IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 8, August 2015.
www.ijiset.com
ISSN 2348 – 7968

A Discussion on the different types of Security Attacks in Mobile Ad Hoc Networks on Protocol Stack

Anto Ramya. S. I

Assistant Professor, Department of Computer Science,
St. Joseph's College of Arts and Science for Women, Hosur - 635126,
Tamil Nadu, India

Abstract

A MANET is a network without infrastructure, which consists of a number of mobile nodes with wireless network interfaces to make the nodes communicate with each other. The nature and structure of the network makes it attractive to different attackers. MANET is vulnerable to various kinds of security attacks like worm hole, black hole, rushing attack etc because of its wireless medium, dynamic topology and distributed co-operation. Attackers against a network can be classified into two: outsider and insider. An outsider attacker is not a legitimate user of the network whereas an insider attack is an authorized node and a part of the routing mechanism. On the basis of the nature of attack interaction, the attacks against MANET may be classified into active and passive attacks. The major focus of this paper is on security issues connected with mobile ad hoc networks. The discussion of the paper is on the different types of attacks on various layers under the network protocol stack.

Keywords: *MANET, Attacker, Wireless Medium, Dynamic Topology, Rushing Attack, Active, Passive.*

1. Introduction

Wireless cellular system has been in utilized since 1980's. Access points are present in the wireless system. For the user to be connected to the wireless system, access points are required. In MANET, the mobile nodes are dynamically located and the interconnections between the nodes are capable of changing on a continuous basis. MANET is a collection of independent mobile nodes that communicate with each other through radio waves. The mobile nodes within the range communicate directly, whereas other nodes need the aid of intermediate nodes to route their packets. Each node has a wireless interface to interact with one other. MANETs are fully distributed and can work at any place without the help of any fixed infrastructure as access points or base stations.

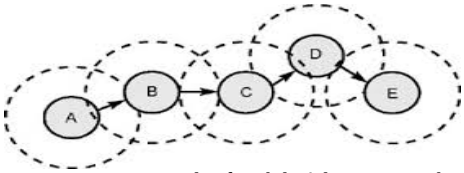

Figure 1: Example of Mobile Ad Hoc Network

1.1 MANET characteristics

- *Distributed operation:* There is no central control of the network operations, but the control of the network is distributed among the nodes. The nodes in MANET co – operate and communicate among themselves and each node acts as a relay to implement specific functions such as routing and security.
- *Multihop Routing*: When a node tries to send information to other nodes out of its range, the packet will be forwarded through one or more intermediate nodes.
- *Autonomous Terminal:* Each node in MANET is an independent node, so each node should functions as both a host as well as a router.
- *Dynamic Topology:* Nodes move freely with different speeds, hence the network topology may change randomly and at unpredictable time.
- *Light – Weight Terminals:* Most of the nodes at MANET are mobiles with less CPU capability, low power storage and small memory size.
- *Shared Physical Medium:* The wireless communication medium is accessible to any entity with appropriate equipment and adequate resources.

1.2 Security Goals of MANET

- *Authentication:* It means that the user has rights to use the resource. It is an assurance that the traffic received is sent by a genuine user.
- *Integrity:* It is an assurance that the data received by the receiver has not been altered or modified after being sent by the original user.
- *Confidentiality*: It means that the data is not examined by a non – authorized party.
- *Non – Repudiation:* This authentication service cannot deny or disallow a transaction. It's an assurance that someone cannot deny something.

ISSN 2348 – 7968

- *Access Control:* It is the prevention of unauthorized use or resource**.**

2. Attacks in MANET

Mobile Ad hoc networks are exposed to many attacks not only from outside but also from within the network itself. Ad hoc network are mainly subjected to two different levels of attacks:

- The first level of attack occurs on the basic mechanisms of the ad hoc network such as routing.
- The second level of attack damages the security mechanisms employed in the network.

The attacks in MANETs are divided into two major types: internal and external.

2.1 Internal Attacks

Internal attacks directly attack the nodes in the network and links between them. This type of attacks may transmit wrong type of routing information to other nodes. Internal attacks are more difficult to handle than external attacks since internal attacks occur due to trusted nodes. The wrong routing information generated by compromised nodes or malicious nodes are difficult to identify. This can be due to the compromised nodes capability to generate the valid signature using their private keys.

2.2 External Attacks

These types of attacks cause congestion in network, Denial of Service (DoS) and advertising wrong routing information. External attacks prevent the network from normal communication and from producing additional overhead to the network. External attacks can be classified into two categories: active and passive.

