IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-6, Issue-8, Aug 2018 E-ISSN: 2347-2693

Different Attacks and their Defense Line in Mobile Ad hoc Networks: A Survey

P. Gupta[1*], P. Bansal[2]

[1]Research Scholar, IET, DAVV, Indore, India
[2]Professor, IT Department, IET, DAVV, Indore, India

[*]*Corresponding Author: praveen.gupta@live.com Tel No:+91-9893091192*

Available online at: www.ijcseonline.org

Accepted: 15/Aug/2018, Published: 31/Aug/2018

***Abstract*—** Mobile Ad hoc Network (MANET) provides on the fly solution for those areas where wired network implementation is difficult. MANETs are network without infrastructure. They do not have central control. All nodes help each other in data communication. The life span of MANET is very small. The main features of MANET are: nodes are dynamic in nature resources availability in scarce and open channel. Due to resource scarcity some nodes may not provide their services to other nodes and some nodes may not participate in data transmission, to save their resources and they become selfish node. MANETs are susceptible for attacks. The open channel, resource scarcity and deployment type of network attract intruders for malicious activities. This survey paper has reviewed various articles from 1999 to 2018, in the view to look at how malicious nodes in a network make attacks on other nodes and what impact goes on network.

Earlier work have been discussed about one or two types of attacks. This paper has studied and tried to bring all attacks under the one umbrella. The paper discussed these attacks in following categories: External and internal, active and passive, at protocol stack layer, security goals, attacks affecting routing. This paper also come along with defense line, have been proposed by various researchers for different attacks. Paper also tries to put attacks and their effect on one place. It includes type of attack, status of attacker, interaction, layer and security goals. It is suggested that what type of, defense, line of action should be taken, so that a network must sustain in adverse situation and available for its users.

***Keywords*—**Wireless, Ad hoc, attack, security, defense, countermeasures.

I. INTRODUCTION

Ease of communication via MANET making them popular. These networks are broadly classified in two modes: Infrastructured mode and ad hoc mode. Communication in infrastructure mode is done with the help of centralized node called Access Point (AP). Access Point forwards data from one node to other nodes in network. Fig-1 shows the illustration of infrastructured and ad hoc networks.

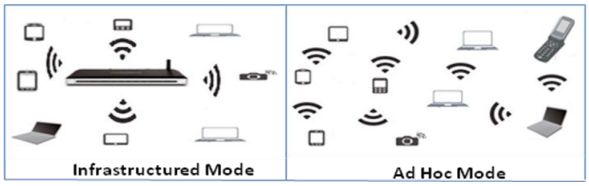

Figure 1. Wireless Network

MANET is self-organized network. Nodes communicate over common channel of the network. Node/s in the network works as a router. A node sends its own data as well as forwards data of other nodes of the network.

[1-3][8,9][12][19][23][25][37][48][55][59,60][64,65][68-70][72]. Resources in MANET are in scarce. Bandwidth, battery power, memory and computation power are considered to be major resources of MANET. Scarcity of resources sometimes makes a node or network unavailable to user.

Nodes are mobile in MANET. They form dynamic topology. They frequently change their position. The exact place of a node in the network is unpredictable. Frequent flow of routing information in the network consumes major part of available bandwidth and battery power of a node [3][8][12][25][33][36][48][53][59-61][70].Basic features of MANET make them suitable for various situations where normal wireless network or wired network deployment is not easy. It includes military operations, hostile operation, natural calamity situation, rescue operations, naxalite areas (In India context), coal mining, conference room, class room etc. There are many more situations, where implementation of MANET is beneficial[3][18][24][36][40,41][48][53][55][60][67][69][72] .

Figure 2. Application area of MANET

Fig-2 shows some application areas of MANET. Nodes, used in such situations may be homogeneous or heterogeneous. The different nodes can be: laptop, smart phones (Phablet), palmtops, Personal Digital Assistant (PDA) and different types of sensor. Security threats are easily possible in MANET. Unauthorized or compromised node does harmful activities in the network. Such types of node are not easily identifiable.

Sometimes node/s do not want to spend their resources for others and may not participate in network activities, such nodes are classified as selfish nodes. Selfishness of a node affects the working of network. Nodes who deliberately performed this activity are termed as malicious nodes [3,4][18,19][29][37][44][46][48][52][59][61,62][68,69].

It is very important to understand the situation for network deployment and then to prepare the nodes for communication. It is an essential task that decides the modus operandi of a network. Sometimes a well and pre planned networks are established to achieve its desired goal without any complications; on the other hand, situation may arise where sudden deployment of network required higher security. In such situation, there is no clear picture of surrounding environment and the presence of malicious node. The above discussions show that there is need to construct strong security measures for MANETs that give both defense and required network performance.

