Prevention and Elimination of Gray Hole Attack in Mobile Ad-Hoc Networks by Enhanced Multipath Approach

Vaishali Mittal

M-Tech Student & Department of CSE & Delhi College of Technology & Management
Palwal, Haryana, India

Abstract

A Wireless ad-hoc network is a temporary network set up by wireless mobile computers (or nodes) moving self-assertive in the spots that have no system foundation. Since the nodes communicate with each other, they cooperate by forwarding data packets to other nodes in the network. Security is one of the major issues in MANET due to dynamically changing topologies, lack of centralized monitoring, open medium and bandwidth constraint. Black hole and gray hole attacks are DOS attacks that pose a great threat to the network integrity. To eliminate the effects of Gray hole attack, we have proposed a packet update scheme in which we fetch information from the neighbors for the enquiry of the suspected nodes in the network. Proposed scheme eliminate the gray hole affects by finding all the malicious nodes which are present in the network and send broadcast to whole network for elimination of malicious nodes. Throughput and delay are the parameters for the performance measurements of the network. The simulation work is carried out by OPNET Modeler.

Keywords: ***Wireless Ad-hoc Network, Black Hole Attack, Simulation, Security, AODV, OPNET***

I. INTRODUCTION

Mobile ad hoc networks (MANET) are an infrastructure less network which consist of several movable nodes which communicate and coordinate with each other to transfer packets within the network. Nodes rely on each other due to limited bandwidth. They are mostly applicable in disaster relief operations, military applications; mine cite operations and collaborative computing. Routing is the mechanism of finding the most efficient path towards the destination. The efficiency of the path is measured by various metrics such as number of hops, traffic security etc. Each node has limited communication range in the network and it node acts as a router to forward packets to another node. It is rapidly deployable and highly adaptive in nature. Nodes have high mobility and communication is done via radio broadcast medium. Among all research issues, though, one of the essential research issues in MANETs is security; Denial-of-Service (DoS) attacks are a major class of threat today. Two of the most common DoS attacks are Gray hole and Black hole attacks in MANET. In Black hole attack, the malicious node generates and propagates fabricated routing information and advertises itself as having a valid shortest route to the destined node [3]. If the malicious node replies to the requesting node before the genuine node replies, a false route will be created. Therefore, packets do not reach to the specified destination node; instead, the malicious node intercepts the packets, drops them and thus, network traffic is absorbed [4]. Gray hole attack is an extension of Black hole attack in which a malicious node's behavior is exceptionally unpredictable. A node may behave maliciously for a certain time, but later on it behaves just like other ordinary nodes. Both Black hole and Gray hole attacks disturb route discovery process and degrade network's performance [5].

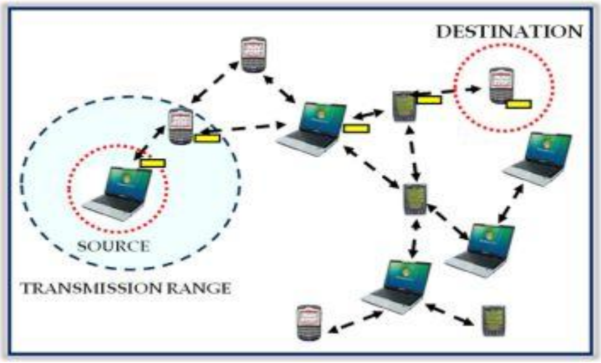

Figure: 1 Mobile Ad hoc Network

II. RELATED WORKS

Research related to MANETs covers many topics such as routing, security, and defence strategies against threats like black hole attacks. This section gives a brief discussion of some of the research that is closely related to the topic of this paper.

Marti et al. [2] presented a method that uses Watchdog and Pathrater to detect black hole attacks. The Watchdog enables neighbour nodes to overhear and detect malicious nodes. Watchdog makes it possible to detect malicious nodes by finding nodes that are deliberately discarding packets. Pathrater assigns a default value to each node and then observes the transmitting behaviour of each node. The value for each node changes based on the transmitting behaviour of that node. After a period of time, if the value for a node is below a certain threshold, the node will be added to the list of black hole nodes. These methods have the same defection to find malicious node, when the neighbour reply wrong observing message. In other words, this method cannot handle collaborative attacks. If the neighbor nodes collude with each other, they may be able to avoid detection.

