Volume 6, Issue 6, June 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

# A Study of Attacks at Different Layers in Mobile Ad-Hoc Network

**Shikha Sharma**
Research Scholar, CGC COE, Landran,
Mohali, India

**Manish Mahajan**
Head of Department, CG CCOE, Landran,
Mohali, India

***Abstract***— ***A Mobile Ad Hoc Network (MANET) is an autonomous system of mobile nodes with routing capabilities connected by wireless links, the union of which forms a communication network [14]. Therefore, it can be considered as a temporary infrastructure less network formed by a set of wireless mobile hosts that dynamically establish their own network on the fly without relying on any central administration [3]. All participants at these networks act as both hosts and routers forming an autonomous network heavily depended on the belief that all participants give and take resources in a fairly manner. In this paper we investigate the different types of attacks which are at the different layers of MANET. Moreover, we can easily understand the serious challenges that exist in the implementation of MANETs.***

***Keywords***— ***MANET, Attacks, Security, Protocols***

## I. INTRODUCTION

A MANET is a rapidly growing technology which is based on a self-organized and rapidly deployed network. Due to its infrastructure less feature, MANET changes its network topology very quickly. Nodes in MANETs can join and leave the network dynamically [1]. There is no fixed set of infrastructure and centralized management in this type of networks. Nodes present in the network are connected through wireless interface. The dynamic nature of such type networks is more vulnerable to link attacks. The basic necessities for a secured networking are secure protocols which can ensure the confidentiality, availability, authenticity, integrity of network.

## II. SECURITY OF AD HOC NETWORKS

Security is an essential service for wired and wireless network communications. The success of mobile ad hoc networks (MANET) strongly depends on people’s confidence in its security. However, the characteristics of MANET pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and non-repudiation. The need for security in MANET is very high because there is no fixed infrastructure for the network and the nodes are mobile with open and dynamic structure. The most important parameters that security depends on are authentication, integrity, confidentiality, availability and non-repudiation [7]. The wireless ad hoc networks need more security because it is more vulnerable to attacks by design. The use of wireless links makes an ad hoc network more susceptible to attacks ranging from passive eavesdropping to active interfering [6]. Unlike in wired networks, where an attacker must gain physical access to the network wires or pass through the several lines of defense like firewalls and gateways. When compared to a wired network, it’s easier to attack a wireless network because of its structure and also the attack may come in any direction and any node can be attacked at any point of time. MANETs are more vulnerable to attacks because:

- Limited computational capabilities: Typically, nodes in ad-hoc networks are modular, independent, and limited in computational capability and therefore may become a source of vulnerability when they handle public-key cryptography during normal operation.
- Limited power supply: Since nodes normally use battery as power supply, an intruder can exhaust batteries by creating additional transmissions or excessive computations to be carried out by nodes.
- Challenging key management: Dynamic topology and movement of nodes in an Ad Hoc network make key management difficult if cryptography is used in the routing protocol.

So, that’s the reason each and every node in the network has to prepare for attacks at any point of time. And also as there is no central based controlling identity for the participating nodes; the attacks are much easier to launch in MANET. The intruder may insert spurious information into routing packets, causing erroneous routing table updates and thus misrouting [10].

## III. CLASSIFICATION OF ATTACKS

Nodes in MANET can be broken, malicious or selfish. Broken nodes become nonfunctional due to some link failure so cannot forward the traffic that they earlier agree to forward. Malicious nodes aimed at disrupting the network by dropping the packets or launching denial of service attacks. In Figure 1 the classification of attacks are listed with the attacks corresponding to different layers in MANET.

