An analysis of Security Attacks found in Mobile Ad-hoc Network

Umesh Kumar Singh[1], Kailash Phuleria[1],Shailja Sharma[2] & D.N. Goswami[2]

[1]Institute of Computer Science, Vikram University, Ujjain
[2] School of Studies in Computer Science, Jiwaji University, Gwalior

***Abstract*- MANETs has become an important technology in recent years because of the rapid proliferation of wireless devices. MANETs are highly vulnerable to attacks due to the open access medium, dynamically changing network topology and lack of centralized monitoring point. The various attacks against mobile nodes are flooding, black hole, warm hole, packet dropping and Byzantine attack as well as Collaborative attacks i.e. human attackers or criminal organizations etc. In this research paper, we study the Vulnerabilities of MANETs and address different types of attacks against MANETs. Finally, we have addressed the future research direction.**

***Keywords*- MANETs, Vulnerabilities, Attacks and Collaborative attack.**

I. INTRODUCTION

In a world of fast developing technologies and internet network, accessible for everyone, where there are no clear boundaries between the functionality of the devices and the possibility to communicate is not an option but necessity, the Mobile ad hoc networking (MANETs) play significant role. MANETs has become one of the most prevalent areas of research in the recent years because of the challenges, it poses to the related algorithms. MANETs is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. MANETs has become a rising research area with many practical applications. Its technology provides a flexible way to set up communications in situations with geographical constraints that demand distributed networks without any centralized authority or fixed base station, such as: disaster relief, emergency situations (rescue team), battlefield communications, conference rooms and military applications [1]. Compared to the traditional wireless and wired networks, MANETs is prone to larger security vulnerabilities and attacks because of certain features of MANET like no centralized authorities, distribution cooperation, open and shared network wireless medium, severe resource restriction, and high dynamic nature of network topology. These factors have made MANETs to receive great attentions and also because of their capabilities of self-configuration and self-maintenance. Another unique feature of MANETs that poses security threats is its unclear defense line; i.e. no built-in security. MANETs does not have dedicated routers and switches, its nodes usually operate by forwarding the packets to one another thereby having no security in the communication; granting access to both legitimate users and attackers [2]. For example, node S can communicate with node D by using the shortest path S-A-B-D as shown in Figure 1 (the dashed lines show the direct links between the nodes). If node A moves out of node S' range, he has to find an alternative route to node D (S-C-E-B-D).

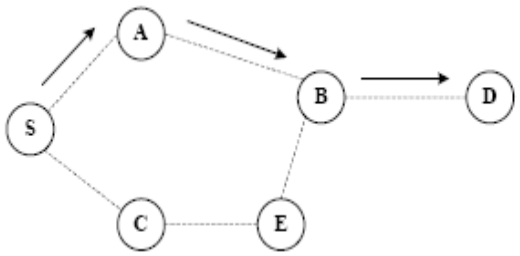

Fig.1: Communication between Nodes on MANETs

Therefore, security in MANETs is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security

issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats [3]. A MANETs is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

The main purpose of this paper is to investigate some of the important attacks might be related to security in MANETs. We discuss the related work in section II. In Section III, we address the different Vulnerabilities of MANETs. In section IV, we identified that most of the attacks against ad hoc networks routing protocols are actually launched. Finally, we conclude our study and present future work in Section V.

II. RELATED WORK

In the last few years, security of computer networks has been of serious concern which has widely been discussed and formulized. Most of the discussions involved only static and networking based on wired systems. However, mobile Ad-Hoc networking is still in need of further discussions and development in terms of security. With the emergence of ongoing and new approaches for networking, new problems and issues arises for the basics of routing. The comparison of wired network Mobile Ad-Hoc network is different. The routing protocols designed majorly for internet is different from the mobile Ad-Hoc networks (MANETs).

Due to various factors including lack of infrastructure, absence of already established trust relationship in between the different nodes and dynamic topology, the routing protocols are vulnerable to various attacks. Major vulnerabilities which have been so far researched are mostly including selfishness, dynamic nature, and severe resource restriction and also open network medium. In MANETs, there are attacks which can be categorized in Passive, Active, Internal, External and network-layer attacks, Routing attacks and Packet forwarding attacks. The attacks may be passive or active, leakage of information, false message reply, denial of service or changing the data integrity. Some of the attacks are to get access inside the network in order to get control over the node in the network using unfair means to carry out their malicious activities. Mobile nodes in MANETs are free to move, join or leave the network in other words the mobile nodes are autonomous. Many studies on MANETs focus on the protocols used their security issues such as data encryption, authentication, trust, cooperation among nodes, attacks on the protocols and proposed solutions or preventions [2, 4-6]. In the face of the different specific attacks on MANET such as Denial-of-Service (DoS), impersonation, Node hijacking and so on that have been exposed [7-8], the attacks involving multiple nodes seem to have received little attention. One of the possible reasons could be that most researchers tend to adopt ideas about security measures from wired networks to ad hoc networks and forget that security issues regarding MANETs are more complicated since MANETs is unable to rely on pre-existing infrastructure. In other words, all nodes are communicating without a central authority or base station to keep a network connected. Therefore, the existing security solutions for wired network cannot be directly applied to the MANETs.