Lu et al. [3] proposed the SAODV black hole detection scheme for MANETs that is designed to address some of the security weaknesses of AODV and withstand black hole attacks.

Deswal and Singh [4] created an enhanced version of the SAODV protocol that includes password security for each of the routing nodes and routing tables that are updated based on timeliness.

Ramaswamy et al. [5] proposed a method for identifying multiple black hole nodes. They were the first to propose a solution for cooperative black hole attacks. They modified the AODV protocol slightly by introducing a Data Routing Information (DRI) table and a cross checking mechanism. Each entry of the node is maintained by the table. This method uses the reliable nodes to transfer the packets.

Hongmei Deng et al. [6] proposed a methodology that asks every intermediate node to return next hop information along with the RREPs once a route to a destination has been determined. The source node does not transmit data packets to an intermediate node immediately. Instead, the source node waits for the RREPs and the next hop information and then sends Further Request to the next hop in order to determine if there is a route between it and the intermediate node and also to determine if there is a route to the destination. The source node receives Further Reply from the next hop. If the answers are yes for both questions, then the route is built. If the answer to either of the questions is no, then the source node will send an alarm packet to alert other nodes on the network. This methodology has an obvious drawback though. It only can address a single black hole. It cannot prevent cooperative black hole attacks if the next hop colludes with the former. In a situation like this, the source gets the wrong message. Most of the research papers above discussed methods for avoiding black hole attacks against MANETs that are based on the AODV protocol and other protocols. However, our proposed mechanism is a new solution that provides high performance and prevents black hole attacks on the AODV protocol.

III. AODV PROTOCOL

The Ad hoc on demand distance vector routing protocol is one of the widely used routing protocols in MANET. The route is established only when it is desired by the source node for transmitting data packets. Whenever a node requires a route to the destination, a route discovery process is initiated. The source node floods the Route Request packet to its neighbours as shown in fig. 2. The Route Request packet contains source identifier, destination identifier, source sequence number, destination sequence number, broadcast ID and TTL (Time to live). The intermediate node either forwards the packet or prepares a Route Reply if it has a fresh or valid route to the destination. This validity is determined by comparing the sequence number of intermediate node with the destination sequence number of Route Request packet. The destination node or the Intermediate node that has the freshest route sends the Route Reply message back to the source node in the reverse path (fig 3). The source node receives many Route Reply packets and the fresher and shorter path is selected to send the data packet.

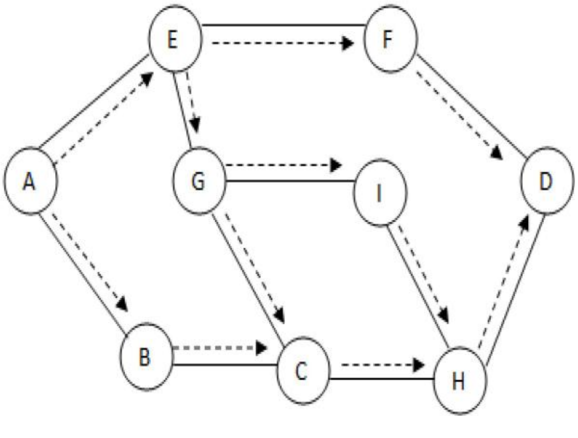

Fig. 2 Propagation of Route Request message

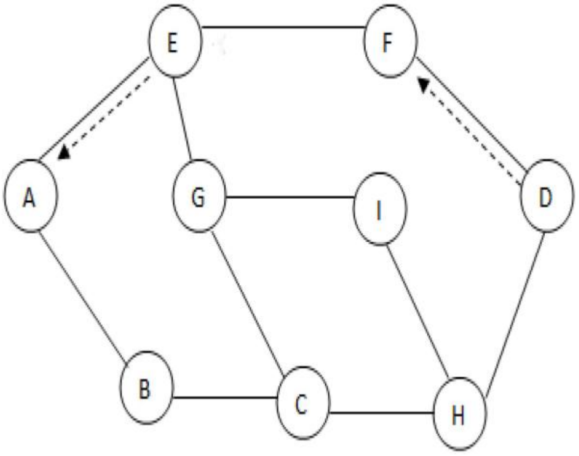

Fig. 3. Path of Route Reply Message

IV. Gray Hole Attack

Gray Hole attack is a variation of the black hole attack in which the malicious node may behave as an honest node first during the route discovery process and then may change its state to malicious and vice versa. This malicious node may then drop all or some of the data packets. The gray hole attack is difficult to detect due to congestion, overload and also due to malicious nature and ability of changing states.

