Volume 4, Issue 8, August 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Efficient Approach for the Detection of Wormhole Attack Using Dynamic Source Routing Protocol in MANET

Farman Ahmed
ECE, GRDIMT, Dehradun,
India

Ankit Jha
ECE,GRDIMT, Dehardun,
India

Neeraj Kumar
CSE ITR, Roorkee,
India

Abstract -Wireless networks are playing very important role in the present world. Mobile Ad hoc Networks (MANET) are the extension of the wireless networks. These networks are playing crucial role in the each and every field of the human life. They are used in those places where a simple wireless network cannot use. They play a significant role in real tile applications such as military applications, home applications wireless sensor applications etc. Due to their adaptive nature they are threatened by number of attacks such as Modification, Black Hole attack, Wormhole attack etc. Wormhole attack is one of the dangerous active attacks in the mobile Ad hoc Networks (MANET). In this thesis we described a secure and efficient approach for the detection of the wormhole attack in the Mobile Ad Hoc Networks (MANET). The algorithm is implemented in a very popular on demand routing protocol, called DSR (Dynamic Source Routing) protocol. In this approach we provide the solution by sending the Hound Packet in the order of Fibonacci series and also modify the table entries in terms of storing them in sorted order, so that the processing of Route Discovery becomes faster.

Keywords- Wormhole attack, DSR, AODV, MANET, Packet Delivery.

I. INTRODUCTION

Wireless network enables communication between computers using standard network protocols, without network cabling. These networks use radio waves or microwaves as a communication medium. These networks are widely used nowadays because of their great advantages over a wired network. Some of them are:

- Setup of these networks is easy and fast as compare to wired networks.
- These networks are more flexible than the wired network as they can be used in those places where a wired network cannot be used.

Wireless Networks can be classified mainly into two categories

- Infrastructure Wireless networks
- Infrastructure less Wireless Networks

A. *Infrastructure Wireless Networks*

In these types of networks, communication takes place between the Wireless nodes through the Access Point (AP) and the wireless nodes cannot communicates directly. The access point just not works as a control medium access, but acts as a bridge as well. In these types of networks base stations are fixed as the node goes out of the range of a particular base station; it gets the service of other base station.

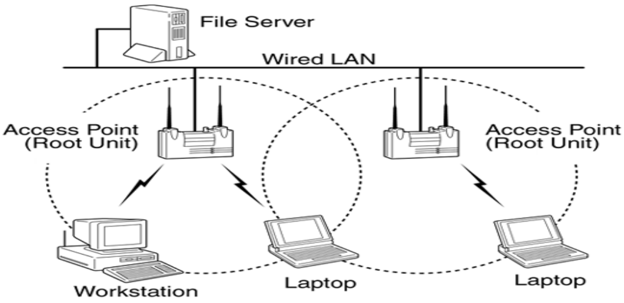

Fig.1. An Infrastructure Network

B. *Infrastructure-less Wireless Networks*

These types of networks do not need any fix infrastructure for the communication. These networks are also called Ad Hoc Networks. In these types of networks, each node can communicate directly with other node and thus there is no requirement of the access point. These networks don't have any fixed or static topology. The nodes can move anywhere at any time, so they form a dynamic topology. These networks use multi hop wireless links. An important example of this type of network is Mobile Ad hoc Networks (MANET).

II. MOBILE AD HOC NETWORKS (MANET)

Mobile Ad hoc networks are collection of mobile nodes that use wireless transmission for communication. These networks have no fixed infrastructure, no fixed configuration and no other controlling device such as router etc. The setup or deployment of these networks is very easy because these networks don't have a fixed infrastructure or a fixed topology also they have a very less setup time. . The routers are free to move randomly and organize themselves dynamically.

It means, these networks don't have static topology, they form the topology dynamically temporary network without the aid of any established infrastructure or centralized administration. Such networks received considerable attention in recent years in both commercial and military applications, due to the attractive properties of building a network on the fly and not requiring any preplanned infrastructure such as a base station or central controller. These networks are mainly used in military, researchers, business, students, and emergency services.

