Threats & Security Issues in Ad Hoc Network: A Survey Report

Sarvesh Tanwar, Prema K.V.

Abstract- With the advancement in radio technologies like Bluetooth, IEEE 802.11, a new concept of networking has emerged; this is known as ad hoc networking where potential mobile users arrive within the range for communication. As network is becoming an increasingly important technology for both military and commercial distributed and group based applications, security is an essential requirement in mobile ad hoc network (MANETs). Compared to wired networks, MANETs are more vulnerable to security attacks due to the lack of a trusted centralized authority and limited resources. Attacks on ad hoc networks can be classified as passive and active attacks or internal attack and external attacks, the security services such as confidentiality, authenticity and data integrity are also necessary for both wired and wireless networks to protect basic applications. One main challenge in design of these networks is their vulnerability to security attacks. In this paper, we study the threats an ad hoc network faces and the security goals to be achieved.

Keywords: MANET, Security, IEEE802.11, vulnerability, authenticity, threats, ad hoc networks.

I. INTRODUCTION

Recent advances in computer networking have introduced a new technology for future wireless communication, a mobile ad hoc network (MANET). Ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. Nodes in ad hoc network are mobile and they can communicate with each other within radio range through direct wireless links or multihop routing.

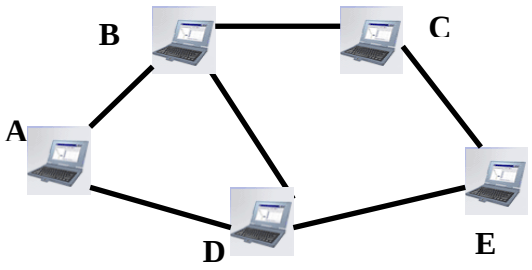

Figure 1: An ad- hoc network

The military tactical and other security-sensitive operations are still the main applications of ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties. However, similar to other networks, MANET also vulnerable to many security attacks.

Manuscript received on January, 2013.

Sarvesh Tanwar, Department of Computer Science & Engineering , FET, Mody Institute of Technology & Science, (MITS) University, Laxmangarh (Rajasthan), India.

Dr. Prema K.V., Department of Computer Science & Engineering,, FET, Mody Institute of Technology & Science, (MITS) University, Laxmangarh (Rajasthan), India.

MANET not only inherits all the security threats faced in both wired and wireless networks, but it also introduces security attacks unique to itself [1]. In Mobile Ad Hoc Networks (MANET), security is a challenging issue due to the vulnerabilities that are associated with it.

Intrusion detection is therefore incorporated as a second line of defense in addition to key based authentication schemes. The ranges of attacks that can be mounted on MANETs are also wider than in case of conventional static networks. In mobile wireless networks there is no infrastructure as such and so it becomes even more difficult to efficiently detect malicious activities by the nodes inside and outside the network. As a matter of fact, the boundary of the network is not properly defined. Nodes can intermittently come into the network or leave it. Moreover malicious nodes can flood the network with junk packets hampering the network service or intentionally drop packets. But these nodes can But these nodes can subtly manipulate their harmful activities in such a manner that it becomes difficult to declare a node as malicious.

1.1 Mobile Ad-hoc Network Characteristics

Ad-hoc network is becoming popular for its unique characteristics. To achieve the attractive features, ad-hoc network should attain distinguish properties such as peer-to-peer among host; multi-hop routing protocol, dynamic; and finally the network is autonomous and auto configured. Some of the characteristics which differentiate ad hoc wireless networks from other networks are:-

1. Dynamic Network Topology: This is triggered by node mobility, nodes leaving or joining the network, node inoperability due to the lack of power resources, etc. Nonetheless, the network connectivity should be maintained in order to allow applications and services to operate undisrupted.
2. Fluctuating Link Capacity: The effects of high bit error rate are more profound in wireless communication. More than one end-to-end path can use a given link in ad hoc wireless networks, and if the links were to break, could disrupt several sessions during period of high bit transmission rate.
3. Distributed Operations: The protocols and algorithms designed for an ad hoc wireless network should be distributed in order to accommodate a dynamic topology and an infrastructure less architecture.
4. Limited Energy Resources: Wireless devices are battery powered, therefore there is a limited time they can operate without changing or replenish their energy resources. Designing energy efficient mechanisms are thus an important feature in designing algorithms and protocols.