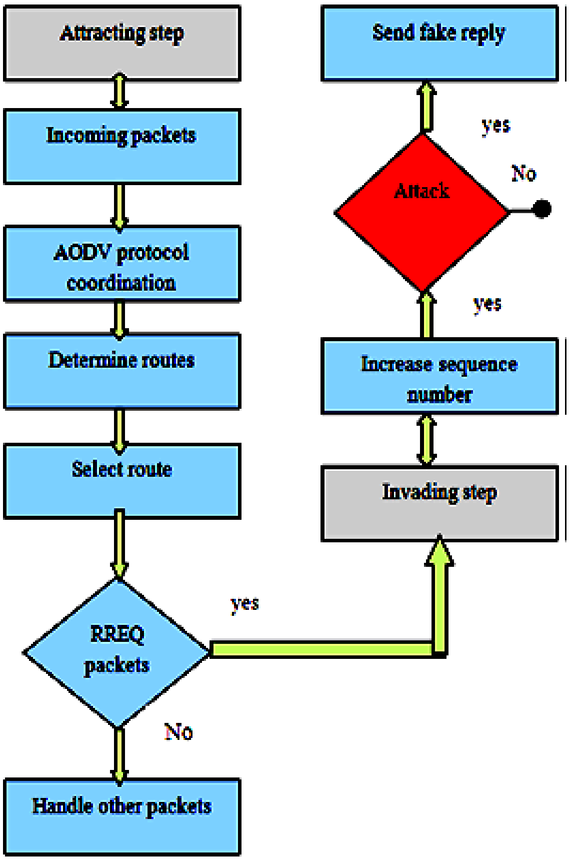

Fig. 4: Gray Hole Attack

V. RESEARCH METHODOLOGY

This research concern to providing solution for the gray hole problem by using multipath algorithm resulting in regaining of the average no. of hops by excluding the attacker nodes. Research has started with creating a MANET in the OPNET simulator by using Random Waypoint mobility Model for providing mobility with AODV as routing protocol as described in figure 5. Basic parameters like, speed of nodes, mobility rate energy carrying capacity, buffer size and average error rate for AODV have been used. Mobility for all the nodes is random waypoint and the trajectory selected for the nodes movement is Vector.

