International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 1 Issue: 12 876 – 881

Impact Analysis of Wormhole and Black hole attacks over Mobile Ad Hoc Networks

Pratibha Kaswan*, Deepika Gupta**
*M.Tech scholar, Marudhar Engineering College Bikaner
Pratibha.kaswan@gmail.com
**Assistant Professor, Marudhar Engineering College Bikaner
deepika.gupta1218@gmail.com

***Abstract*—**In this paper, we will implement two attacks over mobile ad hoc networks known as Wormhole attack and Blackhole attack. We will also analyze the impact of these attacks on data communication when using a reactive routing protocol for data communication. The reactive routing protocol used is well known Ad-hoc On-demand Distance Vector (AODV) protocol. In the Wormhole attack, at least two malicious nodes i.e., attackers disseminates wrong network information to its neighbors during the routing table formation due to which these attacks become the intermediate nodes on the selected route and drop data packets during the communication process. These two attackers form a tunnel through which they can sent the control packets to each other and if one of them are is placed near the destination then they can make sure that they are being selected on the discovered path. Due to the wrong information spread by the malicious nodes the routing tables of its nearby nodes contains untrue information about routes to various or specific destinations. When this wrong information is used for data communication during the communication process the all the data packets will go to wrong nodes and eventually dropped by attacker nodes. This decreases the network throughput and packet delivery ratio while wastes the scarce network bandwidth. On the other hand, in blackhole attack the attacker node comes on the discovered route and drop all the packets received for destination. To implement the proposed attacks, we used a network simulator called Exata simulator. The simulation results are collected for performance analysis of the underlying network. Various metrics such as packet delivery ratio and network throughput are used to show the effect of the proposed attack over a wide range of network scenarios.

Keywords: *Attacks on MANETs, Simulation, Wireless communication, Multi-hop routing, Network bandwidth, Attack detection.*

*****

1 INTRODUCTION

MANET routing protocols in general lack security mechanisms. For proper operation of routing protocol, it is assumed that intermediate nodes included in routing paths are trustworthy and follow protocol rules. It is required that each node in the network generate and forward routing control traffic according to protocol specifications. Absolute trust on intermediate nodes is a significant issue in networks that are characterized by dynamic topology. It is comparatively easy to eavesdrop wireless communication and to physically capture and compromise legal nodes. Without appropriate network level or link-layer security provisions, routing protocols [1] are susceptible to many form of malicious activity that can freeze the whole network. In this chapter we study various attacks that can be launched on MANETs [2] by exploiting the vulnerabilities inherent in routing protocols. We study how basic routing protocol functions like packet or message forwarding and routing can easily jeopardize the whole network.

It is imperative to secure networks - wired or wireless for its proper functioning. Wireless ad hoc network is more vulnerable to security threats than wired network due to inherent characteristics and system constraints. The nodes are free to join, move and leave the network making it susceptible to attacks - both from inside or outside the network. The attacks can be launched by nodes within radio range or through compromised nodes. The compromised nodes exploit the flaws and inconsistencies present in routing protocol to destroy normal routing operation of the network. A compromised node may advertise nonexistent or fake links or flood honest nodes with routing traffic causing Denial of Service (DoS) attacks [3] that may severely degrade network performance. Thus we see that routing protocols are one of the main areas of vulnerability. There is a need to study the vulnerabilities in routing protocols that may be exploited by malicious nodes to launch attacks.

In this paper, we will implement two most common attacks over Mobile Adhoc Networks [4] and analysis its impact on data communication when using a reactive routing protocol for data communication. The reactive routing protocol used is well known Ad-hoc On-demand Distance Vector (AODV) protocol [5]. In the proposed attacks, the malicious nodes i.e., attacker disseminates wrong network information to its neighbors or change the fields in the control packets with

the wrong information during the routing table formation during the route discovery phase. Due to the wrong information spread by the malicious nodes the routing tables of its nearby nodes contains untrue information about routes to various destinations. When this wrong information is used for data communication during the communication process the all the data packets will go to wrong nodes and eventually dropped by some intermediate node.

The rest of the paper is structures as follows. In Section 2, we will discuss various kinds of existing attacks on MANETs and their detection methods as part of related work. The detailed implementation and working methodology of our implemented Wormhole and Blackhole attacks are given in Section 3. In Section 4, we analyze the effects of our proposed attack on the data communication based on the various simulation results collected on different MANET scenarios. Finally, in Section 5 the conclusion and future work of the thesis is presented.