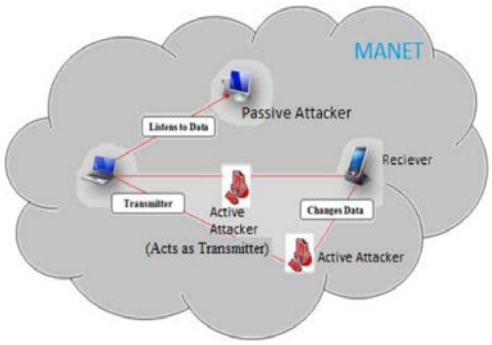

Figure 2: Types of Attacks

2.2.1 Passive Attacks

A Passive attack does not modify the data transmitted within the network, but includes unauthorized "Listening" to the network traffic or accumulates data from it. Passive attacker does not disrupt the operation of a routing protocol, but attempts to discover the important information from routed traffic.

2.2.2 Active Attacks

Active attacks are very severe attacks on the network that prevent message flow between nodes. Active attacks can be either internal or external. Active external attacks can be carried out by outside sources that do not belong to the network. Active internal attacks are from malicious nodes which are a part of the network. Active attacks are classified into four groups:

- *Dropping Attacks:* Compromised nodes or selfish nodes drop all packets that are not destined for them. Dropping attacks can prevent end – to – end communications between nodes when the dropping node is the critical point. Most of the routing protocols have no mechanism to detect whether the data packets have been forwarded or not.
- *Modification Attacks:* These attacks modify packets and disrupt the overall communication between network nodes. An example of modification attack is sinkhole attack. In sinkhole attack, the compromised node advertises itself as the shortest path to the destination. Malicious node captures important routing information and uses it for further attacks such as dropping and selective forwarding attacks.
- *Fabrication Attacks:* The attacker sends a fake message to the neighboring nodes without receiving any related message. The attacker also sends a fake route reply message in response to related legitimate route request messages.
- *Timing Attacks:* Attackers attract other nodes by advertising itself as a node closer to the actual node. Rushing attacks and hello flood attacks use this technique.

3. Active Attacks on Various Layers of Network Protocol

3.1 Attacks at Physical Layer

ISSN 2348 – 7968

The attacks on physical layer are hardware oriented and they need help from hardware sources to get into effect. These attacks are simple to execute as compared to other attacks. They do not require the complete knowledge of technology. Some of the attacks identified at physical layer include eavesdropping, interference and jamming etc.

- *Eavesdropping:* It is an interception and reading of messages and conversations by unintended receivers. The main aim of such attacks is to obtain the confidential information that should be kept secret during the communication. As the communication takes place on wireless medium, it can easily be intercepted with receiver tuned to the proper frequency. The information can include private key, public key, location or passwords of the nodes.

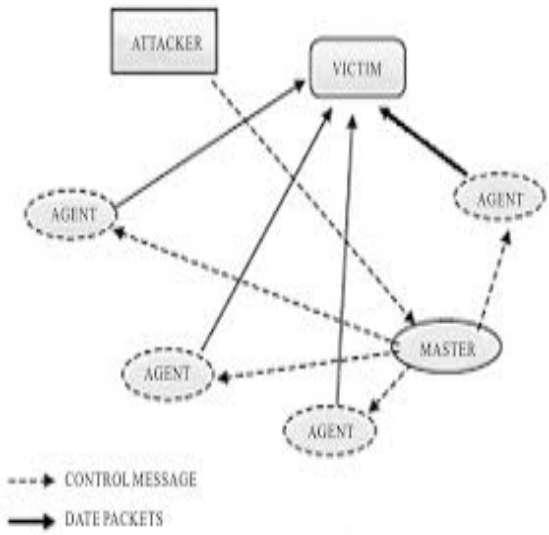

Figure 3: Eaves dropping Attack

- *Jamming:* Jamming is a special class of DoS attack which is initiated by malicious node after determining the frequency of communication. The jammer transmits signals along with security threats. It also prevents the reception of legitimate packets.
- *Active Interference:* An active interference is a DoS attack which blocks the wireless communication channel. The effects of such attacks depend on their duration and the routing protocol in use. Attackers can change the order of messages or attempt to replay old messages. Old messages may be replayed to reintroduce out dated information.

