Performance Analysis of DYMO Routing Protocol under Wormhole Attack in MANET

Sanghita Deka, Department of CSE, ManavRachna International University Faridabad, India
Madhumita Khaturia, Department of CSE, ManavRachna International University Faridabad, India

***Abstract*— In Mobile Ad-hoc Network routing is a very challenging task because of the dynamic topology and lack of pre-existing infrastructure network. In these type of network, each mobile node communicating with each other and can be able to move expeditiously in any direction. In MANET routing protocols must adapt to frequent or continual changes in the topology. Dynamic Mobile Ad-hoc Network On-demand (DYMO) routing protocol is one of the protocols which is intended for the use by the mobile nodes. In this paper, we simulated the Wormhole Attack on DYMO routing protocol using NS-2.34 simulator and analyse the performance of network by using the parameters like Packet Delivery Fraction, end-to end delay and throughput and finally plot the graphs for packet loss and throughput by using the xgraph.**

***Index Terms*—MANET, DYMO, Wormhole Attack, Security, NS-2.34.**

.

I. INTRODUCTION

MANET (Mobile Ad-hoc Network) is a infrastructure less network where nodes can leave or join the network at any time and play a dual role of host as well as router. Without a centralized authority control the communication takes place among the nodes, where each node independently transmits the packets by evaluating the nearest proximity of next available node. The main advantages of such network are rapid deployment and low cost of operation, since the mobile nodes and wireless hardware are inexpensive and readily available and the network is self-configuring and self-maintaining.

II. ROUTING PROTOCOL

There are many types of routing protocols like proactive routing protocol is also known as table-driven routing protocol, Reactive routing protocol also known as on-demand routing protocol and hybrid routing.

In proactive protocols each node maintains routing information i.e., how to reach the destination node. Here the nodes must be able to exchange messages periodically with routing information to keep the routing tables up-to-date. Because of the dynamic nature of ad hoc networks, a considerable number of routing messages may have to be exchanged in order to keep routing information updated among the nodes.

Unlike proactive protocols, reactive protocol creates the routes on demand whenever necessary. In case of these types of protocols, nodes compute the routes and maintain routing

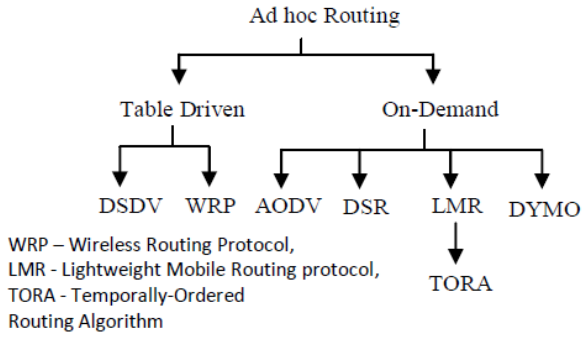

Fig: Classification of routing protocols

information only when it is needed, thereby establishing routes as and when required by the source. The routes are maintained as long as the route is required and the destination is accessible along every possible path from the source. As reactive routing protocols flood the networks to discover the route, they are not optimal in terms of bandwidth utilization, but they scale well in the frequency of topology change. Again hybrid protocols are the combination of both the proactive and reactive protocol.

III. DYMO PROTOCOL

Dynamic Mobile Ad-hoc Network On-demand (DYMO) It is a reactive routing protocol which generates a path on demand source wants to send data to destination. It is a successor of AODV protocol with a path accumulation feature. It uses hop by hop routing concept of sequence number and link reversal. Each node maintains its own sequence number. The sequence number is incremented each time the node sends a route request message. this allows other nodes to determine the order of discovery message to avoid stale routing information, to detect duplicate message, and to ensure loop freedom. The protocol has two basic operations: Route discovery and Route maintenance which is describe below.

A. Route discovery:

Route discovery is a process of creating a route to a destination when a node needs a route to it. When S wishes to communicate with a node T, it initiates a route request (RREQ) message. The sequence number is incremented before it is added to the RREQ. The message is broadcasted in the network. Each node forward an RREQ may append its own address, sequence number, prefix and gateway information to the RREQ similar to the originator node.