III. ROUTING PROTOCOLS

A. Routing in MANET:

Routing is an important function of the network layer. Routing is a process used to determine the route between the source and the destination. The main purpose of the routing is to determine the shortest route between the source and the destination.

The routing can be classified into two types:

- Non adaptive Routing
- Adaptive Routing

Non Adaptive routing (also called, Static routing) refers to the routing strategy being stated manually or statically, in the router. In this type of routing, each node maintains a routing table. Adaptive routing (also called, Dynamic Routing) refers to the routing strategy that is being learnt by an interior or exterior routing protocol. In this type of routing, every time a node search the shortest path, when it want to communicate with another node.

Some important routing techniques, which mostly used are

- Distance Vector Routing
- Link State Routing
- Flooding
- Source Initiated Routing

B. Classifications of Routing Protocols

Routing protocols can be classified as:

- **Pro-Active Routing Protocols :**

In this type of protocols each node maintains one or more tables containing routing information about all other node in the network.some are mention below:

- **DSDV** (Destination sequenced distance vector routing) protocol
- **WRP** (Wireless Routing Protocol)
- **STAR** (Source Tree Adaptive Routing) Protocol
- **CGSR** (cluster head gateway Switch routing)

- **Reactive Routing:**

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. Examples are:

- **DSR** (Dynamic Source Routing) Protocol
- **AODV** (Ad Hoc on Demand Distance Vector) Routing Protocol
- **TORA** (Temporary Ordered Routing algorithm) Protocol
- **(ZRP)** Zone Routing Protocol

IV. DSR AND WORMHOLE ATTACK

A. Dynamic Source Routing (DSR) Protocol:

Dynamic Source Routing (DSR) protocol is one of the most popular Reactive routing protocols. It is very useful for multi hop Mobile Ad Hoc Networks. In Mobile Ad Hoc Networks the nodes can move or join a network at any time. So we need a protocol which maintains the routing dynamically. So we use reactive routing protocol for these types of networks. DSR is one of the most popular of them. DSR is highly reactive in nature, so it maintains the successful delivery of packets in a very reliable manner.

There are two important mechanisms in DSR

- Route discovery mechanism
- Route maintenance mechanism

Route discovery mechanism is used to find the route between the sender and the receiver. When a node want to send some data to another node it called the route discovery mechanism.

With the help of Route Maintenance mechanism source node can detect that the communication route is OK or it is broken. It can detect that a route is broken by checking that there is no communication since a long time.

B. Security Threats in DSR

Mobile Ad Hoc Networks are unwired network with continuous changing topology (dynamic topology). So, they are very vulnerable to security threats. In protocol stack, Physical layer, which is the first layer is provide the functions like forming the network topology, synchronization, medium access control and flow control etc. this layer has security issues like Denial of Service (DoS) attacks and preventing signal jamming. Network layer is the second layer that provides one of the important the function called routing and logical addressing. Network layer has to deal with security of ad-hoc routing protocol and related parameters. Some dangerous attacks occur in network layer are black hole attack, wormhole attack, gray hole attack and message altering etc. transport layer is the third layer in the protocol stack.

Transport layer is responsible for end to end communication, segmentation and reassembly, flow and error control etc. Transport layer has issues with end to end data security with encryption methods and Authentication. Session hijacking is one kind of attack that can be occurring in the transport layer.

- **Active Attacks:**

Active attacks are the kind of attack in which the attacker can see the information of a user and can modify it too. These attacks contain some modification on the actual data or a false data. In these attacks, the attacker injects arbitrary packets into the network.

- **Passive Attacks:**

In a passive attack the attacker can learn or use the information of a user but does not modify nor change it. In a passive attack, the attacker does not change or alter the operation of a routing protocol but only attempts to discover valuable information

- **The Wormhole Attack**

In Physics, a **Wormhole** is a hypothetical shortcut through space and time that connects one universe with another or allows faster-than-light travel between two locations in the same universe. The term wormhole describes an attack on Mobile Ad-hoc Network (MANET) routing protocols in which two or more malicious nodes shows that two remote regions of a MANET are directly connected through nodes that appear to be neighbours, while in reality they are not [20]. the network so that it is routed through them.