3.2 Attacks at Data Link Layer/MAC Layer

The data link layer can classify attacks based on the effect it has on the state of the network. The algorithms used in this layer are susceptible to many DoS attacks. Effects can be measured in terms of route discovery failure, energy consumption, link breakage initiating route discovery, etc. The misbehavior of a node can be merely with malicious intents.

3.2.1 Selfish Misbehavior of Nodes

The selfish nodes may refuse to take part in the forwarding process or drops the packets intentionally in order to conserve the resources and to conserve the battery power. These kinds of attacks directly affect the self – performance of nodes and do not interfere with the operation of the network. It may include two important factors:

- Conservation of battery power.
- Gaining unfair share of bandwidth.

These attacks exploit the routing protocol. The main attack by the selfish node is packet dropping, which leads to congestion in network. Most of the routing protocols have no mechanism to detect whether the packets are being forwarded or not, except Dynamic Source Routing (DSR).

3.2.2 Malicious Behavior of Nodes

The major task of the malicious node is to disturb the normal operation of routing protocol. The impact of such attack is increased when the communication takes place between neighboring nodes. Such attacks fall into the following categories:

- *Denial of Service (DoS):* These types of threats produce malicious action with the help of compromised nodes that forms severe security risks. Detection of compromised routing is difficult in the presence of compromised nodes. The compromised route appears like a normal route, but leads to severe problems. Ex: A compromised node could participate in the communication, but drops some packets which lead to degradation in the quality of service being offered by network.
- *Attacks on Network Integrity:* Network integrity is an important issue to provide secure communication and quality of service in network. There are so many threats which exploit the routing protocol to introduce wrong routing information.
- *Misdirecting Traffic:* A malicious node advertises wrong routing information in order to get secure data before the actual route. These nodes receive the information that was intended for the owner of the address. A malicious node advertises fake request, so that the other nodes will direct the replies to the node.

ISSN 2348 – 7968

- *Attacking Neighboring Sensing Protocols:* Malicious nodes advertise fake error messages, so that the links of important interfaces are marked as broken. This will result in decrease in network throughput and quality of service.

3.2.3 Traffic Analysis

In MANETs, the data packets and traffic pattern are important for adversaries. Ex: Confidential information about network topology can be derived by analyzing traffic patterns. Traffic analysis can also be conducted as active attack by destroying nodes, which stimulates self organization in the network and valuable data about the topology can be gathered. Traffic analysis in ad hoc networks may reveal following type of information:

- Location of nodes.
- Network topology used for communication.
- Roles played by nodes.
- Available source and destination nodes.

3.3 Attacks at Network Layer

The basic idea behind the network layer is to introduce itself in the active path from source to destination or to absorb the network traffic. The network layer protocols allow MANET nodes to be connected to one another through hop – by – hop. The malicious node easily attacks a network where every single node decides the path to forward the packet. Figure 4 shows an example of attack on the network layer. The malicious node "X" can absorb important data by placing itself between the source node "A" and the Destination node "D" as shown in the figure. "X" can also divert the packets exchanged between "A" and "D", which results in end – to – end delay.

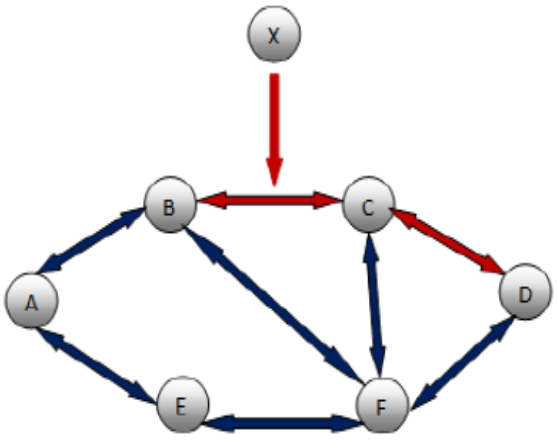

Figure 4: Attacks on Network Layer

3.3.1Blackhole Attack

In this type of attack, the malicious node claims to have an optimum route to the node whenever it receives RREQ packets and sends the REPP with highest destination sequence number and minimum hop count value to the originator node, whose RREQ packets it wants to intercept. For example, in figure 5, malicious node 4 advertises itself in such a way that it has a shortest route to the destination. When source node "S" wants to send data to destination node "D", it initiates the route discovery process. When the malicious node 4 receives the route request, it immediately sends response to source. If reply from node 4 reaches first to the source, then the source node "S" ignores all other reply messages and begins to send packet through route node 2. As a result, all data packets are consumed or lost at malicious node.