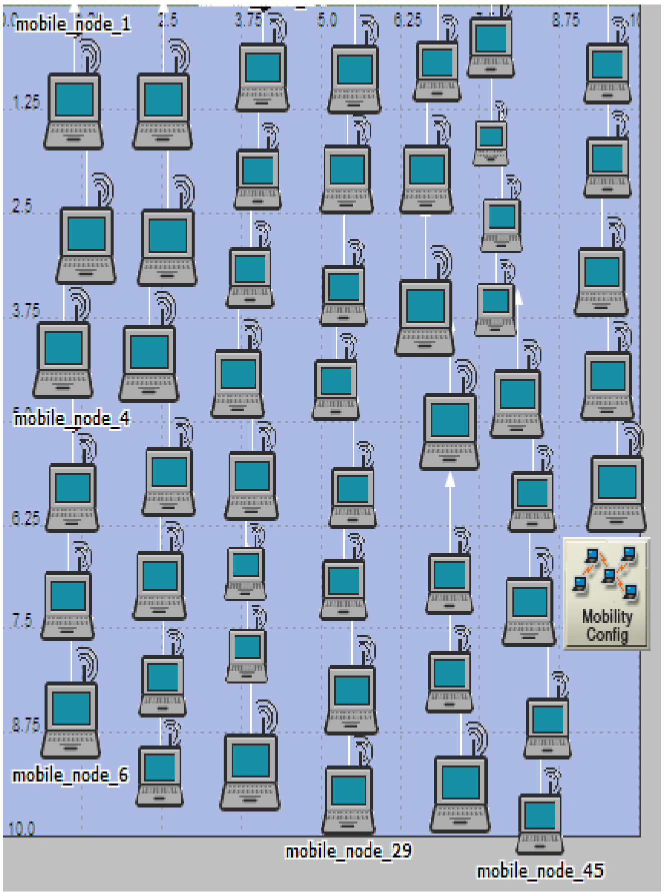

Figure 5: Overall simulation with random waypoint model for mobility

VI. PROPOSED ALGORITHM

To avoid the gray hole attack, proposed algorithm has been implemented in scenario affected by gray hole attacks and this tried to normalize the scenario to its original state. Proposed algorithm, randomly generate a number in between 0 to maximum number of nodes and make the node with same number as transmitter node as gray hole attack is done by transmitter and receiver so have to decide the transmitter and receiver. Then generate the route from selected transmitting node to any destination node with specified average route length. After this it will send packet according to selected destination and start timer to count

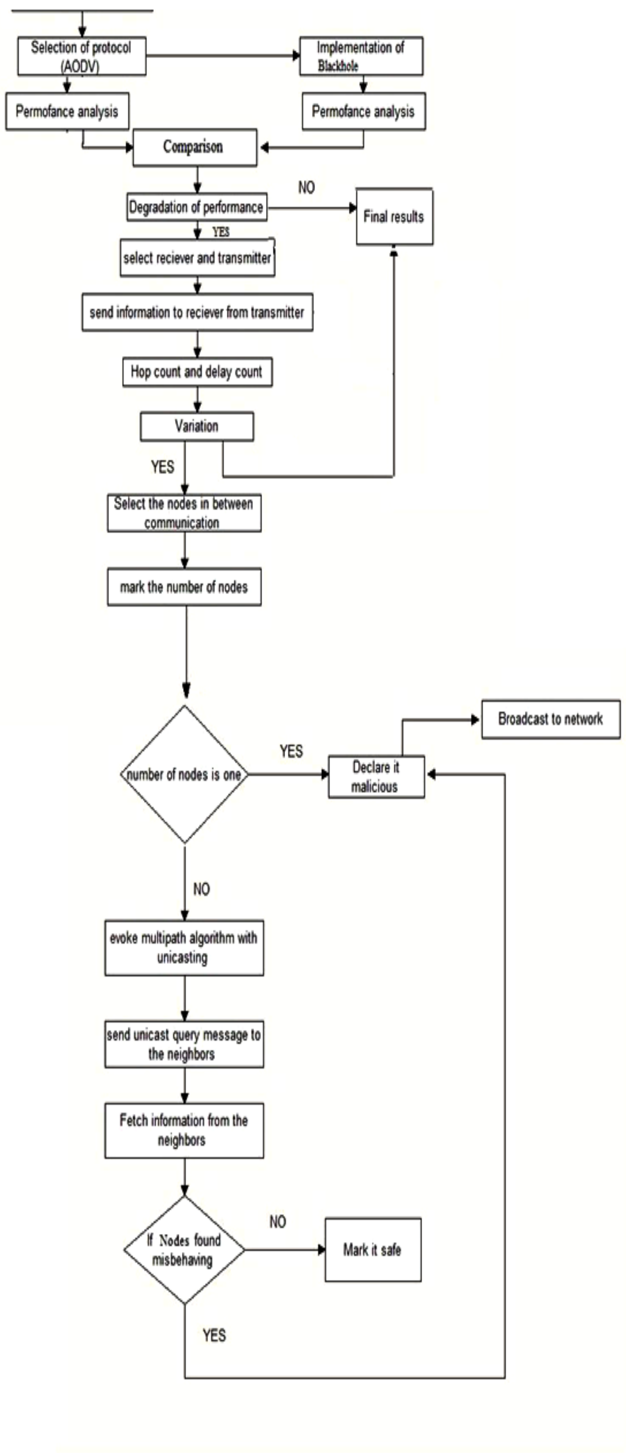
Selection of protocol (AODV)
Implementation of Blackhole
Permofance analysis
Permofance analysis
Comparison
NO
Degradation of performance
Final results
YES
select reciever and transmitter
send information to reciever from transmitter
Hop count and delay count
Variation
YES
Select the nodes in between communication
mark the number of nodes
Broadcast to network
YES
number of nodes is one
Declare it malicious
NO
evoke multipath algorithm with unicasting
send unicast query message to the neighbors
Fetch information from the neighbors
NO
If Nodes found misbehaving
Mark it safe
YES

