International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-1 Issue-5, June 2012

Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review

Gagandeep, Aashima, Pawan Kumar

Abstract--- A MANET is an infrastructure-less type network, which consists of number of mobile nodes with wireless network interfaces In order to make communication among nodes, the nodes dynamically establish paths among one another. The nature and structure of such networks makes it attractive to various types of attackers. In this paper we discuss various types of attacks on various layers under protocol stack. Different types of attacker attempts different approaches to decrease the network performance, throughput. In this paper the principal focus is on routing and security issues associated with mobile ad hoc networks which are required in order to provide secure communication. On the basis of the nature of attack interaction, the attacks against MANET may be classified into active and passive attacks. Attackers against a network can be classified into two groups: insider and outsider. Whereas an outsider attacker is not a legitimate user of the network, an insider attacker is an authorized node and a part of the routing mechanism on MANETs.

Keywords: MANET, DoS, DSR, AODV,

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies [1, 6]. Mobile ad hoc networks are collection of wireless networks, which consists of large number of mobile nodes. Nodes in MANETs can join and leave the network dynamically. There is no fixed set of infrastructure and centralized administration in this type of networks. Nodes are interconnected through wireless interface. The dynamic nature of such type networks makes it highly susceptible to various link attacks. The basic requirements for a secured networking are secure protocols which ensure the confidentiality, availability, authenticity, integrity of network. Many existing security solutions for wired networks are ineffective and inefficient for MANET environment.

As the transmission takes place in open medium makes the MANETs more vulnerable to security attacks. In the presence of security protocol affect of various attacks can be reduced. The mobile hosts dynamically establish paths among one another in order to communicate. Therefore, the success of MANET communication highly relies on the collaboration of the involved mobile nodes.

Manuscript published on 30 June 2012.
***** Correspondence Author (s)
Gagandeep, Department of Computer Science & Engineering, Shaheed Bhagat Singh, State Technical campus, Ferozepur (Punjab) India
Aashima Department of Computer Science & Engineering, Shaheed Bhagat Singh, State Technical campus, Ferozepur (Punjab), India
Pawan Kumar Assistant Professor, Department of Computer Science & Engineering, Shaheed Bhagat Singh, State Technical campus, Ferozepur (Punjab), India

Such dynamism of MANET-based architectures leads to some inherent weaknesses and a wide variety of attacks target these weaknesses [3].

In this paper, we discuss some of the existing malicious attacks against MANETs and also the techniques to detect them. These types of attacks consist of replication, modification, or removing information exchanged by other nodes.

A. *Vulnerabilities of MANETs*

- *Dynamic Topology:* In MANETs, nodes can join and leave the network dynamically and can move independently [2]. Due to such type nature there is no fixed set of topology works in MANETs. The nodes with inadequate physical protection may become malicious node and reduce the network performance.
- *Wireless Links:* As the nodes in such networks are interconnected through wireless interface that makes it highly susceptible to link attacks. The bandwidths of wireless networks are less as compared to wired networks, which attracts many attackers to prevent normal communication among nodes.
- *Cooperativeness:* In MANETs, all routing protocols assume that nodes provide secure communication. But some nodes may become malicious nodes which disrupt the network operation by changing routing information etc [1].
- *Lack of clear line of defence:* There is no clear line of defence mechanism available in the MANETs; attacks can come from any directions. Attackers can attack the network either internally or externally.
- *Limited resources:* The MANETs consists of different set of devices such as laptops, computers, mobile phones etc. All of such devices having different storage capacity, processing speed, computational power etc. This may attracts the attackers to focus on new attacks.

B. *Attackers*

There are different types of attacker present in MANETs, which tries to reduce the performance of network. In this paper we study about various attackers, which are classified in the figure 1.

Fig 1: Classification of Attackers

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

II. SECURITY ATTACKS IN MANETS

Mobile Ad hoc networks are vulnerable to various 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. Whereas the second level of attacks tries to damage the security mechanisms employed in the network. The attacks in MANETs are divided into two major types.