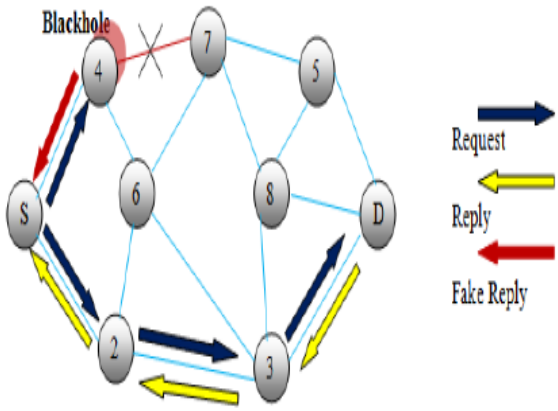

Figure 5: Black hole Attack

3.3.2 Rushing Attack

They are mainly against on – demanding protocols. On – demanding routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack. When compromised node receives a route request packet from the source node, it floods the packet quickly throughout the network before other nodes, which also receive the same route request packet can react. For example, in figure 6, the node 4 represents the rushing attack node, where "S" and "D" refers to source and destination nodes. The rushing attack of compromised node 4 quickly broadcasts the route request messages to ensure that the RREQ message from itself arrive earlier than from other nodes. This result in when the neighboring node of "D" (i.e.) 7 and 8 when they receive the actual route request from source, they simply discard requests. So in the presence of such attacks "S" fails to discover any useable route without the involvement of attacker.

ISSN 2348 – 7968

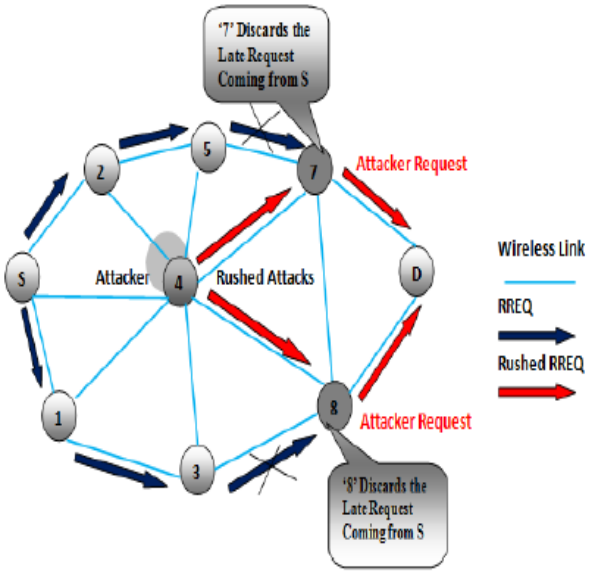

Figure 6: Rushing Attack

3.3.3 Wormhole Attack

The tunnel that exists between two malicious nodes is referred to as a wormhole. The malicious node receives data packet at one point in the network and tunnels them into another malicious node. To make their nodes more attractive and to make more data to route through them, attackers use wormholes in their network. When the wormhole attacks are used by the attackers in routing protocols such as DSR and AODV, the attack could prevent the discovery of any routes other than through wormhole. For example, in figure 7, the nodes "X" and "Y" are malicious nodes that form the tunnel in the network. When the source node "S" initiates the RREQ message to find the route to node "D" destination node, the immediate neighbor node of the source node "S" namely 2 and 1 forwards RREQ message to their respective neighbors 5 and "X". When the node "X" receives the RREQ, it immediately shares it with "Y" and later it initiates RREQ to its neighbor node 8, through which the RREQ is delivered to the destination node "D". Due to the high speed link, it forces the source node to select the route<S-1-8-D> for destination. It results in "D" ignores RREQ that arrives at a later time and thus invalidates the legitimate route<S-2-5-7-D>.

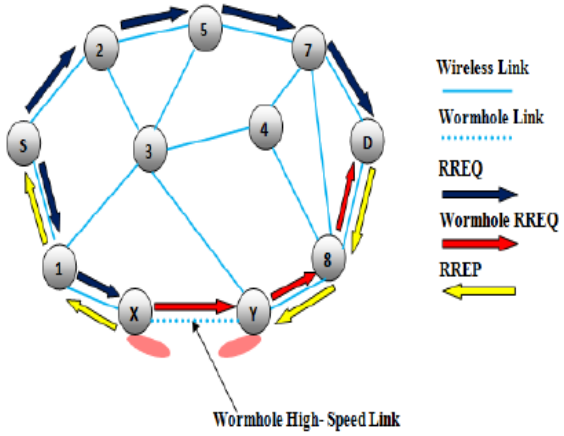

Figure 7: Wormhole Attack

3.3.4 Greyhole Attack

The malicious node claims to have optimum route to the node whose packets it wants to intercept. It is similar to black hole attack, but it drops data packets of a particular node.

