Comparative on AODV and DSR under Wormhole Attacks Detection Scheme Using Secure OLSR Protocol in MANET

Vibha Nigam [1], Navneet Kumar[2]

[1]Assistant Prof. OIST Bhopal, [2] PG Scholar, MITS, Bhopal (India)

Abstract - Ad-hoc networks are more vulnerable to security issues compared to the wired network due to their communication channel being with there wireless the co-operative nature of the nodes forming a network. Security vulnerabilities can occur on all layers of Open System Interconnection (OSI) model. Attacks can be categorized based on the mode of operation under one of the following categories: Wormhole attack, Flooding attack, Spoofing attack, Rushing attack, Detour attack, and Falsified route error generation attack. The current MANET systems generally use encryption based techniques to secure the network. Detection of symptoms for a network attack and blocking potential threats are based on these methods.Various mechanisms have been proposed by modifying the existing OLSR routing protocol to add security features. Encryption based methods place high overhead on the nodes where power and processing speed are constraints. Similarly, many of the proposed techniques in the literature rely on the location of the malicious node which needs to be computed continuously as the Mobile Ad-hoc Network (MANET) is dynamic. The proposed research methodology investigates the performance of OLSR protocol and studies the effect of wormhole attack in MANET. It is proposed to improve the security in OLSR by means an enhanced OLSR called Secure Replay OLSR (SR-OLSR), which specifically addresses wormhole attacks and thereby increase the overall security of the routing protocol. The proposed work emphasis wormhole attacks. The work can be enhanced to mitigate Greyhole attacks and Black hole attacks. Similarly, there is also an emphasis on reducing the network and processing overheads due to which synchronization of time between the nodes in the network became essential. Further investigation can be carried out to provide a solution using asynchronous mode.

Keywords - MANET, aodv, dsr, wormhole, attacks, security.

1. INTRODUCTION

The Mobile Ad-hoc Networks (MANETs) are part of today's revolution in technology. MANETs are groups of wireless devices and nodes that communicate by dispatching packets to others or on behalf of another device/node, without a central network authority and infrastructure controlling data routing. In MANETs, each node acts as router/network manager for other nodes. MANETs are vulnerable due to their basic characteristics which include topological changes, no point of network management, restriction of resources, no certifiable or centralized authority, etc.

Threats to personal and company privacy, and assets by attacks upon networks and computers continue in spite of efforts of network administrators and IT vendors to safe as environments. Secured transmission and communication in MANET is a major challenge as this network is open to many types of attacks.

Understanding probable security attacks to MANETs is a serious issue as they are targeted by attacks including Flooding attack, Wormhole attack, Black hole attack, Denial of Service (DoS), Selfish-node misbehaving, Routing table overflow attack, Impersonation attack, etc. Earlier studies reveal the different attack categories on MANETs like Passive/Active attacks, Internal/External attacks and Routing and Packet Forwarding attacks. Some of the attacks aim at single nodes and others aim at multiple nodes. Malicious and selfish nodes are other types of attack which severely degrade the security and performance of the network.

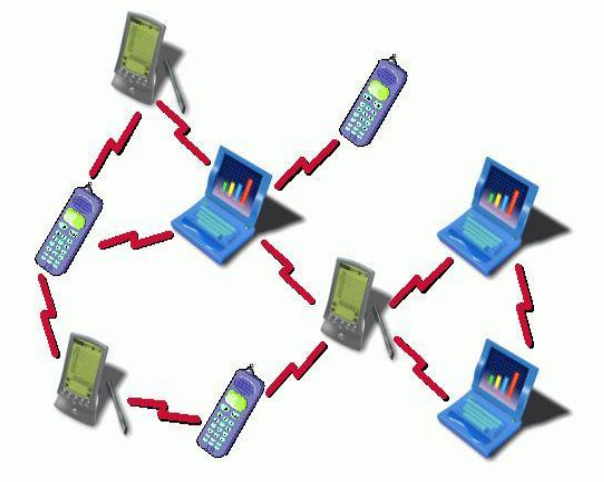

Figure 1: Mobile Ad hoc Network

1.1 ROUTING PROTOCOLS

To ensure delivery of packets from sender to destination in ad-hoc networks, a node must create a routing protocol and maintain the related routing tables in memory. Routing protocols can be categorized as reactive, proactive, and hybrid. As of date there are almost one hundred routing protocols, most of which are standardized by the Internet Engineering Task Force (IETF). This section gives an overview of the some of the important ones for each category.