A. Internal Attacks

Internal attacks are directly leads to the attacks on nodes presents in network and links interface between them. This type of attacks may broadcast wrong type of routing information to other nodes [1, 2]. Internal attacks are sometimes more difficult to handle as compare to external attacks, because internal attacks occurs due more 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 are able to generate the valid signature using their private keys.

B. External attacks

These types of attacks try to cause congestion in the network, denial of services (DoS), and advertising wrong routing information etc [2]. External attacks prevent the network from normal communication and producing additional overhead to the network. External attacks can classify into two categories:

1) Passive attacks

MANETs are more susceptible to passive attacks. A passive attack does not alter the data transmitted within the network. But it includes the 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, 10, 13]. Detection of such type of attacks is difficult since the operation of network itself doesn't get affected. In order to overcome this type of attacks powerful encryption algorithms are used to encrypt the data being transmitted.

2) Active Attacks

Active attacks are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. Active external attacks can be carried out by outside sources that do not belong to the network. Internal attacks are from malicious nodes which are part of the network, internal attacks are more severe and hard to detect than external attacks [2, 4, 13]. These attacks generate unauthorised access to network that helps the attacker to make changes such as modification of packets, DoS, congestion etc. The active attacks are generally launched by compromised nodes or malicious nodes. Malicious nodes change the routing information by advertising itself as having shortest path to the destination.

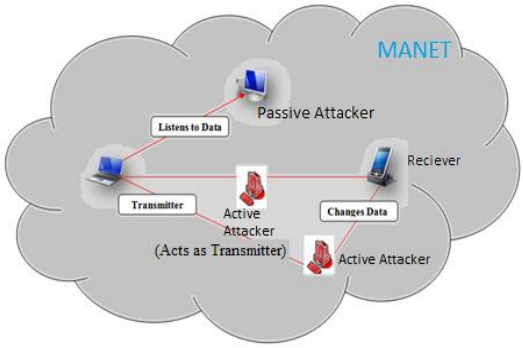

Fig 1: Active & Passive attacks in MANETs

Active attacks are classified into four groups:

- ***Dropping Attacks:*** Compromised nodes or selfish nodes can drop all packets that are not destined for them. Dropping attacks can prevent end-to-end communications between nodes, if the dropping node is at a critical point [13]. Most of routing protocol has no mechanism to detect whether data packets have been forwarded or not.
- ***Modification Attacks:*** Sinkhole attacks are the example of modification attacks. These attacks modify packets and disrupt the overall communication between network nodes. In sinkhole attack, the compromised node advertises itself in such a way that it has shortest path to the destination. Malicious node than capture important routing information and uses it for further attacks such as dropping and selective forwarding attacks.
- ***Fabrication Attacks:*** In fabrication attack, the attacker send fake message to the neighbouring nodes without receiving any related message. The attacker can also sends fake route reply message in response to related legitimate route request messages.
- ***Timing Attacks:*** In this type of attacks, attackers attract other nodes by advertising itself as a node closer to the actual node. Rushing attacks and hello flood attacks uses this technique.

III. TYPES OF ACTIVE ATTACKS ON VARIOUS LAYERS IN PROTOCOL STACK

The characteristics of MANETs make them susceptible to many new attacks. These attacks can occur in different layers of the network protocol stack.

Table 1: Attacks on the Protocol Stack

Layer	Types of Attacks
Application	Malicious code, Data corruption, viruses and worms
Transport	Session hijacking attack, SYN Flooding attack
Network	Blackhole, wormhole, Sinkhole, Link spoofing, Rushing Attack, Replay attacks, Link Withholding, Resource Consumption Attack, Sybil attack
Data Link	Selfish misbehaviour, malicious behaviour, traffic analysis
Physical	Eavesdropping, jamming, active interference

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

A. Attacks at Physical Layer

The attacks on physical layer are hardware oriented and they need help from hardware sources to come into effect [4]. 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.

1) Eavesdropping

Eavesdropping can also be defined as interception and reading of messages and conversations by unintended receivers [4]. As the communication takes place on wireless medium can easily be intercepted with receiver tuned to the proper frequency. The main aim of such attacks is to obtain the confidential information that should be kept secret during the communication. The information may include private key, public key, location or passwords of the nodes. Classified data can be eavesdropped by tapping communication lines, and wireless links are easier to tap.

