International Journal of Advanced Research in

Computer Networking,Wireless and Mobile Communications

Volume: 1 Issue: 2 18-May-2015,ISSN_NO: 2320-7248

A STUDY OF ROUTING ATTACKS IN WIRELESS MOBILE ADHOC NETWORKS

Dr. N. Elamathi
Asst. Professor, Dept.of Computer Science
Trinity college for Women, Namakkal Dt., Tamilnadu, India

Abstract: *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, depending on whether the normal operation of the network is disrupted or not. In MANET research has mainly focused on developing an efficient routing mechanism in such a highly dynamic and resource constrained network. At present, several efficient routing protocols have been proposed for MANET. Most of these protocols assume a trusted and cooperative environment. However, in the presence of malicious nodes, the networks are vulnerable to various kinds of attacks. In MANET, routing attacks are particularly serious. In this paper, describing the all prominent attacks described in literature in a consistent manner to provide a concise comparison on attack types.*

Keywords: Ad hoc network, MANET, AODV, OLSR

1. Introduction

A mobile ad hoc network (MANET) is a self configuring network of mobile nodes. It lacks any fixed infrastructure like access points or base stations. It lacks centralized administration and is connected by wireless links/cables. Wireless ad hoc network can be build up where there is no support of wireless access or wires backbone is not feasible. All network services of ad hoc network are configured and created on the fly. Thus it is obvious that with lack of infrastructural support and susceptible wireless link attacks, security in ad hoc network becomes inherent weakness. Nodes within nomadic environment with access to common radio link can easily participate to set up ad hoc infrastructure. But the secure communication among nodes requires the secure communication link to communicate. Before establishing secure communication, the node should be capable enough to identify another node. As a result node needs to identify as well as associated credentials to another node. However delivered identity and credentials need to be authenticated and protected so that authenticity and integrity of delivered identity and credentials cannot be questioned by receiver node. Every node wants to be sure that delivered identity and credentials to recipient nodes are not compromised. Therefore it is essential to provide security architecture to secure ad hoc networking.

Any routing protocol must encapsulate an essential set of security mechanism. These mechanisms are used to prevent, detect and respond to security attacks. These are five major

security goals that need to be addressed in order to maintain a reliable and secure ad hoc network environment. They are namely:

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

Availability: Service 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 be 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.

Non-repudiation: Ensure 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, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or 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.

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, thereby 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 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.

3.2 Traffic analysis & monitoring

Traffic analysis attack adversaries monitor packet transmission to infer important information such 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.

5. Routing Protocol In MANET

The goal of routing in a MANET is to discover the most recent topology of a continuously changing network to find a correct route to a specific node. Routing protocols in a MANET can be classified into two categories: reactive routing protocols (e.g., AODV) and proactive routing protocols (e.g., OLSR). In reactive routing protocols, nodes find routes only when they must send data to the destination node whose route is unknown. In proactive protocols, nodes periodically exchange topology information, and hence nodes can obtain route information any time they must send data.

AODV (Ad hoc On Demand Distance Vector Protocol)

AODV is a reactive routing protocol designed for a mobile ad hoc network. In AODV, when a source node S wants to send a data packet to a destination node D and does not have a route to D, it initiates route discovery by broadcasting a route request (RREQ) to its neighbors. The immediate neighbours who receive this RREQ rebroadcast the same RREQ to their neighbours. This process is repeated until the RREQ reaches the destination node. Upon receiving the first arrived RREQ, the destination node sends a route reply (RREP) to the source node through the reverse path where the RREQ arrived. The same RREQ that arrives later will be ignored by the destination node. In addition, AODV enables intermediate nodes that have sufficiently fresh routes (with destination sequence number equal or greater than the one in the RREQ) to generate and send an RREP to the source node.

OLSR (Optimized Link State Routing Protocol)

OLSR is a proactive routing protocol, that is, it is based on periodic exchange of topology information. The key concept of OLSR is the use of multipoint relay (MPR) to provide an efficient flooding mechanism by reducing number of transmissions required. In OLSR, each node selects its own MPR from its neighbours. Each MPR node maintains the list of nodes that were selected as an MPR; this list is called an MPR selector list. Only nodes selected as MPR nodes are responsible for advertising, as well as forwarding an MPR selector list advertised by other MPRs.