1.1.1. Reactive protocols

Reactive protocols set up routes on-demand. When a node wants to communicate with another without a route, the routing protocol will try to create route and the Ad-Hoc on-Demand Distance Vector (AODV) routing protocol is one such protocol [1] (Perkins et al. 2003). The characteristic of an AODV is that the topology information is transmitted only on-demand by nodes. When a node transmits to a particular host of which it has no route, it will create a Route REQuest (RREQ) that is passed on to other nodes. This leads control traffic overhead to be dynamic which results in an initial delay when communication is initiated. A route is located when the RREQ reaches either the destination or an intermediate node with a valid route entry for the destination. The AODV remains passive when a route exists between end points. When the route either becomes invalid or lost, the AODV will again issue a request.

1.1.2. Proactive protocols

A proactive approach to MANET routing requires a constant update on topology information. The entire network should be known to all nodes, in theory. This leads to a constant overhead in routing traffic without initial communication delays.

1.1.3. Hybrid protocols

Hybrid protocols combine both proactive and reactive approaches. The Zone Routing Protocol (ZRP) is an example [2] (Haas et al. 2002). This protocol divides topology into zones and uses different routing protocols within/between zones depending on their strengths and weakness. ZRP is modular and so any routing protocol can be used within and between zones. The zone size is defined by the parameter '*r*' which describes the radius in hops. Intra zone routing is through a proactive protocol as protocols keep updating views of zone topology and so there are no initial delays when communicating within zone nodes. Inter zone routing uses reactive protocol thereby eliminating the need for nodes to be proactively fresh in the entire network.

1.2. ATTACKS AGAINST MANET

As MANET is a group of nodes forming a temporary networks and a central administration, and communication among nodes is based on trust. Hence, a MANET is more likely to be attacked from inside the network when compared to other network types. MANET can be attacked in several ways through multiple methods. The classification is based on attack behavior (Passive vs. Active), the source of attacks (Internal vs. External), attackers processing capacity (Wired vs. Mobile) and attacker's number (Single vs. Multiple) [3] (Razak et al. 2004, Amitabh 2008). These attack classifications were chosen as they are applicable to collaborative attacks being categorized.

1.2.1. Passive vs. Active attack

Passive attacks plan theft of valuable information from two communicating nodes or even the entire network. There are many variations, but for MANET, there are two types: eavesdropping and traffic analysis. Based on situations, passive attacks can be legitimate or illegitimate. If the purpose is benign, for example, if the administrator plans to use some tools to probe network traffic to troubleshoot the network then it is termed legitimate. But if the purpose is malicious, one attacker could steal valued information such as credit card information, credential email, by probing the network traffic and use this information to illegally withdraw money from bank accounts or blackmail victims.

Passive attacks generally do not aim to disrupt the operation of a particular network, but active attacks will alter normal network operations (Ghazizadeh et al. 2002). Typical examples of active attacks are masquerade attacks, replay attacks, modification of the message and Denial of Service (DoS).