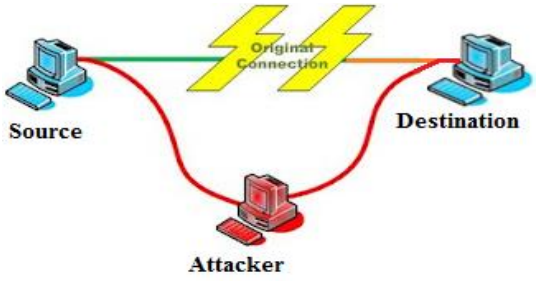

Fig 2: Attacker attack on communication between Source and destination

2) Jamming

Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication. In this type of attack, the jammer transmits signals along with security threats. Jamming attacks also prevents the reception of legitimate packets.

3) Active Interference

An active interference is a denial of service attack which blocks the wireless communication channel, or distorting communications. The effects of such attacks depend on their duration, and the routing protocol in use [3, 4]. Attacker can change the order of messages or attempt to replay old messages. Old messages may be replayed to reintroduce out of date information.

B. Attacks at Data link / MAC layer

The algorithms used in data link layer/MAC layer are susceptible to many DoS attacks. MAC layer attacks can be classified as to what effect it has on the state of the network as a whole [4]. The effects can be measured in terms of route discovery failure, energy consumption, link breakage initiating route discovery and so on. The misbehaviour of a node can be purely in selfish interest or with malicious intents.

1) Selfish Misbehaviour of Nodes

Attacks under this category, are directly affects the self-performance of nodes and does not interfere with the operation of the network [4]. It may include two important factors.

- Conservation of battery power
- Gaining unfair share of bandwidth

The selfish nodes may refuse to take part in the forwarding process or drops the packets intentionally in order to conserve the resources. These attacks exploit the routing protocol to their own advantage. Packet dropping is one of the main attacks by selfish node which leads to congestion in network. However most of routing protocols have no mechanism to detect whether the packets being forwarded or not except DSR (dynamic source routing).

2) Malicious Behaviour of nodes

The main of malicious node is to disrupt normal operation of routing protocol. The impact of such attack is increased when the communication takes place between neighbouring nodes. Attacks of such type are fall into following categories.

- *Denial of Service (DoS):* These types of threats produced a malicious action with the help of compromised nodes that forms severe security risks. In the presence of compromised nodes, it is very difficult to detect the compromised routing. The compromised route appears like a normal route but leads to severe problems. For example, 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, in order 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 information that was intended for owner of the address. A malicious node may advertise fake route request, so that other nodes will then direct route replies to the node.
- *Attacking neighbour sensing protocols:* malicious nodes advertise fake error messages so that important links interface are marked as broken. This will result in decrease in network throughput and quality of service.

3) Traffic Analysis

In MANETs the data packets as well as traffic pattern both are important for adversaries. For example, 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 an destination nodes

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

C. Attacks at Network Layer

The network layer protocols enable the MANET nodes to be connected with another through hop-by-hop [3, 4, 10]. In MANETs every individual node takes route decision to forward the packet, so it's very easy for malicious node to attack on such network. The basic idea behind network layer attacks is to inject itself in the active path from source to destination or to absorb network traffic. In such attacks, the attackers can create routing loops to form severe congestion. Different type of attacks are identified which are initiated by malicious node. The malicious node "X" can absorb important data by placing itself between source "A" and destination "D" as shown in fig 3. "X" can also divert the data packets exchanged between "A" and "D", which results in significant end to end delay between "A" and "D". In this type of attacks attackers attacks against Routing and Path Selection

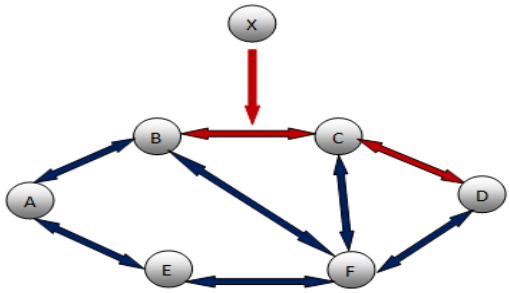

Fig 3: Routing Attack by Malicious Node

The malicious node can disrupt the route discovery process by creating routing loops and overflow routing tables.