Routing Message in OLSR

Two types of routing messages are used, namely, a HELLO message and a topology control (TC) message. A HELLO message is the message that is used for neighbour sensing and MPR selection. In OLSR, each node generates a HELLO message periodically. A node's HELLO message contains its own address and the list of its one-hop neighbours. By exchanging HELLO messages, each node can learn a complete topology up to two hops. HELLO messages are exchanged locally by neighbor nodes and are not forwarded further to other nodes. A TC message is the message that is used for route calculation. In OLSR, each MPR node advertises TC messages periodically. A TC message contains the list of the sender's MPR selector. In OLSR, only MPR nodes are responsible for forwarding TC messages. Upon receiving TC messages from all of the MPR nodes, each node can learn the partial network topology and can build a route to every node in the network.

6. Routing Attacks against Protocol in MANET

i. Flooding Attack

The aim of the flooding attack is to exhaust 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.

ii. Blackhole Attack

In a black hole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic. Figure 1 shows an example of a Black hole attack, where attacker A sends a fake RREP to the source node S, claiming that it has a sufficiently fresher route than other nodes.

Since the attacker's advertised sequence number is higher than other nodes sequence numbers, the source node S will choose the route that passes through node A.

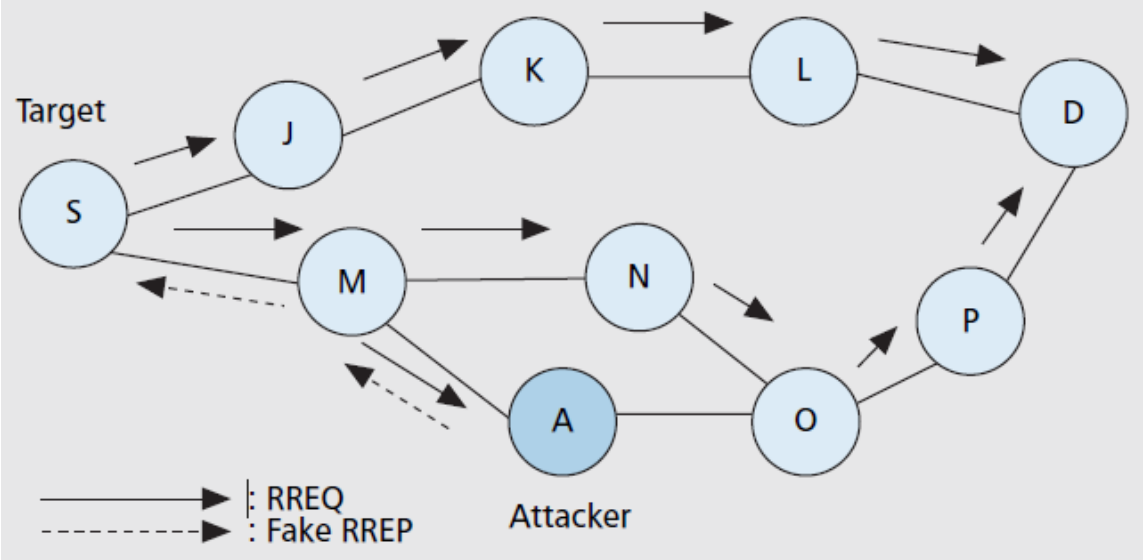

Figure1. Example of blackhole attack on AODV

iii. Link Spoofing Attack

In a link spoofing attack, a malicious node advertises fake links with non-neighbours to disrupt routing operations. For example, in the OLSR protocol, an attacker can advertise a fake link with a target's two-hop neighbours. 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. Figure 2 shows an example of the link spoofing attack in an OLSR MANET. In the figure, we assume that node A is the attacking node, and node T is the target to be attacked. Before the attack, both nodes A and B are MPRs for node T. During the link spoofing attack, node A advertises a fake link with node T's two hop neighbour, that is, node D. According to the OLSR protocol, node T will select the malicious node A as its only MPR since node A is the minimum set that reaches node T's two-hop neighbours. By being node T's only MPR, node A can then drop or withhold the routing traffic generated by node T.

