ISSN:0975-9646

A Literature Survey on Challenges and Issues on Mobile Ad Hoc Networks

Rajneesh Singla
Assistant professor, UIET,
Punjab University, Chandigarh

Abstract- This paper tells about the security issues and their current solutions in the mobile ad hoc network. There are numerous security threats that disturb the development of vulnerable nature of the mobile ad hoc network. Firstly, we analyze the main vulnerabilities in the mobile ad hoc networks, which have made it much easier to suffer from attacks than the traditional wired network. After this we discussed the security criteria of the mobile ad hoc network and present the main attack types that exist in it. Finally we survey the current security solutions for the mobile ad hoc network.

Key Words: Mobile Ad Hoc Network, Security, Attacks, Challenges

1. INTRODUCTION

With recent performance advancements in computer and wireless communications technologies, advanced mobile wireless computing is expected to see increasingly widespread use and application, much of which will involve the use of the Internet Protocol (IP) suite. The vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Such networks are envisioned to have dynamic, sometimes rapidly-changing, random, multihop topologies which are likely composed of relatively bandwidth constrained wireless links.

A Mobile Ad hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically Self-organize in arbitrary and temporary network topologies. People and vehicles can thus be Internetworked in areas without a pre-existing communication infrastructure or when the use of such infrastructure requires wireless extension [3]. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network. The mobile ad hoc network has the following typical features:

- Unreliability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.
- Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes.
- Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol. Because of the features listed above, the mobile ad hoc networks are more prone to suffer from the malicious behaviours than the traditional wired networks. Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks.

2. CHALLENGES IN MOBILE AD HOC NETWORKS

The technology of Mobile Ad hoc Networking is somewhat synonymous with Mobile Packet Radio Networking (a term coined via during early military research in the 70's and 80's), Mobile Mesh Networking (a term that appeared in an article in The Economist regarding the structure of future military networks) and Mobile, Multihop, Wireless Networking (perhaps the most accurate term, although a bit cumbersome). There is current and future need for dynamic ad hoc networking technology. The emerging field of mobile and nomadic computing, with its current emphasis on mobile IP operation, should gradually broaden and require highly-adaptive mobile networking technology to effectively manage multihop, ad hoc network clusters which can operate autonomously or, more than likely, be attached at some point(s) to the fixed Internet. MANET can be established extremely flexibly without any fixed base station in battlefields, military applications, and other emergency and disaster situation.

3. SECURITY SOLUTIONS TO THE MOBILE AD HOC NETWORKS

A. Security

The aims of Ad hoc networks and particularly MANET have in recent years not only seen widespread use in commercial and domestic application areas but have also become the focus of intensive research. Applications of MANET's range from simple wireless home and office networking to sensor networks and similarly constrained tactical network environments. Security aspects play an important role in almost all of these application scenarios given the vulnerabilities inherent in wireless ad hoc networking from the very fact that radio communication

takes place (e.g. in tactical applications) to routing, man-in-the-middle and elaborate data injection attacks.

B. Protecting Mobile Ad-Hoc Network

An ad hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad-hoc network. In ad hoc networks, nodes do not start out familiar with the topology of their networks; instead, they have to discover it. The basic idea is that a new node may announce its presence and should listen for announcements broadcast by its neighbours. Each node learns about nodes nearby and how to reach them, and may announce that it, too, can reach them. Note that in a wider sense, ad-hoc protocol can also be used literally, that is, to mean an improvised and often impromptu protocol established for a specific purpose.

C. Reactive Approach

Seeks to detect security threats and react accordingly. This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. The main disadvantages of such algorithms are:

1. Respective amount of data for maintenance.
2. Slow reaction on restructuring and failures.

There are two main things in re-active routing protocols first is that it never take initiative in order to take routes for network, second is that whenever it creates routes it will developed on demand by flooding mechanism. In such kind of routing protocols there are some advantages and disadvantages which are given below:

- Whenever they need to find out the routes they use bandwidth otherwise it will not use bandwidth.
- There is lot of overhead because of the flooding process.
- At start there is delay in the network.

There are three steps which will explain the complete procedure of the re-active routing protocols.