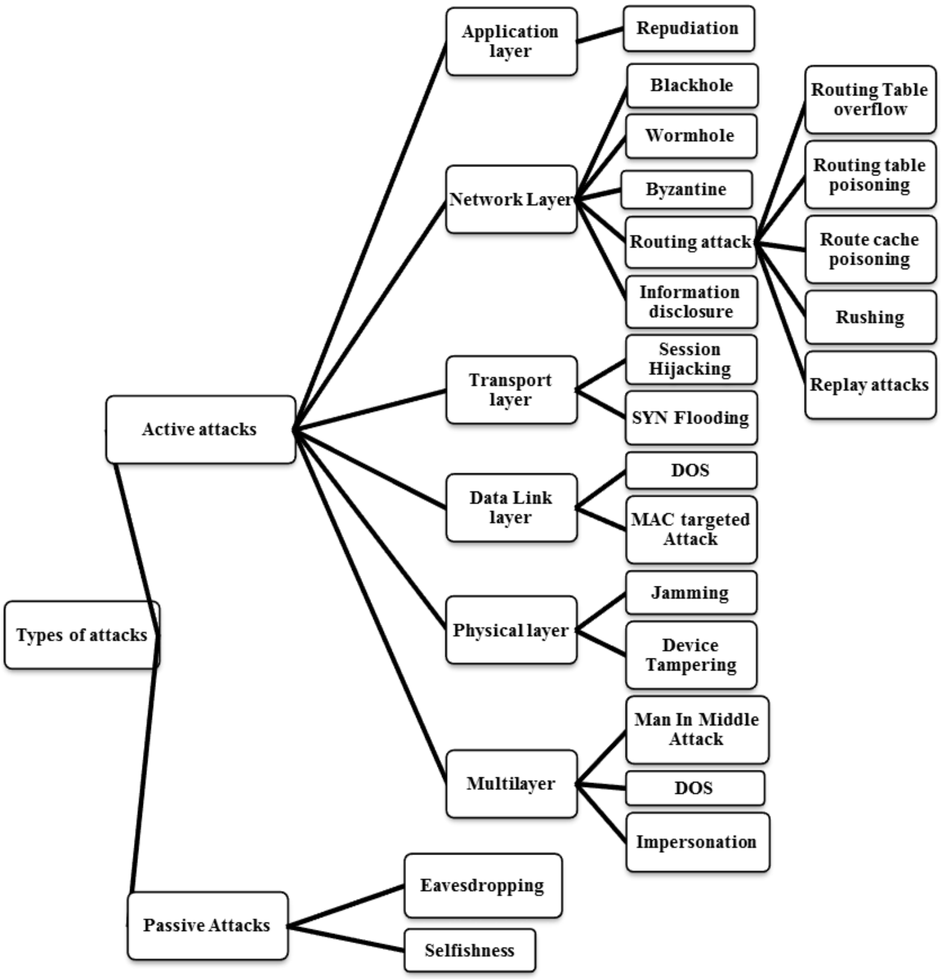

Figure 1: Classification of Attacks

Selfish nodes hinder the routing by dropping packets in order to conserve their energy and bandwidth. MANET found applications in military, disaster relief operations etc as it is easy to deploy. In order to encourage its use in future it is important to ensure secure and reliable routing in MANET. Before providing security we need to know attacks related to such networks. Security aspects were not considered when adhoc protocols were designed. Later researchers tried to incorporate security mechanisms on existing routing protocols. Attacks can be classified into two broad categories [4]:

**Passive Attacks:** The attacker just snoops the network without disrupting the network operation. These attacks compromise the confidentiality of the data and tell which nodes are working in promiscuous mode.

**Active Attacks:** Attacks in which attacker disrupts the normal operation of the network by fabricating messages, dropping or modifying packets, replaying packets or tunneling them to other part of the network. Basically the content of message is modified. These can be internal attacks and external attacks.

- **External attacks:** In external attack the attacker wants to cause congestion in the network this can be done by the propagation of fake routing information. The attacker disturbs the nodes to avail services [12].
- **Internal attacks:** In internal attacks the attacker wants to gain the access to network & wants to participate in network activities. Attacker does this by some malicious impersonation to get the access to the network as a new node or by directly through a current node and using it as a basis to conduct the attack [9].

## IV. ATTACKS CORRESPONDING TO DIFFERENT LAYERS IN MANET

### Application Layer Attacks

The application layer communication is also vulnerable in terms of security compared with other layers. The application layer contains user data, and it normally supports many protocols such as HTTP, SMTP, TELNET, and FTP, which provide many vulnerabilities and access points for attackers. The application layer attacks are attractive to attackers because the information they seek ultimately resides within the application and it is direct for them to make an impact and reach their goals.

- **Repudiation:** Transport and network layer security measures are not enough to prevent attacks in MANETs. Repudiation attack can even bypass both these layers. It is an act of refusal in participating in all or part of the communication. For example, repudiation attacks on a commercial system in which a selfish node can refuse conducting credit card purchase, or any on-line bank transaction.