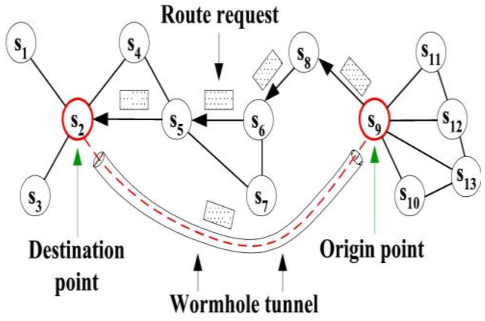

Fig.2 Wormhole Attack

Wormhole attack is one of the most dangerous attacks in the mobile Ad Hoc Networks. It is a Kind of attack which works on the network layer.

In wormhole attack, two or more malicious nodes combined together and makes a tunnel (create a link from a private connection) in the network, in which the traffic is enter from one end and passes through the tunnel and leaves from the other end. This is one kind of active attack, which generally occurs in the network layer. It is the one of the most dangerous attack in mobile ad hoc networks. This exploit allows a node to use the short route than the normal route flow which is controlled by the attacker nodes (wormholes) [20].A wormhole attack is composed of two or more attacker (malicious) nodes and a wormhole tunnel. To create a wormhole attack, malicious nodes create a direct link among them, referred to as a wormhole tunnel. 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.

C. Types of Wormhole Attacks :

The wormhole attacks are classified as

- In-band wormhole attacks
- Out-of-band wormhole attacks

- **In-band wormhole attacks:**

It require a covert overlay over the existing wireless medium and in-band wormholes, which covertly connect the purported neighbors via multi-hop tunnels through the primary link layer [22]. In-band wormholes are important for several reasons

- **Out-of-band wormhole attack:**

It requires a hardware channel to connect two colluding nodes. It covertly connects purported neighbours via a separate communication mechanism, such as a wire line network or additional RF channel that is not generally available throughout the network.

V. THE PROPOSED WORK

Wormhole attack is one of the most dangerous attacks in the Mobile Ad Hoc Networks. A lot of work has been done by the researchers on this attack. A lot of solutions proposed to identify and detect the wormhole attack in the mobile ad hoc networks. We studied a lot of research papers based on the identification and the removal of the wormhole attack and select one of them as my base paper to start the work and provide the modification on this. Next subsections will describe about the gaps in the previous approaches, proposed algorithm, and about the simulator used for the simulation. In this paper, the proposed research work provides some modification on the existing approach and designs a secure and very efficient approach for the detection of the Wormhole nodes. In the proposed work following things are done:

A. It is implemented on DSR (Dynamic Source routing) Protocol:

The first change did in the propped work is that this work is implemented in the DSR protocol instead of the AODV protocol as most of the implementations on the wormhole attack are implemented on the AODV protocol.

B. Send Hound Packets in the Fibonacci Pattern:

In this proposed work, rather than sending the Hound packet as did in the previous work, the Hound packets are sent in the Fibonacci series pattern. The main benefit of this approach is that this approach will take less time (reduce the processing delay) than the previous approach because, simply we know that when we start the routing process, the sender doesn't know anything about the other nodes, so the chance of the attacking by the attacker (wormhole) node is much more at the time of starting means if there is an attack we can find in earlier stage in dense broadcast.

C. Stored table Entry in Sorted Form

In this proposed work, the table entries always stored in the sorted form. So this will improve the speed of the searching. Means the searching will be faster than some of the previous approaches.