This survey includes research paper from 1999 to 2018. This time span has covered almost various types of attacks that are possible on MANET and its impacts on it. The major development in security issues and solutions grow in this time span, though a concrete solution is not available till date. The remaining paper covers in following sections. Section II discusses the challenges in MANET. Section III discusses general security features of any wireless networks. Section IV gives the literature review, Section V gives findings and discussions section VI gives the defense line and section VII discusses the conclusion and suggestion for work.

II. CHALLENGES IN MANET

As it has discussed so far that MANET are susceptible for network threats. The major problems for attacks and threats are: open wireless channel, resource scarcity, absences of central authority, nodes are dynamic in nature and they can be easily compromised.

According to its deployment MANET faces many problems during its working. In military operation it is desired to have very high secure communication in deployment area. In such area location disclosure of a node is big threat.

In other deployment like hostile operation a malicious node may spoof address of a node. Similarly monitoring and analysis of traffic by an external entity may create problem. A malicious node can use this information in future. Some of the major attacks in any MANET is on routing information or in data transmission. In both categories an adversary can alter or add information by many ways.

Other problem is the dynamic topology, it affects network in many ways, first, movement of a node from one area to other breaks the communication going through it. Second, this movement may require new authentication process for a node in a new area. Third, nodes require frequent route details updation, which also consumes time and resources of network. Fourth, in a larger network a node may be compromised by other nodes and will not participate in data forwarding task.

Various types of attacks under these categories disturb the working of network. These problems required security measures that spread on multiple nodes to provide defense line over the entire network.

III. General Security Features of Wireless Networks

Security in any wireless network is a primary concern. Security measures are required to define aspects of network security. Securing an MANET is a challenging work. Fig-3 depicts basic security features for wireless network[2] [4] [7][9] [18,19] [23] [25] [31,32] [40] [43] [47] [49] [59-61] [66][69] [72].

3.1 Privacy: It is also called confidentiality. MANETs have open channel for all users and eavesdropping may possible in the network. A message must be encrypted so that others cannot read its contents.

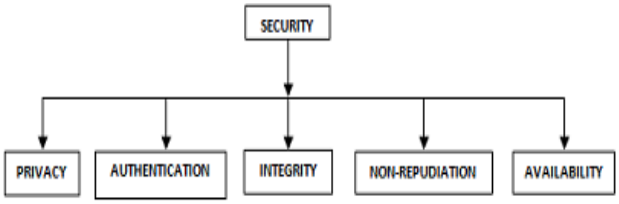

Figure 3. Security Goals

3.2 Authentication: Only an authorized user is capable to send or receive data in the network. Here intention is to keep the message safe. Receiver can determine the origin of the message and an intruder cannot impersonate.

3.3 Integrity: When message flows across the network an attacker not only see the message but can modify it. It is important that message is not tampered during transmission.

Receiving node must be able to confirm that the message has not been modified in transit.

3.4 Non-repudiation: This attribute assures that a sender should not be able to deny that a message was not sent by it.

3.5 Availability: It defines the availability of the network and its services both. It ensures survivability of the network.

IV. LITERATURE SURVEY

MANETs are deployed on the fly fashion. Military and hostile operations are most suitable application area of MANET. As it has been discussed that few characteristics of MANET makes it vulnerable. It is required to keep it free from attacks. One cannot expect same security level as available in wired network. Security issues for MANET are gaining popularity among researchers. Many researchers have classified security issues in various ways. Each has given emphasis on specific categories. After analyzing and study of other researcher's work, this paper broadly grouped attacks in following categories:

1. External and Internal
2. Active and Passive
3. Protocol Stack Layer
4. Security Goals
5. Attacks affecting Routing

The literature reviews of various attacks are discussed below:

4.1 External and Internal Attacks:

These attacks are categorized as per the position of the node in the network. Source of attack in the network either may be from inside of network or may be from outside of network [3][17][19][31][34][42][47,48][59-61][65][69].

An external attacker, is an unauthorized node that wants to access resources of network. These nodes can interrupt the services of network in many ways like by signal jamming, inserting packets to congest the network traffic, inserting false route details. Threats by external attacks are broadly classified as eavesdropping, monitoring, traffic analysis, forge route etc. External attacks are slow and do not damage network directly. While indirectly, it can be very dangerous because, leaking some information in the network without harming the current flow and network does even not know it. An internal node may be compromised by an external node or nodes to perform illegal activities.