ISSN: 2278 – 7798 All Rights Reserved © 2014 IJSETR

Upon sending the RREQ, the originating node will await the reception of an RREP message from the target. If no RREP is received within RREQ WAIT TIME, the node may again try to discover a route by issuing another RREQ. RREQ WAIT TIME is a constant defined in the DYMO specification and the default value is 1000 milliseconds. When a node receives an RREQ, it processes the addresses and associated information found in the message. If the originator entry in the RREQ is found to be stale or disregarded, the RREQ is dropped. For other nodes, the information is removed from the RREQ. If an RREQ is not dropped, each node processing the RREQ can create reverse routes to all the nodes for which addresses are accumulated in the RREQ. An RREP message is then created as a response to the RREQ, containing information about node 9, i.e., address, sequence number, prefix, and gateway information, and the RREP message is sent back along the reverse path using unicast. Since replies are sent on the reverse path, DYMO does not support asymmetric links. The packet processing done by nodes forwarding the RREP is identical to the processing that nodes forwarding an RREQ perform, i.e., the information found in the RREP can be used to create forward routes to nodes that have added their address block to the RREP.

B. *Route maintenance:*

It is the process of responding to changes in topology that happens after a route has initially been created. To maintain paths, nodes continuously monitor the active links and update the Valid Timeout field of entries in its routing table when receiving and sending data packets. If a node receives a data packet for a destination it does not have a valid route for, it must respond with a Route Error (RERR) message. When creating the RERR message, the node makes a list containing the address and sequence number of the unreachable node. In addition, the node adds all entries in the routing table that is dependent on the unreachable destination as next hop entry. The purpose is to notify about additional routes that are no longer available. The node sends the list in the RERR packet. The RERR message is broadcasted. When a node receives an RERR, it compares the list of nodes contained in the RERR to the corresponding entries in its routing table. If a route table entry for a node from the RERR exists, it is invalidated if the next hop node is the same as the node the RERR was received from and the sequence number of the entry is greater than or equal to the sequence number found in the RERR. If a route table entry is not invalidated, the corresponding entry in the list of unreachable nodes from the RERR must be removed. If no entries remain, the node does not propagate this RERR further. Otherwise, the RERR is broadcasted further. The sequence number check mentioned is performed to only invalidate fresh routes and to prevent propagating old information. The intention of the RERR distribution is to inform all nodes that may be using a link, when a failure occurs. RERR propagation is guaranteed to terminate as a node only forwards an RERR message once. The mechanisms used by a node to monitor active links can be Hello messages, link layer feedback, neighbour discovery, or route timeouts. Hello messages are packets that are periodically broadcasted with the intent of detecting the presence or disappearance of neighbours. However, the fourth revision DYMO specification draft does not specify the use or packet layout of Hello messages. As of the fifth revision of the DYMO specification draft, the use of Hello messages and the unspecified neighbour discovery have been updated to suggest the use of neighbourhood discovery as specified in the MANET Neighbourhood Discovery Protocol (NHDP). If a broken link is detected, the node may disseminate an RERR to notify other nodes about the broken link. The process is identical to the one described above. Finally, when a node receives an RERR for a destination, to rediscover a route, the node can initiate a route discovery for the unreachable destination by sending an RREQ message.

IV. ATTACKS IN MOBILE AD-HOC NETWORK

A. Flooding attack

The flooding attack aims to exhaust the network resources like bandwidth and resources of node, such as battery and computational power or to interrupt the routing process to cause extreme degradation of performance of network. For instance, a malicious node can send multiple numbers of Route Requests (RREQs) in a short span of time to a hypothetical destination node which does not exist in the network. The network will be flooded with the RREQs sent by the malicious node as no node reply to route requests. This, results in draining of battery power of nodes and consuming bandwidth of the network. It could lead to the DoS attack.

B. *Replay Attack*

The attackers intercept encrypted packets with signatures and resend them without making any changes, so the receivers consider them as original packets as shown in (Figure 1.3). Using outdated information and the authentication of legitimate identity, the attackers can obtain secret data or useful information. To prevent such attacks, a time stamp or a sequence number can be added to check if the packet has been resent or not.