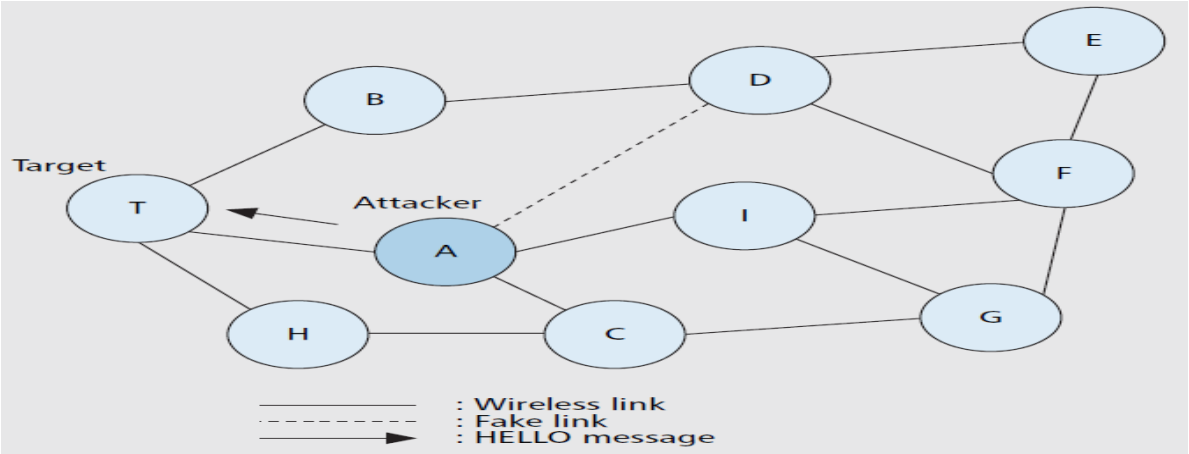

Figure 2. Example of link spoofing attack on OLS

iv. Wormhole Attack

A wormhole attack is one of the most sophisticated and severe attacks in MANETs. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality. Figure 3 shows an example of the wormhole attack against a reactive routing protocol. In the figure, we assume that nodes *A*1 and *A*2 are two colluding attackers and that node S is the target to be attacked. During the attack, when source node S broadcasts an RREQ to find a route to a destination node D, its neighbours J and K forward the RREQ as usual. However, node *A*1, which received the RREQ forwarded by node J, records and tunnels the RREQ to its colluding partner *A*2. Then, node *A*2 rebroadcasts this RREQ to its neighbour P. Since this RREQ passed through a high speed channel, this RREQ will reach node D first. Therefore, node D will choose route D-P-J-S to unicast an RREP to the source node S and ignore the same RREQ that arrived later. As a result, S will select route S-JP- D that indeed passed through *A*1 and *A*2 to send its data.