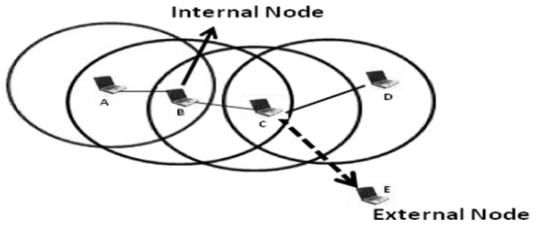

Figure 4. Node Position

In fig-4 node 'C' is an internal authorized node that do malicious activity. It forwards data to an external node 'E'. Sometimes an internal node does not want to actively participate in the network activities i.e. it can deny to provide its services to other; it is named as Denial of Services (DoS) attack. The reason for DoS may be that the node wants to preserve its resources like battery power, band width, computational capability etc. These types of nodes are called selfish node [2][4][6,7][12-14][17][21][29-31][33][36][38] [41][43][45][47][51,52][58][60,61][66,67].

Internal attacks are fast and give a direct impact on working of network. They give a higher level of threats and they are not easily recognized. The major internal attacks are flooding, resource consumption activities, wormhole, blackhole, greyhole, byzantine etc. These attacks are discussed in details in next section.

4.2 Active and Passive Attacks:

Previous section discussed the position of node in network. External or internal attackers are involved directly or indirectly to damage the working of network. Attacks can be divided in active and passive mode [3][6][8][10][17][19][23] [25][29][31][33,34][43][47,48][59-61][65][67][69].

In both the mode, node is either part of network or an outsider. In passive mode, a malicious node does not perform harmful activities that directly change the data. It can analyze the flow of data in the network. Main objective of such activities is to discover important information that can be used later. In this category, e.g. a node can listen authentication process going on between two nodes or it may observe the encryption/decryption pattern used in network. Discovery of such type of node or attack is very difficult. Major passive attack is eavesdropping attack. As MANET works in open channel environment. Attack mostly occurs at the physical layer of protocol stack.

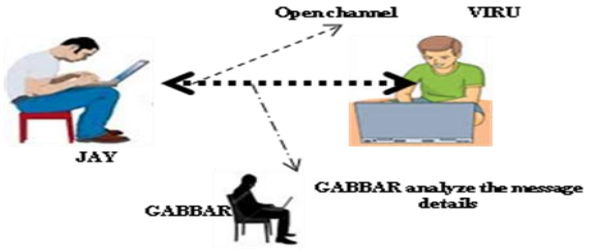

Figure 5. Passive Attacks

Fig-5 shows how these attacks are occurred in network. In active mode a malicious node either part of network or an outsider. These nodes alter the data, flowing in the network. Their motto is to degrade the network performance or to steal important information. The attacks come under active attack category are: DoS, fabrication, modification, interception, message alteration, flooding, routing data replay etc. These attacks are occurred majorly at physical layer, network layer, transport layer and application layer of protocol stack. In fig-

6 an intruder (Gabbar) is acting as man in middle and trying to capture information by spoofing.

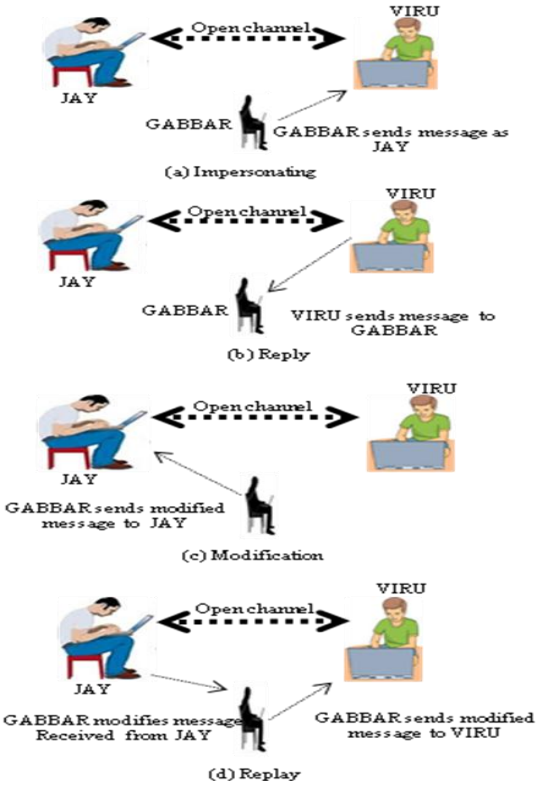

Figure 6. Active Attacks

The most dangerous attack is DoS. This attack makes services unavailable by draining resources of other nodes. In a MANET, DoS attacks can be done by consuming node's battery power or bandwidth by providing it too much job. Nodes without resources are of no importance and a network with such nodes does not provide services to its users [72].
In fig-7, a node 'C' becomes selfish node and it denies to participate in network activities to save its resources. In other scenario node will not forward incoming packet and dropped them.