C. *Selective forwarding*

Malicious nodes may refuse to forward certain messages, drop them, ensuring that they are not propagated any further. A simple form of this attack is when a malicious node behaves like a black hole refuses to forward every packet it sees. It is most effective when the attacker is explicitly included on the path of a data flow.

D. Sink hole

Adversary tries to take control of all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole [15] with the adversary at the centre. Due to either real or imagine high quality route through compromised node, each neighboring node of the adversary will forward packets destined for a base station through the adversary. Since all packets share the same destination (the only base station), a compromised node needs only to provide a single high quality route to the base station to influence a large number of nodes.

E. Worm hole

ISSN: 2278 – 7798 All Rights Reserved © 2014 IJSETR

Wormhole attack is a network layer attack in which an attacker receives packet at one location in the network "tunnels" them to a different point in the network and then replays them from this point. Tunnel packets received in one place of the network and replay them in another place the attacker can have no key material. All it requires is two colluding attackers and one high quality out-of-band channel. Most packets will be routed to the wormhole. The wormhole can drop packets or more subtly, selectively forward packets to avoid detection.

V. RELATED WORKS

Yih-Chun Hu, Adrian Perrig and David B. Johnson in [4] defined a particularly challenging attack to defend against, which we call a *wormhole* attack, and present a new, general mechanism for detecting and, thus defending against wormhole attacks. In this attack, an attacker records a packet or individual bits from a packet, at one location in the network, tunnels the packet (possibly selectively) to another location, and replays it there. They introduced the general mechanism of *packet leashes* to detect wormhole attacks, and present two types of leashes: *geographic leashes* and *temporal leashes*. They have designed an efficient authentication protocol, called TIK, for use with temporal leashes, and also analyze other detection approaches, such as *topology-based wormhole detection*, and show that topology-based detection cannot detect some wormholes. They focused their discussion on wireless ad hoc networks, but their results were applicable more broadly to other types of networks, such as wireless local area networks (LANs) and cellular networks.

P. G. Arfaat and A.H. Mir [16] simulated the Wormhole attack in AODV in wireless Ad-hoc networks and MANET's and studied its impact on the performance of the network. For this purpose they have modified & implemented a new AODV routing protocol which behaves as Wormhole. The packet loss was measured. Similarly other parameters like throughput and end-to-end delay due to Wormhole attack was calculated and results were produced in the form of graphs using MS Excel 2010. The main advantage of this study is that it enlightens the vulnerabilities of the AODV protocol. Besides the study will help us to overcome the AODV protocol flaws so that it could be made more robust against the attack. The limitation of the simulation is that the measurement of the impact on MANETs becomes difficult when the mobility of the nodes increases too much.

K. Singh, R. S. Yadav, Ranvijay [19] have analyzed the behaviour and different performance matrices for MANETs using different protocols i.e., AODV, DYMOUM and DSR and compared their performance matrices, like End to end delay, Packet delivery Fraction and Throughput with and without any attack. The performance comparisons of routing protocols AODV, DYMOUM, DSR with and without black hole attack respectively are shown using ns2 simulator. For Throughput AODV behaving the best and for End to End delay is concern DYMOUM is taking less delay.

Shefi Mehta, Dr. Mukesh Sharma [11] analyzed the performance of MANET under the wormhole and black hole attack. As for any network delay and throughput are the main parameters. So the authors use the throughput parameters to analyze the performance and plotting the graph for the respective. Their result shows that performance of the network degrades in the presence of both the attacks.