1. If there are two nodes at position A and position B which want to communicate.
2. In order to communicate with the B, A needs to flood the routes towards the B.
3. In order to create communication between A and B unicast feedback will come back.

4. NETWORK LAYER OPERATION

There are two main network-layer operations in MANET.

1. Ad hoc routing
2. Data packet forwarding

They interact with each other and delivering packets from source to destination. The main function of the ad hoc routing protocols is to provide routing among nodes; they exchange routing messages between different mobile nodes in order to maintain routing information at each node. According to the routing states, the second network layer operation data packets are used to forward data by intermediate next node which is an established route to the destination node. These both operations are vulnerable to malicious attacks, and which will lead to various types of malfunction in network layer.

5. ATTACKS

There are two mainly protocols are used in MANET networks, Link layer protocol are used to provide connectivity between different mobile nodes in order to ensure one-hop connectivity by using multihop wireless channels. On the other hand if we like to extend connectivity to different multiple hops then MANET network uses network layer protocols. In the coordination process distributed protocols typically assume that all mobile nodes are cooperating with respect to communication but actually this assumption is not possible in hostile mobile networks environment because cooperation is not enforced in MANET. The question arises why? The reason is because of malicious attackers violating protocol specification in order to disrupt network operations.

5.1. Network Layer Attack

Due to this reason network-layer generally fall into two categories attacks:

1. Routing attacks
2. Packet forwarding attacks (based on the target operation of the attacks)

There are different categories of routing attacks that does not follow routing protocol specification. There are different routing protocols in MANET so therefore different attack behaviours related to different routing protocols. Some of them are discuss below:

1. According to the context of DSR [1] MANET routing protocol there are following different attacks which are given below

- An attacker modifies source routing list with respect to RREQ or RREP packets.
- Switching order of different nodes in the routing list.
- Deleting entries from the list.
- Appending new node entries into the list.

2. According to the context of AODV [2] MANET routing protocol there are also different attacks which are given below

- An attacker advertise route with wrong distance metric with respect to actual distance to the destination.
- Advertise wrong routing updates with a large sequence number with respect to actual sequence number.
- An attacker invalidates all routing updates from other nodes.

3. According to the context of TORA routing protocol, there are also different attacking methods:

- Attackers construct routing paths by interfering with the protocols' mechanisms, e.g. routes can be forced to use attacking nodes to go through them.
- Attackers can also exhaust network resources by maliciously act of injecting, modifying and dropping data packets.

In order to divert traffic attackers attack on the routing protocols and divert traffic towards certain destinations under their control, and then they cause problematic situation in the network along a route which is not optimal or even nonexistent. The attackers can also create routing loops in the network, due to this way it creates network congestion in certain areas. There are also some other attacks like multiple colluding attacks which may cause to prevent source in order not to find route to the destination and also partition the network in the worst.

5.2. Active Attacks

There are also some different active attacks which are really difficult to locate or identify because these attacks are more sophisticated and they are considered as subtle routing attacks some of them are given below

- Attacker may further subvert existing nodes in the network.
- They can also fabricate their identity
- They can also impersonate other legitimate node
- Attackers in pair nodes may create a wormhole
- They also creates shortcut in normal flows between each other
- The attackers target the route maintenance process and advertise operational link is broken

According to context of routing attacks there are also some other kind of attacks like attacker launch attacks against packet forwarding operations as well due to this way it will not only disrupt the routing protocol it also poison the routing states at every node. For example, the attacker established route and drop packets, or also modify the content of the packets, or duplicate the packets. Another type of packet forwarding attack is denial-of-service (DoS) attack through network-layer packet blasting, in this type of attack attacker inserts large amount of junk packets in network. Due to this action significant portion of the network resources are wasted, and introduce severe wireless channel contention and network congestion in the network.

There are identified vulnerabilities of the link-layer protocols, especially in the IEEE standard 802.11 MAC protocols [3], for mobile ad hoc network. It's true that 802.11 WEP is vulnerable to different types of cryptography attacks by misusing the cryptographic primitives [10]. The IEEE 802.11 protocol is vulnerable to many DoS attacks due to this way it targeting reservation schemes and channel contention. The attacker exploits binary exponential back off scheme in order to deny access to the wireless channel from its local neighbours [11, 17].