1.1 RELATED WORK

In this Section, we discuss various types of attacks that are proposed in the recent years by various researchers working on the areas of attacks over MANETs with their detection methods (if given and available in the literature).

In flooding attack [6], a malicious node generates a large number of fake route requests (RREQ) addressed to a destination that does not exist in the network. Since these route requests will never receive a reply, they will flood the entire network and congest the links. This results in the exhaustion of network resources, like bandwidth consumption, as well as consumption of a node's resources, like computational and battery power. Hence this attack is also known as sleep deprivation or resource consumption attack. This attack deteriorates the performance of the network by disrupting the routing operation. It eventually leads to denial of service.

In a black hole attack, after hearing the route request packet in the network the attacker node claims to have an extremely short route to the requested destination. The attacker does so by sending a fabricated RREP to the source node [7]. In this RREP, the destination sequence number is set to be equal to or greater than the one contained in RREQ. This gives the source node the false impression that the malicious node has the freshest route to the destination. Hence the source node chooses the route passing through the attacker to send the data packets. Now since most of the network traffic passes through the malicious node, it can either drop the packets or manipulate the traffic in any way it wants.

Wormhole attack which is also known as the tunneling attack [8][9][10], this attack is possible even if the attacker has not compromised any other legitimate nodes and even if all communication provides authenticity and confidentiality. Hence it is one of the most severe and sophisticated attacks in mobile ad hoc networks. In this attack, a pair of malicious nodes is connected through a high speed network, also known as the tunnel. Here, when the attacker receives a RREQ, it forwards it to its colluding partner through the tunnel. The malicious node on the other side of the tunnel, after receiving this RREQ, replays it to its neighboring nodes. This route request would be the first to reach the destination node since it has travelled through a faster medium than the links between legitimate nodes. Therefore the colluding nodes would most probably be included in the route, which would give them the freedom to misuse or discard packets.

2. Proposed Attacks and Implementation Method

In this Section, we present the detailed working and implementation details of the Wormhole and Blackhole attacks in MANETs. To implement these attacks we have used a well known network simulator. Required changes in the simulator codes are done to make these attacks effective during the data communication through the MANET scenarios. The effects of both of these attacks on routing process and received data quality are measured during and after data communication through a reactive MANET routing called Ad-hoc on-demand distance vector routing protocol (AODV).

2.1 BLACKHOLE ATTACK

Black hole attack is one of the very severe attacks that can be launched on Mobile Ad Hoc Networks. In this attack, the attacker works in two steps. First the attacker makes the source node believe that it has an optimal path. And after this, when the malicious node is included in the route, it misuses the data packets or just simply drops the packets.

In a black hole attack, the malicious entity enters the system and fools the sender by providing with false information of having the shortest and fresh/updated route to the destination and then manipulates the networks resources. In case of AODV protocol, the attacker, first, in response to the RREQ (Route Request) received sends a fake RREP, indicating that it has an optimum path available for the intended destination. This is done by the attacker by setting the Destination sequence number off the malicious node to a very high value.

Due to the dynamic topologies in MANETs, there's a requirement of a mechanism in routing protocols in order to differentiate between fresh and stale information stored by the nodes. In AODV protocol, destination sequence number and hop count are a major criterion in selecting the route; it gives indication of how fresh is the route. Higher the sequence number fresher is the route. Hence the node having the highest destination sequence number is given the utmost importance and is selected in the route discovery process. The malicious node now uses this principle of the AODV protocol in its favor and sets its destination sequence

number to a high value and sends a fake RREP to the source having this high sequence number. Now this increases the chances or in fact makes sure that the route to be selected for routing data packets includes the attacker.