1.2.2. Internal vs. external attack

External attacks are launched by attackers who are physically outside the attacked network and try to deny access to a specific function in the network (i.e. http traffic), or cause network congestion or disrupt the entire network. While external attacks are hard to launch if the network is correctly configured/protected, internal attacks are tougher to defend against. One reason is because of the tendency to protect the network from outsider attacks rather than by insiders. Also

external attacks can be easily traced compared to the internal attacks. An external attacker node can hijack an internal node, and use it to attack other nodes in MANET. Therefore, an external attack converts into an internal attack and have more serious non sequences. The two types of internal attacker nodes are the one which is compromised node as mentioned above and the other is the misbehaving node which accesses system resources but does not use them for the purpose for which it was meant (Ghazizadeh et al. 2002). Attacks by internal misbehaving nodes are hard to find out, i e., a selfish attack. In selfish attack, the node doesn't want to use its battery power, or network bandwidth to forward packets though it expects such service from other nodes.

1.3. BLACKHOLE ATTACK

When a malicious node impersonates the destination node or forges a route reply message forwarded to the source node which does not contain areal route to the destination, then it is called a Blackhole attack. The malicious nodes create unwanted traffic and discards packets received by the network [5] (Weerasinghe et al. 2007). When a malicious node (Blackhole node) affects one or more nodes, making them malicious as well, then this attack is labelled multiple node attack or collaborative attack. In Blackhole attacks, the malicious node acts as if it has the shortest path to the node and it impersonates making message interception easier. The malicious node tries to get replies from nearby nodes to locate a safe, valid route [6] (Tamilselvan and Sankaranarayanan2008) which could be forged, illegitimate or an imitation but which appears genuine.

1.3.1 Co-Operative Blackhole Attack

In case of black hole, we have multiple algorithms to prevent the attack from a single black hole. But in case of multiple black hole attack, more than one black hole node cooperates with each other by sending requests to each other. If the source node requests to send the data packet to the destination, it has to pass through the intermediate nodes. Suppose source node S releases Route Request (RReq) to black hole node B1 then B1 refers to its associative black hole node B2, the source node S sends a Further Request (FRq) to B2. The source node S asks B2 that if it has a route to destination node or B1. As B2 is black hole node its Further Reply (FRp) will be "OK" to both the enquiries. So here the data will be lost.

1.3.2. Wormhole attack

A wormhole attack is one where the attacker provides two choke-points to degrade the network or analyze traffic at any time. False impressions are used to create choke-points by combining two or more nodes (Mahajan et al. 2008). In simple, a wormhole attack creates a tunnel to records traffic data (in bits or packets) in one network place and swerves it to another network location. Such attacks are against many ad-hoc routing protocols with the attacker hidden at a higher layer. Hence the wormhole and colluding attacker nodes at wormhole choke points are invisible in the MANET route (Hu et al. 2006).