5.3. Routing Attacks

Generally there are four different types of MANET routing protocol attacks which is divided in to two main types which are given below:

1. Routing disruption attacks
2. Resource consumption attacks

In case of routing disruption attacks, the main task of attacker is to disrupt routing process by routing packets in order to introduce wrong paths. In case of resource consumption attacks are concerned the main task of the attacker is to introduce some non-cooperative or selfish nodes that can be used to inject false packets due to this way load on the network increases and it will become a cause of consuming network bandwidth. Mainly both of these attacks in MANET routing protocols are the best examples of Denial of Service (DoS) attacks. In Figure 1 there is a broader classification attacks in MANET routing protocols which are given below.

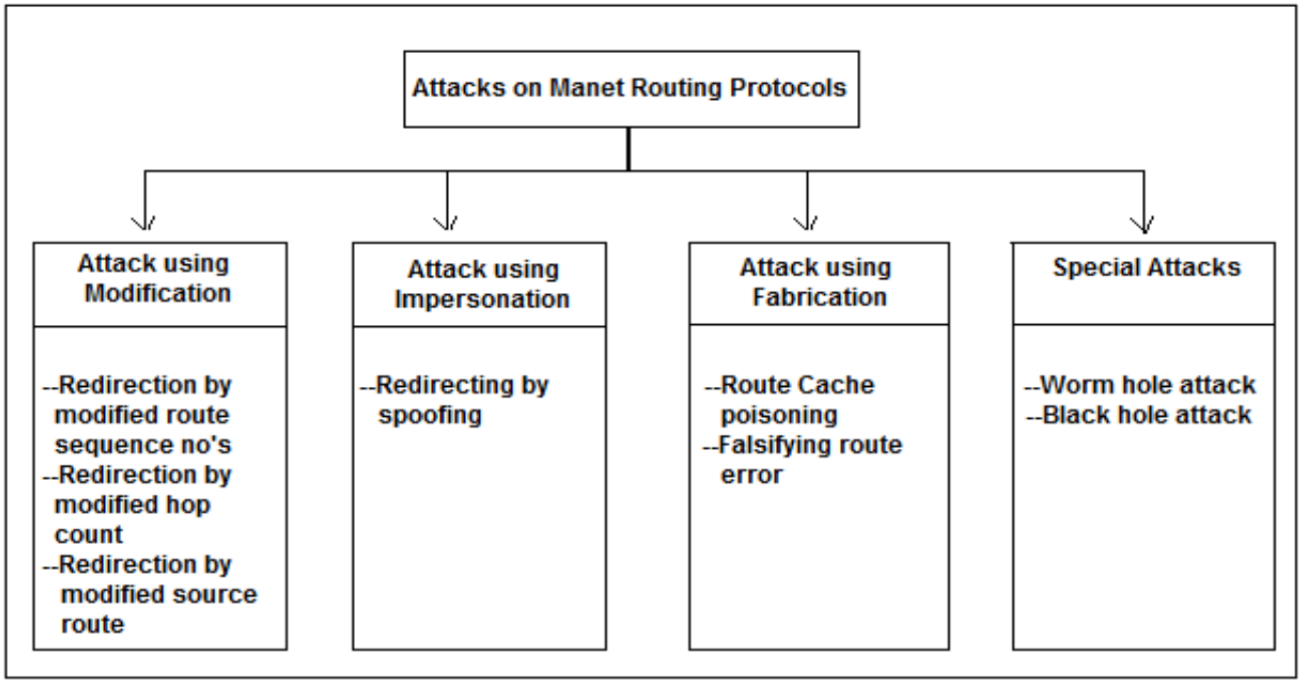

Figure 1. Broader classification attacks in MANET routing protocols

5.4. Attacks Using Modification

In case of modification type of attacks some of the messages in the protocol fields are modified and then these messages passed among the nodes, due to this way it become the cause of traffic subversion, as well as traffic redirection and also act as a Denial of Service (DoS) attacks.

5.5. Route Sequence Numbers Modification

In this type of attack which is mainly possible against the AODV protocol. In this case an attacker (i.e. malicious node) used to modify the sequence number in the route request packets.