Pardeep Kaur, 2, Deepak Aggarwal [10] analyzed the performance of reactive routing protocols under the wormhole attacks. They have considered DYMO and AODV as the reactive protocol to measure the performance under the three types of attacks using the parameters like packet delivery ratio, throughput, end-to-end delay, jitter etc. finally they have concluded from simulation result that AODV performs better than DYMO in the absence of attack, but DYMO has more throughput and less packet delay in the presence of attack**.**

VI. WORMHOLE ATTACK IN DYMO PROTOCOL

The implementation details of our proposed methodology are being described in this section. Wormhole attack is launched in DYMOUM routing protocol. The malicious nodes create a high speed tunnel, thereby causing RREQ to reach the destination at a faster rate as compared to usual path. According to DYMOUM protocol, destination discards all the later RREP packets received, even though they are from authenticated node because destination node already receives RREQ from the colluding node. The destination then chooses the false wormhole tunnel infected path to send the RREP causing the inclusion of wormhole tunnel in the data flow route.

Wormhole attack is simulated in ns2 by using encapsulation of packet approach in routing protocol. At one end of the wormhole tunnel, the packets are encapsulated and at the other ending end of tunnel, packets are de-capsulated. Here, wormhole peers are far apart but this tunnel creates an illusion that wormhole peers are one hop count apart. However the latency of the wormhole link is very high. Once wormhole tunnel is created, wormhole peer nodes would drop the packets.

The nodes selected as cluster heads announce their identity to other nodes in broadcast each member node will choose its target cluster according to the comparatively strong signal of cluster head after choosing target cluster, member node responds to cluster head, stating clearly to join the cluster. A new wormhole DYMOUM agent is created and attached to the wormhole peer nodes via the front end Otcl of the ns2. The actual tunneling of the packet is done in the protocol implementation.

VII. SIMULATION AND ANALYSIS RESULT

The purpose of testing the methodology is to verify that if implementation works correctly and to see the performance is suitable. To test the proposed methodology, we have created 50 nodes, there are 5 sub networks of these nodes and implemented in NS2 simulator. Each sub-network consists of 10 nodes. Since wormhole attack is of two types we follow the working of hidden type where the nodes do not know the existence of malicious nodes. In these type of attack the malicious nod does not update packet header. The simulation result shows the value of packet delivery fraction, ene to end

ISSN: 2278 – 7798 All Rights Reserved © 2014 IJSETR

delay and throughput. The obtained results are shown in the form of graph for the packet loss and throughput.

Fig: Simulation Parameters

Parameter	Value
Simulator	Ns-2(ver. 2.34)
Simulation Time	100s
Number of Nodes	50
Pause time	20s
Terrain Area	750 x 750
Max. Speed	20s
Routing Protocol	DYMO

Performance metric used to measure the performance are given below:

A. Throughput:

This is the ratio of total number of packets received successfully by the destination nodes to the number of packets sent by the source nodes. As throughput is determined using the bit rates.

B. Packet delivery fraction:

It is defined as the ratio of number of packets received by the destination to that of the generated packets**.**

C. Packet Loss:

It occurs when one or more packets traveling across a network fail to reach their destination. Packet loss can be caused by a number of factors, including signal degradation over the network, oversaturated and highly congested network links, corrupted and faulty packets rejected, faulty networking hardware.

D. End-to end delay:

It is the time that is taken by a data packet to reach to destination in seconds. It is calculated by subtracting "time at which first packet was transmitted by source from "time at which first data packet arrived to destination".

