www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 10, October 2024, pp : 150-156

e-ISSN : 2583-1062
Impact Factor : 5.725

A REVIEW OF VARIOUS ATTACKS IN MOBILE ADHOC NETWORK

Ajay Verma[1], Mr. Ankit Navgeet Joshi[2], Rishi Kushwah[3]

[1]Research Scholar, School of Engineering, SSSUTMS, Sehore (M.P.), India.

[2,3]Assistant Professor, School of Engineering, SSSUTMS, Sehore (M.P.), India.

ABSTRACT

Security is a requirement for mobile ad hoc networks (MANETs). Compared to mesh networks, MANETs are more vulnerable to security attacks due to the lack of centralized trust and limited resources. Even if the network operation is affected. In this article, we will describe all major attacks described in the literature in the same way to provide a comparative analysis of attack types. To the best of our knowledge, this is the first paper to examine all existing MANET attacks.

Keywords: MANET, Survey, Security attacks, Authentication, Integrity.

1. INTRODUCTION

In MANET, a group of mobile hosts with wireless network interfaces form a private network without the help of a fixed infrastructure or central control. MANETs are called infrastructure-less networks because mobile nodes in the network dynamically create paths between themselves to send packets periodically. In MANET, nodes within each other's wireless transmission can communicate directly; however, nodes outside each other must use some form of communication. All policies must cover the security process. This system is used to prevent, detect, and respond to security attacks. To ensure a reliable and secure private network environment, five security objectives must be addressed. They are mainly:

Confidentiality: Protection of any information from being exposed to unintended entities. In ad hoc networks this is more difficult to achieve because intermediates nodes receive the packets for other recipients, so they can easily eavesdrop the information being routed.

Availability: Services should be available whenever required. There should be an assurance of survivability despite a Denial of Service (DOS) attack. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services.

Authentication: Assurance that an entity of concern or the origin of a communication is what it claims to be or from. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

Integrity: Message being transmitted is never altered.

4 10, October 2024 October

Non-repudiation: Ensures that sending and receiving parties can never deny ever sending or receiving the message.

2. TYPE OF SECURITY ATTACKS

2.1. External vs. Internal attacks

External attacks The attacker's goal is to cause controversy, spread false information, or interfere with nodes providing services. Internal attack The attacker hopes to access the normal network and participate in network operation or enter the network through a malicious attack on the new node or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

The security attacks in MANET can be roughly classified into two major categories, namely passive attacks and active attacks are as described in the figure 1.The active attacks further divided according to the layers.

3. PASSIVE ATTACKS

A passive attack does not disrupt the normal operation of the network; the attacker snoops the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated. Detection of passive attack is very difficult since the operation of the network itself doesn't get affected. One of the solutions to the problem is to use powerful encryption mechanism to encrypt the data being transmitted, there by making it impossible for the attacker to get useful information from the data overhead.

3.1. Eavesdropping

Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. It aims to obtain some confidential information that should be kept secret during the communication. The information may include the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 10, October 2024, pp : 150-156

e-ISSN : 2583-1062
Impact Factor : 5.725

3.2. Traffic Analysis & Monitoring

Traffic analysis attack adversaries monitor packet transmission to infer important information such as a source, destination, and source-destination pair.

4. ACTIVE ATTACKS

An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks can be internal or external. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation, modification, fabrication and replication. As shown in figure 1, the active attacks

MAC LAYER ATTACKS

4.1.1 Jamming attack

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.

NETWORK LAYER ATTACKS

4.2.1 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. 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.