5.6. Hop Count Modification Attack

In this type of attacks where it is also mainly possible against the routing protocol AODV, here attacker mostly change hope count value and due to this way it will become the cause of attract traffic. They are mainly used to include new routes in order to reset the value of hop count field to a lower value of a RREQ packet or sometime even it is used to set to zero.

5.7. Source Route Modification Attack

In this type of attack which is possible against DSR routing protocol where attacker (malicious node) modify source address and move traffic towards its own destination. In Figure 3.4 the mechanism is defined, where the shortest path between source S and destination X is defined (S-A-B-C-D-X). Which shows that node S and the node X cannot communicate each other directly, and in the scenario (3.4) where the node M which act as a malicious node which are going to attempt a denial-of service attack. Let suppose that the node S which act as a source try to send a data packet towards the node X but if the node M intercept the packet and remove the node D from the list and the packet forward towards node C, where the node C will try to send the picket towards the distention X which is not possible because the node C can't communicate with X directly, Due to this way the M node has successfully established a DoS attack on X.

5.8. Attacks Using Impersonation

In this type of attacks where attacker is used to violates authenticity and confidentiality of a network. In this attack an attacker (i.e. malicious node) uses to impersonate the address of other user node in order to change the network topology. This type of attack can be described in the Figure 2 given below:

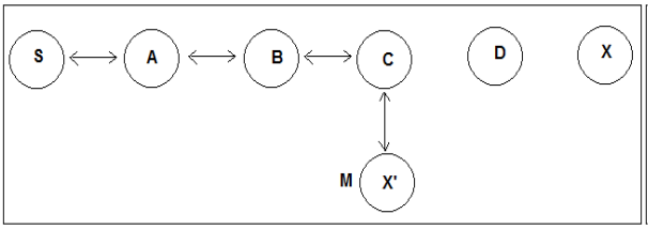

Figure 2. Type of Impersonation attack

In the above figure where the S node wants to send data towards the node X and before sending data to node X it starts a Route Discovery process. During route discovery process there is a malicious node M, when it receive route discovery packet regarding the node X then it modify its address and change to node X, like impersonates node X as X'. After that it send packet back to source node S that I am the destination node by RREP packet request. When the source node receives RREP packet information it doesn't authenticate node and accept the route and send data to the malicious node. This type of attacks also called routing loop attack which will become the cause of loops within the network.

5.9. Attacks Using Fabrication

In this type of attacks, where an attacker as a malicious node try to inject wrong messages or fake routing packets in order to disrupt the routing process. The fabrication attacks are very much difficult to detect in the mobile ad hoc network. Attacks using fabrication process are discussed very well in [20] and [21]. In Figure 3. where fabrication attacks is explained by an example. In the example where the source node S wants to send data towards the destination node X, so therefore at start it sends broadcast message and request for route towards the destination node X. An attacker as a malicious node M try to pretends and modify route and returns route reply to the node (S). Furthermore, an attacker's nodes use to fabricate RERR requests and advertise a link break nodes in a mobile ad hoc network by using AODV or DSR routing protocols.

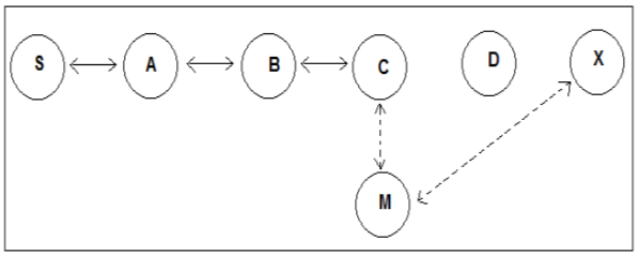

Figure.3. Fabrication attack example

5.10. Special Attacks

There are also some other severe attacks in MANET network which are possible against routing protocols such as AODV and DSR.

5.11. Wormhole Attack

The wormhole attack [15] is one of the severe types of attack in which an attacker introduces two malicious nodes in the network where an attacker used to forward packets through a private "tunnel". This complete scenario described in Figure 3.7 which is given below:

5.12. Black Hole Attack

This kind of attack is described very well in detail in [21]. In this type of attack, node is used to advertise a zero metric to all destinations, which become cause to all nodes around it in order to route data packets towards it. The AODV protocol is vulnerable to such kind of attack because of having network centric property, where each

node of the network has to shares their routing tables among each other.