In a blackhole attack, several malicious nodes falsely claim a new route to the destination in order to absorb all packets coming from the source. To combat this kind of routing protocol attack, Deng et al. proposed a solution that revolved around waiting and checking the replies from all other neighboring nodes and then deciding on the safe route. Using a fidelity table is another solution, in which every node will be assigned a fidelity level and the node with “0” level will be considered as malicious and be eliminated from the MANETs [1]. Distributed Denial of Service (DDoS) attack is another kind of attack on multiple nodes; it is because of the nature characteristic of this attack. DDoS attack involves breaking into hundreds or thousands of machines and from those machines, attacker launches several attacks aim at target machine in order to consume bandwidth and create bottleneck in the network [9]. The basic vulnerabilities in MANETs have been researched previously, ranging from their open network medium, severe resource restriction, selfishness, dynamic nature, to vulnerabilities in some protocols. In addition, there are different categories of attacks against MANETs. These categories in pair are Passive and Active attacks, Internal and External attacks and the two categories of network-layer attacks: Forwarding attacks [1, 2, 6].From our perspectives, collaborative attacks are non-single attacks; they are attacks launched in multiple malicious nodes acting as a group. Typical examples of these kinds of attacks are Black hole attack, Sybil attack and Wormhole attack on nodes in a MANETs.

Previous studies show that there are different categories of attacks on MANETs [1-2, 6] such as Passive and Active attacks, Internal and External attacks and the Routing and Packet Forwarding attacks. Some of these attacks are termed as single attacks while some are referred to as attacks on multiple nodes and are malicious. MANETs is open to vulnerabilities as a result of its basic characteristics like: no point of network management, topology changes vigorously, resource restriction, no certificate authority or centralized authority, to mention a few.

III. VULNERABILITIES OF MANETS

Vulnerability is a weakness in security system or Wireless System. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANETs is more vulnerable than wired network. Some MANETs vulnerabilities are as follows [1-4, 7-9]:-

- *Wireless Links:* First of all, the use of wireless links makes the network susceptible to attacks such as eavesdropping and active interference. Unlike wired networks, attackers do not need physical access to the network to carry out these attacks. Furthermore wireless networks typically have lower bandwidths than wired networks. Attackers can exploit this feature, consuming network bandwidth with ease to prevent normal communication among nodes.

- *No predefined Boundary:* In MANETs, we cannot exactly define a physical boundary of the networks. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network. As soon as an adversary comes in the radio range of a node it will be able to communicate with that node.

- *Scalability:* Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.
- *Resource availability*: Resource availability is a major issue in MANETs. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.

- *Lack of Centralized Management Facility:* Ad hoc networks do not have a centralized piece of management machinery such as a name server, which lead to some vulnerable problems. Now let us discuss this problem in a more detailed manner First of all, the absence of centralized management machinery makes the detection of attacks a very difficult problem because it is not easy to monitor the traffic in a highly dynamic and large scale ad hoc network. Second, lack of centralized management machinery will delay the trust management for the nodes in the ad hoc network. Third, important algorithms in the mobile ad hoc network rely on the cooperative participation of all nodes and the infrastructure. Because there is no centralized authority, and decision-making in mobile ad hoc network is sometimes decentralized, the adversary can make use of this vulnerability and perform some attacks that can break the cooperative algorithm.

- *Cooperativeness:* In MANETs, all routing protocols assume that nodes provide secure communication. But some nodes may become malicious nodes which disrupt the network operation by changing routing information etc.
- *Infrastructure less:* MANETs is an infrastructure less network, there is no central administration. Each device can communicate with every other device, hence it becomes difficult to detect and manage the faults. In MANETs, the mobile devices can move randomly. The use of this dynamic topology results in route changes, frequent network partitions and possibly packet losses.

- *Limited power supply***:** The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply.

- *Dynamic topology:* Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.

- *Bandwidth Constraint:* Variable low capacity links exists as compared to wireless network which are more susceptible to external noise, interference and signal attenuation effects.