Mechanisms used to reduce energy consumption include (a) having nodes enter sleep state when they cannot send or receive data, (b) choose routing paths that minimize energy consumption, (c) selectively use nodes based on their energy status, (d) construct communication and data delivery structures that minimize energy consumption, and (e) reduce networking overhead.

1.2 Goals in Ad-hoc Networks

When the concept of Ad-hoc network was first established, a set of initial goals was fixed. These goals were scalability, quick convergence, bi-directional communication, loop freedom, unicast etc. But with the rapid proliferation of ad-hoc network in different applications for the last few years, the applications require some other properties such as:-

Secure routing and data transfer [4]: Nodes are generally mobile nature in adhoc network. Currently all routing protocols cope with the dynamic topology without adequate security measure. So node may compromise any time. As the network serves various sensitive applications. So secure routing protocol and secure data transfer mechanism require for this network.

Quality of service (QoS): QoS define as the ability of a network element such as node to provide some level of assurance for consistent of the network data delivery. It is a set of service requirements to be met by the network while transporting a packet stream from source to destination. Due to dynamic nature, limited resource availability, insecure medium it is needed to maintain QoS of this network.

Service discovery: Nodes may want to get any service from this wireless network in ad-hoc basis in emergency situation such as in battlefield, rescue operation. Node may search for service after discovery the route. That's why ad-hoc network need to provide service discovery process for the mobile node in the network [11].

II. ATTACKS VARIATIONS [2]

A. Ad hoc networks environments:

In MANET all the nodes are free; there is no centralized authority to make control on the nodes in the network. Mobile ad hoc networks are based on the assumption that all participants of the network cooperate and forward packets towards destinations. Unfortunately, there are no mechanisms to enforce cooperation. Thus, altruism and trust are two of the most important characteristics in mobile ad hoc networks. However, what happens if there are selfish or even malicious nodes? Those nodes do not forward all packets to the next station. If the fraction of misleading nodes becomes too big, the throughput decreases significantly. However, this is not a big issue in a localized environment, because nodes in that environment might have a physical contact with each other to employ any security measures. Security could also be easily enforced in the organized environment because nodes in that environment are usually pre-employed with appropriate security measures before they participate in any specific tasks such as in a military operation.

B. Communication layers:

Each layer in the ad hoc networks communication protocols has its own vulnerabilities. In a physical layer, mobile nodes as well as the communication links are vulnerable to both passive and active attacks. Passive eavesdropping, signal jamming, denial of service (DoS) attacks, and physical hardware tampering are among the most popular attacks in this layer [2]. Such attacks could be made less useful by encrypting the communication signal, employing spread-spectrum communication technology, and using a tamper-resistant hardware.

C. Attack level:

There are two main levels of attack in the ad hoc network; attacks against the basic mechanisms and attacks against the security mechanisms [4]. Ad hoc networks have their own unique basic mechanisms, such as the use of wireless links for communications, employing their own routing strategies, and operate in a distributed manner.

III. AD HOC NETWORK THREATS

Mobile ad hoc networks are highly susceptible to routing attacks because of their dynamic topology and lack of any infrastructure. As people will be encouraged to use a secured network, it is important to provide MANET with reliable security mechanisms. Before the development of any security measure to secure mobile ad hoc networks, it is important to study the variety of attacks that might be related to such networks. With the knowledge of some common attack issues, researchers might have a better understanding of how mobile ad hoc networks could be threatened by the attackers, and thus might lead to the development of more reliable security measures in protecting them.

IV. CLASSIFICATION OF ATTACKS

Attacks on network are divided into two categories – (i) Internal attack and (ii) External attack.

In Internal attacks, the adversary (attacker) 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.

In External attacks, the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services.