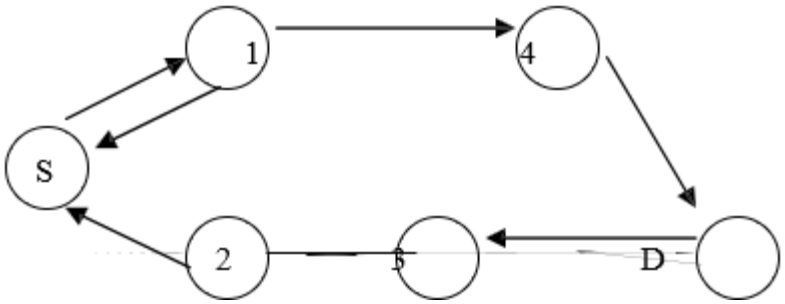


Figure 2: Wormhole attack

4.2.2 Blackhole attack

The blackhole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding. However, the attacker runs the risk that neighboring nodes will monitor and expose the ongoing attacks. There is a more subtle form of these attacks when an attacker selectively forwards packets. An attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected, which limits the suspicion of its wrongdoing.

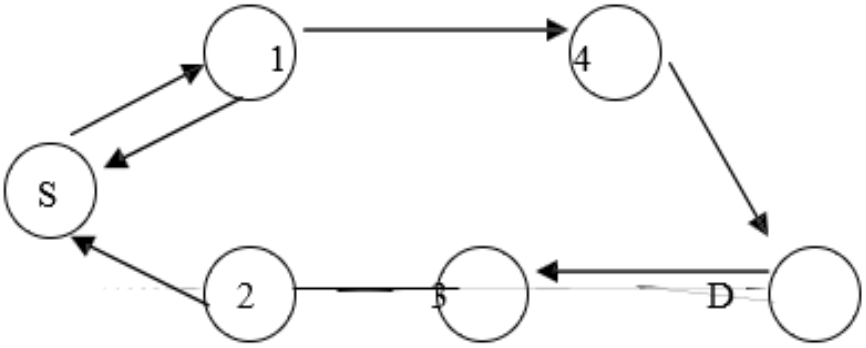


Figure 3: Blackhole attack

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 10, October 2024, pp : 150-156

e-ISSN : 2583-1062
Impact Factor : 5.725

4.2.3 Byzantine attack

A compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services.

4.2.4 Routing Attacks

There are several types of attacks mounted on the routing protocol which are aimed at disrupting the operation of the network. Various attacks on the routing protocol are described briefly below:

1) Routing Table Overflow: In this attack, the attacker attempts to create routes to nonexistent nodes. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. Proactive routing algorithms attempt to discover routing information even before it is needed, while a reactive algorithm creates a route only once it is needed. An attacker can simply send excessive route advertisements to the routers in a network. Reactive protocols, on the other hand, do not collect routing data in advance.

2) Routing Table Poisoning: Here, the compromised nodes in the networks send fictitious routing updates or modify genuine route update packets sent to other uncompromised 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.

3) Packet Replication: In this attack, an adversary node replicates stale packets. This consumes additional bandwidth and battery power resources available to the nodes and also causes unnecessary confusion in the routing process.

4) Route Cache Poisoning: In the case of on-demand routing protocols (such as the AODV protocol [11]), 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.

5) Rushing Attack: On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack. An adversary node which receives a Route Request packet from the source 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 adversary node and hence discard those packets. Any route discovered by the source node would contain the adversary node 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 adversary node. It is extremely difficult to detect such attacks in ad hoc wireless networks.

4.2.5 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.

4.2.6 IP Spoofing attack

In conflict-detection allocation, the new node chooses a random address (say y) and broadcast a conflict detection packet throughout the MANET. Any veto from a node will prevent it from using this address. If the malicious node always impersonates a member that has occupied the same IP address and keeps replying with vetoes, it is called an IP Spoofing attack as illustrated in below figure.

Figure 4: IP spoofing attack

In figure 4, N represents the new node, and M represents a malicious node. Node P is a neighbor of node M. Although node P may be aware that it has no direct neighbor with the address of y by means of a neighbor detection mechanism, it still thinks that the veto message is forwarded by node M from another node N'.

4.2.7 State Pollution attack

If a malicious node gives incorrect parameters in reply, it is called the state pollution attack. For example, in best effort allocation, a malicious allocator can always give the new node an occupied address, which leads to repeated broadcast of Duplication Address Detection messages throughout the MANET and the rejection of new node.

