ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 201 – 206 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

Security challenges of Routing protocols in MANETS: An Overview

K. Kalpana
Assoc.professor
Malla Reddy Institute of Engineering and Technology
Dhoolapally, Secunderabad, Andhra Pradesh.

Sampath Pallavi
MRIET
Dhoolapally, secundrabad
Andhra Pradesh

Vijaya Durga
MRIET
Dhoolapally, secundrabad
Andhra pradesh

***Abstract*—**Mobile Adhoc network(MANETS) are a set of mobile nodes that form temporary network without aid of any existing network infrastructure or central access point. The nodes communicate with each other by interchange of packets ,which for those nodes not in wireless range goes hop by hop. So lack of defined central authority the routing process becomes a challenging task there by leaving MANETS vulnerable to attacks which results in performance degradation as well as issues related to reliability of such networks. In this paper we are giving an overview of several routing protocols and some of the common routing attacks and their counter measures.

Keywords—MANETS,routingprotocols,routing attacks,counter measures.

1. INTRODUCTION

Mobile Adhoc Network(MANET)[1] is a set of mobile devices which are self configurating and communicate with each other over a shared wireless medium with out the presence of a predefined infrastructure or central authority. The member nodes are themselves responsible for the creation ,operation and maintenance of the network. Each node in the MANET is equipped with a wireless transmitter and receiver with the aid of which it communicates with the other nodes in its wireless vicinity. The nodes which are in its wireless vicinity communicate with each other hop by hop following a set of rules (routing protocol)for hopping sequence to be followed.

MANETS show distinct characteristics which are as follows.

Cooperation:

If the source node and destination node are out of range with each other then the communication between them takes place with the cooperation of other nodes such that a valid and optimum chain of mutually connected nodes is formed .This is known as multi hop communication. Hence each node acts a s a host as well as a router.

Dynamic Topology:

The nodes of the MANET are randomly, frequently and unpredictably move with in the network[2].These nodes may leave or join the network at any point of time, there by significantly affecting the status of trust among nodes and the complexity of routing.

Lack of infrastructure:

The absence of a fixed or central infrastructure is a key feature of MANETs. This eliminates the possibility to establish a centralized authority to control the network characteristics. Due to this absence of authority, traditional approaches of network management and security are scarcely applicable to MANETs.

Resource constraints:

MANETs are a set of mobile devices which are of low or limited power capacity, computational capacity, memory ,bandwidth etc. In order to achieve a secure and reliable communication between nodes ,these resource constraints make the task more enduring.

2. APPLICATIONS OF MANETS

With the increase of portable devices as well as progress in wireless communication , adhoc networking is gaining importance with the increasing number of wide spread applications. Adhoc networking can be applied where there is little or no communication infrastructure .Some of the applications include

- Miltary battle field
- Sensor networks
- Natural disasters
- Commercial sector
- Medical services
- Personal area networks

3.ROUTING IN MANETS

Ad hoc network's dynamic topology with no centralized administration makes it highly vulnerable for its security-breach, particularly secure routing in ad hoc networks has been a challenging task for researchers. Currently researchers are proposing a variety of secure routing protocols to meet their specified security requirements. In these proposals, different secure protocols fulfill different security requirements and counter against certain attack patterns. Researchers evaluate these protocols in context to how

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 201 – 206 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

resistant these are, to security attacks and performance appraisal is done through simulation. Based on route discovery time ,MANET routing protocols fall into three general categories.

a)Proactive routing protocols

b)Reactive routing protocols

c)Hybrid routing protocols

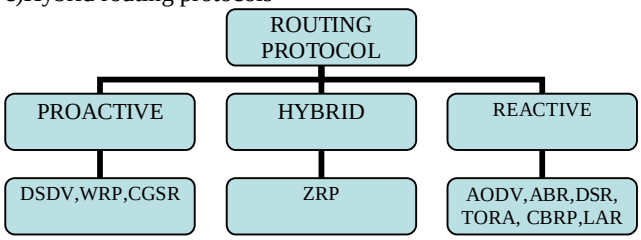

Fig:1 classification of routing protocols

3.1 Proactive routing protocols:

Proactive MANET protocols are table driven and will actively determine the layout of the network. The complete picture of the network is maintained at every node, so the route selection time is minimal. But if the mobility of the nodes is high then routing information in routing table invalidates very quickly, resulting in many short lived routes. This also causes a large amount of traffic overhead generated when evaluating these unnecessary routes. For large size networks and the networks whose member nodes make sparse transmissions, most of the routing information is deemed redundant. Energy conservation being very important in MANETs, the excessive expenditure of energy is not desired.