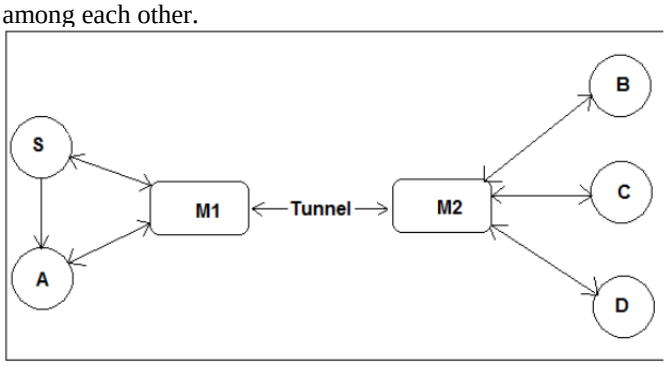

Figure 4. Wormhole attack example

In the above example where there are two malicious nodes M1 and M2 which link through a private connection. In this type of attack every packet which an attacker receive from network 1 forward to other network where another malicious node exist, simple speaking these two nodes use to exchange network information and fabricate traffic among each other. The traffic between the two nodes passes through "wormhole" among each other. Due to this way it will become the cause of disrupts routing protocols and violating normal flow of routing packets. These types of attacks are very difficult to detect in a network, and become the cause of severe damages to the nodes. These types of attacks can be prevented by using mechanism packet leashes [15], which are used to authenticate nodes among each other by timing information process

6. SECURITY CONSIDERATIONS

Mobile wireless networks are generally more prone to physical security threats than are fixed, hardwired networks. Existing link-level security techniques (e.g. encryption) are often applied within wireless networks to reduce these threats. Absent link-level encryption, at the network layer, the most pressing issue is one of interrouter authentication prior to the exchange of network control information. Several levels of authentication ranging from no security (always an option) and simple shared-key approaches, to full public key infrastructure based authentication mechanisms will be explored by the group. As an adjunct to the working groups efforts, several optional authentication modes may be standardized for use in MANETs.

Security Requirements of Ad-Hoc Network Security Requirements of Ad-Hoc Network are:

- Route signaling can't be spoofed
- Fabricated routing messages can't be injected into the network
- Routing messages can't be altered in transit
- Routing loops can't be formed by through malicious action
- Routes can't be redirected from the shortest path by malicious action
- Unauthorized nodes should be excluded from route computation and discovery.

7. CONCLUSION

Importance of MANET cannot be denied as the world of computing is getting portable and compact. Unlike wired networks, MANET pose a number of challenges to security solutions due to their unpredictable topology, wireless shared medium, heterogeneous resources and stringent resource constraints etc. Security is not a single layer issue but a multilayered issue. It requires a multi fence security solution that provides complete security spanning over the entire protocol stack. The Study of this important issue reveals that security is divided into different directions of the work like secure routing, key exchange, distribution and management, secure architecture, intrusion detection and protection etc. The Security research area is still open as many of the provided solutions are designed keeping a limited size scenario and limited kind of attacks and vulnerabilities. As in wired network role definition has been very crucial in security, keeping the same idea in mind we can apply the role based security in MANETs. Community based solution can be used in role specification. Under these scenario policy distribution techniques, grouping policy, membership management are the major areas to work on.

Agent oriented solutions are very useful in many areas. Similarly MANETs security can also be exploited due to its distributed nature.

Ad Hoc networks pose an interesting problem in networking with dynamic routing and highly insecure working environment Need of Secure, Scalable, Reliable and Efficient algorithms for Key management and Routing.

Passive attacks: Necessary and sufficient condition is cooperation between nodes; The network performance severely degrade when a large percentage of node do not cooperate in p.f. function; Then: need to enforce collaboration between nodes.

Active attacks: Routing protocols do not care of security aspect;

Then: Need of securing routing protocol; Need of authentication mechanism to prevent spoofing attack; Need of integrity of routing messages

REFERENCE

[1]. D. Johnson and D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," *Mobile Computing*, T. Imielinski and H. Korth, Ed., Kluwer, 1996.