4.2.8 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. 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.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 10, October 2024, pp : 150-156

e-ISSN : 2583-1062
Impact Factor : 5.725

4.2.9 Fabrication

Instead of modifying or interrupting the existing routing packets in the networks, malicious nodes also could fabricate their own packets to cause chaos in the network operations. They could launch the message fabrication attacks by injecting huge packets into the networks such as in the sleep deprivation attacks. However, message fabrication attacks are not only launch by the malicious nodes. Such attacks also might come from the internal misbehaving nodes such as in the route salvaging attacks.

4.2.10 Modification

In a message modification attack, adversaries make some changes to the routing messages, and thus endanger the integrity of the packets in the networks. Since nodes in the ad hoc networks are free to move and self-organize, relationships among nodes at some times might include the malicious nodes. These malicious nodes might exploit the sporadic relationships in the network to participate in the packet forwarding process, and later launch the message modification attacks. Examples of attacks that can be classified under the message modification attacks are packet misrouting and impersonation attacks.

TRANSPORT LAYER ATTACKS

4.3.1 Session Hijacking attack

Session hijacking takes advantage of the fact that most communications are protected (by providing credentials) at session setup, but not thereafter. In the TCP session hijacking attack, the attacker spoofs the victim's IP address, determines the correct sequence number that is expected by the target, and then performs a DoS attack on the victim. Thus the attacker impersonates the victim node and continues the session with the target.

4.3.2 SYN Flooding attack

The SYN flooding attack is a denial-of-service attack. The attacker creates a large number of half-opened TCP connections with a victim node, but never completes the handshake to fully open the connection.

APPLICATION LAYER ATTACKS

4.4.1 Repudiation attack

In the network layer, firewalls can be installed to keep packets in or keep packets out. In the transport layer, entire connections can be encrypted, end-to-end. But these solutions do not solve the authentication or non-repudiation problems in general. Repudiation refers to a denial of participation in all or part of the communications. For example, a selfish person could deny conducting an operation on a credit card purchase, or deny any on-line bank transaction, which is the prototypical repudiation attack on a commercial system

OTHER ATTACKS

4.5.1 Denial of Service attack

Denial of service (DoS) is another type of attack, where the attacker injects a large amount of junk packets into the network. These packets overspend a significant portion of network resources, and introduce wireless channel contention and network contention in the MANET. A routing table overflow attack and sleep deprivation attack are two other types of the DoS attacks. In the routing table overflow attack, an attacker attempts to create routes to non- existent nodes. Meanwhile the sleep deprivation attack aims to consume the batteries of a victim node. For example, consider the following Fig. 3. Assume a shortest path exists from **S** to **X** and **C** and **X** cannot hear each other, that nodes **B** and **C** cannot hear each other, and that **M** is a malicious node attempting a denial of service attack. Suppose **S** wishes to communicate with **X** and that **S** has an unexpired route to **X** in its route cache. **S** transmits a data packet toward **X** with the source route **S --> A --> B --> M --> C --> D --> X** contained in the packet's header. When **M** receives the packet, it can alter the source route in the packet's header, such as deleting **D** from the source route. Consequently, when **C** receives the altered packet, it attempts to forward the packet to **X**. Since **X** cannot hear **C**, the transmission is unsuccessful.

S ↔A↔ B↔ M ↔C↔ D↔ X

Figure 5: Denial of Service attack

4.5.2 Location disclosure attack

An attacker reveals information regarding the location of nodes or the structure of the network. It gathers the node location information, such as a route map, and then plans further attack scenarios. Traffic analysis, one of the subtlest security attacks against MANET, is unsolved. Adversaries try to figure out the identities of communication parties and analyze traffic to learn the network traffic pattern and track changes in the traffic pattern. The leakage of such information is devastating in security sensitive scenarios.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 10, October 2024, pp : 150-156

e-ISSN : 2583-1062
Impact Factor : 5.725

4.5.3 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.