- **Malicious Attack:** In this attack, a malicious node disrupts the normal operation of the other nodes in the network by attacking the operating system. Malicious node sends virus, worm or Trojan horse to a victim node. A virus is a computer program that attaches itself to legitimate program causing damage to nodes and keeps spreading around the network. A Trojan horse silently sits behind legitimate program and allows an attacker to get some confidential information about a node or the network.

### Transport Layer Attacks

The objectives of TCP-like Transport layer protocols in MANET include setting up of end-to-end connection, end-to-end reliable delivery of packets, flow control, congestion control, and clearing of end-to-end connection. Similar to TCP protocols in the Internet, the mobile node is vulnerable to the classic SYN flooding attack or session hijacking attacks. However, a MANET has a higher channel error rate when compared with wired networks. Because TCP does not have any mechanism to distinguish whether a loss was caused by congestion, random error, or malicious attacks, TCP multiplicatively decreases its congestion window upon experiencing losses, which degrades network performance significantly [5].

**Session Hijacking:** In this an attacker gets access to the session state of a particular user by stealing session ID which is used to get into a system and snoops the data. Since most of the times authentication only occurs at the beginning of session, this allows an attacker to gain access to a node. Hijacking is done only after the victim node has established the connection. At first attacker predicts the correct sequence number and then spoofs victim's IP address. Meanwhile to take over the session attacker has to launch DOS attack against the victim. The victim node hangs and attacker communicates as if it is a legitimate system.

**SYN Flooding:** On the internet, nodes communicate using TCP/IP protocol so they need to establish connection using three-way handshake. A malicious node sends a huge number of SYN packets to a victim node. The victim node sends back SYN+ACK packets and keeps the entry for the incomplete connection request. The attacker never sends ACK so a large amount of memory of victim node is consumed for storing pending requests and node may come to a halt even. Another way of launching this attack is spoofing the return address of SYN packets with non-existent node so SYN+ACK packets never reach any node fooling the victim node.

### Network Layer Attacks

Network layer protocols extend connectivity from neighboring 1-hops nodes to all other nodes in MANET. The connectivity between mobile hosts over a potentially multi-hop wireless link relies heavily on cooperative reactions among all network nodes. A variety of attacks targeting the network layer have been identified and heavily studied in research papers. By attacking the routing protocols, attackers can absorb network traffic, inject themselves into the path between the source and destination, and thus control the network traffic flow. The traffic packets could be forwarded to a non-optimal path, which could introduce significant delay. In addition, the packets could be forwarded to a nonexistent path and get lost. The attackers can create routing loops, introduce severe network congestion, and channel contention into certain areas. Multiple colluding attackers may even prevent a source node from finding any route to the destination, causing the network to partition, which triggers excessive network control traffic, and further intensifies network congestion and performance degradation.

**Wormhole attack:** An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled [2]. This tunnel between two colluding attackers is referred as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole.

An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole.

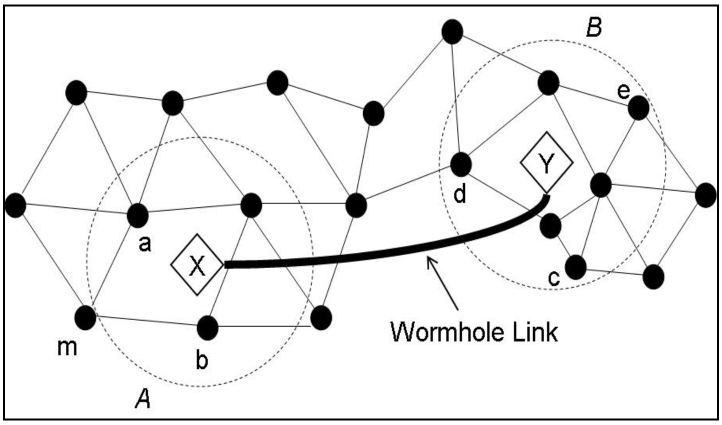

Figure 2 Wormhole attack in MANET

An example is shown in the above Figure 3.4. Here X and Y are the two end-points of the wormhole link (called as wormholes). X replays in its neighborhood (in area A) everything that Y hears in its own neighborhood (area B) and vice versa. The net effect of such an attack is that all the nodes in area A assume that nodes in area B are their neighbors and vice versa. This, as a result, affects routing and other connectivity based protocols in the network. Once the new routes are established and the traffic in the network starts using the X-Y shortcut, the wormhole nodes can start dropping packets and cause network disruption. They can also spy on the packets going through and use the large amount of collected information to break any network security.