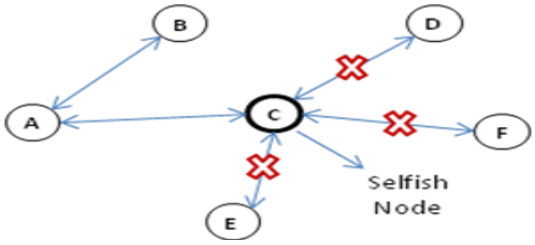

Figure 7. Denial of Service

Some other DoS attacks are: jamming, sleep deprivation, packet replay, routing table overflow, wormhole, greyhole, rushing etc. [1,2][6][11][14-17][19][23][28][31][40][45][47, 48][51-53][56][59][61][65][69][71,72].

4.3 Protocol Stack Layer Attack:

It is another dimension to look into attack on various layers of network. This classification helps us to understand the type of attack and their effects. So far it has been discussed that attack can be active or passive or by node's position in the network (internal) or an outsider (external). It is important on technical point of view to know that which part of protocol stack is affected most and which type of vulnerability occurs in network.

Physical layer deals with flow of raw bit transmission in the network. A malicious node may produce jamming signal to interrupt the activities. At data link layer, a node may monitor and analyze the traffic pattern of network. Network layer is backbone of any network. Basic job of network layer is routing and IP addressing. As nodes are mobile in nature, it is necessary to have the current location of node in the network for data forwarding. A malicious node/s may present false route details to capture the floating data. Other attacks at this layer are: replay attack, packet flooding, routing table over flow, black hole, warm hole, byzantine, Sybil, impersonation etc [2,3][17][19][23][29][33][36][47][64][70].

Transport layer provides end to end communication in the network. The major threat at this layer is session hijacking, as unauthorized node may want to access resources of the network. Application layer provides interface to its users. Virus, warms, trojan attacks are possible to degrade the network performance and sometimes makes network unavailable.

Table 1. *Protocol Stack and Attacks*

LAYER	WORK of LAYER	ATTACK
Application	Application Interface	Worm, Trojan Attacks, Virus, Repudiation, DOS.
Transport	End to end Communication	Session Hijacking, SYN Flooding, DOS.
Network	Routing, Logical Addressing (IP Addressing)	Modification, Fabrication, Flooding, Sybil Impersonation, Blackhole, Wormhole, Greyhole, Byzantine, False route information, Location disclosure, Routing table overflow DOS etc.
Data link	Flow control, Error Control, Physical Addressing	Traffic monitoring and Analysis, DOS.
Physical	Raw bit Transmission	Signal Jamming, Eavesdropping, DOS.

Table-1 summarizes the basic work of each layer and also shows different types of attacks that occur at all layers of

protocol stack. It has been analyzed that network layer is having maximum number of threats among all protocol stack layers.

From table-1, it has found that some attacks are multi layer attacks. They appeared at two or three layers of protocol stacks. First attack is DoS. It occurs at all the layers of protocol stack. At physical layer it is done by signal jamming, at data link layer channel is occupied or get busy by malicious node, at network layer routing process is interrupted by many ways which will discussed in detail in next section, at transport layer session hijacking and SYN flooding are most common techniques to disturb the working of a node. At application layer repudiation and other virus attacks are possible.

The second multi layer attack is impersonations or spoofing. It is occurred at Medium Access Control (MAC) layer, network layer and transport layer. On these protocol stack layers, a malicious node spoof either MAC address or IP address or Port address of a legal node or it do link spoofing. In fig-8, a malicious node 'T' sends route details by advertising that it has a direct link to node 'H'. This information may lead to incorrect route details in neighbors routing table. It also termed as cache poisoning.

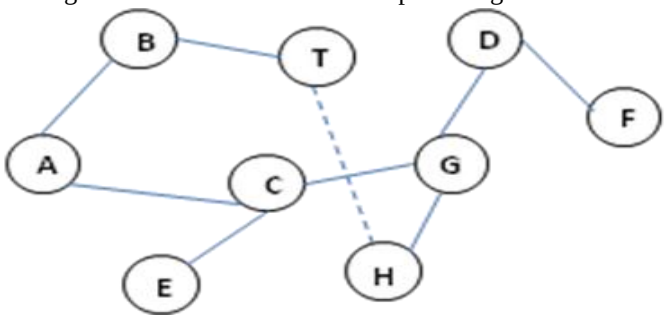

Figure 8. Link Spoofing

The third multi layer attack is man in middle attack; a malicious node positioned between sender and receiver and can steal the information or impersonate other nodes to get information from either side.