Thus proactive MANET protocols work best in networks that have low node mobility or where the nodes transmit data frequently. Examples of proactive MANET protocols include Optimized Link State Routing (OLSR)[3]

Topology Broadcast based on Reverse Path Forwarding (TBRPF)[4], Fish-eye State Routing (FSR)[5], Destination-Sequenced Distance Vector (DSDV)[6],Clustered Gateway Switch Routing Protocol(CGSR)[7], Landmark Routing protocol(LANMAR)[8].

3.2 Reactive routing protocols:

Reactive MANET protocols only find a route to the destination node when there is a need to send data. The source node will start by transmitting route requests through out the network. The sender will then wait for destination node or an intermediate nodes between the source and destination. This is known as the global flood search, which in turn brings about a significant delay before the packet can be transmitted. It also requires the transmission of a significant amount of control traffic. Thus reactive protocols are most suited for networks with high node mobility or where the nodes transmit data infrequently. Examples of reactive protocols for MANETS are Ad Hoc On-Demand Distance Vector (AODV)[9], Dynamic Source Routing(DSR)[10],Temporally Ordered Routing Algorithm (TORA)[11], Dynamic MANET on Demand(DYMO)[12].

3.3 Hybrid Routing Protocols:

Since proactive and reactive routing protocols each work best in oppositely different scenarios, There is a good reason to develop hybrid routing protocols, which use a mix of both proactive and reactive routing protocols. These hybrid protocols can be used to find a balance between the proactive and reactive protocols.

The basic idea behind hybrid routing protocols is to use proactive routing mechanisms in some areas of the network at certain times and reactive routing for the rest of the network. The proactive operations are restricted to a small domain in order to reduce the control overheads and delays. The reactive routing protocols are used for locating nodes outside this domain as this is more bandwidth efficient in a constantly changing network. Examples of hybrid routing protocols include Core extraction Distributed Ad Hoc Routing protocol(CEDAR)[13],Zone routing protocol(ZRP)[14], and Zone Based Hierarchical Link State Routing Protocol(ZHLS)[15].

4. SECURITY IN MANETs

When discussing network security in general, two aspects needs to be considered; the security goals and the potential attacks. The security goals includes the functionality that is required to provide a secure networking environment while the security attacks cover the methods that could be employed to break these security services.

4.1 Network Security Goals

In providing a secure networking environment, followings goals are to be implemented:

- *Confidentiality*: Ensures that the destined receivers can only access transmitted data. Encryption can be classified into two types. Symmetric Encryption, where 2 nodes share a key .Symmetric encryption generally requires less computational resources than public key encryption. Public Key Encryption, here all nodes generate a public\private key pair pubKn/privKn.
- *Integrity*: Ensures that the data has not been changed during transmission. The integrity can be ensured using cryptographic hash functions along with some form of encryption.
- *Authentication*: Both sender and receiver of data should be sure of other's identity. Authentication can be provided using encryption along with cryptographic hashing techniques, digital signatures and certificates.
- *Non-repudiation*: Ensures that parties can ensure the transmission of information by another party without denying it. It requires the use of public key cryptography to provide digital signatures.
- Availability: Ensures that the network security services listed above are available to the destined parties when required. The availability ensures redundancy, physical protection and other non-cryptographic means.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 201 – 206 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

4.2 Routing attacks in MANETs

All of the routing protocols in MANET s depend on active cooperation of nodes to provide routing between the nodes and to establish and operate the network. The basic assumption in such a setup is that all nodes are well behaving and trustworthy. Albeit in an event where one or more of the nodes turn malacious, security attacks can be launched which may disrupt routing operations or create a DOS(Denial of Service) condition in the network. The accessibility of the wireless channel to both the genuine user and attacker make the MANET susceptible to both passive eavesdroppers as well as active malicious attackers. The limited power backup and limited computational capability of the individual nodes hinders the implementation of complex security algorithms and key exchange mechanisms. There is always a possibility of a genuine trusted node to be compromised by the attackers and subsequently used to launch attacks on the network. Node mobility makes the network topology dynamic forcing frequent networking reconfiguration which creates more chances for attacks.