**Blackhole Attack:** In this attack a malicious node advertises valid and shortest route to a victim node and thereafter secretly drop data and control packets as they pass through it [13]. In order to have shortest route blackhole node creates forged packet by modifying hop count and sequence number of the routing protocol message such as AODV. So attacker node can eavesdrop or drop the packets. Malicious node is known as blackhole since it consumes data packets forwarded to it and never forwards them.

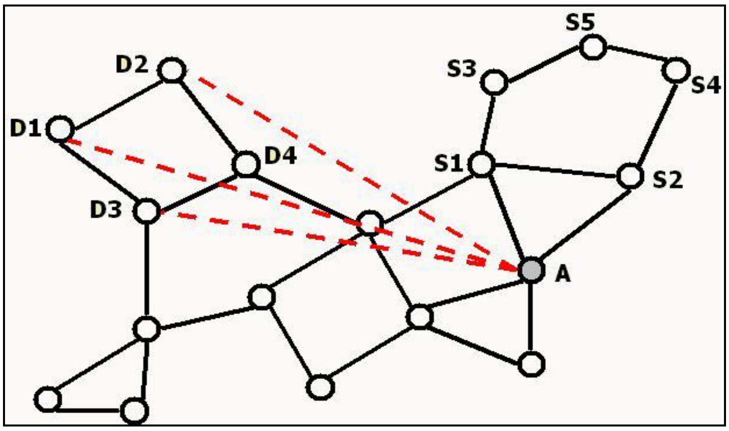

Figure 3 Black hole Attack

**Byzantine Attack:** This attack involves multiple attackers that work in collusion to degrade the network performance such as creating loops, selectively dropping packets, choosing non optimal paths for packet forwarding. For example attacker A1 forwards routing packets of S normally to A2 but second attacker A2 drops or forges these routing packets. In [8] collusion attack in OSLR protocol is discussed and it has been shown that pair of colluding attackers can disrupt 100 % of data packets.

**Information disclosure:** A compromised node may violate the confidentiality principle of security and disclose important information like private and public keys, status of node, passwords, optimal route to authorized nodes, geographic location of nodes and other control data in packet headers to unauthorized nodes present in the network. The location information revealed give better understanding of the network topology. Routing packets are then sent with inadequate hop-limit and ICMP error messages returned by the intermediate nodes are recorded [11]. So it gives blueprint of the network i.e. which nodes are situated in close proximity to the target node.

**Routing Table Overflow:** This attack prevents creation of new legitimate routes by overflowing the routing table with routes to nonexistent nodes. This exploits the limited memory of mobile nodes. A malicious node initiates route discovery to non-existent nodes so that limited memory of mobile node gets consumed by having such entries in their routing table which in turn prevents the creation of new routes to authorized nodes in the network. The proactive ad hoc protocols are more prone to this attack because in such networks routes to all the nodes are already stored before they are needed, in contrast to reactive protocols in which information is discovered when needed.

**Routing table poisoning:** In this attack, malicious node sends fabricated routing update and error messages or modified legitimate updates to authorized nodes in the network. It may result in forwarding packets along sub optimal routes, congestion in the network, formation of loops or blackmail attack in which an attacker sends false route error messages against benign node in order to report benign node as malicious and thus launching denial of service attack against it.

**Routing Cache poisoning:** Route cache is maintained by on demand protocols like DSR that stores the routes known to it by overhearing neighborhood transmissions in the recent past. A malicious node can launch DOS attack on any node by simply broadcasting spoofed packets with source routes to D via itself. Any neighboring node overhearing the packet transmission adds the route entry in their route cache [31].

**Replay Attack:** An attacker instead of modifying packet's contents just replay stale packets in order to exploit battery power, bandwidth and computational constraint of mobile nodes. It leads to congestion in the network and confusion among the routing nodes because of conflicting information, thus delaying packet delivery or preventing them from reaching destination.