- *Adversary inside the Network*: The mobile nodes within the MANETs can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behavior of the node is malicious. Thus this attack is more dangerous than the external attack. These nodes are called compromised nodes.

IV. ATTACKS IN MANETS

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. Security means protecting the privacy (confidentiality), availability, integrity and non-repudiation. Security implies the identification of potential attacks from unauthorized access, use, modification or destruction. Earlier, various attempts have been made by various researchers [10-13] to classify the attacks on various layers. A complete picture of attack types on layers is helpful for the effectively mitigations of these attacks. In figure-2, attacks on layers are broadly classified for this purpose.

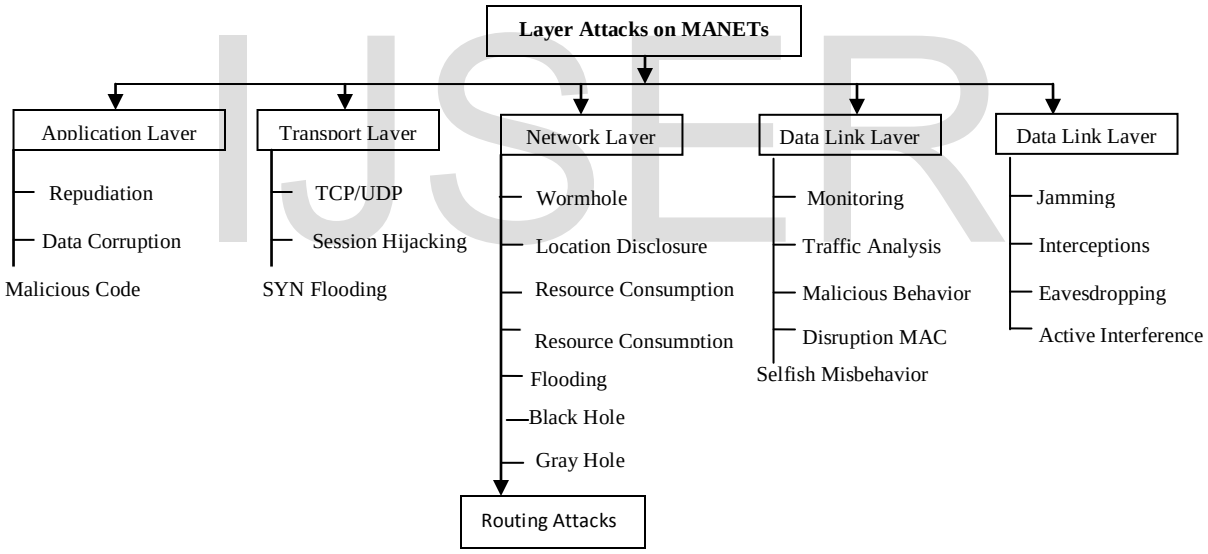

Fig. 2: Attacks in various layers of MANET

Attacks can also be categorized on the basis of its source, behavior and nodes. Figure-3, shows such categorization:

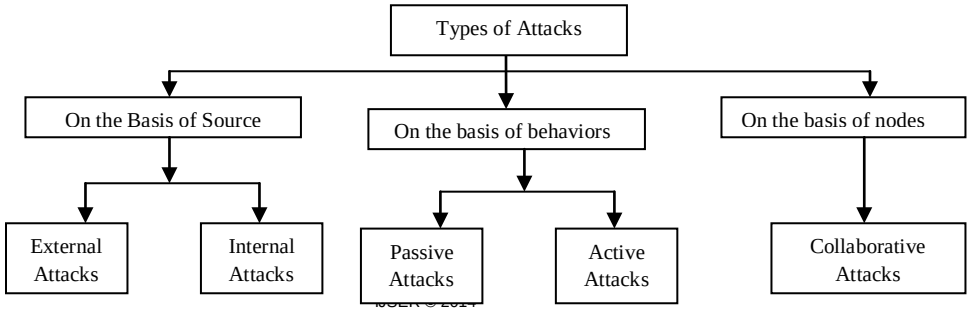

Figure 3: Categorization of Attacks in MANETs

I. ***On the Basis of Source:*** On the basis of source, attacks can be classified as external and internal attacks. External attacks are caused by the nodes which are not a part of the network. External attackers are the aims to cause congestion, propagate fake routing information or disturb nodes from providing services. Internal attacks are caused by the nodes which are a part of the network. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

II. ***On the basis of Behavior:*** A passive attack attempts to retrieve valuable information by listening to traffic channel without proper authorization, but does not affect system resources and the normal functioning of the network. Passive attacks are very hard to detect because they do not involve any alteration of the data. An active attack attempts to change or destroy the system resources. It gains an authentication and tries to affect or disrupt the normal functioning of the network services by injecting or modifying arbitrary packets of the data being exchanged in the network. An active attack involves information interruption, modification, or fabrication.