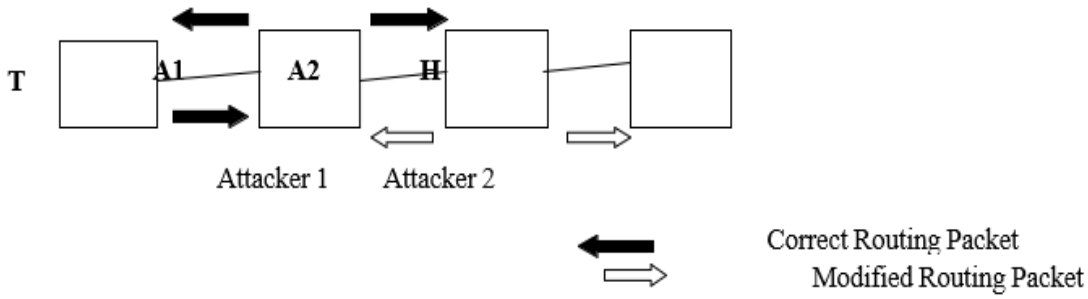
4.5.4 Impersonation or Spoofing attack

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.

4.5.5 Colluding misrelay attack

In colluding misrelay attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET. This attack is difficult to detect by using the conventional methods such as watchdog and pathrater. Figure 4 shows an example of this attack. Consider the case where node A1 forwards routing packets for node T. In the figure, the first attacker A1 forwards routing packets as usual to avoid being detected by node T. However, the second attacker A2 drops or modifies these routing packets. In [8] the authors

discuss this type of attack in OLSR protocol and show that a pair of malicious nodes can disrupt up to 100 percent of data packets in the OLSR MANET.



4.5.6 Device tampering attack

Unlike nodes in a wired network, nodes in ad hoc wireless networks are usually compact, soft, and hand-held in nature. They could get damaged or stolen easily. In the process of route discovery, control messages created by a node must be signed and validated by a receiving node.

Thus the route discovery prevents anti-authenticating attacks, such as creating routing loop, fabrication because no node can create and sign a packet in the name of a spoofed or invented node. In the absence of centralized administration it is easy for MN's to change their identities.

4.5.7 Gray hole attack

We now describe the gray hole attack on MANETS. The gray hole attack has two phases. In the first phase, a 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. 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.

4.5.8 Link spoofing attack

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.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 10, October 2024, pp : 150-156

e-ISSN : 2583-1062
Impact Factor : 5.725

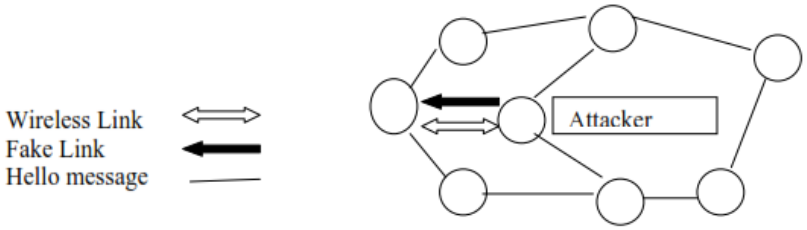


Figure 7: Link spoofing attack

4.5.9 Neighbor attack

Upon receiving a packet, an intermediate node records its ID in the packet before forwarding the packet to the next node. However, if an attacker simply forwards the packet without recording its ID in the packet, it makes two nodes that are not within the communication range of each other believe that they are neighbors (i. e. one-hop away from each other), resulting in a disrupted route.

4.5.10 Jellyfish attack

Similar to the blackhole attack, a jellyfish attacker first needs to intrude into the forwarding group and then it delay data packets unnecessarily for some amount of time before forwarding them. This result in significantly high end-to- end delay and delay jitter, and thus degrades the performance of real time applications.

4.5.11 Packet dropping attacks

Direct interruption to the routing messages could be done by using the packet dropping attacks. In a standard packet dropping attack, an adversary collaborates as usual in the route discovery process and launches the constant packet dropping attacks if it is included as one of the intermediate nodes. In addition, instead of constantly dropping all the packets, adversaries might vary their techniques using random, selective, or periodic packet dropping attacks to help their interrupting behavior remain concealed.