[2]. C. Perkins and E Royer, "Ad Hoc On-Demand Distance Vector Routing," *2nd IEEE Wksp. Mobile Comp. Sys. and Apps.*, 1999.

[3]. IEEE Std. 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 1997.

[4]. B. Schneier, *Secret and Lies, Digital Security in a Networked World*, Wiley, 2000.

[5]. Shuyao Yu, Youkun Zhang, Chuck Song, and Kai Chen. A security architecture for Mobile Ad Hoc Networks.

[6]. Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks," *ACM MOBICOM*, 2002.

[7]. M. Zapata, and N. Asokan, "Securing Ad Hoc Routing Protocols," *ACM WiSe*, 2002.

[8]. B. Dahill *et al.*, "A Secure Protocol for Ad Hoc Networks," *IEEE ICNP*, 2002.

[9]. Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," *IEEE INFOCOM*, 2002.

[10]. N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," *ACM MOBICOM*, 2001.

[11]. V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks," *IEEE MILCOM*, 2002.
[12] P. Kyasanur, and N.Vaidya, "Detection and Handling of MAC Layer Misbehavior in Wireless Networks," *DCC*, 2003.
[13]. Kimaya Sanzgiri, Bridget Dahill, Brian N. Levine, and Elizabeth M. Belding-Royer. *"A Secure Routing Protocol for Ad Hoc Networks"*. Proceedings of 10th IEEE International Conference on Network Protocols (ICNP'02), Paris, France, November 2002, pp. 78-90.
[14]. Yi-an Huang and Wenke Lee. *"Attack analysis and Detection for Ad-hoc Routing protocols"*. Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), French Riviera, France. September 2004.
[15]. Y. Hu, A. Perrig, D. Johnson. "*Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks"*. Proceedings of The 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), March 2003.
[16]. M. Alicherry and A.D. Keromytis, "Securing MANET Multicast Using DIPLOMA", in Proc. IWSEC, 2010, pp.232-250.
[17]. Panagiotis, Papadimitratos; Zygmunt, J. Haas;,"Secure Routing for Mobile Ad hoc Networks," SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.63
[18]. Zhang, Chenxi; Lin, Xiaodong; Ho, Pin-Han; Sun, Xiaoting; Zhan, Xin; , "PPBR: Privacy-Aware Position-Based Routing in Mobile Ad Hoc Networks," MilitaryCommunications Conference, 2007. MILCOM 2007. IEEE , vol., no., pp.1-7, 29-31 Oct.2007 doi: 10.1109/MILCOM.2007.4454856
[19]. Biswas, J.; Nandy, S.K.; , "Efficient Key Management and Distribution for MANET," Communications, 2006. ICC '06. IEEE International Conference on , vol.5, no., pp.2256- 2261, June 2006 doi: 10.1109/ICC.2006.255106
[20]. Karygiannis, A.; Antonakakis, E.; Apostolopoulos, A.; , "Detecting critical nodes for MANET intrusion detection systems," Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2006. SecPerU 2006. Second International Workshop on , vol., no., pp.9 pp.-15, 29-29 June 2006 doi: 10.1109/SECPERU.2006.
[21]. IACSIT International Journal of Engineering and Technology, Vol.2, No.2, April 2010 ISSN: 1793-8236 "Performance analysis of AODV, DSR & TORA Routing Protocols" Anuj K. Gupta, Member, IACSIT, Dr. Harsh Sadawarti, Dr. Anil K. Verma
[22].Bharat Bhargava), Michael Zoltowski and Pascal Meunier "Trusted Routing and Intruder Identification in Mobile Ad Hoc Networks" Research Proposal for CERIAS 2002 Purdue University, West Lafayette, IN 47907, USA
[23]. Hao Hao Yang, Haiyun Luo et.al. "Security in Mobile Ad Hoc Networks: Chanllenges and Solutions." Computer Science Department.
[24]. Hongmei Deng, Wei Li, and Dharma P. Agrawal. "*Routing Security in Wireless Ad Hoc Network*,". IEEE Communications Magazine, vol. 40, no. 10, October 2002.