**Rushing Attack:** This attack involves entire network traffic to pass through an attacker. The source node is unable to find any secure route without the attacker [32]. Malicious node after receiving RREQ packet from initiating node reacts immediately and floods the network quickly with these packets before other nodes receiving the same RREQ can react. Nodes receiving legitimate RREQ packets assume them as duplicates and discard them. So every route established has attacker as one of the intermediate nodes.

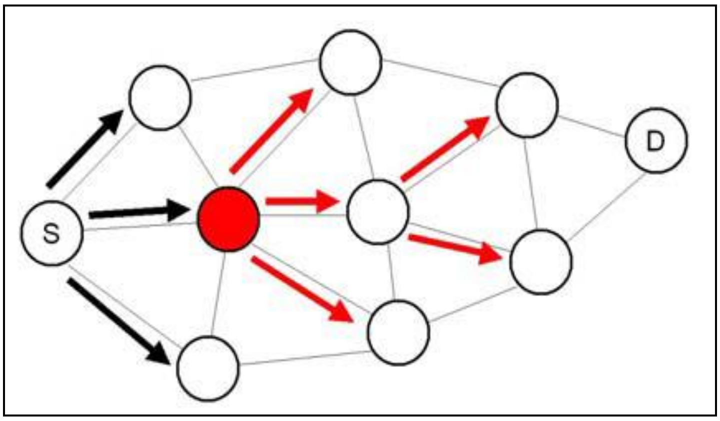

Figure 4 Rushing Attack

**Jellyfish Attack:** It is a selective black hole attack in which malicious node attacks the network by reordering packets, dropping selective packets or increasing jitter of the packets that pass through it in order to prevent it from being detected and it seems to the network that loss or delay is due to environmental reasons.

**Data Link Layer Attacks**

The MANET is an open multipoint peer-to-peer network architecture. Specifically, one-hop connectivity among neighbors is maintained by the link layer protocols, and the network layer protocols extend the connectivity to other nodes in the network. Attacks may target the link layer by disrupting the cooperation of the layer's protocols.

**Denial of service:** There is a single wireless channel shared by all the nodes so a malicious node keeps this channel busy by sending false packets to drain node's battery power.

**MAC targeted Attack:** In MANET nodes share a wireless medium so medium access control (MAC) protocols are used to coordinate the transmission and to resolve the contention. These attacks disrupt the MAC procedure. For example, an attacker can corrupt the frames by introducing extra bits.

**Physical Layer Attacks**

Wireless communication is broadcast by nature. A common radio signal is easy to jam or intercept. An attacker could overhear or disrupt the service of a wireless network physically.

**Device Tampering:** Nodes in ad hoc wireless networks are small, compact and hand-held unlike wired devices so can be easily stolen or damaged.

**Jamming:** The attacker monitors the wireless medium in order to find frequency at which destination node is receiving from sender node. An attacker must have powerful transmitter to sends the signals to the destination at that frequency, thereby interfering with its operations. The most common types of signal jamming are random noise and pulse.

**Multilayer attacks**

These attacks can be launched from several layers instead of a single layer. Examples of multi-layer attacks are jamming, denial of service attacks, impersonation attacks and man-in-the-middle attack.

**Denial of service attack:** In this, an attacker renders a system unusable, or significantly slows it down for legitimate users by overloading its resources. The goal is that if an attacker can't access the node, it will crash the node. In wired networks, DOS is launched against centralized resource, so it is not available to other legitimate nodes. But in wireless networks there is no single centralized resource so there are many other ways by which it can be launched from several layers. At the physical layer, signal jamming disrupts normal communications. At the link layer, malicious nodes prevent other nodes from channel access. At the network layer, DOS attacks are mounted on routing protocols and disrupt the network performance through routing packets modification, selective dropping or routing table overflow. An example of DoS attack on DSR with modified source route - In DSR, source nodes are explicitly stated in routes in data packets. The routing mechanism lacks integrity checks so denial-of-service attack can be launched by modifying the source routes in packet headers. At the transport layer, SYN flooding and session hijacking can cause DOS attacks.