4.4 Attacks at Security Goals:

Any wireless networks have following basic security features: Privacy, Authentication, Integrity, Non-repudiation and Availability. These factors make sure that any wireless network provides its services without interruption to achieve its goals. There are many attacks that give its direct or indirect impact on these security goals. Let's discuss these goals one by one: [2][4][7][9][18,19][23][25][31,32][40][43][47][49][59-61][66][69][72].

4.4.1 Privacy

It ensures that information is always reached to receiver. It is highly required in military operations. Location disclosure and message content disclosure will give an adverse effect in such condition. A malicious node can use sniffing i.e. it may steal information flowing in network like login id, passwords, files, routing details etc.

4.4.2 Authentication

It is the most important feature of security goal. Only an authorized user is allowed to access network resources. An unauthorized node in network slowly compromises other nodes and after some time takes the control of network. Impersonation (IP spoofing, MAC Spoofing and TCP spoofing) is the methods that do this activity. In rushing attack (A node request at high speed and catch the route request first generated by destination node in network, modifies it and retransmits it) the route details may have malicious node between sender and destination. This node catches the routing data or message, alter it and then forward to other nodes. It becomes essential to authenticate a node at the entry level to avoid such activities.

4.4.3 Integrity

This feature gives assurance to a user that message will not be changed during transmission. A malicious node may capture all incoming data, modified user data or route details to misguide the other user.

A malicious node may propagate fake message that may include modified sequence number, hop count, or move network traffic to a specific node, it is called Detour. In misrouting, an unauthorized node can send message to a wrong destination in network by changing the given address. A node can act as man in middle; this node situated between two other nodes and can alter the message flowing between sender and receiver nodes.

4.4.4 Non-repudiation

A sender node after data transmission cannot deny that it is not the originator of message. This feature ensures that message generators identity. A compromised node in the network may send the erroneous message and later on, it can deny.

4.4.5 Availability

It implies that network and its services must be available as and when required. Network services may not be available by DoS or by dropping incoming packets. A malicious node can do network jamming, produces false route information that either route to destination node is not available or node itself is a mediator node towards the destination node. Other attacks causes unavailability are: fabrication, it includes black hole, gray hole, routing table poisoning, resource depletion (A malicious node which causes more energy consumption). Tunneling (When two or more nodes exchange data using available routes in network). Fig-9 shows different attacks that affect the security goals of MANETs.

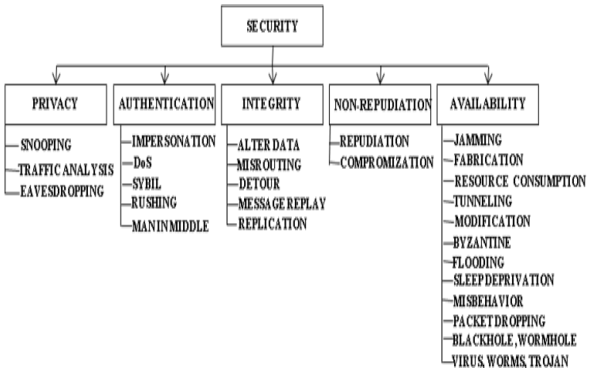

Figure 9. Attack at Security Goals

4.5 Routing Attacks

Nodes in MANET are dynamic in nature. It often changes its position hence network topology also changes. Routing details in network establish relationship among the nodes. This category of attacks is included as it has been realized that the majority of the attacks generally occur at the network layer [2] [6] [10] [12] [19] [22,23] [29] [31] [33,34] [40][47,48][52,53][59][61][64, 65][68,69].

Routing attacks are possible in many ways. A malicious node may attack during packet delivery or it may attack during flow of routing detail. The main plan of any attacker is to divide the network or make network unavailable to user. It can create loop in the network, it also does other malicious activities to consume resources. During packet forwarding process, a malicious node either drops the packet to save its own resources or perform DoS where a node sends too many packets to exhaust battery power of other node.

In broad sense researchers have majorly categorized routing attacks in: impersonation, fabricating, modification, flooding, interruption, interception, rushing the routing messages. The above mentioned attacks are below described in brief:

4.5.1 Impersonation:

It is also termed as spoofing. In this attack a malicious node either uses MAC address or IP address or TCP port address of any other node of the network. By doing this a malicious node can receive/send data of other node. The span of this attack is from data link layer to transport layer. The other attacks in this category are discussed below:

Man in Middle: A malicious node situated between sender and receiver. It impersonates these nodes by claiming as a sender to receiver and as a receiver to the sender [2][10][23][31][40][47].