VI. THE ALGORITHM

The first thing did in this work is that it is implemented DSR routing protocol. And the algorithm always stores the table entries in the sorted form and the main thing of the algorithm is that the Hound packets are sent in the Fibonacci series pattern. So the numbers of packets are less than as in the previous approaches and because every hound packets need extra processing delay, this approach reduces the processing delay in comparison to the previous approaches. The algorithm is given below,

Algorithm:

```
Step 1:
 Initialization Process:
        Start the route discovery phase (process) with the source node S.
 Step 2:
At source Node
    Initially $S3_{src}$=1, $S2_{src}$=1, $S1_{src}$=0;
    Initially $Pcount_{src}$=0;
    $Pcount_{src}$ = $Pcount_{src}$ + 1
    If ($Pcount_{src}$ == $S3_{src}$)
        {
          Source node creates a Modified Root Reply packet which contain all nodes identity of  recent   path,
          And MD of packed signed by its private key.
          And then send this Packet to its all neighbor node
         }
        $S1_{src}$=$S2_{src}$;
         $S2_{src}$=$S3_{src}$;
        $S3_{src}$=$S1_{src}$+$S2_{src}$;
Step 3:
All Network Nodes
   Each node periodically sends its public key to its one hope neighbor. Nodes who receive MRR packet first increments
the CRNH field for the first node entry whose P.B is 0.
```

```
 If (Any of the nodes listed in the MRR packet is its neighbor)
Then
        Set all P.B in the packet till node entry to which it is a neighbor
 Otherwise
        Forward it.
```

Step 4:

At Destination Node

```
        Destination node create table for each entry of special RR packet.
        This table contain three fields “Node id”, “Process bit” and “count to reach next hope”
```

Step 5:

```
        Calculate difference of each row
        If (difference > 4)
        Node and its previous node in the path may forming wormhole and will be malicious    node.
```

- **Network Simulator (NS) -2**

We used one of the most popular and well known simulators, called NS-2 simulator and also trace the simulation in NAM (Network Animator. The next subsection describes about these.

VII. RESULTS

- **Computational results:**

Comparison results are shown based on various parameters. The sub sections below showing the results based on mobile nodes, comparison graphs etc.

- **Simulation Scenario of 50 mobile nodes:**

The mobile Ad Hoc network comprising of 50 mobile nodes is constructed in the NS-2 simulator with the use of OTCL script in the topological boundary area of 670 m x 670 m. The position of mobile nodes is defined in terms of X and Y coordinates values and it is written in the movement scenario file. Simulation is shown on the NAM (Network Animator).

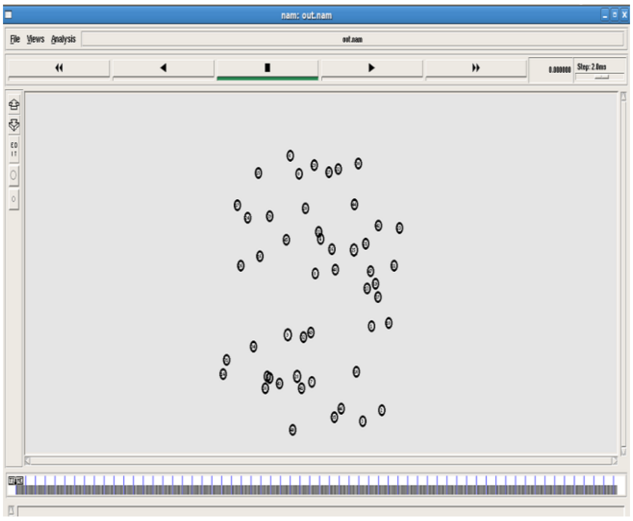

Fig.2 A Screenshot of 50 Mobile Nodes Implementing DSR Protocol

.

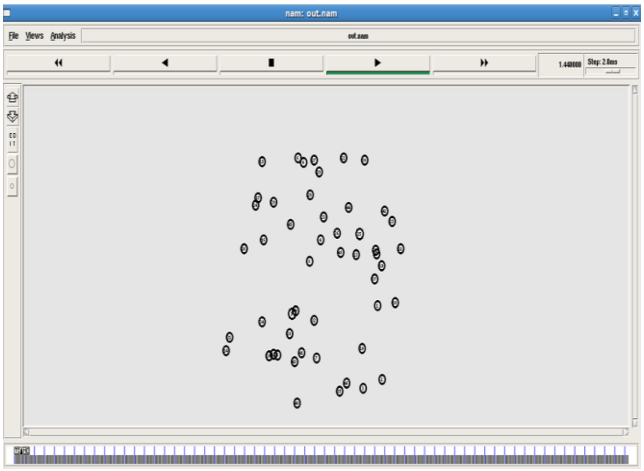

Fig. 6.2(a) A Screenshot of 50 Mobile Nodes at time t=1.440 sec.