**Impersonation attacks:** Impersonation attacks are launched by using other node's identity, such as MAC or IP address. Impersonation attacks sometimes are the first step for most attacks, and are used to launch further, more sophisticated attacks. A malicious node can masquerade itself as an authorized user and give false routing information or change the configuration of the network. Examples of impersonation attack are Sybil attack and trust attack. In Sybil attack, a malicious node or entity has one physical device and forges multiple identities. A faulty node may present multiple identities to an ad-hoc network in order to function as multiple distinct nodes. After becoming part of the network, the adversary overhears communications or acts maliciously. In threshold scheme where a message or key shares are fragmented into different parts and each part takes different path, the attacker may get access to all pieces of fragmented information as it has imposed several different identities.

**Man-in-the-middle attack:** An attacker sits quietly between the sender and the receiver and makes the actual communicator believe that they are talking to each other but in actual they are talking to the man-in-the-middle who is talking to each of them.

## V. CONCLUSION AND FUTURE WORK

In this paper, we have studied the security threats an ad-hoc network faces and presented the security objective that need to be achieved. There is a need to make ad hoc networks more secure and robust to adapt to the challenging requirements of these networks. The research on MANET security is still in its initial stage. This paper can be further extended to give the solutions corresponding to these attacks which we discussed at different layers of MANET, we can add more detection techniques if it is possible to invent them.

## REFERENCES

[1] Azzedine Boukerche, Begumhan Turgut, Nevin Aydin, Mohammad Z. Ahmad, Ladislu Boloni, Damla Turgut, "Routing protocols in Adhoc network: A survey", Elsevier, Computer Network, pp. 3-32, 2011.

[2] D.B.Roy, R.Chaki and N.Chaki, "A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Neworks," International Journal of Network Security and Its Application (IJNSA), Vol. 1, No.1, April, 2009.

[3] Gagandeep, Aashima, Pawan Kumar, Analysis of Different Security Attacks in MANETs on Protocol Stack AReview ,International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[4] Goyal, Priyanka, Vinti Parmar, and Rahul Rishi. "Manet: vulnerabilities, challenges, attacks, application." IJCEM International Journal of Computational Engineering & Management, pp.32-37, 2011.

[5] H. Hsieh and R. Sivakumar, Transport OverWireless Networks. Handbook of Wireless Networks and Mobile Computing, Edited by Ivan Stojmenovic. John Wiley and Sons, Inc., 2002.

[6] I. Noman and Z. A. Shaikh, "Security Issues in Mobile Ad Hoc Network," Wireless Networks and Security, Springer Berlin Heidelberg, pp. 49-80, 2013.

[7] Ishrat, Z. (2011). Security issues, challenges & solution in MANET. IJCST,2(4).

[8] Kannhavong, B., Nakayama, H., Jamalipour, A., 'NIS01-2: A Collusion Attack Against OLSR-based Mobile Ad Hoc Networks', Global Telecommunications Conference, GLOBECOM '06, IEEE , pp.1-5, 2006,.

[9] Pani, N. K., Mishra, S., Secure Hybrid Routing for MANET Resilient to Internal and External Attacks, ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India, Springer International Publishing, pp. 449-458, 2014.

[10] Rai, Abhay Kumar, Rajiv Ranjan Tewari, and Saurabh Kant Upadhyay. "Different types of attacks on integrated MANET-Internet communication." International Journal of Computer Science and Security, pp. 265-274, 2010.

[11] Renu mishra, Sanjeev Sharma, Rajeev Agrawal., 'Vulnerabilities and security for ad-hoc networks', International Conference on Networking and Information Technology, IEEE 2010, pp. 192-196.

[12] Shanthi, N., L. Ganesan, and K. Ramar. "STUDY OF DIFFERENT ATTACKS ON MULTICAST MOBILE AD HOC NETWORK." Journal of Theoretical & Applied Information Technology 6.4 (2009).

[13] Tarunpreet Bhatia and A.K. Verma, Performance Evaluation of AODV under Blackhole Attack, International Journal Computer Network and Information Security, 5 (2), pp 35-44, 2013.

[14] Tavil B., Heinzelman W., "Mobile Ad Hoc Networks – Energy-efficient real-time data communications ", Chapter 1.1 Characteristics of MANETs, Springer, 2006.