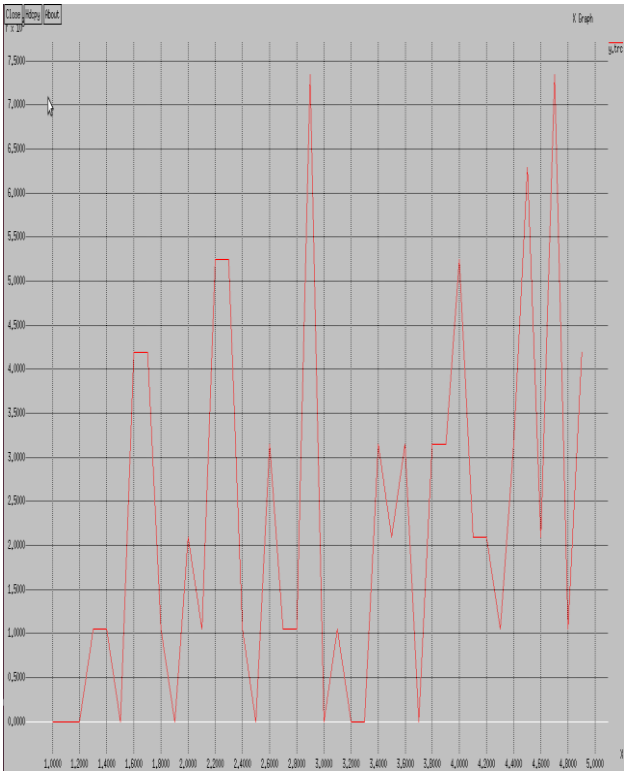

Fig 1: Throughput of DYMO protocol

The above figure shows the throughput of the DYMO routing protocol in the absence of wormhole attack. The figure represents the throughput for each given fraction of time.

We evaluate the throughput of simple DYMO protocol using different values of mobility and we also evaluate the throughput with wormhole attack using DYMO and the variation in throughput with the variation in the value time.

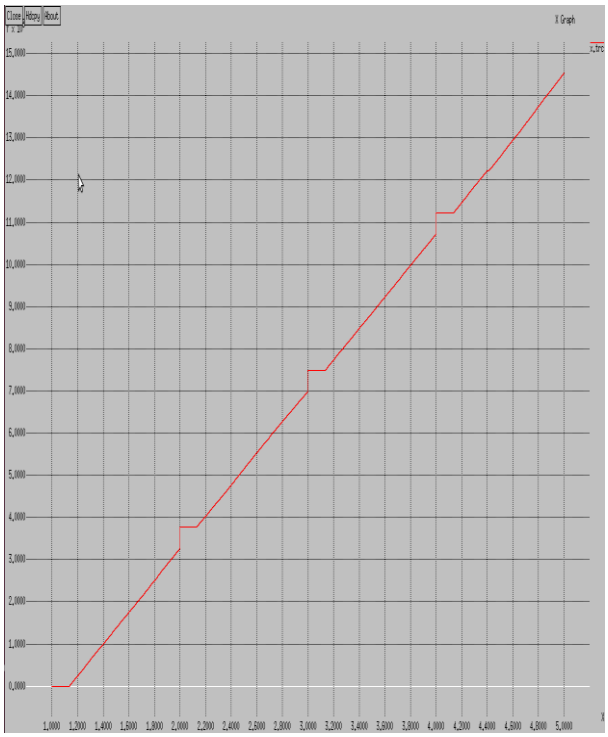

Fig 2: Packet loss of DYMO protocol

ISSN: 2278 – 7798 All Rights Reserved © 2014 IJSETR

Figure 2 shows the packet loss in the DYMO protocol. It is measured by subtracting the no. of received packets by no. of sent packets.