1) Blackhole Attack

In this type of attacks, malicious node claims having an optimum route to the node whose packets it wants to intercept. On receiving the request the malicious node sends a fake reply with extremely short route [11]. Once the node has been able to place itself between the communicating nodes, it is able to do anything with the packets passing between them. For example, in fig.4, 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. The malicious node "4" when receives the route request, it immediately sends response to source. If reply from node "4" reaches first to the source than the source node "S" ignores all other reply messages and begin to send packet via route node "2". As a result, all data packets are consumed or lost at malicious node.

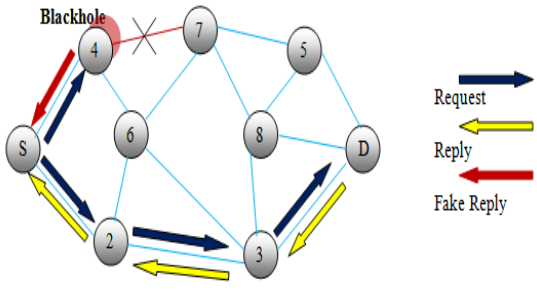

Fig 4: Blackhole Attack

2) Rushing Attack

Rushing attacks are mainly against the on-demand routing protocols. These types of attacks subvert the route discovery process. On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack [3, 6]. 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 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 do those from other nodes. This result in when neighbouring node of "D" i.e. "7" and "8" when receive the actual (late) route request from source, they simply discard requests. So in the presence of such attacks "S" fails to discover any useable route or safe route without the involvement of attacker.

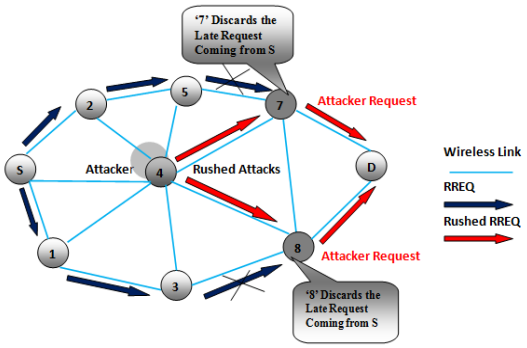

Fig 5: Rushing Attack

3) Wormhole Attack

In wormhole attack, malicious node receive data packet at one point in the network and tunnels them to another malicious node. The tunnel exist between two malicious nodes is referred to as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. Attackers use wormholes in the network to make their nodes appear more attractive so that more data is routed through their nodes [7, 8]. When the wormhole attacks are used by attacker in routing protocol such as DSR and AODV, the attack could prevent the discovery of any routes other than through the wormhole. If there is no defence mechanism are introduced in the network along with routing protocols, than existing routing protocols are not suitable to discover valid routes. For example in fig.6, the nodes "X" and "Y" are malicious node that forms the tunnel in network. The source node "S" when initiate the RREQ message to find the route to node "D" destination node.

The immediate neighbour node of source node "S", namely "2" and "1" forwards the RREQ message to their respective neighbours "5" and "X". The node "X" when receive the RREQ it immediately share with it "Y" and later it initiate RREQ to its neighbour node "8", through which the RREQ is delivered to the destination node "D". Due to high speed link, it forces the source node to select route <S-1-8-D> for destination.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

It results in "D" ignores RREQ that arrives at a later time and thus, invalidates the legitimate route <S-2-5-7-D>.