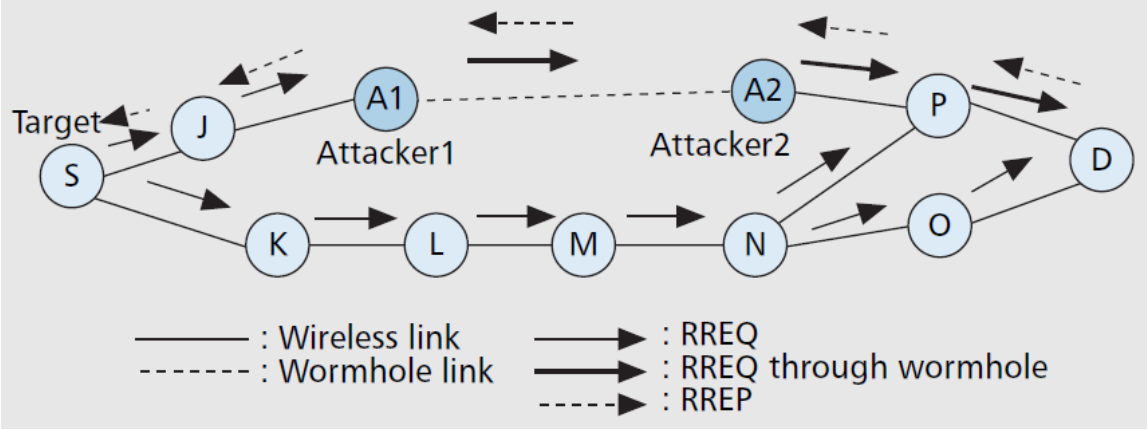

Figure 3. Example of wormhole attack on reactive routing

v. Rushing Attack

In AODV or related protocol, each node before transmitting its data, first establishes a valid route to destination. Sender node broadcasts a RREQ (route request) message in neighborhood and valid routes replies with RREP (route reply) with proper route information. Some of the protocols use duplicate suppression mechanism to limit the route request and reply chatter in the network. Rushing attack exploits this duplicate suppression mechanism. Rushing attacker quickly forwards with a malicious RREP on behalf of some other node skipping any proper processing. Due to duplicate suppression, actual valid RREP message from valid node will be discarded and consequently the attacking node becomes part of the route. In rushing attack, attacker node does send packets to proper node after its own filtering is done, so from outside the network behaves normally as if nothing happened. But it might increase the delay in packet delivering to destination node.

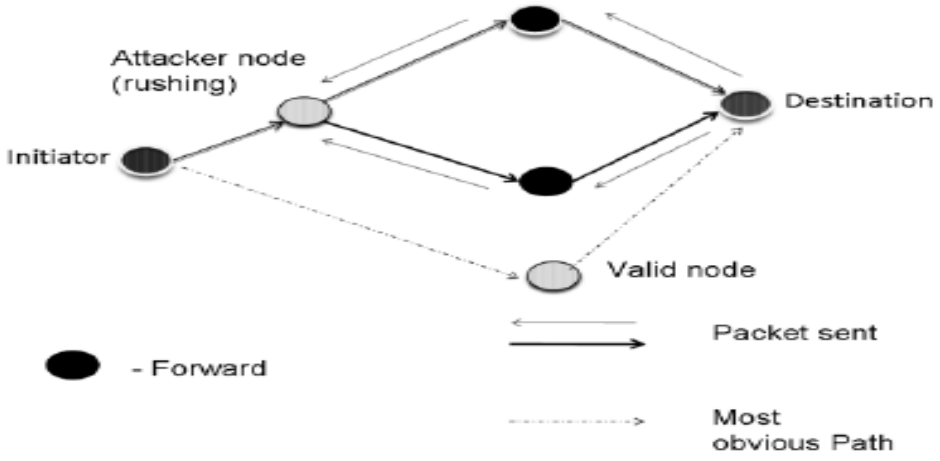

Figure 4: Rushing Attack

Few of the protocols that might help in resolving Rushing attack:

(i) SEDYMO : Secured Dynamic MANET On-Demand is similar to DYMO but it dictates intermediate node must add routing information while broadcasting the routing messages and no intermediate node should delete any routing information from previous sender while broadcasting. It also incorporates hash chains and digital signature to protect the identity.

(ii) SRDP : Secure Route Discovery Protocol is security enhanced Dynamic Source routing (DSR) protocol.

(iii) SND : Secure Neighbor Detection is another method of verifying each neighbor's identity within a maximum transmission range.

vi. 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 nonexistent nodes. Meanwhile the sleep deprivation attack aims to consume the batteries of a victim node. 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

vii. 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. 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 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.