III. ***On the basis of Nodes:*** In these types of attacks, there are numerous nodes involved during the attack. These nodes can be physically existent or not existing at all.

In this paper we discuss the different attacks related to on the basis of behavior and on the basis of nodes.

A. ***Passive Attacks:*** Some important passive attacks are: Snooping Attacks, Eavesdropping Attacks, Traffic Analysis Attacks, and Traffic Monitoring Attacks.
Snooping Attack is also known as masquerade or impersonation or spoofing Network attack. In this attack, a single malicious node attempts to take out the identity of other nodes' in the network by advertising false/fake routes. It then attempts to send packets over network with identity of other nodes making the destination believe that the packet is from original source [14]. The eavesdropping attack is a serious security threat to a wireless sensor network (WSN) since the eavesdropping attack is a prerequisite for other attacks. Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence or counter-intelligence, and is a concern in computer security. In this type of attack, an attacker tries to sense the communication path between the sender and receiver. This way attacker found the amount of data which is travel between the route of sender and receiver. There is no alteration in data by the traffic analysis. Monitoring is another passive attack in which attacker can see the confidential data, but he cannot change the data or cannot modify the data.

B. ***Active Attacks***: Active attack: Some important passive attacks are: Blackmail, Denial of service attack, Fabrication, Gray hole Attacks, Disclosure Attacks, Routing Attacks and Recourse Consumption Attacks.
A black mail attack is relevant against routing protocols that uses mechanisms for identification of malicious nodes and propagate messages that try to blacklist the offender. Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network. The notation "fabrication" is used when referring to attacks performed by generating false routing messages. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages, which claim that a neighbor can no longer be contacted [15]. Gray hole, a gray hole attack is a variation of the black hole attack, where the malicious node is not initially malicious, it turns malicious sometime later. In this attack, an attacker drops all data packets but it lets control messages to route through it [16]. Disclosure attacks are aimed at acquiring system-specific information about a website such as software distribution, version numbers, and patch levels. The acquired information might also contain the

location of backup files or temporary files [17]. In Routing Attacks, attackers try to alter the routing information and data in the routing control packet. There are several types of routing attacks mounted on the routing protocol which are intended for disturbing the operation of the network In Resource Consumption Attack, a malicious node intentionally tries to consume or misuse of the resources (battery power, bandwidth, and computational power) of other nodes' exist in the network by requesting excessive route discovery (unnecessary route request control messages), very frequent generation of beacon packets, or by forwarding unnecessary packets (stale information) to that node [18].

C. ***Collaborative attacks***: Collaborative attacks (CA) occur when more than one attacker or running process synchronize their actions to disturb a target network. Multiple attacks occur when a system is disturbed by more than one attacker, but not necessarily in collaboration. We have study different types of attacks and then provided the definition of collaborative attacks; we are now going to categorize these attacks into two different categories. First: Direct Collaborative Attacks and Second: Indirect Collaborative Attacks.

Here, the attacker nodes are already in existence in the original network or a malicious node joins the network or an internal node is compromised in the network. This kind of collaborative attacks can be referred to as direct collaborative attacks. A Blackhole and Wormhole attack belongs to this category. In the black hole attack, attacker uses the routing protocol to advertise itself as having the best path to the node whose packets it want to intercept. An attacker use the flooding based protocol for listing the request for a route from the initiator, then attacker create a reply message he has the shortest path to the receiver . As this message from the attacker reached to the initiator before the reply from the actual node, then initiator assume that it is the shortest path to the receiver. So that a fake route is create. Once the attacker has been able to insert himself between the communications node, then attacker may able to do anything with the packet which is send by the initiator for the receiver [19]. In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole.

The attacks in this category use different non-existent nodes in order to fake other nodes to redirect data packets to malicious node. This kind of collaborative attacks can be referred to as indirect collaborative attacks. A Sybil and Routing table overflow attacks belongs to this category. Sybil attack refers to the multiple copies of malicious nodes. It can be happen, if the malicious node shares its secret key with other malicious nodes. This way the number of malicious node is increased in the network and the probability of the attack is also increased. If we use the multipath routing, then the possibility of choosing a path in the network, those contain the malicious node will be increased [20-21]. The malicious node makes routing services a target because it's an important service in MANETs. There are two flavors to this routing attack. One is attack on routing protocol and another is attack on packet forwarding or delivery mechanism. The first is aimed at blocking the propagation of routing information to a node. The latter is aimed at disturbing the packet delivery against a predefined path.