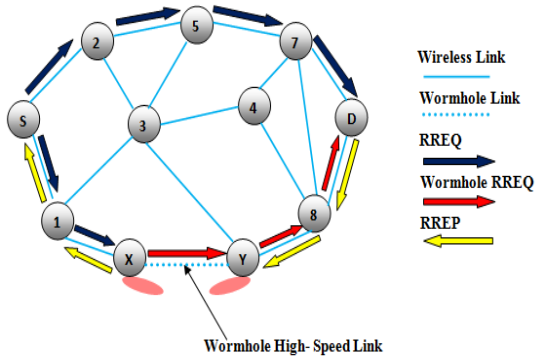

Fig 6: Wormhole Attack

4) *Sinkhole Attack*

Sinkhole attack is one of the severe attacks in wireless Ad hoc network. In sinkhole Attack, a compromised node or malicious node advertises wrong routing information to produce itself as a specific node and receives whole network traffic. After receiving whole network traffic it modifies the secret information, such as changes made to data packet or drops them to make the network complicated. A malicious node tries to attract the secure data from all neighboring nodes. Sinkhole attacks affects the performance of Ad hoc networks protocols such as AODV by using flaws as maximizing the sequence number or minimizing the hop count [9,10]. In this way the path presented through the malicious node appears to be the best available route for the nodes to communicate. In DSR protocol, sinkhole attack modifies sequence no in RREQ.

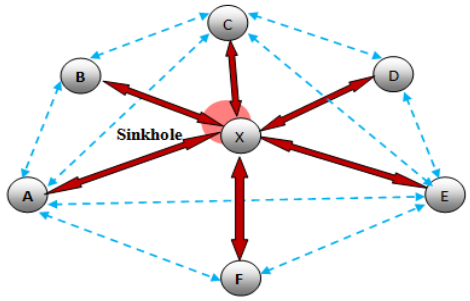

Fig 7: Sinkhole attack

5) *Replay Attacks*

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

6) *Link Withholding & Link Spoofing Attacks*

In link withholding attack, the malicious node does 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 the fake route information to disrupt the routing operation [7]. It results in, malicious node manipulate the data or routing traffic.

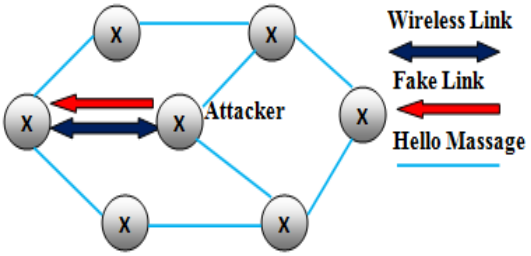

Fig 8: Link Spoofing

7) *Resource Consumption Attack*

In 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 [7]. These types of attacks are also known as sleep deprivation attack and mainly occur against the devices that don't offer any services to the network.

8) *Sybil Attack*

In Sybil attack, Sybil attacker may generate fake identities of number of additional nodes. In this, a malicious node produces itself as a large number of instead of single node. The additional identities that the node acquires are called 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:

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

D. *Attacks at Transport Layer*

1) *Session Hijacking*

Attacker in session hijacking takes the advantage to exploits the unprotected session after its initial setup. In this attack, the attacker spoofs the victim node's IP address, finds the correct sequence number i.e. expected by the target and then launches various DoS attacks. In Session hijacking, the malicious node tries to collect secure data (passwords, secret keys, logon names etc) and other information from nodes. Session hijacking attacks are also known as address attack which make affect on OLSR protocol.

Fig 9: Session hijacking

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The TCP-ACK storm problem may occur when malicious node launches a TCP session hijacking attack. The attacker "X" injects session data, and node "1" sends acknowledgement packet to node "2". Packet will not contain any sequence number that node 2 is expecting. It results in, when node "2" receive the packet and tries to resynchronize the TCP session with node "1". This process is repeated over and over 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.

2) SYN Flooding Attack

The SYN flooding attacks are the type of Denial of Service (DoS) attacks, in which attacker creates a large number of half opened TCP connection with victim node. These half opened connection are never completes the handshake to fully open the connection.

E. 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, TALNET and FTP, which provides many vulnerabilities and access points for attackers.

1) Malicious code attacks

Malicious code attacks include, Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application.

2) Repudiation attacks

Repudiation refers to a denial of participation in all or part of the communications. Many of encryption mechanism and firewalls used at different layer are not sufficient for packet security. Application layer firewalls may take into account in order to provide security to packets against many attacks. For example, spyware detection software has been developed in order to monitor mission critical services.

IV. SECURITY GOALS

The goal of system security is to have controlled access to resources. The key requirements for networks are confidentiality, authentication, integrity, non repudiation, and availability [13, 14].