The Black hole attack is more clearly understandable with the help of Figure 1:

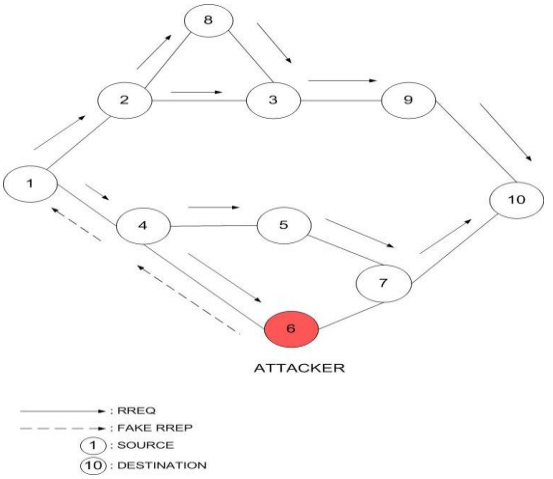

Figure 1 Attack methodology in Blackhole attack

2.2 WORMHOLE ATTACK

This attack severely degrades the network performance and is very difficult to detect and prevent. This attack is also known as the tunneling attack, this attack is possible even if the attacker has not compromised any other legitimate nodes and even if all communication provides authenticity and confidentiality. Hence it's a very sophisticated attack. Here the malicious node can attack the packet which is not even addressed to itself by over hearing them in wireless transmissions. The attacker takes advantage of this vulnerability of the wireless network. This attack can heavily affect the topology construction in the network. Also, in this attack the attackers might have their own identity or they might have even stolen or impersonated some other nodes identity. This allows them to stay hidden and less prone to detection.

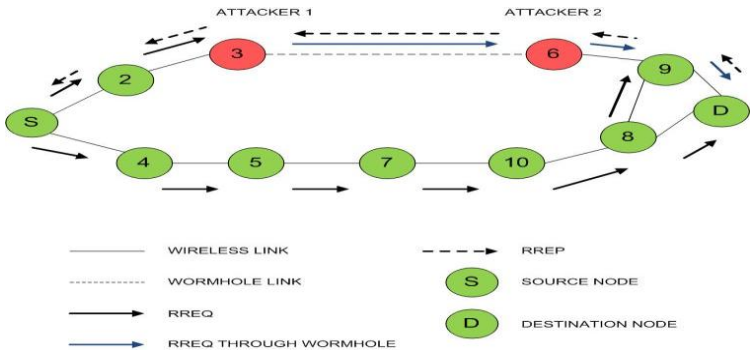

Figure 2 Wormhole attack process

As can be seen in the figure 1, there are 2 attackers indicated as red circles, '3' and '6', connected through a high transmission link, known as wormhole link or tunnel. In the above scenario Out-of-Band Wormhole attack is launched in the manner as described below:

Here first the source, indicated by 'S', checks if has a route to the destination 'D' in its routing table.

If it does have it then data packets are transferred through that route else a route discovery procedure is started using AODV protocol.

In that process first the source sends a RREQ to all its one hop neighbors which in turn check their routing tables and rebroadcast the RREQ if it doesn't has the route for the destination.

In this the attacker '3' receives the RREQ through node '2' , it then using the high speed transmission link or tunnel passes on the packet to its colluding partner '6'. Here the message is recorded at one place by one attacker and is then replayed at the other end of the tunnel by another attacker.

After '6' receives the RREQ, it sends it to the next node '9' and through it the RREQ reaches the destination.

Since this RREQ is transmitted through a high speed channel, it becomes the first RREQ to reach the destination.

Now all other RREQs coming from the legitimate are discarded.

Hence the RREP is sent through the colluding attackers which are included in the route to transfer data packets.

Now when the data packets are sent by the source, the attacker can misuse them in any way it wants. Mostly the attackers drop the packets silently without forwarding them.

Hence this attack is very destructive and also it makes the detection and prevention of this mechanism very difficult.

3. SIMULATION AND RESULT ANALYSIS

In this Section, we present the detailed performance analysis and impact analysis of the implemented Blackhole and Wormhole attacks on different scenarios over mobile ad-hoc networks (MANETs).

Parameters	Values
Network Size	1200 x 1200 meter square
Simulation time	700 Seconds
Application Layer Process	Constant Bit Rate (CBR)
Transport Layer Protocols	User Datagram Protocol (UDP)
Routing protocol	AODV, BH-AODV and WH-AODV
Number of Nodes	60
Mobility model	Random way point
Node pause time	10 Seconds
Mobility speed	0 to 25 meters/sec
MAC specification	IEEE 802.11
Network Bandwidth	24 Mbps
Performance Metrics	Packet Delivery Ratio, End-to-end delay and Routing Control Overhead
PHY Specification	802.11a/g

In order to compare and evaluate performances of the three protocols (AODV, BH-AODV and WH-AODV) in different network conditions, three parameters are varied in the simulations:

• Maximum mobility of the nodes
• Number of Attackers

In Figure 3.1, the average packet delivery ratios (PDR) of all the comparing routing protocols are shown with the increase in the number of attackers in the network. As, it can be shown from Figure 3.1 that as the number of attackers increases in the network, the PDR for BH-AODV and WH-AODV decreases very rapidly. This is because as the number of attackers in the network increases their probability to become part of a selected route also increases. Due to this, the number of packets dropped by the attackers during the communication process also increases. The WH-AODV protocol has lesser effective then the BH-AODV attack due to the fact that in BH-AODV protocol, the attacker uses false information during the route discovery phase and make sure that he will be the part of every route that is discovered in any route discovery process. On the other hand, an attacker in WH-AODV has to be near in physical location to launch an attack which depends on the current network topology.

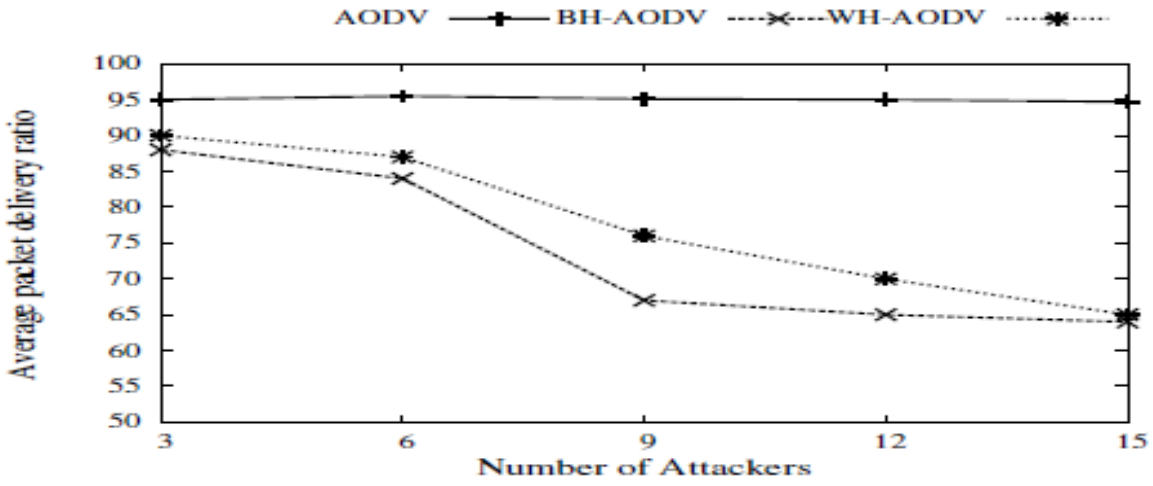

Figure 3.1 Average packet delivery ratios with increase in number of attackers in the network

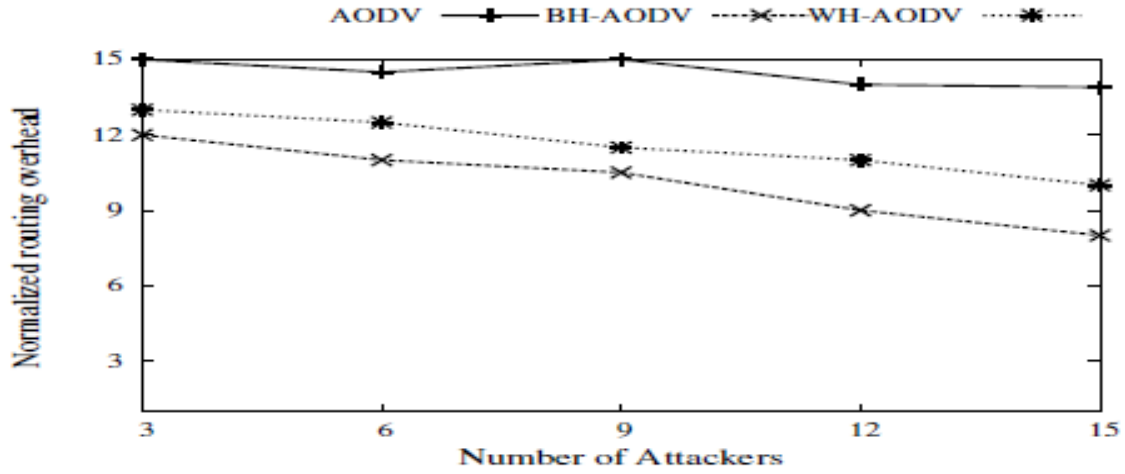

Figure 3.2 Average normalized routing overhead (in percentage) with increase in number of attackers in the network