Sybil: It is a dangerous attack in network. A malicious node impersonates and uses identity of non-existent node. It can create multiple identities and work in network [2][6][10][12][29][31][48][52].

Session Hijacking: An attacker impersonates the target node's IP address, find out the correct sequence number of TCP session that is expected by the receiver, and then performs a DoS attack on the victim [23][29][40][47].

4.5.2 Fabrication

In such attacks a malicious node delivered fake route details to other nodes even a reply is not requested from this node. Fabrication in data is also possible by these nodes. Fig-10 shows how a malicious node 'X' shows that it has best route to the other node and later may it will drop or modify the packets received from other nodes.

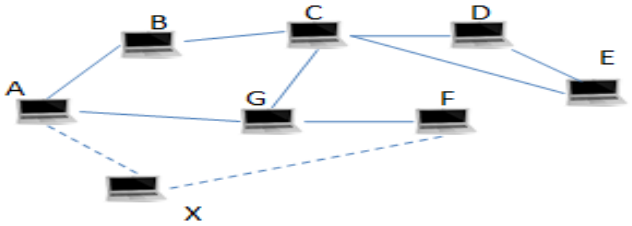

Figure 10. Routing Attack

Some most known attacks in this category are:

Blackhole: A malicious node catches the route request and in reply, declares that it has shortest path towards the destination. This activity is done to transfer all the network traffic from it. Later the node may drops the packet or analyze the data for further use [6][12][17][21][24,25][40, 41][43][53].

Greyhole: It is also termed as selective forwarding attack. An attacker node either drops all or some data packets of all neighbors or specific node. It can be DoS attack for other nodes [1][6][11][14][31][72].

Rushing attack: A node catch the route request generated by other node in network, and transmit it very fast to destination node. The reply got from destination, modified and retransmits in the network by this node. This route detail has a malicious node that catches the data [1][6][11][14,15][21][25,26][29][41][45][47][51,52][54].

Resource Consumption: A malicious node consumes resources of other legitimate nodes by sending too many route request or data packets for forwarding. This attack slowly and gradually removes nodes as they are out of resources [2][6][12][19][23][29][31][40][47][52][64].

Routing Table Poisoning: An attacker creates fabricated route details to other genuine nodes. These details can have long route, route may have congestion or even some routes may not exist, this misleads the flow of packets [25][31][40][47][52].

Routing Cache Poisoning: This attack is similar to routing table poisoning but in this case, an attacker fabricate route details present in cache [19][29][34][47][59][68].

Routing Table Overflow: The aim of attacker is to run over the routing table of a node. An attacker creates too many routes in network to prevent new route creation [1][6][15,16][19][25][29][47].

4.5.3 Modification

A malicious node/s attempt to alter packet information either by altering sequence number of packet or by increasing or decreasing the hop count of destination. It can also change the data of packet. Some attacks in this category are:

Detour: A malicious node includes false node in its route details so that all other nodes forward data packets through this route considering best path. These nodes can capture all incoming data and modified it. [31][40][52].

Sink hole: A malicious or compromised node aim to capture data from surrounding node/s. It can be done by floating route detail that claims it has best route. It is a severe attack in network and will result in major loss of data packets [2][12][19][29][47,48].

Misrouting Information: An unauthorized node can send message to wrong destination in network by changing the given address [36].

4.5.4 Replay

A malicious node replayed the routing details in network that can create problem for other nodes to differentiate this detail from real one [6][12][21][25][27][29][44][53][57].

The attacks in this category are:

Worm hole: In this attack there are two possibilities:

a. Malicious node transfers network traffic to other malicious node, that malicious node put back this packet after modification on the network.

b. Malicious node forwards data to an external node. Such attacks are difficult to detect.

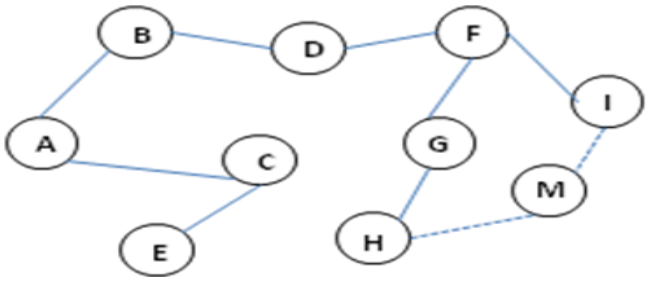

Figure 11. Wormhole Attack

In fig-11, malicious node 'M' creates a wormhole between node 'H' and 'I'. Node 'M' may forward data or control messages, after changes, between 'H' and 'I' [57][71]

Tunneling: In tunneling, data always flows between two specific nodes. This can be done by providing false route details [19][31][48][52][59][68].