IV. CONCLUSION AND FUTURE DIRECTIONS

In this paper we addressed existing potential security threats in MANETs. In this study we found that most of the work on MANET security focused on single layer attacks i.e. active and passive attacks. In the meanwhile some attacks involving multiple nodes have received little attention since they are surprising and combined attacks i.e. collaborative attacks. There have been no proper definition and categorization of these kinds of collaborative attacks in MANETs. Thus, protection of communication system against these types of attacks is a challenging task. Therefore, deep study on collaborative attacks and development of new protocols/algorithms/model to manage these attacks is the need of hour. Development of a multi-fence security solution that is embedded into possibly every component in the network, resulting in depth protection that offer multiple line of defense against many known and unknown security threats is also given importance. Further, there is also a need to develop a detection and defense mechanism for managing messages in secure manner.

REFERENCES:

[1]. H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," IEEE Communications Magazine, vol. 40, pp. 70-75, 2002.
[2]. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Communications, vol. 11, pp. 38-47, 2004.
[3]. Vesa Kärpijoki. "Security in Ad Hoc Networks", Helsinki University of Technology.
[4]. Shuyao Yu, Youkun Zhang, Chuck Song and Kai Chen, security architecture for Mobile Ad Hoc Networks". http://www.portal.prozhe118.com, , PP-1-4.
[5]. L. Peters, F. De Turck, I. Moerman, B. Dhoedt, P. Demeester, and A. A. Lazar, "Network layer solutions for wireless shadow networks," Proceedings of the International Conference on networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, , vol. 2, 2006.
[6]. S. A. Razak, S. M. Furnell, and P. J. Brooke, "Attacks against Mobile Ad Hoc Networks Routing Protocols," www.scm.tees.ac.uk, pp.-1-6, 2004.
[7]. A. Mishra, Security and Quality of Service in Ad Hoc Wireless Networks, 2008.
[8]. L. Tamilselvan and V. Sankaranarayanan, "Prevention of co-operative black hole attack in MANET," Journal of networks, vol. 3, pp. 13-20, 2008.
[9]. S. Saraeian, F. Adibniya, M. GhasemZadeh, and S. Abtahi, "Performance Evaluation of AODV Protocol under DDoS Attacks in MANET," Proceedings of World Academy of Science, Engineering and Technology, vol. Vol. 33, pp. 501 - 503, September 2008.
[10]. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks, WIRELESS/MOBILE NETWORK SECURITY Y. Xiao, X. Shen, and D.-Z. Du (Eds.), year-2006 Springer, pp. 1-38.
[11]. Sevil Şen, John A. Clark, Juan E. Tapiador, Security Threats in Mobile Ad Hoc Networks, Department of Computer Science, University of York, YO10 5DD, UK, pp.1-22.
[12]. Rakesh Kumar Singh, Rajesh Joshi, Mayank Singhal, Analysis of Security Threats and Vulnerabilities in Mobile Ad Hoc Network (MANET), International Journal of Computer Applications (0975 – 8887) Volume 68– No.4, pp.25-29, April 2013.
[13]. Amandeep Kaur, Hardeep Singh, A Study of Secure Routing protocols, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 2, pp. 176-179, February 2013.
[14]. J. Douceur, "The Sybil Attack", Proceedings of the 1st International Workshop on Peer-to- Peer Systems (IPTPS'02), pp.251-260, Cambridge, MA, 2002.
[15]. S. Desilva, and R. V. Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks," Proc. IEEE Wireless Commun. and Networking Conf., New Orleans, LA, 2005.
[16]. Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy and P. Balamuralidhar, "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", Proceedings of IEEE 6th International Conference on Information, Communications and Signal Processing, pp.1-5, 2007.
[17]. http://pic.dhe.ibm.com
[18]. C. Siva Ram Murthy and B.S Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols", Pearson Education, ISBN: 978-81-317-0688-6, 2006.
[19]. Sheenu Sharma, Roopam Gupta, "Simulation study of blackhole attack In the mobile ad hoc networks", Journal of Engineering Science and Technology Vol. 4, No. 2 , 2009.
[20]. Kuldeep Sharma, Neha Khandelwal, Prabhakar.M. "An Overview Of security Problems in MANET". http://psrcentre.org/images/extraimages/155.pdf, pp.-1-5.
[21]. Ali Ghaffari, "Vulnerability and Security of Mobile Ad hoc Networks", Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization, Lisbon, Portugal, September 22-24, 2006.