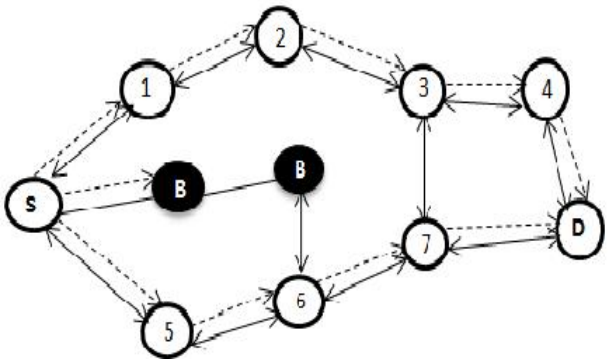

Fig.2. Network flooding by RREQ messages

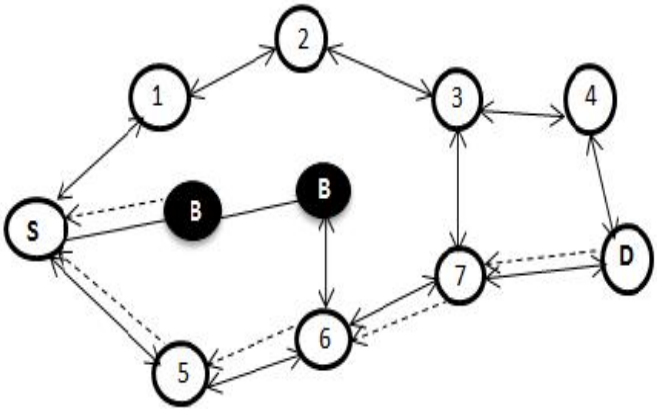

Fig.3. Propagation of RREP messages

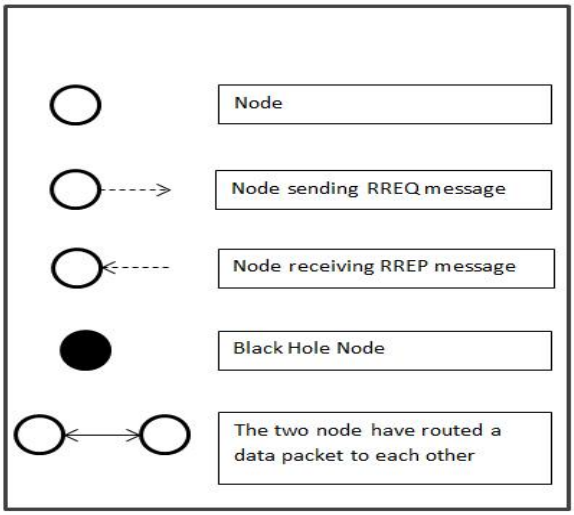

Fig 4. Symbolic notations used in diagrams

2. SYSTEM MODEL

2.1. NETWORK SECURITY

A secure system is one that does what it is conceived for by its designers and it shows no unexpected behaviour when an attacker tries to make it act differently.

Security goals are defined by the following terms and the attacks to which they are Susceptible:

- **Confidentiality:** Confidentiality means that transmitted information is revealed only to authorize parties as sensitive information disclosed to dversaries can lead to severe consequences.

- **Integrity:** Integrity ensures that messages are not changed in route between the sender and receiver as messages can be corrupted by network malfunctioning or malicious attacks.

- **Non-repudiation:** Non-repudiation means that the message originator accepts having sent the message. An attacker can forge wrong messages which appear to originate from an authorized party, with the object of making the latter the culprit. If non-repudiation is guaranteed, a wrong message receiver can prove the origin of the message and hence that the originator misbehaved.

Other security goals could be tougher to achieve. Sometimes attacks can occur jointly, e.g. an intruder may break into the system to prepare a DoS from inside, or eavesdrop to gain unauthorized access later.

- Authentication: Authentication ensures identities of parties with whom communications are exchanged, before granting network access. Without authentication, an attacker can behave as legitimate (identity spoofing) and interfere with network security.
- Access control: Access control ensures that only authorized parties take part in communications; others are denied access. Access control presumes authentication of parties wanting network access.
- Service availability: Service availability guarantees that all communications network resources are utilizable by authorized parties. An attacker may launch a DoS attack by saturating the medium, jamming communications or keep system

2.2. CRYPTOGRAPHY BASICS

Encryption is disguising a message so that its content is hidden, it comprises of transforming messages from plaintext to cipher text. The reverse is called decryption. It is possible to include a message digest called hashing or digital fingerprint to verify their integrity.

Signing a message signifies addition of sequence of bits known as a digital signature to it, which helps to identify the real originator. Cryptographic algorithm (cipher) and a key are used for achieving digital signature. It is necessary to apply more than one technique for additional security, i.e. a message can be encrypted using key of the requestor and then digitally signed with agent's key.

With respect to the abovementioned security attributes the characteristics of cryptography are as follows:

- Encryption provides confidentiality, as the messages are transmitted in cipher text, and can be decrypted only by the owner of the key.
- The message digest provides integrity.
- The signature provides non-repudiation, as only the owner of the key can be the generator.
- Authentication and access control are more complicated, requiring the use of advanced cryptographic primitives.