3.3.5 Sinkhole Attack

A Compromised node or malicious node advertises wrong information to produce itself as a specific node and receives the whole network traffic. After receiving the traffic, it modifies the secret information such as changes made to the data packet or drops them to make the network complicated. A malicious node tries to attract the secure data from all neighboring nodes. Sinkhole attack affects the performance of ad hoc network protocols such as AODV by using flaws as maximizing the sequence number or minimizing the hop count. Figure 8 shows an example of sink hole attack.

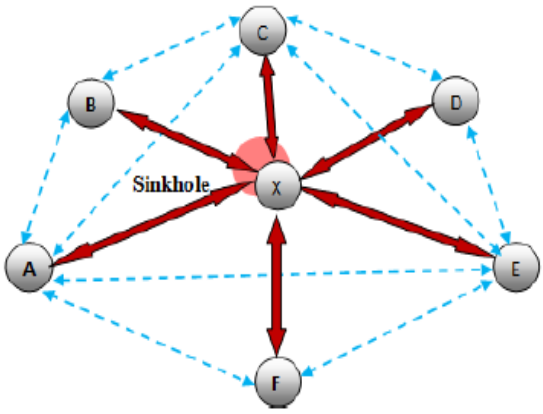

Figure 8: Sinkhole Attack

ISSN 2348 – 7968

3.3.6 Replay Attack

The topology is not fixed in MANETs; it changes frequently due to the mobility of nodes. In replay attack, a malicious node record control messages of other nodes and resends them later. Because of which, other nodes record their routing table with stale routes. These replay attacks are misused to disturb the routing operation in MANETs.

3.3.7 Link Withholding and Link Spoofing Attacks

In link withholding attack, the malicious nodes do not broadcast any information about the links to specific nodes. It results in losing the links between nodes. In link spoofing attacks, a malicious node broadcasts or advertises fake route information to disrupt the routing operation. It results in malicious node to manipulate the data or routing traffic. Figure 9 shows an example of spoofing attack.

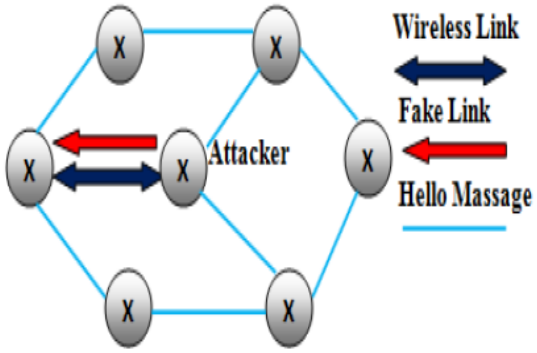

Figure 9: Spoofing Attack

3.3.8 Resource Consumption Attack:

A compromised node can attempt to consume battery life by requesting excessive route discovery or by forwarding unnecessary packets to the victim. These types of attacks are called as sleep deprivation attack, which mainly occur against the devices that don't offer any services to the network.

3.3.9 Sybil Attack

Sybil attacker generates fake identities of additional nodes. In this, a malicious node produces itself as a large number instead of a single node. The additional identities that the node acquires are sybil nodes. A sybil node may fabricate a new identity for itself or it steals an identity of the legitimate node. Various effects due to presence of sybil attacks are:

- It may be difficult to identify the misbehaving node in a network among the misbehaving nodes.
- Sybil attacks prevent fair resource allocation among the nodes in network.
- In certain applications, sensors can be used to perform voting for decision making. The outcome of the voting process may vary because of the duplicate identities.
- Sybil nodes affect the normal operation of routing protocols by appearing itself at various locations in a network.

3.4 Attacks at Transport Layer

3.4.1 Session Hijacking

The attacker exploits the unprotected session after the initial setup. In this attack, the attacker spoofs the victim node's IP address, finds the correct sequence number and launches various DoS attacks. The malicious node collects secure data such as passwords, secret keys, login names and other information from nodes. Session hijacking attacks are also known as address attacks which affect OLSR protocol. The TCP – ACK storm problem may occur when malicious node launches a TCP session hijacking attack. Figure 10 shows an example of session hijacking. The attacker "X" injects session data, node 1 sends acknowledgement packet to node 2. Packet will not contain any sequence number that node 2 is expecting. So, when node 2 receives the packet, it tries to resynchronize the TCP session with node 1. This process is repeated again and again that leads to ACK storm. Hijacking a session in a connectionless transport protocols such as User Datagram Protocol (UDP) is even easier than connection oriented protocols.