4.2.1 Attacks

We divide attacks into two types such as passive or active.

1.**Passive attacks**: In a passive attack an unauthorized node monitors and aims to find out information about the network. The attackers do not disrupt communications or cause any direct damage to the network. They can be used to get information for future harmful attacks. Some of the passive attacks are eavesdropping and traffic analysis.

Eavesdropping Attacks: The attacker analyzes the broadcasting messages to reveal useful information about the network. This attack is also known as disclosure attack. Answers protecting the radio interface from such attacks have been proposed in the literature e.g. spread spectrum communication etc.

Traffic Analysis is not necessarily an entirely passive activity. It is perfectly feasible to engage in protocols or initiate the communication between nodes. Attackers may use methods like as traffic rate analysis, and time-correlation. For example, by timing analysis it can be revealed that two packets in and out of an explicit forwarding node at time t and t+€ are likely to be from the same packet flow [16]. Traffic analysis in ad hoc networks may reveal:

- The existence and location of nodes;
- The communications network topology;
- The roles played by nodes;
- The current communication between the source and destination nodes.

2. **Active Attacks**: These attacks cause unauthorized state changes in the network such as DoS, modification of packets, etc. These attacks are initiated by the nodes with authorization to operate within the current network. Active attacks are divided into four groups: dropping, modification, fabrication, and timing attacks.

Dropping Attacks: Malicious or selfish nodes deliberately drop all packets. These nodes aim to damage the network connection in order to preserve their resources. This attack can help to prevent end-to-end communications between nodes. It could also lower the network performance by making the packets to be resend via new routes to the destination.

An attacker can choose to drop only some packets to avoid being detected by causing the source node to be unaware of failed links (thus interfering with the discovery of alternative routes to the destination); this is called a *selective dropping attack.*

Modification Attacks: Insider attackers modify packets to damage the network. For example, in the *sinkhole attack* the attacker tries to attract almost all the traffic from a particular area via compromised node by making it attractive to one another. It is useful in the route discovery process in routing protocols that use advertised information such as remaining energy and nearest node to the destination. This type of attack can be used as a basis for further attacks like *dropping and selective forwarding* attacks.

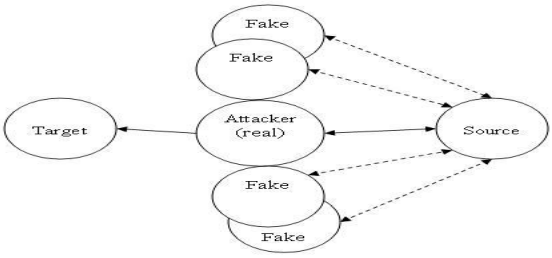

Fig 2: Sink hole attack

A black hole attack is like a sinkhole attack that attracts traffic through itself and uses it as the basis for further attacks. It aims to prevent data packets being forwarded to other nodes. This type of attack is hard to detect for a virtual node [17].

Fabrication Attacks: Here the attacker forges network packets. In [18], fabrication attacks are classified into “active forge” in which attackers send faked messages without receiving any related message and “forge reply” in which the attacker sends fake route reply messages in response to genuine route request messages.

Attackers can initiate frequent packets to cause *denial of service (DoS)*. Example DoS attacks that exploit MANETs" features are sleep deprivation torture attacks, routing table overflow attacks, flooding attacks, and the like.