Figure 6: Proposed Algorithm Overview

hops and delay. By repeating the whole process up to this point will be required as to store routes and their hops and delay. Now for detection of malicious node; if the hop count for a particular route decreases abruptly for average hop count then at least one node in the route must be attacker. Algorithm checked the delay of all previous routes which involve any on node of the suspicious route. The node not encounter previously should be malicious. Now to find out exact malicious node, there is need to repeat the whole algorithm if more than one node is misbehaving and that will take time and resources. So to avoid this condition, transmitter will be seeking help from directly connected neighbours. Neighbours can tell the history of particular node under suspect. The node which is not involved in any of the previous activity considered to be the malicious node. Malicious nodes have been blacklisted by the nodes and hence they are not involved in future routes.

SN: Source Node
DN: Destination Node
IN: Intermediate Node
TH: Threshold
D_Seq : Destination Sequence Number
Seq: Sequence Number

```
1. SN broadcasts RREQ to all Nodes
2. IN receives RREQ and forwards until reach DN
3. DN receives RREQ from SN or IN
4. DN gets Seq from RREQ and verifies with Seq in its routing table
5. If Seq of RREQ is greater than Seq of its routing table
6. DN selects Seq of RREQ and plus one
7. Else
8. DN selects Seq of its routing table and plus one
9. If number of packet drop is large then start discovery of malfunctioning nodes.
10. Source and destination will be decided. Randomly Generate a Number in between 0 to maximum number of nodes. Initiate a source by making transmitter node same selected.
11. Generate the Route from selected transmitting node to any destination node with specified average route length.
12. Send packet to destination
 {
13. Start timer (Record (Hop Count, Delay))
14. Counter (Threshold (Hop Count, Delay))
{
15. Store (Route, Hop Count, Delay)
Continue the process
}
16. Gray hole Detection
 {
17. Hop count < Threshold Then Check Delay
 }
18. Malicious Node Selection N is the number of nodes.
 {
19. If N = 1 Then it is the attacker Else Send Route Query to neighbours
{
20. If neighbour detect similar malfunctioning Then mark it malicious.
21.  Else
 {
22.  Repeat process
```

}

23. Send gray_ announcement message to all nodes. Any node receives gray_ announcement message it removes gray hole node id from its neighbour table and Routing Table.

24. If any forwarding node receives gray_ announcement message it will send RERR message to source. It will reinitiate route discovery process, and find the new path to the destination without gray hole node.

25. End.

VII. RESULTS

Basic parameters used for experimentation with OPNET simulator. Area for communication is 2000 × 2000 meters with 60 mobile nodes. The performance comparison of three scenarios in term of throughput is explained in figure 3 The overall simulation performance is presented in nutshell in the following table, which indicates that the elimination of gray-hole attack scenario provides the better results and try to normalize the gray-hole effected network to its normal state as close as possible. The Throughput represents the packets travels from source to destination. In first scenario of our experimentation, packets travels are shown as throughput with peak value of approx. 268678 and it is represented as bits per second. In second scenario which is with gray hole attack, packets drops which are represented as throughput, decreases to value of approx. 188933 bits per second.