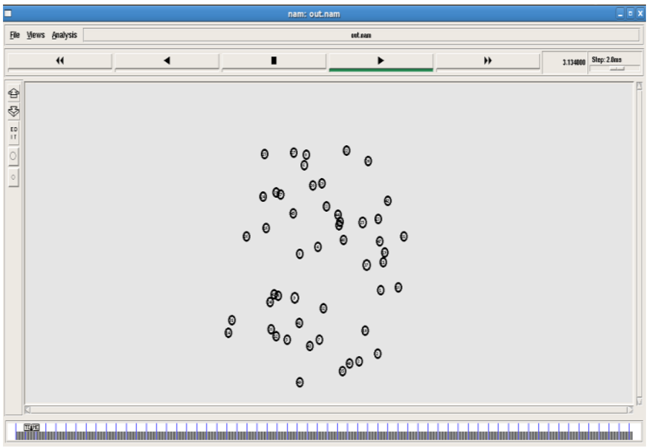

Fig. 3 A Screenshot of 50 Mobile Nodes at time t=3.13440 sec.

- **Average End to End Delay Graph:**

This metric is basically used to describe the average time to send a packet from source to the destination. This time is always measured in seconds. Basically this graph is used to describe the end to end delay in msec. in this case the end to end delay for the simple DSR protocol is shown by the dark blue color, for the case where there are attacker nodes presented the end to end delay is shown by the red color and in the case where we implement our algorithm in the wormhole infected network, the graph is shown by the green color**.** And we can clearly see that our algorithm reduces the average end to end delay.

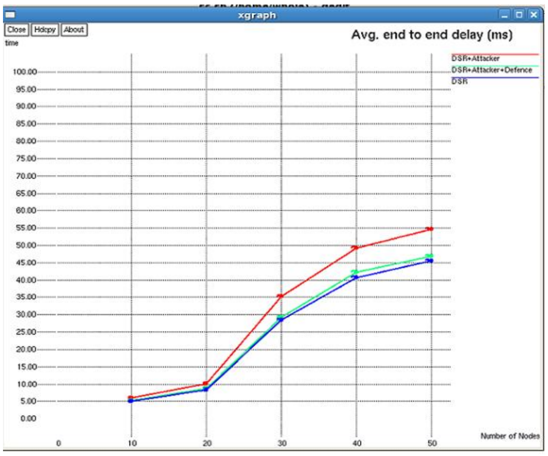

Fig.4 A Screenshot of Average End to End Delay (in msec.)

- **Packet Delivery Ratio Graph:**

This metric is one of the important metric used to simulate the performance of the routing protocols. This metric is basically used to describe the ratio of the total incoming packets and the actual received packets by the destination. Basically this graph is used to describe the Packet delivery ratio. In this case the Packet delivery ratio for the simple DSR protocol is shown by the dark blue color, for the case where there are attackers nodes presented the Packet delivery ratio is shown by the red color and in the case where we implement our algorithm in the wormhole infected network, the Packet delivery ratio graph is shown by the green color**.** And we can clearly see that our algorithm increases the packet delivery ratio.