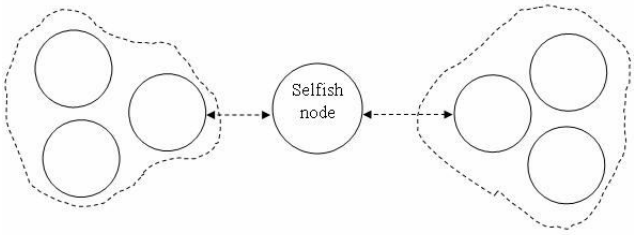

Fig 3: Denial of service attack

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 201 – 206 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

The sleep deprivation torture attack takes a node's battery power and so disables the node by persistently making service requests of one form or another. This attack was discovered by Stajano et al. [19] who stated that it is stronger in impact than DoS attacks such as CPU exhaustion.

The flooding attack, introduced in [20], is another attack against on-demand protocols; here nodes send Route Request messages when so ever they require. The attacker exploits the Route Discovery route by broadcasting many false Route Request messages to a node which is not present.
Another interesting fabrication attack on MANETs is the routing cache poisoning attack [21]. A node can update its table with the routing information in the packets that it hears, even if it is not on the route of the packets. The attacker can poison the routes to a victim node by sending spoofed routing information packets, causing neighboring nodes to update their tables erroneously.

Timing Attacks: An attacker attracts other nodes by causing itself to appear closer to those nodes than it really is. Rushing attacks and hello flood attacks use this technique. *Rushing attacks* [22] occur during the Route Discovery phase.
Rushing attacks can be carried out in many ways by ignoring delays at MAC layers, by wormhole attacks, or by transmitting packets at a higher wireless transmission power.
The hello flood attack [23] is another attack that makes the adversary attractive for many routes. The attacker broadcasts many Hello packets with large enough transmission power that each node receiving Hello packets assumes the adversary node to be its neighbor. It can be highly effective in both proactive and reactive MANET protocols.
A further significant attack on MANETs is the collaborative *wormhole attack*. Here an attacker receives packets at one point in the network, passes them to another point in the network by forwarded by multi-hop routes, and then replays them into the network from this final point .Since the packets sent over tunneling are the same as the packets sent by normal nodes, wormhole attacks can be detected by software approaches such as IDS[24].

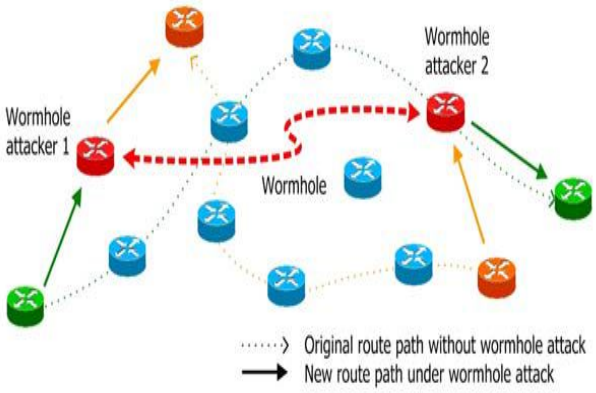

Fig 4: warm hole attack

5. CASE STUDIES OF ATTACK PATTERNS ON ROUTING PROTOCOLS

5.1 Secure Efficient Ad hoc Distance Vector (SEAD)

SEAD was developed based on Destination Sequence Distance Vector (DSDV) and incorporates One-Way Hash function [25] to authenticate in the routing update mechanism in order to enhance the routing security. Securing a table driven protocol is harder than securing an on demand protocol due to the existence of predefined routes. Distance vector protocols encapsulate the route information into a hop count value and a next hop. An attacker cannot create a valid route with a larger sequence number that it received due to the properties of hash function. As SEAD incorporates neighbor authentication through Hash functions, an attacker cannot compromise any node.

SEAD is prone through wormhole attack. Even if authentication is provided using hash functions, a wormhole attack is possible through tunneling the packets from one location and retransmitting them from other location into the network. All packets in the wormhole attack flow in a circle around instead of reaching the destination. Routing table overflow attacks are possible in SEAD, as SEAD is developed based on a table driven approach. A compromised node can advertise routes to nodes which are not in the network and there by fill in the space allocated in the routing table with false node routes. Spoofing attack is possible through compromised node acting like a destination node in the route discovery process by spoofing the identity of the destination node that can cause route destruction. Black hole attack is also possible through a compromised node advertising the shortest roots to non-existing nodes in the network. Tunneling and DOS attacks are also possible through compromised nodes. Table driven protocols are much more prone to security threats.