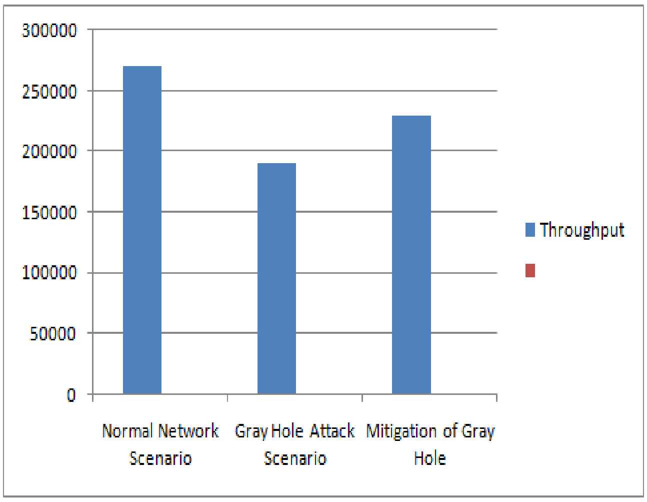

Figure 6: Throughput variation for three scenarios

This drop of packets in form of throughput is due to the gray hole effect as in case of gray hole packet drop increases as explained in this s scenario with throughput decrease. The recovery of the throughput takes place with proposed mechanism by elimination of the gray hole attack as throughput comes to similar to the normal scenario. Similarly delay decreases due to the gray hole introduction into the second scenario due to the property of gray hole scenario as in gray hole attack, delay is low so in our experimentation delay is low and with solution of gray hole delay comes to normal.

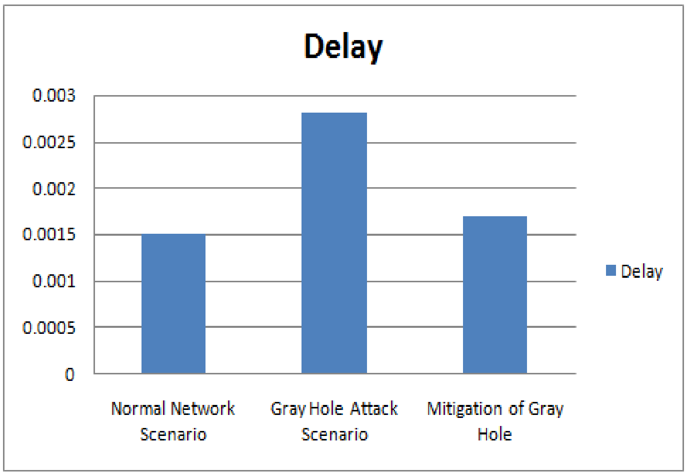

Figure 7: Delay variation for three scenarios

CONCLUSION

The main concern of this work to show the performance of AODV under normal surroundings, under gray hole attack and performance after elimination of gray hole attack in term of delay, throughput and traffic received. The network performance with gray hole attack in term of throughput decreases around 188933 bits per second. By our proposed approach, we have recovered around 234544 in throughput. The network performance with gray hole attack in term of end to end delay increases around 54% and with our proposed approach, we have recovered around 45% in delay. Concept has shown improved results after elimination of the gray-hole attack in the simulation. Elimination of malicious nodes takes place on Network layer by broadcasting the information of malicious nodes. Overall, elimination of gray hole attack has been done so that ad-hoc communication can be normalized as normal communication. It will be very useful in saving a lot of resources for mobile ad-hoc communication as we have used unicasting process instead of broadcasting which saves resources as malicious nodes are only detected through partial multicasting process.

REFERENCES

[1] Fatima Ameza, Nassima Assam and Rachid Beghdad, “Defending AODV Routing Protocol Against the Black Hole Attack”, International Journal of Computer Science and Information Security, Vol. 8, No.2, 2010, pp.112-117.

[2] Nital Mistry, Devesh C. Jinwala and Mukesh Zaveri, “Improving AODV Protocol against Blackhole Attacks”, International Multiconference of Engineers and Computer Scientists 2010, vol. 2, March 2010.

[3] Payal N. Raj and Prashant B. Swadas,”DPRAODV: A dynamic learning system against black hole attack in AODV based Manet”,

International Journal of Computer Science Issues, Vol. 2, Issue 3, 2010, pp: 54-59.

[4] Hoang Lan Nguyen and Uyen Trang Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks", International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, April 2006, pp. 149-149

[5] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah, "MANET Routing Protocols and Wormhole Attack against AODV", International Journal of Computer Science and Network Security, vol. 10 No. 4, April 2010, pp. 12-18.