- *Confidentiality:* it protects data or a field in message. It is also required to prevent an adversary from traffic analysis.
- *Integrity:* it ensures that during transmission the packets are not altered.
- *Authorization:* it authorizes another node to update information or to receive information.
- *Availability:* it ensures that services are available whenever required.
- *Resilience to attacks:* it is required to sustain the network functionalities when a portion of nodes is compromised or destroyed.
- *Freshness:* it ensures that malicious node does not resend previously captured packets.
- *Anonymity:* this service helps for data confidentiality and privacy.
- *Access control:* it prevents unauthorised access to a resource.
- *No repudiation:* No repudiation prevents the source from denying that it sends the packet.

V. CONCLUSION AND FUTURE WORK

Due to dynamic infrastructure of MANETs and having no centralized administration makes such network more vulnerable to many attacks. In this paper, we discuss about how different layers under protocol stack become vulnerable to various attacks. These attacks can classified as a active or passive attacks. Different security mechanisms are introduced in order to prevent such network. In future study we will try to invent such security algorithm, which will be installed along with routing protocols that helps to reduce the impact of different attacks.

VI. ACKNOWLEDGEMENT

We are grateful to Shaheed Bhagat Singh College of Engineering & Technology, Ferozepur (India) for providing continuous support throughout the work.

REFERENCES

[1] Mohammad Ilyas, "The Handbook of Ad Hoc Wireless Networks",
[2] Amitabh Mishra, "SECURITY AND QUALITY OF SERVICE IN AD HOC WIRELESS NETWORKS" (chapter 1, 3), ISBN- 13 978-0-521-87824-1 Handbook.
[3] Zubair Muhammad Fadlullah, Tarik Taleb, and Marcus Schöller, "Combating against Security Attacks against Mobile Ad *Hoc* Networks (MANETs)".
[4] Vikrant Gokhale, S.K.Gosh, and Arobinda Gupta, "Classification of Attacks on Wireless Mobile *Ad Hoc* Networks and Vehicular *Ad Hoc* Networks *a Survey".*
[5] Kamanshis Biswas and Md. Liakat Ali, "Security Threats in Mobile Ad Hoc Network".
[6] Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks - A Survey".
[7] 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, 4063-4071
[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] Kisung Kim and Sehun Kim, "A Sinkhole Detection Method based on Incremental Learning in Wireless Ad Hoc Networks".
[10] Ad hoc network specific attacks held by Adam Burg.
[11] Akanksha Saini, Harish Kumar, "Effect of Black Hole Attack on AODV Routing Protocol in MANET".
[12] Sevil ¸ Sen, John A. Clark, and Juan E. Tapiador, "Security Threats in Mobile *Ad Hoc* Networks".
[13] Panagiotis Papadimitratos and Zygmunt J. Haas "Securing Mobile Ad Hoc Networks".
[14] Dan Zhou "Security Issues in Ad Hoc Networks".
[15] C. Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols".

Gagandeep has received his B.Tech. Degree in Computer Science and Engineering in 2011 from Guru Teg Bahadur Khalsa Institute of Engineering & Technology, Malout, Punjab (India). He is currently pursuing M.Tech in Computer Science and Engineering at Shaheed Bhagat Singh, State Technical campus, Ferozepur, Punjab (India), His areas of interest in research are Network Security and Cryptography, Digital Image Processing

Aashima has received her B.Tech. Degree in Information Technology in 2011 from Lala Lajpat Rai Institute of Engineering & Technology, Moga, Punjab (India). She is currently pursuing M.Tech in Computer Science and Engineering at Shaheed Bhagat Singh, State Technical campus, Ferozepur, Punjab (India), Her areas of interest in research are Network Security and Data Mining, Digital Image Processing.

Pawan Kumar has received his B-tech degree in Computer Science & Engineering from Giani Zail Singh college of Engineering & technology Bathinda, Punjab, India in 2004 and Master Degree in from Lovely Institute of Engineering & Technology, Phagwara, India in 2012. Since 2005 he has been with Shaheed Bhagat Singh College of Engineering & Technology, Ferozepur, Punjab, Where he is currently working as an Assistant Professor in the Department of Computer Science & Engineering. His current research interest includes Data Mining and Information security.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)