Figure 3.2 shows the routing overhead incurred (in percentage) by all the three TCP-variants when the two attacks are launched in MANETs. The effect on packet delivery ratio with the increase in network mobility is depicted in Figure 4.3 for AODV, WH-AODV and BH-AODV routing protocols. As it can be seen that the PDR of all the comparing routing protocols is decreases with increases in network mobility because the number of route breaks increases with increase in network mobility. The PDR of BH-AODV protocol is very high when compare with the other two routing protocols because with the increase in network mobility the number of packet drops increases and when these drops are combined with the drops caused by the attacker node the total PDR of the network decreases very fast. It can be seen from the Figure 3.3 that the PDR of WH-AODV protocol is in between to the other two comparing protocols because of the same reason given above that the probability of an attacker to be selected on an active route might decrease with increase in network mobility.

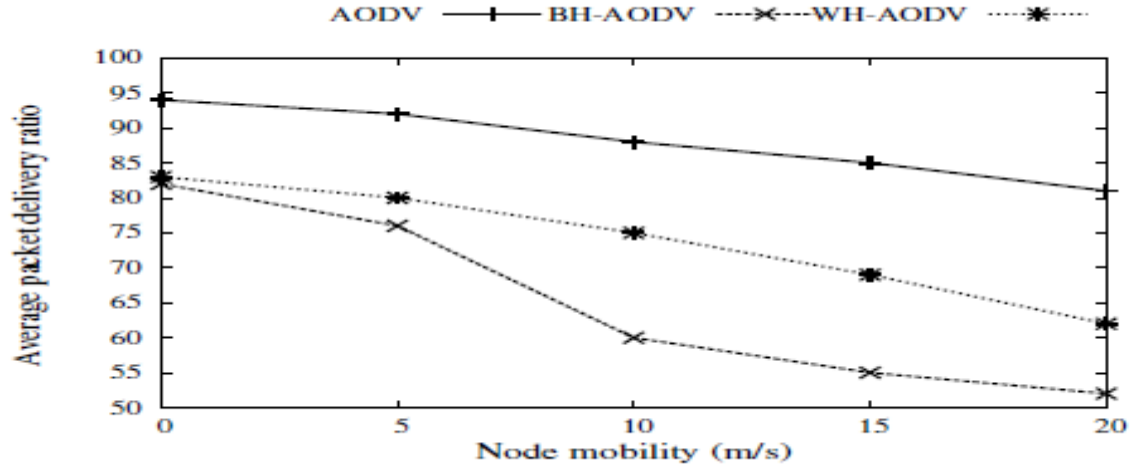

Figure 3.3 Average packet delivery ratios with increase in network mobility

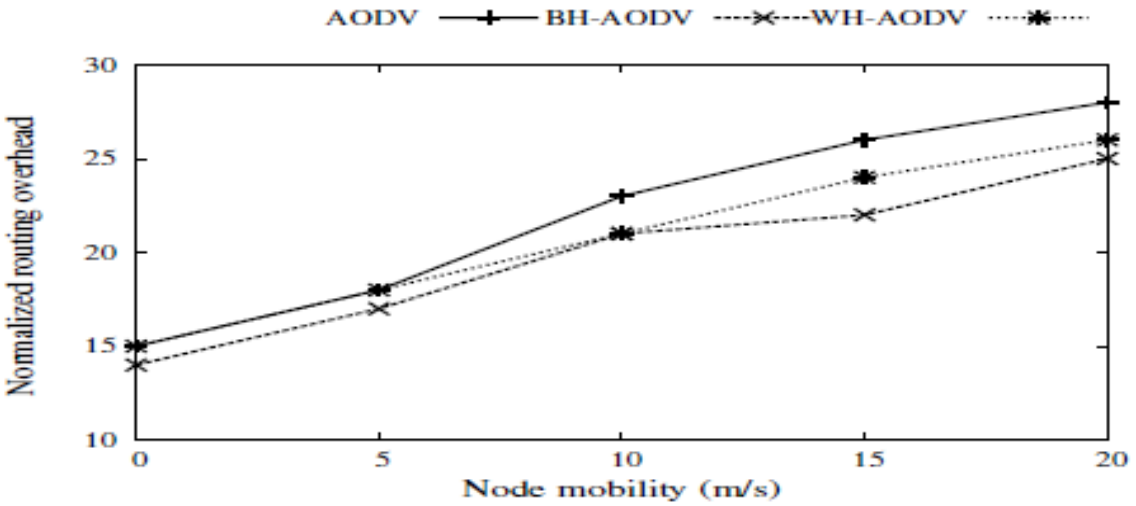

Figure 3.4 Normalized routing overhead with increase in network mobility

In Figure 3.4 the effect of network mobility on normalized network routing overhead is shown for all the three comparing routing protocols. It can be seen from Figure 4.4 that with the increase in network mobility the routing overhead in the network increases as well due to the increase in the route discovery process caused by increased in number of route breaks. Again, as it can be seen that the overhead of the attacking protocols is lower than the traditional AODV protocol due to the same reasons mentioned in the last section for increase in the routing overhead.

4. Conclusion and Future Work

We have seen during the simulation results analysis section that both the attacks decreases the network throughput and packet delivery ratio in the network by dropping the data packets that they receive for forwarding towards the

destination node. As it has been also inferred from the simulation result section that the blackhole attack is more effective in MANETs as compared to the wormhole attack. This is due to the fact that in blackhole attack the attacker forcefully makes himself an intermediate node on a selected route. Due to this the attacker is almost always able to launch an attack during the communication process. On the other hand, in case of wormhole attack the effect of attack is not always very high and highly depends on the position of both the colluding attackers. If none of the attackers are near to either source or destination node, it's very hard for the attackers to still keep themselves on the selected route during the route discovery process. This conclusion is clearly demonstrated in our simulation results that we have shown in Section 3.