4.5.5 Interruption:

In such attacks an attacker or malicious node either drops the data or routing packets of all or specific node of the network to interrupt the network services. Some major attacks in this category are discussed below:

Byzantine: Either single or many malicious nodes perform this attack in the network. These nodes either drop packets or forward network traffic on non-optimal path [7][23][29][34][40][47,48][52][64][69].

These nodes may also create loop in the network. These activities waste resources of many nodes in the network. It degrades the overall network performance.

The nodes are involved in byzantine attacks are authenticated nodes of network. They start misbehaving after words.

Route Packet Replication: An attacker produces old route information and flow it in the network to consume resources of other nodes [2][29][31][40].

Location Disclosure: In such attack, an attacker by eavesdropping (Traffic monitoring and analysis) find out the location of node/s. After sufficient amount of time it will have a clear picture of network [2][6][23][25][31][34][40] [47,48].

4.5.6 Interception

In such of type of attack an intermediate node, which is malicious and unauthorized accept data packets for forwarding and modifies the content. Majorly such activities are done at network layer specially with routing messages. It violates the rule of confidentiality or privacy. The major attacks in this category are blackhole and wormhole. The details for these attacks have been discussed earlier [23][29][31][34][47,48][65][68][71].

V. FINDINGS AND DISCUSSIONS

MANET's flexible characteristics helps to deploy it easily but they are susceptible to attacks. Robustness of a node decides the survivability of any network. Nodes are easily compromised and can be exhausted due to various attacks done by other malicious nodes.

Based on literature survey and analysis of different categories of attack in MANET, it is found that attacks are either active or passive in nature. An attacker may be part of network or an outsider. An unauthorized node may compromise other node/s in a network to degrade the performance of network. Such attackers are difficult to identify. Risk factor becomes high if attacker is part of network.

The outcome of study is summarized in table-2. This table comprises of various types of attacks, which has been discussed from section 4.1 to 4.5.

Table-2 describes the attack on following attributes: Type of attack, status of an attacker (internal or external), attacker's interaction (Active or passive), which layer of protocol stack,

is affected by these attacks. The security goal attribute defines on which security aspect attack, gives its impact.

Table 2. Major Attacks and its Implications

Type of Attack	Attacker Status	Interaction	Layer	Security Goals
Eavesdropping	Internal/External	Passive	Physical	Privacy
Monitoring	Internal/External	Passive	Data link	Privacy
Traffic analysis	Internal/External	Passive	Data link	Privacy
Snooping	Internal/External	Passive	Network/Application	Privacy
Jamming	Internal/ External	Active	Physical/Data link	Integrity, Availability
Man in middle	Internal	Active	Network	Authentication
Sybil	Internal	Active	Network	Authentication, Non-repudiation
Fabrication	Internal	Active	Network	Availability, Authentication
Sink/Black hole	Internal	Active	Network	Availability
Greyhole	Internal	Active	Network	Availability
Rushing	Internal	Active	Network	Authentication
Resource Consumption	Internal	Active	Network	Availability
Route Table Poisoning	Internal	Active	Network	Availability, Authentication
Route Cache Poisoning	Internal	Active	Network	Availability, Authentication
Route Table Overflow	Internal	Active	Network	Availability
Modification	Internal	Active	Network	Integrity
Detour	Internal	Active	Network	Integrity
Misrouting	Internal	Active	Network	Authentication, Integrity
Message Replay	Internal	Active	Network	Integrity
Tunneling	Internal/External	Active	Network	Availability
Warm hole	Internal	Active	Network	Availability
Byzantine	Internal	Active	Network	Availability
Location Disclosure	Internal	Active	Network	Privacy
Packet Replication	Internal	Active	Network	Authentication, Integrity
Packet flooding	Internal	Active	Network	Availability
Misbehaving	Internal	Active	Network	Availability
Sleep Deprivation	Internal	Active	Network	Availability
Packet Dropping	Internal	Active	Network	Availability
Selfishness	Internal	Active	Network	Integrity, Availability
Compromization	Internal/ External	Active	Data link / Network / Transport	Authentication, Non Repudiation
Impersonation (false node/ node replication) / Spoofing	Internal	Active	Data link/ Network / Transport	Authentication
Session Hijack	Internal/ External	Active	Transport	Availability
SYN Flooding	Internal	Active	Transport	Availability
Repudiation	Internal	Active	Application	Authentication, Non Repudiation
Virus/warms/Trojan	Internal/ External	Active	Application	Availability
DoS	Internal	Active	Multi-layer App	Availability, Authentication

From above given table following conclusion about the attacks can be drawn:

i) Attackers are part of the network i.e. they are internal nodes
ii) The attacks mostly occur at network layer.
iii) Maximum attacks are of active nature.
iv) The security goal that regularly affect is availability, it shows that after attacks either node/s or network is not available to its users.