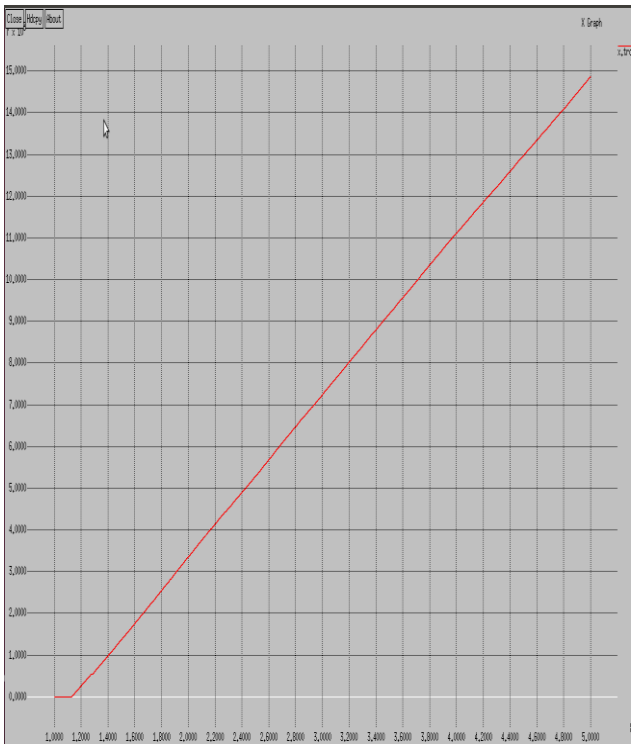

Fig 3: Packet loss of DYMO protocol under the wormhole attack

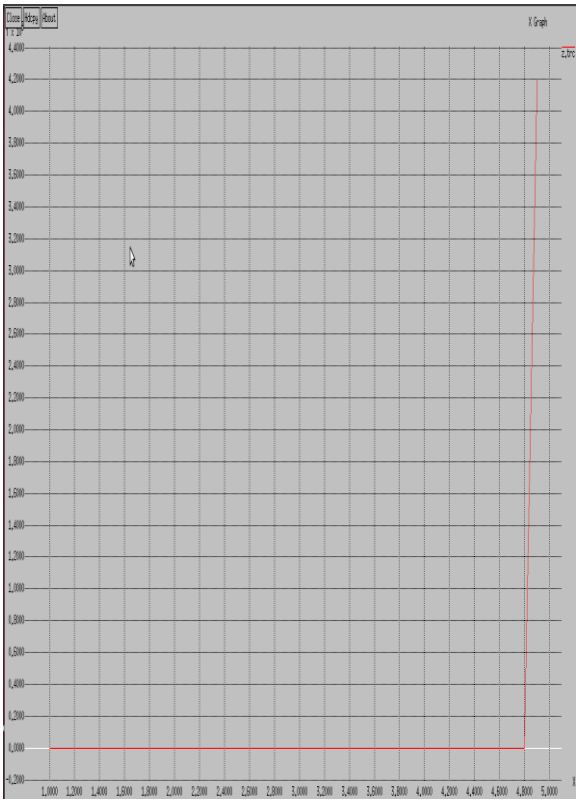

Fig 4: Throughput of DYMO protocol under the wormhole attack

From the above figure it has been analyzed that the performance of the protocol degrades in the presence of wormhole attack as the no. of packet loss increases and there is a fall in throughput.

VIII. CONCLUSION

In this proposed work, we have used NS2 to simulate the DYMO protocol of the Ad-hoc network under Wormhole attack. Although Wormhole link tunnel give a high speed route, for travelling of packets. The impact of Wormhole attack on network performance is very dangerous. Because after simulated the wormhole attack we came to know that the number of packet loss is increased, there is also fall in throughput, and less number of packets is received. In this Dissertation, Our algorithm implemented wormhole attack and we also studied the performance of DYMO protocol in the situation of attack. The following objectives have been met by the current study i.e., Study and analysis of DYMO routing protocol, network simulator Ns 2.34, Implementation of Wormhole attack, Analysis of network performance using network parameter under attack ..

REFERENCES

[1] C.E.Perkins and E.M.Royer, "Ad-Hoc on Demand Distance Vector Routing", *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp.90-100, Feb, 1999.

[2] A. Ephremides, J. E. Wieselthier and D. J. Baker, "A design concept for reliable mobile radio networks with frequency hopping signaling," *Proceedings of IEEE,* vol. 75, no. 1, pp. 56-73, Jan. 1987.

[3] Anita, Singh gopal, "An Analytical Study of DSR, AODV and DYMOUM Protocols in MANET", *IJCSMS International Journal of Computer Science & Management Studies*, Vol. 13, Issue 05, July 2013 ISSN : 2231 –5268.

[4] Y. C. Hu, A. Perrig and D. B. Johnson, "Wormhole Attacks in Wireless Networks," *IEEE Journal on Selected Areas in Communications*, vol 24, issue no.2, pp. 370-380, 2006.

[5] Sukant Kishoro Bisoyi**,** Sarita Sahu2, "Performance analysis of Dynamic MANET On- demand (DYMO) Routing protocol", *Special Issue of IJCCT,* Vol.1 Issue 2, 3, 4; 2010 for International Conference [ACCTA-2010], 3-5 August 2010.

[6] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication", *International Journal of Computer Science and Security (IJCSS)*, Volume (4): Issue (3) 265.