[6] N. Shanthi, Dr. Lganesan and Dr.K.Ramar, "Study of Different Attacks on Multicast Mobile Ad hoc Network", Journal of Theoretical and Applied Information Technology, December 2009, pp. 45-51.

[7] Abhay Kumar Rai, Rajiv Ranjan Tewari and Saurabh Kant Upadhyay , "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security, vol. 4 issue 3, July 2010, pp. 265-274.

[8] Jakob Eriksson, Srikanth V. Krishnamurthy, Michalis Faloutsos, "TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks", 14th IEEE International Conference on Network Protocols, November 2006, pp.75-84.

[9] Mahdi Taheri, Dr. majid naderi, Mohammad Bagher Barekatain, "New Approach for Detection and defending the Wormhole Attacks in Wireless Ad Hoc Networks", 18th Iranian Conference on Electrical Engineering,, May 2010, pp. 331-335.

[10] Dang Quan Nguyen and Louise Lamont, "A Simple and Efficient Detection of Wormhole Attacks", New Technologies, Mobility and Security, November 2008, pp. 1-5.

[11] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, "Analysis of Wormhole Intrusion Attacks in MANETs", Military Communications Conference, November 2008, pp.1-7.

[12] Maria A. Gorlatova, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano, "Detecting Wormhole Attacks in Mobile Ad HocNetworks through Protocol Breaking and Packet Timing Analysis", Military Communications Conference, October 2006, pp. 1-7.

[13] Mani Arora, Rama Krishna Challa and Divya Bansal, "Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", Second International Conference on Computer and Network Technology, 2010, pp. 102-104.

[14] Yih-Chun Hu, Adrian Perrig,and David B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, February 2006, pp. 370-380.

[15] W. Weichao,B. Bharat, Y. Lu and X. Wu, "Defending against Wormhole

[16] Attacks in Mobile Ad Hoc Networks", Wiley Interscience, Wireless Communication and Mobile Computing, January 2006.

[17] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multipath," IEEE Wireless Commuunication. and Networking Conference,

[18] I. Khalil, S. Bagchi, N. B. Shroff," A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", International Conference on Dependable Systems and Networks, 2005.

[19] L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach", IEEE Communication Society, WCNC 2005.

[20] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", 11th Network and Distributed System Security Symposium, pp.131-141, 2003.

[21] L.Lazos, R. Poovendran, "Serloc: Secure Range-Independent Localization for Wireless Sensor Networks",ACM Workshop on Wireless Security, pp. 21-30, October 2004.

[22] W. Wang, B. Bhargava, "Visualization of Wormholes in sensor networks", ACM workshop on Wireless Security, pp. 51-60, 2004.

[23] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE, April 2004, pp.96- 97.

[24] Anu Bala, Munish Bansal and Jagpreet Singh, "Performance Analysis of MANET under Blackhole Attack", First International Conference on Networks & Communications, 2009, pp. 141-145.

[25] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007, pp. 21-26.

[26] Geng Peng and Zou Chuanyun,"Routing Attacks and Solutions in Mobile Ad hoc Networks", International Conference on Communication Technology, November 2006, pp. 1-4.

[27] S. Lee, B. Han, and M. Shin, "Robust Routing in Wireless Ad Hoc Networks", International Conference on Parallel Processing Wowrkshops, August 2002.

[28] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato1, Abbas Jamalipour, and Yoshiaki Nemoto1," Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, vol..5 no..3, Nov. 2007, pp.338–346.

[29] Nadia Qasim, Fatin Said, and Hamid Aghvami, "Performance Evaluation of Mobile Ad Hoc Networking Protocols", Chapter 19, pp. 219-229.

[30] G.S. Mamatha and S.C. Sharma, "A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS", International Journal of Computer Science and Security, vol. 4, issue 3, Aug 2010, pp. 275-284.

[31] Preetam Suman, Dhananjay Bisen, Poonam Tomar, Vikas Sejwar and Rajesh Shukla, "Comparative study of Routing Protocols for Mobile Ad- Hoc Networks", International Journal of IT & Knowledge Management, 2010.