Current MANETs are basically vulnerable to two different types of attacks: active attacks and passive attacks. Active attack is an attack when misbehaving node has to bear some energy costs in order to perform the threat. On the other hand, passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly [8]. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish. We have classified the attacks as modification, impersonation, fabrication wormhole and lack of cooperation. Some of the active attacks are as follows:-

A. Network layer Attack

- ✓ Black hole
- ✓ Byzantine
- ✓ Wormhole
- ✓ spoofing attack
- ✓ Sybil

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

I. *Black hole:*

In a black hole attack a malicious node injects false route replies to the route requests it receives advertising itself as having the shortest path to a destination. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.

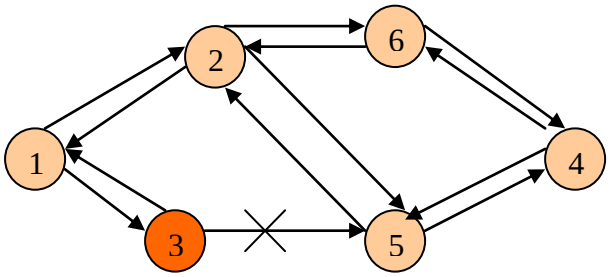

Figure 2 : Problem of black hole

II. *Byzantine Attack:*

In this attack, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets [10] which results in disruption or degradation of the routing services. It is hard to detect byzantine failures. The network would seem to be operating normally in the viewpoint of the nodes, though it may actually be showing Byzantine behavior. Possible Byzantine behaviour in proactive routing protocols includes the possibility of a malicious node:

- ✓ Advertising high willingness to forward control packets;
- ✓ Advertising false links in a Hello packet;
- ✓ Advertising false links in a topology control packet;
- ✓ Including itself in topology control packets it receives for forwarding, and
- ✓ Removing links from topology control packets.

Once a malicious node receives a route request, it can respond in a variety of ways:

- ✓ Modify the metric,
- ✓ Delay sending the route request, and
- ✓ Drop the route request without rebroadcasting it.

III. *Wormhole attack:*

In a wormhole attack, an attacker receives packets at one location in the network, and "tunnels" them to another point in the network, and then replays them into the network from that point. For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive with better metric than a normal multihop route, for example, through use of a single long-rang directional wireless link or through a direct wired link to a colluding attacker. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole. If the attacker performs this tunneling honestly and reliably, no harm is done; the attacker actually provides a useful service in connecting the network more efficiently. However, the wormhole puts the attacker in a very powerful position relative to other nodes in the network, and the attacker could exploit this position in a variety of ways. 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.

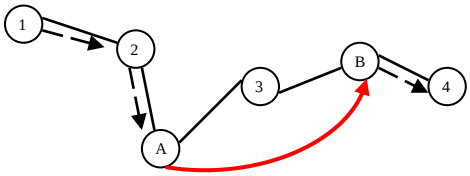

Figure 3: A wormhole attack performed by colluding malicious nodes A and B

IV. *Spoofing attack:*

Spoofing is a special case of integrity attacks whereby a compromised node impersonates a legitimate one due to the lack of authentication in the current ad hoc routing protocols. The main result of the spoofing attack is the misrepresentation of the network topology that may cause network loops or partitioning. Lack of integrity and authentication in routing protocols creates fabrication attacks that result in erroneous and bogus routing messages.

V. Sybil attack:

If a malicious node impersonates some nonexistent nodes, it will appear as several malicious nodes conspiring together, which is called a Sybil attack. A Sybil attack is one in which an attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous entities, using them to gain a disproportionately large influence. A reputation system's vulnerability to a Sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the reputation system treats all entities identically.

This attacks aims at network services when cooperation is necessary, and affects all the auto configuration schemes and secure allocation schemes based on trust model as well. However, there is no effective way to defeat Sybil attacks.

Validation techniques can be used to prevent Sybil attacks and dismiss masquerading hostile entities. A local entity may accept a remote identity based on a central authority which ensures a one-to-one correspondence between an identity and an entity and may even provide a reverse lookup.

Sybil prevention techniques based on the connectivity characteristics of social graphs can also limit the extent of damage that can be caused by a given sybil attacker while preserving anonymity, though these techniques cannot prevent sybil attacks entirely, and may be vulnerable to widespread small-scale sybil attacks.