4.5.12 Sleep deprivation torture

These kinds of attacks are most specific to wireless ad hoc networks, but may be encountered in conventional or wired networks as well. The idea behind this attack is to request the services a certain node offers, over and over again, so it can not go into an idle or power preserving state, thus depriving it of its sleep (hence the name). This can be very devastating to networks with nodes that have limited resources, for example battery power. It can also lead to constant business of the component, hindering other nodes to (legitimately) request services, data or information from the targeted entity.

5. CONCLUSION

In this review paper, we try to inspect the security threats in the mobile adhoc networks, which may be a main disturbance to the operation of it. 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.

During the survey, we also find some points that can be further explored in the future, such as to find some effective security solutions and protect the MANET from all kinds of security risks. We will try to explore deeper in this research area.

6. REFERENCES

[1] 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.

[2] Sukla Banerjee , “Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks”, Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[3] 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.) pp, @ 2006 Springer.

[4] Nishu Garg and R.P.Mahapatra, “MANET Security Issues ,” IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[5] N.Shanthi, Dr.Lganesan and Dr.K.Ramar , “Study of Different Attacks on Multicast Mobile Ad hoc Network,” Journal of Theoretical and Applied Information Technology.

[6] V. Madhu Viswanatham and A.A. Chari, "An Approach for Detecting Attacks in Mobile Adhoc Networks Journal of Computer Science 4 (3): 245-251, 2008 ISSN 1549-3636 © 2008 Science Publications.

[7] Hoang Lan and Uyen Trang Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad hoc Networks", Proceedings of ICNICONSMCL'06, 0-7695-2552-0/06@ 2006 IEEE.

[8] S. Murphy, "Routing Protocol Threat Analysis," Internet Draft, draft-murphy-threat-00.txt, Octomber 2002.

[9] P. Papadimitratos and Z.J.Haas, "Securing the Routing Infrastructure", IEEE Communications, vol. 10, no. 40. Octomber 2002, pp. 60-68.

[10] J. Lundberg, "Routing Security in Ad-hoc NEtworks ," http://citeseer.nec.com/400961.html..

[11] Y.C. Hu, A. Perrig, and D.B.Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad hoc Network," Proc. 22nd Annual Joint Conf. IEEE Computer and Communication Societies San Francisco, CA, April 2003.

[12] Amitabh Misgra and Ketan M. Nadkarni, "Security in Wireless Ad hoc Networks", in Book The Handbook of Ad hoc Wireless Networks(Chpter 30),CRC Press LLC, 2003.

[13] J.R.Douceur, "The Sybil Attack," in Proc. of 1st International Workshop on Peer-to-Peer Systems, Pages 251-260, March 2002, LNCS 2429.

[14] I. Aad and J.P. Hubaux, E.W. Knightly, "Denial of Service Resilience in Ad hoc Networks", Proceedings of ACM MobiCom 2004, Philadelphia, PA, Sep. 2004, pp. 202-215.

[15] Sonja Buchegger and Jean-Yves Le Boudec, "Cooperative Routing in Mobile Ad hoc Networks: Current Efforts Against Malice and Selfishness",In Lecture Notes on Informatics, Mobile Internet Workshop, Germany, Octomber 2002.Springer.

[16] Ping Yi, Yue Wu and Futai Zou and Ning Liu, "A Survey on Security in Wireless Mesh Networks", Proceedings of IETE Technical Review, Vol. 27, Issue 1, Jan-Feb 2010.

[17] P. Yi, Y.P. Zhong, S.Y. Zhang, and Z.L.Dai, "Flodding Attack and Defence in Ad hoc NEtwork", J Syst Engineer Electro, Vol. 17 , no. 2, pp. 410-6, 2006..

[18] F. Nait-Abdesselam, B. Bensaou, and T. Taleb."Detecting and Avoinding Wormhole Attack in Wireless Ad hoc Networks", IEEE Communicat Magaz, Vol 46, no. 4, pp.127-33, Apr. 2003.

[19] Lidong Zhou, Zygmunt J. Haas:," Securing Ad hoc Networks",IEEE Network Magzine, 13, 6, Pages 24-30, 1999.