3. PREVIOUS WORK

[8] Gupta et al. (2011) analyzed MANET's Black hole attack with Proactive routing protocol i.e. OLSR and Reactive routing protocol AODV. Comparisons of Black hole attack for both protocols were considered. Attack impact on MANET performance is evaluated to learn which is more vulnerable and how much the attacks impact both protocols. The analysis is on performance metrics like throughput, network load and end to end packet delay. After many comparisons, Black Hole attack was analyzed with regard to parameters including end to end packet delay, throughput and network load.

[9] Zapata (2002) provides a summary of many approaches to security features in routing protocols in mobile ad-hoc networks (MANET) describing at the same time, secure AODV (an extension to AODV providing security features) with a summary of its operation and future enhancements. Two mechanisms secure AODV messages: digital signatures

to authenticate a message non-mutable fields and hash chains to safeguard hop count information. Every node generating/forwarding route error messages) uses digital signatures to sign a full message verifiable by a neighbor receiving it.

[10] Khalil et al. (2005) presented A Lightweight Countermeasure for the Wormhole Attack in Multi hop Wireless Network (LITEWORP), a simple protocol to detect/mitigate wormhole attacks in ad-hoc and sensor wireless networks. It uses a secure two-hop neighbor discovery and monitors local control traffic to detect nodes involved in such attacks and also has a countermeasure which isolates malicious nodes from the network thereby doing with the chance of more damage.

[11] Kannhavong et al. (2008) proposed a unique acknowledgement between two hop neighbours whenever the control traffic was successfully received. The proposed methodology was able to protect the network from link spoofing, wormhole attack without requiring location information or the full topology of the network. The proposed system was able to achieve higher packet delivery ratio compared to standard OLSR.

4. PROPOSED METHODOLOGY

Various attacks target MANET's weakness such as routing messages which are essential for mobile network communications as every packet has to be forwarded quickly via intermediate nodes from its source to destination. Malicious routing attacks could target routing discovery/maintenance by keeping away from routing protocol specifications. Attacks also target specific routing protocols like DSR, or AODV. Sophisticated and subtle routing attacks were identified in recently published papers and include the blackhole, Byzantine, and wormhole attacks. Currently routing security is a hot research area in MANET. MANET attacks can be compartmentalized into passive and active attacks based on the means of the attack. A passive attack obtains network exchanged data without disrupting communications; whereas an active attack involves information interruption, modification or fabrication which disrupts normal MANET functioning. Active attacks examples include jamming, impersonating, modification, Denial of Service (DoS) and message replay (wormhole attack).

4.1. WORMHOLE ATTACK

Wormhole attack is the most common of attacks. It records traffic from one network region and replays it in another region. It is launched by an intruder node 'X' being within transmission range of legitimate nodes 'A' and 'B', where 'A' and 'B' are not within transmission range of each other. The intruder 'X' node just routes control traffic between 'A' and 'B' and vice versa, without the modification presumed by the routing protocol. Examples are without stating its address as source in packet headers and making 'X' practically invisible.

4.1.1 Wormhole Attack in OLSR

As a wormhole attack can affect topology construction greatly, it is lethal for many ad hoc routing protocols, especially proactive routing protocols like OLSR, which exchange control packets for neighbour discovery and topology construction regularly. Figure 5.1 depicts an ad-hoc network with a wormhole tunnel. When node 'A' broadcasts a 'HELLO' message, node 'X' (attacker) copies it and routes it to node 'Y' (colluding attacker) through a wormhole. 'Y' receives A's HELLO message and replays it. When node 'B' receives replayed HELLO message, it thinks that the node 'A 'is to be its one-hop neighbour. Following the same process node 'A' may be thought to assume node 'B' to be its one-hop neighbour. After some time, a symmetric link is established between 'A' and 'B' based on OLSR mechanism. Once this spoofed-symmetric link is established, 'A' and 'B' in all likelihood choose each other as Multi-Point Relays (MPRs) leading to a Topology Control (TC) message exchange and data packets through the wormhole tunnel. Only MPR nodes can forward TC messages in OLSR, so choosing MPRs that forward flawed topology information results in incorrect topology information spread through the network. This ultimately results in disruption and major performance degradation for the network totally.