B. Denial of Service attack

In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. A denial of service (DoS) attack is an attack that clogs up so much memory on the target system that it cannot serve its users, or it causes the target system to crash, reboot, or otherwise deny services to legitimate users.

These days, DoS attacks are very common; indeed, just about every server is bound to experience such an attack at some time or another. Denial of Service can easily be launched and flood the network with spurious routing messages through a malicious node that gives incorrect updating information by pretending to be a legitimate change of routing information. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.

- RREQ Flood Attack: The flood attack introduces unnecessary broadcast messages into the network to hinder normal operation of the network.
- RREP Route loop Attack: A routing loop is a path that goes through the same node more than once.

C. Distributed denial-of-service (DDoS) attack:

In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses. The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attack.

Such attacks include:

- ✓ Injecting routes to false destinations,
- ✓ Flooding attacks involving control packets, and
- ✓ False removal of working routes.

a.) Resource consumption attack: This is also known as the sleep deprivation attack. An attacker or a compromised node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim node.

b) Replay [6]: An attacker that performs a replay attack injects into the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

c) Flooding attack: In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service.

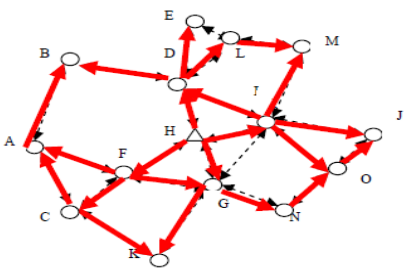

Figure 4: Flooding attack

d) Link spoofing attack or IP spoofing attack [3] [10]:

In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations. For example, in the OLSR protocol, an attacker can advertise a fake link with a target's two-hop neighbors. This causes the target node to select the malicious node to be its MPR. As an MPR node, a malicious node can then manipulate data or routing traffic, for example, modifying or dropping the routing traffic or performing other types of DoS attacks. Firstly, the attacker selects many IP addresses which are not in the networks if he knows the scope of IP address in the networks. Because no node can answer RREP packets for these RREQ, the reverse route in the route table of node will be conserved for longer. The attacker can select random IP addresses if he cannot know scope of IP address. Secondly, the attacker successively originates mass RREQ messages for these void IP addresses.

V. ATTACKING THE ROUTING PROTOCOL

There are several attacks which can be mounted on the routing protocols and may disrupt the proper operation of the network. Brief descriptions of such attacks are given below [13][14]:

Routing Table Overflow: In the case of routing table overflow, the attacker creates routes to nonexistent nodes. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. In the case of proactive routing algorithms we need to discover routing information even before it is needed, while in the case of reactive algorithms we need to find a route only when it is needed. Thus main objective of such an attack is to cause an overflow of the routing tables, which would in turn prevent the creation of entries corresponding to new routes to authorized nodes.

***a) Routing Table Poisoning*:** In routing table poisoning, the compromised nodes present in the networks send fictitious routing updates or modify genuine route update packets sent to other authorized nodes. Routing table poisoning may result in sub-optimal routing, congestion in portions of the network, or even make some parts of the network inaccessible.

b.) Packet Replication: In the case of packet replication, an attacker replicates stale packets. This consumes additional bandwidth and battery power resources available to the nodes and also causes unnecessary confusion in the routing process.

c.) Route Cache Poisoning: In the case of on-demand routing protocols (such as the AODV protocol [14]), each node maintains a route cache which holds information regarding routes that have become known to the node in the recent past. Similar to routing table poisoning, an adversary can also poison the route cache to achieve similar objectives.

d) Rushing Attack: On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack [12]. An attacker which receives a route request packet from the initiating node floods the packet quickly throughout the network before other nodes which also receive the same route request packet can react. Nodes that receive the legitimate route request packets assume those packets to be duplicates of the packet already received through the attacker and hence discard those packets.