In the future work, we will try to find effective solutions to detect the malicious nodes and will remove them from network for further communication. The effectiveness of the proposed solution will be measured for both the attacks and its detection rate should be kept as much as high that we can. We also work to provide a single defense mechanism for both the attacks with the lowest routing overhead possible.

REFERENCES

[1] .Mehran Abolhasan, Tadeusz Wysocki, Eryk Dutkiewicz, A review of routing protocols for mobile ad hoc networks, Ad Hoc Networks, Volume 2, Issue 1, January 2004.

[2] [2] R.H. Jhaveri, S.J. Patel, and D.C. Jinwala. Dos attacks in mobile ad hoc networks: A survey. In Advanced Computing Communication Technologies (ACCT), 2012 Second International Conference on, 2012.

[3] [3] Yih-Chun Hu; Perrig, A.; Johnson, D.B., "Wormhole attacks in wireless networks," Selected Areas in Communications, IEEE Journal on , vol.24, no.2, pp.370,380, Feb. 2006.

[4] [4] IEFT, MANET Working Group Charter, http://www.ietf.org/html.charters/manet-charter.html.

[5] [5] C.E. Perkins and E.M. Royer. Ad-hoc on-demand distance vector routing. In Second IEEE Workshop on Mobile Computing Systems and Applications, WMCSA 99, pages 90 –100, feb 1999.

[6] [6] Yih Chun Hu Adrian Perrig and David B. Johnson. Ariadne. a secure on-demand routing protocol for ad hoc networks. In Eighth ACM International Conference on Mobile Computing and Networking(MobiCom 2002), September 2002.

[7] [7] Jiwen Cai; Ping Yi; Jialin Chen; Zhiyang Wang; Ning Liu, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network," Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on , vol., no., pp.775,780, 20-23 April 2010

[8] [8] Nait-Abdesselam, F., "Detecting and avoiding wormhole attacks in wireless ad hoc networks," Communications Magazine, IEEE , vol.46, no.4, pp.127,133, April 2008.

[9] [9]Saurabh Upadhyay , Brijesh Kumar Chaurasia "Impact of Wormhole Attacks on MANETs"International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044- 6004) 77 Volume 2, Issue 1, February 2011.

[10] [10]Ranjeeta Siwach1, Vanditaa Kaul "A Study of Manet and Wormhole Attack in Mobile Adhoc Network" International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 2, Issue. 6, June 2013, pg.413 – 420

.