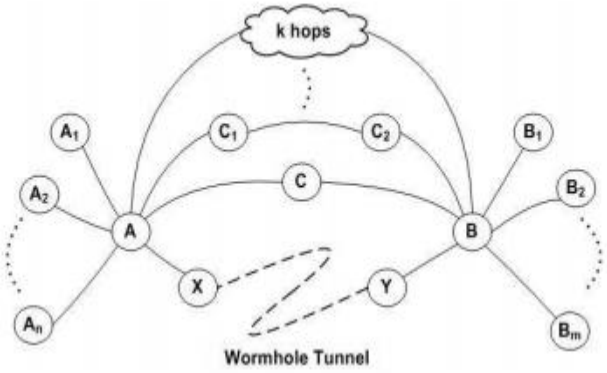

Figure 6 .Wormhole attack model.

5. SIMULATION/EXPERIMENTAL RESULTS

For our simulations we used ns-2.34 [9], a packet-level discrete event simulator. Ns-2.34 includes the simulation model for mobile ad hoc networks. The model includes a physical layer, an 802.11 MAC layer, and a data link layer [8]. The wireless channel capacity is 2Mb/sec. As mentioned earlier, we performed our study with AODV and modified AODV.

The default overall buffer size of the scheduler of each node is 64 packets. The buffer is shared by multiple queues when the scheduler maintains multiple queues. The AODV protocol implementation in ns-2.34 also maintains a buffer of 64 packets used during route discovery. The maximum waiting time in the send buffer during route discovery is 30 seconds. If a packet remains in the send buffer for over 30 seconds, the packet is dropped.

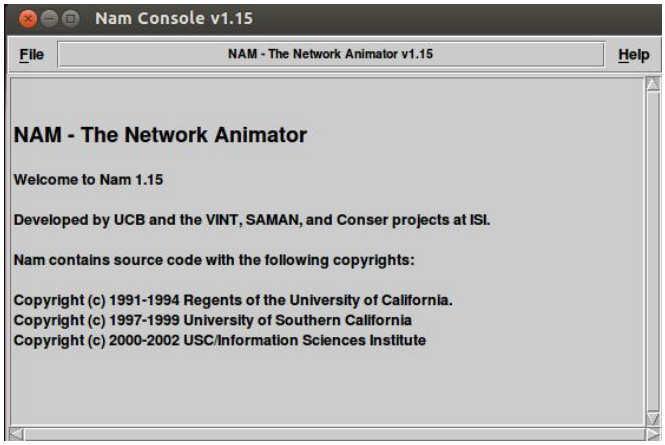

Figure 7 : NAM Front IN NS2

Table 2: The following parameters for simulation are used

Sr. No.	Parameter	Value
1	Simulator	NS 2.35
2	DoS Attack	Black hole Attack
3	Channel Type	Wireless channel
4	Antenna Type	Omni directional
5	The Protocol user	AODV,DSR
6	Underlying MAC Protocol	IEEE 802.11
7	Propagation Model	Two-Ray Ground
8	Queue	PriQueue
9	The number of Nodes Detected	Two or more node which are dropping packet
10	Nodes	10

6. CONCLUSION

OLSR has been found to be highly efficient in medium sized networks with low mobility. However the network characteristics make it more vulnerable to attack. Challenges in wireless network include low bandwidth, high latency, asymmetric links and low processing speed. In this research, it was proposed to mitigate wormhole attacks in table driven routing protocol based networks.