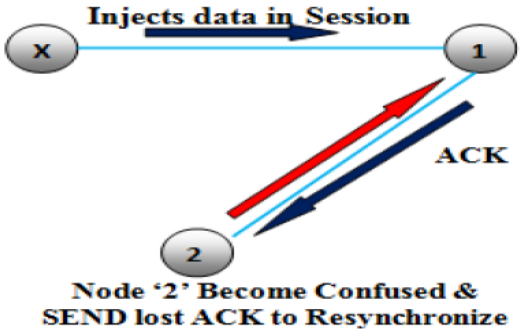

Figure 10: Session Hijacking

3.4.2 SYN Flooding Attack

ISSN 2348 – 7968

The attacker creates a large number of half opened TCP connections with victim nodes. These connections never complete the handshake to fully open the connection.

3.5 Attacks at Application Layer

Application layer protocols are also vulnerable to many DoS attacks. The application layer contains user data. It supports protocols such as HTTP, SMTP, TELNET and FTP, which provide many vulnerabilities and access points for attackers.

3.5.1 Malicious Code Attacks

Malicious code attacks include viruses, worms, spywares and trojan horses which can attack both operating system and user application.

3.5.2 Repudiation Attack

Repudiation refers to denial of participation in all or part of the communication. Firewalls and encryption mechanisms used at different layer are not sufficient for packet security. Application layer firewalls provide security to packets against many attacks.

4. Conclusion and Future Work

MANETs are vulnerable to many attacks because of its dynamic infrastructure and no centralized administration. The discussion of this paper is entirely about how the different layers under protocol stack become vulnerable to various attacks. Various security mechanisms are introduced to prevent such networks. In future, security algorithms will be implemented to reduce the impact of different attacks along with the routing protocols.

Acknowledgments

First of all, I am glad to thank THE LORD ALMIGHTY for giving me the spirit in completing this paper. I would thank my family for the constant support they provided throughout my preparation.

References

[1]. Amitabh Mishra, “Security and Quality of service in Ad Hoc wireless networks” ISBN – 13 978-0-521-87824-1 Handbook.

[2]. Mohammad Ilyas, “The Handbook of Ad Hoc Wireless Networks”.

[3]. Vikrant Gokhale, S.K.Gosh, and Arobinda Gupta, “Classification of attacks on wireless mobile ad hoc networks and vehicular ad hoc networks a survey”.

[4]. Zubair Muhammad Fadlullah, Tarik Taleb, and Marcus Scholler, “Combating against security attacks against mobile ad hoc networks(MANETs)”.

[5]. Kamanshis Biswas and Md. Liakat Ali, “Security threats in mobile ad hoc network”.

[6]. Pradip M. Jawandhiya, Mangesh M.Ghonge, “A survey of mobile ad hoc network attacks” International Journal of Engineering Science and Technology Vol. 2(9), 2010,4.63-4071.

[7]. Wenjia Li and Anupam Joshi, “Security issues in mobile ad hoc networks – a survey”.

[8]. K.P.Manikandan, Dr. R. Satyaprasad, Dr. Rajasekhararao, ” Analysis and diminution of security attacks on mobile ad hoc network”, IJCA special issue on “Mobile Ad hoc Networks MANETs’ 2010”.

[9]. Ad hoc networks specific attacks held by Adam Burg.

[10]. Sevil, Sen, John A. Clark and Juan E. Tapiador, “Security threats in mobile ad hoc networks”.

[11]. Kisung Kim and Sehun Kim, “A sinkhole detection method based on incremental learning in wireless ad hoc networks”.

[12]. Panagiotis Papadimitratos and Zygmunt J.Haas, “Securing mobile ad hoc networks”.

Anto Ramya. S. I was born in Cochin, Kerala (KE), India, in 1985. She received the Bachelor of Commerce (B.Com.)degree from the Periyar University (PU), Salem, TN, India, in 2005 and the Master of Computer Applications (M.C.A.) degree from Anna University, Chennai, TN, India, in 2008 and Master of Philosophy(M.Phil.) of Computer Science Degree from the PU, in 2012. Her research interests include neural networks, mobile computing and MANET.