Any route discovered by the source node would contain the attacker as one of the intermediate nodes. Hence, the source node would not be able to find secure routes, that is, routes that do not include the attacker. It is extremely difficult to detect such attacks in ad hoc wireless networks.
Attacking the routing of data packets

- ✓ Modifying the packet header
- ✓ Flooding attacks
- ✓ Replaying and reordering packets

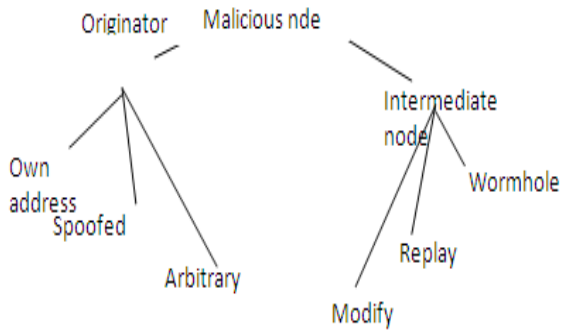

Figure 5: malicious attack tree

The scope of attacks arising from malicious behavior

- ✓ Replay attacks
- ✓ Byzantine
- ✓ Denial of service
- ✓ Sybil attacks

VI. SOME OTHER ATTACKS

- ✓ Rushing Attack
- ✓ Gray hole attack
- ✓ Sinkhole attacks
- ✓ Location disclosure
- ✓ Jamming attack
- ✓ Information Disclosure

a.) Rushing attacks: Rushing attack on ad hoc networks which is carried out on on-demand routing protocols that keep a copy of packets at every node. In this attack, an attacker constantly spreads fabricated routing messages which suppress the legitimate routing messages as the nodes discard them as duplicate copies. Another type of attack is spoofing. In spoofing, a malicious node attempts to misrepresent its identity by changing its IP or MAC address in order to change the perception of a network by an incoming node (Pirzada & McDonald, 2006).

b.) Gray hole attack: We now describe the gray hole attack on MANETS. The gray hole attack has two phases. In the first phase, malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the black hole attack where the malicious node drops the received data packets with certainly [5]. A gray hole may exhibit its malicious behavior in different ways. It may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of gray hole node may behave maliciously for some time duration by dropping packets but may switch to normal behavior later. A gray hole may also exhibit a behavior which is a combination of the above two, thereby making its detection even more difficult.

c) Sinkhole attacks: By carrying out a *sinkhole attack*, a compromised node tries to attract the data to itself from all neighboring nodes. Since this would give access to all data to this node, the sinkhole attack is the basis for many other attacks likes eavesdropping or data alteration. Sinkhole attacks make use of the loopholes in routing algorithms of ad hoc networks and present themselves to adjacent nodes as the most attractive partner in a multihop route. Even though by definition nodes on the network layer of an ad hoc network are equal, sinkhole attacks might be very effective on application level, where nodes may have different roles. This means, that as stated in [2], the effect of sinkhole attacks on networks with centralized entities can be especially grave, because by impersonating the centralized node or its neighbors, the adversary can get access to the biggest part of the data flowing through the network. Effective against sinkhole attacks is the use of multipath (SMR [11], derivates of AODV and DSDV) and/or probabilistic (PRB [12]) routing protocols. Multipath protocols send data redundantly, not relying on one path only. Probabilistic protocols measure the trustworthiness of a message based on the probability of the packet arriving from a certain source, which can help detecting sinkholes within the network (if many packets arrive from a rather improbable source).

d) Location disclosure [9]: Location disclosure is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques or with simpler probing and monitoring approaches an attacker is able to discover the location of a node, or even the structure of the entire network.

e) Jamming attack: This attack is occurred at MAC layer. Jamming is the particular class of DoS attacks. The objective of a jammer is to interfere with legitimate wireless communications. A jammer can achieve this goal by either preventing a real traffic source from sending out a packet, or by preventing the reception of legitimate packets.

f) Information Disclosure [12]: Any confidential information exchange must be protected during the communication process. Also, the critical data stored on nodes must be protected from unauthorized access. In ad hoc networks, such information may contain anything, e.g., the specific status details of a node, the location of nodes, private keys or secret keys, passwords, and so on. Sometimes the control data are more critical for security than the traffic data. For instance, the routing directives in packet headers such as the identity or location of the nodes can be more valuable than the application-level messages. A compromised node may leak confidential or important information to unauthorized nodes present in the network. Such information may contain information regarding the network topology, geographic location of nodes or optimal routes to authorized nodes in the network.

g) *Misdirection attacks:* In an ad hoc network, a malicious node may attempt to misdirect traffic to itself, or to another node.