5.2 Ariadne

Ariadne was developed based on an on demand protocol, Destination Source Routing (DSR). Ariadne uses MACs and shared keys between nodes to authenticate between nodes and use time stamps for packet lifetime [26]. Wormhole attacks are possible in Ariadne through two compromised nodes. Ariadne prevents spoofing attacks with time stamps. The use of source routes prevents loops, since a packet passing through only legitimate nodes will not be forwarded into a loop due to time stamps.

5.3 Authenticated Routing for Ad hoc Network (ARAN)

ARAN uses public key cryptography and a central certification authority server for node authentication and neighbor node authentication in route discovery. Denial-of-service attacks are possible with compromised nodes. Malicious nodes cannot initiate an attack due to the neighbor node authentication through certificates. Participating nodes broadcast unnecessary route requests across the network. An attacker can cause congestion in the network, there by compromising the functionality of the network. Spoofing attacks are prevented by ARAN through node level signatures. Each packet in the network is signed by its private key before

broadcasted to the next level and checked for the authentication. So spoofing the identity of node is hampered by ARAN. Due to the strong cryptographic features of ARAN, malicious nodes cannot participate in any type of attack patterns. Only compromised nodes can participate in any attack pattern. Tunneling attacks are possible in ARAN. Two compromised neighbor nodes can collaborate to falsely represent the length of available paths by encapsulating and tunneling the routing message between them. Wormhole attack is also possible through two compromised nodes. Table overflow, black hole attacks are impossible due to node level authentication with signatures.

5.4 Secure Ad hoc On-Demand Distance Vector Routing (SAODV)

SAODV is a widely implemented protocol in industry due to its strong security features. SADOV uses a central key management in its routing topology. Digital signatures are used to authenticate at node level and hash chain is used to prevent the altering of node counts [27]. Tunneling attacks are possible through two compromised nodes. Wormhole attacks are always possible with compromised nodes in any ad hoc network topology. The use of sequence numbers could prevent most of the possible replay attacks.

6. CONCLUSIONS

This paper discusses common possible attacks on Different routing protocols being used in MANETs. We have tried to analyze them so as to prevent the attacker to intrude in wireless networks. There are lots of techniques with which, one can easily detect most of the attacks. One can choose them in accordance with the protocol being used in the network. However, no protocol is fully secure from attacks being encountered in the MANETs. Hence, one must choose a combination of techniques intelligently to avoid any attack and make the network fully secure.

REFERENCES

[1] C.S.R.Murthy and B.S.Manoj, Ad Hoc Wireless Networks, Pearson Education, 2008.

[2] George Aggelou, Mobile Ad Hoc Networks, McGraw-Hill, 2004. Mobile Ad Hoc Networking and Computing (MobiHOC), October, 2001.

[3] T.H.Clausen, G.Hansen, L.Christensen, and G.Behrmann, "The Optimized Link State Routing Protocol, Evaluation Through Experiments and Simulation," *Proceedings of IEEE Symposium on Wireless Personal Mobile Communications 2001*, September 2001.

[4] R. Ogier, F. Templin, M. Lewis, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)", *IETF Internet Draft*, v.11,October 2003.

[5] A.Iwata, C.C.Chiang, G.Pei, M.Gerla and T.W.Chen, "Scalable Routing Strategies for Ad Hoc Wireless Networks," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1369-1379, August 1999.

[6] C.E.Perkins and P.Bhagwat, "Highly Dynamic Destination- Sequenced Distance-Vector Routing (DSDV) For Mobile Computers," *Proceedings of ACM SIGCOMM 1994*, pp. 233-244, August 1994.

[7] C.C.Chiang, H.K.Wu, W.Liu and M.Gerla, "Routing in Clustered Multi Hop Mobile Wireless Networks with Fading Channel," *Proceedings of IEEE SICON 1997*, pp. 197-211, April 1997.