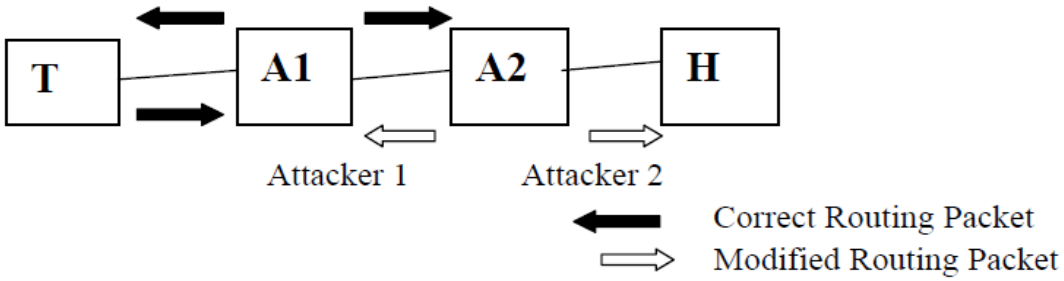

Figure 6: Colluding misrealy attack

viii. Sybil Attack

Sybil attack manifests itself by faking multiple identities by pretending to be consisting of multiple nodes in the network. So one single node can assume the role of multiple nodes and can monitor or hamper multiple nodes at a time. Success in Sybil attack depends on how the identities are generated in the system.

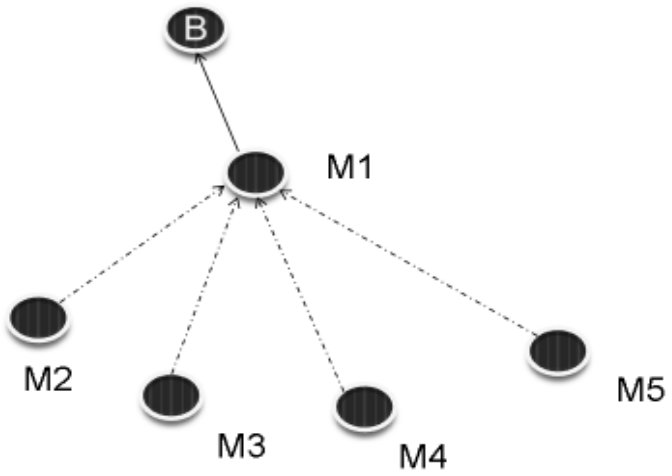

Figure 7: Sybil Attack

In figure 7, node M1 assumes identities of M2, M3, M4, and M5. So, to node B, M1 is equivalent to those nodes. One way of mitigating this attack is maintaining a chain of trust, so

single identity is generated by a hierarchical structure which may be hard to fake. One way of mitigating this attack is maintaining a chain of trust, so single identity is generated by a hierarchical structure which may be hard to fake.

CONCLUSION

Mobile ad hoc networks (MANETs) represent one of the most innovative emerging networking technologies, with broad potential applications in personal area networks. Because these networks can be deployed quickly without relying on a predefined infrastructure, they can be applied in various situations ranging from emergency operations and disaster relief to military service and task forces. Obviously, providing security in such scenarios is critical. The current state of- the-art of routing attacks to inspect the security threats in the mobile ad hoc 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 study, it finds 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.

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] 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.

[4] K. Sanzgiriet al., ―A Secure Routing Protocol for Ad Hoc Networks, Proc. 2002 IEEE Int'l. Conf. Network Protocols, Nov. 2002.

[5] Y-C. Hu, A. Perrig, and D. B. Johnson, ―Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks,‖ Proc. MobiCom '02, Atlanta, GA, Sept. 23–28, 2002.

[6] M. G. Zapata and N. Asokan, ―Securing Ad-Hoc Routing Protocols, Proc. 2002 ACM Wksp. Wireless Sec., Sept. 2002, pp. 1–10.

[7] B. Wu et al., ―A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks, Wireless/Mobile Network Security, Springer, vol. 17, 2006.

[8] 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.

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

BIOGRAPHY

Dr.N.Elamathi received her Ph.D degree from Mother Teresa Women's University, Kodaikanal in 2013, Bachelor's degree from the University of Bharathidasan , Trichy, Tamilnadu in 1995, M.Sc(CS) from the university of Alagappa University, Karikudi in 1998, and M.Phil(CS) from the University of Manonmaniam sundaranar University,Tirunelveli 2003.