[7] F. Nait-Abdesselam, B. Bensaou, T. Taleb. "Detecting and Avoiding Wormhole Attacks in Wireless Ad hoc Network**s**", *IEEE Communications Magazine*, 46 (4), pp. 127 - 133, 2008.

[8] Mohammed Bouhorma, H.Bentaouit and A.Boudhir, "*Performance comparison of Ad hoc Routing protocols AODV and DSR*", IEEE 2009.

[9] R. Maulik and N. Chaki, "A study on wormhole attacks in MANET", *International Journal of Computer Information Systems and Industrial Management Applications*, ISSN 2150-7988 vol. 3 pp. 271-279, 2011

[10] Pardeep Kaur, Deepak Aggarwal, "Performance Evaluation of Routing Protocols in MANETs under Wormhole Attack", *International Journal Of Computational Engineering*

ISSN: 2278 – 7798 All Rights Reserved © 2014 IJSETR

Research, Vol. 2 Issue. 8 , Issn 2250-3005,Decembe| 2012 Page 292

[11] Shefi Mehta, Dr. Mukesh Sharma, "Analysis of Black Hole and Wormhole Attack using AODV Protocol", *International Journal of Research in Management, Science & Technology* (E-ISSN: 2321-3264) Vol. 1; No. 1, June 2013

[12] Perkins, C. E., Royer, E. M. and Das, S. R. 1999. Ad Hoc On-Demand Distance Vector Routing. IETF Internet Draft. *http://www.ietf.org/internet-drafts/draft-ietf-manetaodv-03.txt*

[13] Narendran Sivakumar, Satish Kumar Jaiswal, "Comparison of DYMO protocol with respect to various quantitative performance metrics", *ircse 2009*

[14] Ian D. Chakeres and Charles E. Perkins. Dynamic MANET on demand (DYMO) routing protocol. *Internet-Draft Version 17, IETF*, October 2006, (Work in Progress).

[15] Stefano. B., et. al., "Mobile ad hoc Networking", *IEEE Press*, July 2004

[16] P. G. Arfaat and A.H. Mir, "The impact of wormhole attack on the performance of wireless ad-hoc networks," IJCST, vol. 2, issue 4, pp-421-425, Oct . - Dec. 2011.

[17] Das R., et.al., "Performance Comparison of Two Ondemand Routing Protocols for Ad Hoc Networks", *IEEE Infocom 2000*, March 2000

[18] Ian D. Chakeres and Elizabeth M. Belding-Royer, "AODV routing protocol implementation design", *In ICDCSW '04: Proceedings of the 24th International Conference on Distributed Computing Systems Workshops* - W7: EC (ICDCSW'04), pages 698–703, Washington, DC, USA, *2004. IEEE.*

[19] .Singh, R. S. Yadav, Ranvijay, " A review paper on ad-hoc network security," *International Journal of Computer Science and Security*, vol 1, issue 1, pp. 52-69, 2007

[20] Ian D. Chakeres and Charles E. Perkins, "Dynamic MANET ondemand (DYMO) routing protocol", *Internet-Draft Version 4, IETF, March 2006*. Draft-ietf-manet-dymo-04.txt, (Work in Progress).

[21] NS-2, The ns Manual (formally known as NS Documentation) available at *http: //www.isi.edu/nsnam/ns/doc*

[22] Jeremie Allard, Paul Gonin, Minoo Singh, and Golden G. Richard, "A user level framework for ad hoc routing", *In LCN '02: Proceedings of the 27th Annual IEEE Conference on Local Computer Networks*, page 13, Washington, DC, USA, November 2002. IEEE.

First Author
Sanghita Deka

She is a M.tech scholar in Computer Engineering, MRIU, Faridabad. She Received degree the of B.tech in 2012 from Assam Don Bosco University, Assam. Her research interest in networking. E-mail: sanghitadeka304@gmail.com.

Second Author
Madhumita Khaturia

She is assistant professor in the department of computer Engineering, MRIU, Faridabad. E-mail: Madhumita.fet@mriu.edu.in

ISSN: 2278 – 7798 All Rights Reserved © 2014 IJSETR