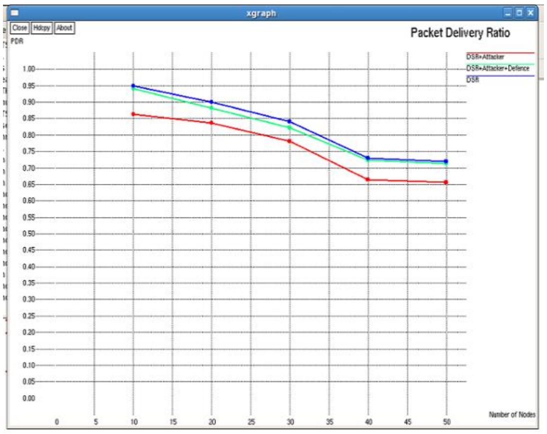

Fig. 5 A Screenshot of Packet Delivery Ratio Graph

- **Throughput Graph :**

This metric is basically used to describe the total number of bits send to the physical layer per second. So it is always measured in bps. It means it describes total data received by the receiver divided by the total time it taken. Basically this graph is used to describe the Throughput in Kbps. In this case the Throughput for the simple DSR protocol is shown by the dark blue color, for the case where there are attacker nodes presented the Throughput is shown by the red color and in the case where we implement our algorithm in the wormhole infected network, the graph for Throughput is shown by the green color**.** And we can clearly see that our algorithm increases the Throughput.

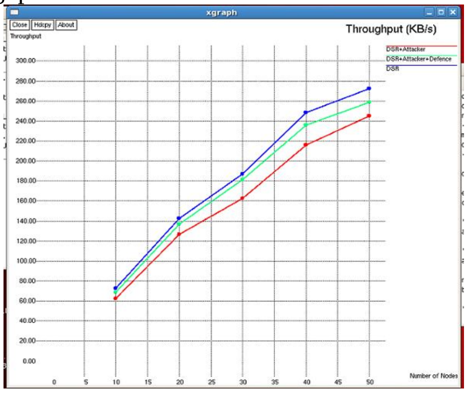

Fig. 6 A Screenshot of Throughput (in Kbps) Graph

VII. CONCLUSION AND FUTURE SCOPE

Mobile Ad hoc Networks (MANET) are playing very important role in today world. Due to their great properties they are used in those places where a wired network or even a simple wireless network cannot use. I have studied a lot of approaches for identification and removal of the wormhole attack and proposed a secure and efficient solution.

In the proposed work we described a secure and efficient approach for the detection of the wormhole attack in the Mobile Ad Hoc Networks (MANET). The algorithm is implemented in DSR (Dynamic Source Routing) protocol. In the proposed approach we provide the solution based on the Hound packet with the two modifications

The comparison graphs show the results in the three cases- when there is no attacker and we are using simple DSR protocol, when there are attacker nodes (wormhole nodes) and the last when there are attacker nodes and we implement the algorithm as well.

REFERENCES

[1] An infrastructure network, URL: http://support.dell.com/support/edocs/network/79pcf/w iredlan.gif.

[2] An infrastructure less network, URL: http://perso.crans.org/raffo/papers/phdthesis/adhoc.png [1] Sunil Taneja and Ashwani Kush, "A Survey of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010 ISSN: 2010-0248 "Ad Hoc Wireless networks" By Shivarammurthy, Pearson Education

[3] T. Lin, S. Midkiff, and J. Park, "A framework for wireless ad hoc routing protocols", in WCNC: Wireless Communications and Networking. IEEE Computer Society, 2003, pp. 1162.1167.

[4] Arun Kumar, lokantha Reddy and Prakash Hiremath, "Performance Comparison of Wireless Mobile Ad-Hoc Network Routing Protocols", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6, June 2008

[5] V. Nazari, K. Ziarati, "Performance Comparison of Routing Protocols for Mobile Ad hoc Networks", IEEE 2006.

[6] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad-Hoc Wireless Networks," Mobile Computing, T. Imielinski and H. Korth, Eds.,Kluwer, 1996, pp. 153–81.

[7] Elizabeth M. Royer and Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communications • April 1999

[8] Broch Joch, Maltz David A., etc., "A performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols", Fouth Annual ACM/IEEE International Conference on Mobile Computing and Networking, 1998.

[9] V. Park and M. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," Proceedings of IEEE NFOCOM 97, April 1997.

