As throughput measure the transmission efficiency in terms of successfully delivered packets in unit time for a specified channel bandwidth. The above graph shows the effectiveness of the suggested approach while comparing it with the existing. The graph interprets the constant throughput for several cases which justify the approach.

#### REFERENCES

- [1] Pallavi Sharma, Aditya Trivedi, "An Approach to Defend Against Wormhole Attacks in Ad Hoc Network using Digital Signature". IEEE ISSN 978-1-61284-486-2/2011.
- [2] Radhika Saini, Manju Khari, "Defining Malicious Behaviour of a Node and its Defensive Methods in Ad Hoc Network" International Journal of Computer Applications (0975-8887) Volume 20-No.4, April 2011.
- [3] Rajbir Kaur, M.S. Gaur, V. Laxmi. "A Novel Attack Model Simulation in DSDV Routing" 978-1-4244-8704-2 IEEE 2011.
- [4] Reshmi Maulik and Nabendu Chaki, "A Study on Wormhole Attacks in MANET" International Journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Volume 3 (2011) pp. 271-279.
- [5] E.A. Mary Anita, V. Thulasi Bai, "Defending Against Wormhole Attacks in Multicast Routing Protocols for Mobile Ad Hoc Networks" 978-1-4577-0787-2/2011 IEEE.
- [6] Saurabh Gupta, Subrat Kar, S. Dharmaraja, "WHOP: Wormhole Attack Detection Protocol Using Hound Packet" 978-1-4577-0314-0/2011 IEEE.
- [7] Xiaomeng Ban, Rik Sarkar, Jie Gao, "Local Connectivity Test to Identify Wormholes in Wireless Networks" ACM 978-1-4503-0722-2/11/05. May 2011.
- [8] Pallavi Sharma, Aditya Trivedi, "Prevention of Wormhole Attack in Ad-Hoc Network" ISSN 0975-8887 ICEICE No.5, Dec 2010.
- [9] Sunil Taneja, Ashwani Kush "A Survey of Routing Protocols in Mobile Ad Hoc networks" International Journal of Innovation Management and Technology, Vol.1 August 2010, ISSN 2010-0248.
- [10] Priyanka Goyal, Sahil Batra Ajit Singh, "A Literature Review of Security Attack in Mobile Ad- Hoc Networks" International Journal of Computer Applications (0975-8887) Volume 9, No. 12 November 2010.
- [11] Marianne Azer, Sherif EI-Kassas, Magdy EI-Soudani, "A Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole Attacks In wireless Ad Hoc Networks" International journal of Computer Science and Information security, IJCSIS Vol. 1, No. 1 May 2009.
- [12] Ashish M. Mishra and Charan Singh, "Worm-Hole Detection Mechanism for Reactive Routing of Mobile Ad-Hoc Network", in International Journal of Emerging Research in Management & Technology ISSN: 2278-9359 (Volume-3, Issue-4), April 2014.