[8] M.Gerla, X.Hong, L.Ma and G.Pei, "Landmark Routing Protocol (LANMAR) for Large Scale Ad Hoc Networks", *IETF Internet Draft*, v.5, November 2002.

[9] C.E.Perkins and E.M.Royer, "Ad Hoc On-Demand Distance Vector Routing," *Proceedings of IEEE Workshop on Mobile Computing Systems and Applications 1999*, pp. 90-100, February 1999.

[10] D.B.Jhonson and D.A.Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," *Mobile Computing*, Kluwer Academic Publishers, vol.353, pp. 153-181, 1996.

[11] V.D.Park and M.S.Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Ad Hoc Networks," *Proceedings of IEEE INFOCOM 1997*, pp. 1405-1413, April 1997.

[12] I. Chakeres and C. Perkins, "Dynamic MANET On-demand (DYMO) Routing Rrotocol", *IETF Internet Draft*, v.15, November 2008, (Work in Progress).

[13] P.Sinha, R.Sivakumar and V.Bharghavan, "CEDAR: A Core Extraction Distributed Ad Hoc Routing Algorithm," *IEEE Journal on Selected Areas in Communications*, vol.17, no.8, pp. 1454-1466, August 1999.

[14] Z.J.Haas, "The Routing Algorithm for the Reconfigurable Wireless Networks," *Proceedings of ICUPC 1997*, vol. 2,pp. 562-566, October 1997.

[15] M.Joa-Ng and I.T.Lu, "A Peer -to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1415-1425, August 1999.

[16]. Kong J., Hong X., Gerla M., "A New Set of Passive Routing Attacks in Mobile Ad Hoc Networks", In IEEE MILCOM, 2003

[17].Buchegger S., Tissieres C., Le Boudec J.-Y.,"A Test-Bed for Misbehaviour Detection in Mobile Ad-Hoc Networks – How Much Can Watchdogs Really Do?", Mobile Computing Systems and Applications (WMCSA "04), pp. 102-111, 2004

[18]. Ning P., Sun K., "How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols", In Proc. of the IEEE Workshop on Information Assurance, pp. 60-67, 2003

[19]. Stajano F., Anderson R., "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", In Proc. of Int. Workshop on Security Protocols, Springer, 1999

[20]. Yi P., Dai Z., Zhang S., Zhong Y., "A New Routing Attack in Mobile Ad Hoc Networks", Int. Journal of Information Technology, vol. 11, No. 2, pp. 83-94, 2005

[21]. Wu B., Chen J., Wu J., Cardei M., "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Chapter 12, Springer, 2006

[22]. Hu Y.-C., Perrig A., Johnson D.B., "Rushing Attacks and Defence in Wireless Ad Hoc Network
Routing Protocols", In Proc. of the ACM Workshop on Wireless Security, 2003

[23]. Karlof C., Wagner D., "Secure Routing in Wireless Sensor Networks: Attacks and
Countermeasures", Ad Hoc Networks, pp. 293-315, 2003

[24]. Hu Y.-C., Perrig A., Johnson D.B., "Packet Leashes: A Defence against Wormhole Attacks inWireless Ad Hoc Networks", In Proc. of INFOCOM, 2003 1413

[25]. Hubaux J.-P., Buttyan L., Capkun S., "The Quest for Security in Mobile Ad Hoc Networks", In Proc. of the 2nd ACM Int. Symp.on Mobile Ad hoc Networking & Computing, pp. 146-155, 2001. Mobile Computing Systems and applications (WMCSA'02).

[26] Adrian Perrig, Ran Canetti, Dawn Song, and J. D. Tygar. Efficient and Secure Source Authentication for Multicast. In Network and Distributed System Security Symposium, NDSS '01, pages 35–46, February 2001.

[27] Anand Patwardhan, Jim Parker and Anupam Joshi. "Secure Routing and Intrusion Detection in Ad Hoc Networks". [On-line] accessed on 6th November, 2005 at URL http://csrc.nist.gov/mobilesecurity/Publications/ nist - umbc- adhocids-ipv6.pdf.