[10] P. Krishna, N. H. Vaidya, M. Chatterjee, and D. K. Pradhan, " A cluster-based approach for routing in dynamic networks". ACM SIGCOMM Computer Communication Review, 27:49–65, 1997.

[11] Tutorial for DSR Protocol. www.ietf.org/**rfc**/**rfc4728**.txt

[12] Josh Broch, David B. Johnson, and David A. Maltz. "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks". Internet-Draft, draft-ietf-manet-dsr-03.txt, October 1999. Work in progress. Earlier revisions published June 1999, December 1998, and March 1998.

[13] H. Lundgren, D. Lundberg, J. Nielsen, E. Nordstr¨om, and C. F. Tschudin. “A Large-scale Testbed for eproducible Ad hoc Protocol Evaluations”. In IEEEWireless Communications and Networking Conference 2002 (WCNC), March 2002.

[14] Anuj K. Gupta, Dr. Harsh Sadawarti, and Dr. Anil K. Verma, “Performance analysis of AODV, DSR & TORA Routing Protocols”. IACSIT International Journal of Engineering and Technology, Vol.2, No.2, April 2010 ISSN: 1793-8236

[15] Pearlman, Marc R., Haas, and Zygmunt J, “Determining the Optimal Configuration for the Zone Routing Protocol”, August 1999, IEEE Journal on Selected Areas in Communications, Vol. 17, No. 8

[16] S. R. Das, R. Castaneda, J. Yan, and R. Sengupta, “Comparative performance evaluation of routing protocols for mobile, ad hoc networks,” in Proceedings of 7th International Conference on Computer Communications and Networks (IC3N ’98) pp. 153 161, Lafayette, La, USA, October 1998

[17] D. B. Johnson and D. A. Maltz, “Dynamic Source Routing in Ad-Hoc Ad hoc Networks," Mobile Computing, ed. T. Imielinski and H. Korth, Kluwer Academic Publishers, 1996, pp. 153-181.

[18] G.S. Mamatha, Dr. S.C. Sharma, “Network Layer Attacks and Defense Mechanisms in MANETS- A Survey”**,** International Journal of Computer Applications (0975 – 8887) Volume 9– No.9, November 2010

[19] N.Shanthi, Ganesan And Ramar**, “**Study of Different Attacks on Multicast Mobile Ad Hoc Networks”, Journal of Theoretical and Applied Information Technology © 2005 - 2009 JATIT. All rights reserved.

[20] Prof. (Dr.) Debika Bhattacharyya , Prof.(Dr.) P. K. Banerjee and Himadri Nath Saha, “A Distributed Administration Based Approach for Detecting and Preventing Attacks on Mobile Ad Hoc Networks” , International Journal of Scientific & Engineering Research Volume 2, Issue 3, March-2011 1 ISSN 2229-5518

[21] Y.-C. Hu, A. Perrig, and D. B. Johnson,” Packet leashes: A defense against wormhole attacks in wireless ad hoc networks”, Technical Report TR01-384, Department of Computer Science, Rice University, December 2001.

[22] Hu, Y.-C., Perrig, A., und Johnson, D.: Ariadne, ” A secure on-demand routing protocol for ad hoc network”, 8th Conference on Mobile Computing and Networking (ACM Mobicom2002), Atlanta, Georgia. S. 12–23. September 2002.

[23] Kuldeep Sharma**,** Dr.G.Mahadevan, “Advance Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET”, Int. J. on Recent Trends in Engineering & Technology, Vol. 05, No. 01, Mar 2011.

[24] .Marianne A. Azer, , IEEE, Sherif M. El-Kassas, and Magdy S. El-Soudani, “ An Innovative Approach for the Wormhole Attack Detection and Prevention In Wireless Ad Hoc Networks”, in IEEE Conference, 2008.

[25] Rajpal Singh Khainwar1, Mr. Anurag Jain, Mr. Jagdish Prasad Tyagi, “Elimination of Wormhole attacker node in MANET using performance evaluation multipath algorithm”, International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459,Volume 1, Issue 2, December 2011)