In this Paper, it was proposed to mitigate wormhole attacks in OLSR based Ad-hoc networks. Since Ad-hoc networks are constrained by bandwidth and processing power and memory, the initial investigations were based on fine tuning of OLSR parameters and the packet delivery ratio and throughput were studied. Based on these studies a novel OLSR routing algorithm to mitigate wormhole attacks was proposed. The proposed system was able to detect wormhole attacks and mitigate the same without affecting the Quality of Service (QOS). The network control overheads do not increase and the throughput remains the same as in network without any attack. Since encryption techniques are not used, the CPU utilization does not increase.

7. FUTURE SCOPES

In the proposed work emphasis was on wormhole attacks. The work can be enhanced to mitigate Greyhole attack, Black hole attacks similarly In future work, and we can use better and fast routing protocol for route establishment and use effective fields for detecting packet. We can improve the table entries at destination to get the detection of pair of malicious nodes faster and improve conformance procedure. The emphasis was to reduce the network

and processing overheads due to which synchronization of time between the nodes in the network is essential. Further investigation can be carried out to provide a solution using asynchronous mode.

REFERENCES

[1] Perkins and Royer,E. "Ad-hoc On-Demand Distance Vector Routing," Second IEEE Workshop on Mobile Computer Systems and Applications, pp. 90-100, February 1999.
[2] Haas, Pearlman, and Samar. ZRP IEFT-MANET DRAFT, 5 Edition, July 2002.
[3] Razak, A. S., Furnell, M. and Brooke, P. J. "Attacks against Mobile Ad-hoc Networks Routing Protocols," 2004.
[4] Ghazizadeh,S.,Ilghami,O.,Sirin,E. and Yaman,F. "Security-Aware Adaptive Dynamic Source Routing Protocol", In Proc. of 27th Conference on Local Computer networks, pp. 751-760, Nov. 6-8, 2002.
[5] Weerasinghe and Fu,H. "Preventing Cooperative Black Hole Attacks in Mobile Ad hoc Networks: Simulation Implementation and Evaluation," IEEE International Conference on Communication, 2007.
[6] Tamilselvan,L. and Sankaranarayanan,V. "Prevention of co-operative blackhole attack in MANET," Journal of networks, vol. 3, pp. 13-20, 2008.
[7] Huhtonen, A. "Comparing AODV and OLSR routing protocols. In Seminar on Internetworking, Sjkulla (pp. 26-27). (2004, April)
[8] Gupta, S., Gill, S. and Joshi, A. "Analysis of Black Hole Attack on AODV and OLSR Routing Protocols in MANET", International journal of Computer application, Issue 1, Vol 1, pp. 11 – 19,October 2011.
[9] Zapata, M.G. " Secure Ad-hoc On-Demand Distance Vector Routing", Mobile Computing and Communications Review, Volume 6, Number 3, pp. 106 – 107.(2002).
[10] Khalil, Bagchi,S. andShroff,N.B. "LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks, in: International Conference on Dependable Systems and Networks (DSN), 2005, pp. 612–621.
[11] Kannhavong,B.,Nakayama,H., Nemoto,Y. and Kato, N."A Survey Of Routing Attacks In Mobile Ad-hoc Networks", IEEE Wireless Communications , pp. 85- 91,October 2007.

AUTHOR'S PROFILE

Prof. Vibha Nigam has received her Bachelor of Engineering in Computer Science and Engineering from SIRT Bhopal under RGPV Bhopal in the year 2008. M.Tech. in Computer Science and Engineering from P.G. Department of Computer Science Engineering from LNCT Bhopal under RGPV Bhopal in the year 2011. At present she is working as an Associate Professor at Oriental Institute of Technology, Bhopal. (India). Her areas of interests are Image Processing, Computer Networks and Programming.

Navneet Kumar has received his Bachelor of Engineering degree in Computer Science and Engineering from Millennium Institute of Technology and Science, Bhopal (India) in the year 2013. At present he is pursuing M.Tech. With the specialization of Computer Science and Engineering in Millennium Institute of Technology and Science, Bhopal (India). His area of interest is Computer networking, Cloud Computing, and Java.