The relevant attack methods are:

- ✓ Masquerading as an existing node,
- ✓ Masquerading as a previously connected node,
- ✓ Replay attacks,
- ✓ Byzantine behaviour to attract traffic,
- ✓ Byzantine behaviour to deflect traffic, and
- ✓ Misdirection using a wormhole.

VII. CONCLUSION

In this survey paper, one can see that attacks against the ad hoc networks may vary depend on (1) which environment the attacks are launched, (2) what communication layer the attacks are targeting, and (3) what level of ad hoc network mechanisms are targeted. One can also see that there are several attack characteristics that must be considered in designing any security measure for the ad hoc network. Due to nature of mobility and open media MANET are much more prone to all kind of security risks as covered. As a result, the security needs in the MANET are much higher than those in the traditional wired networks. We can design our new model of security which can handle these attacks. For security we authenticate all the nodes by using the Digital Certificate or Digital Signature. By providing authentication malicious node can't entered in the network.

REFERENCES

1. T. Karygiannis and L. Owens, "Wireless Network Security, 802.11, Bluetooth and Handheld Devices," NIST Publication, p. 800(48), November 2002.
2. S. A. Razak, S. M. Furnell, P. J. Brooke, Attacks against Mobile Ad Hoc Networks Routing Protocols"
3. Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication," International Journal of Computer Science and Security (IJCSS) Volume: 4 Issue: 3.
4. H. Deng, W. Li, Agrawal, D.P., "Routing security in wireless ad hoc networks", Cincinnati Univ., OH, USA; IEEE Communications Magazine, Oct. 2002, Volume: 40, page(s): 70- 75, ISSN: 0163-6804.
5. H.Deng, H.Li, and D.P.Ararwal, "Routing security in wireless Ad hoc networks", *IEEE Communication magazine*. Vol. 40, No.10. Oct.2002.
6. S. Murphy, "Routing Protocol Threat Analysis," Internet Draft, draft-murphy-threat-00.txt, October 2002.
7. Douceur, John: The Sybil Attack, 2002 http://www.cs.rice.edu/Conferences/IPTPS02/101.pdf
8. V. Gayraud and B. Tharon. Securing Wireless Ad Hoc Networks. ISS Master, MP 71 project, March 2003.
9. K. Sanzgiri, D. Laflamme, B. Dahill, B. Levine, C. Shields and E. Royer. An Authenticated Routing for Secure Ad Hoc Networks. Journal on Selected Areas in Communications special issue on Wireless Ad hoc Networks, March 2005.
10. Pradip M. Jawandhiya et. al. / International Journal of Engineering Science and Technology Vol. 2(9), 2010, 4063-4071
11. Charles P. Pfleeger, Shari Lawerence Pfleeger (2003), Security in Computing, Pearson Education , Singapore.
12.]Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3)
13. L. Zhou and Z. J. Haas. "Securing Ad Hoc Networks". IEEE Network Magazine, Volume. 13, no. 6, Pages 24-30, December 1999.
14. C. E. Perkins and E. M. Royer. "Ad Hoc On-Demand Distance Vector Routing". Proceedings of IEEE Workshop on Mobile Computing Systems and Applications, Pages 90-100, February 1999.

AUTHORS PROFILE

Sarvesh Tanwar is currently working as Asst. Professor, Department of Computer Science & Engineering in Faculty of Engineering & Technology (FET), Mody Institute of Technology & Science(Deemed University), Laxmangarh (Rajasthan). She did her M.Tech Degree from MMU, Mullana with Distinction and doing Ph.D from MITS, Laxmangarh. Her research area is Cryptography, Ad hoc network. She has 8 years teaching experience.

Dr. Prema K.V. is currently working as Professor & Head, Department of Computer Science & Engineering in Faculty of Engineering & Technology (FET), Mody Institute of Technology & Science(Deemed University), Laxmangarh (Rajasthan). Her research areas are Network Security, Computer Networks, Neural Networks and Pattern Recognition. She has around 20 years teaching experience and has published around 50 research papers in National/International Journals/Conferences. She is also on the editorial board of some journals.