As the attacker's position is inside of the network i.e. they are internal nodes. These attacks are majorly done by compromised or malicious node. It has become an essential task for network developer to have secure measures that put off it from various attacks. Next section gives the various proposed solution/s by researchers that try to mitigate problem from root.

VI. DEFENSE LINE

The characteristics of MANET make it prone for various type of attack. This paper has discussed all major possible attacks in following types, internal & external, active & passive, protocol layers' attacks, routing attacks and attacks affect security goals of network.

In any network design process, defining security mechanism is a challenging goal. It is essential to define defense line or countermeasures to protect network from such attacks [4][6][14][19,20][23][25][27][29][31][36,37][40][44][47][49][51][53][61][64].

It is well known that prevention is better than cure. Security for MANET can also be defined using both preventive and reactive mechanism. It is always better to have preventive techniques in network but it must also be consider that an intruder may attack in some other manner therefore some reactive plans should be defined to mitigate problems.

First common preventive technique that ensures entrance of node in the network is by putting strong authentication. If a network has strong authentication mechanism along with some credential system that check node's behavior timely. It helps to isolate such compromised node/s.

Second preventive way is using of firewall in the network but implementation of firewall in MANET is somewhat difficult. Third option is of using cryptography techniques. These are based on symmetric or asymmetric key. Cryptography maintains privacy, authentication and integrity. Threshold key cryptography or Public Key Infrastructure (PKI) can also be used but MANET characteristics do not support it fully. These techniques used heavy algorithms that are not suitable for ad hoc environment. Fourth, access control policy ensures rights of node what it can access freely and what it will not. Fifth, digital signature can also be applied at the initial level. Digital signature avoids fraud by an unauthorized node.

Reactive techniques may apply Intrusion Detection System (IDS), cooperation among the nodes, trust management etc. [4-6][19][24][29,30][47][58][63][66,67]. Main aim is to find a malicious node or an attack or both. Such node/s can be isolated from network by giving them negative credential or by invoking their certificates using IDS and trust management system. Various IDS techniques have been proposed to detect such nodes. Sometimes node/s in the network denies its participation in network activities, cooperative schemes or incentive schemes helps to encourage them to participate in network activities.

Some researchers have defined a third line of action called Intrusion Tolerance, it defines that network achieve its goal in presence of intruder, failures and various attacks. In other words, network must stay alive in these problems and its performance doesn't degrade.

Next given table-3 summarizes the attacks categories and their effect on specific security feature. A defense line for these attacks has been surveyed and various suggested security mechanism are outlined and presented in tabular format to defend the various attacks in MANETs.

Table 3. Major Attacks Category and Defense Line

Security Feature Affected	Type of Attack	Defense Line
i) to iv) Privacy **All attacks are passive in nature**	i) Traffic Monitoring ii) Traffic Analysis iii) Snooping iv) Eavesdropping	i)Encrypted messages provide security from such attacks [19][29][64]. ii)Encryption at data link layer helps to avoid traffic analysis. -Wired Equivalent Privacy (WEP) can be used for data hiding. -Probabilistic Geographic Routing (PGR) protocol avoids this attack. -By random communication between nodes [2][6][19] [29][47][56]. iii)Encrypted data avoid such attacks [31][40]. iv)Encrypted data avoid such attacks. -Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and Orthogonal Frequency Division Multiplexing (OFDM) can be used.

		-Asymmetric and Symmetric Cryptography can be used [6][19][29][31][37][40][47].
v) Integrity and Availability	v)Signal Jamming	v)FHSS, DSSS and OFDM can be used. -Intrusion Detection techniques for jammer can be used [6][19][29][37][40][47][56].
vi) Authentication	vi)Impersonation / Spoofing	vi) Strong authentication for node can be used [73]. -For authentication scheme protocol Authenticated Routing for Ad hoc Networks (ARAN) avoids such attack. -For link spoofing, use of Global Positioning System (GPS) is suggested but not appropriate for ad hoc scenario. -Secure Routing Protocol (SRP) is immune to MAC and IP address spoofing. -Secure Vector Machine (SVM) over Optimized Link State Routing Protocol (OLSR) can be used. -Various routing protocol have protection against impersonation they are: A Secure On-Demand Routing Protocol for Ad hoc Networks (ARIADNE), ARAN, Secure Ad hoc Routing (SAR), Secure Ad hoc On-Demand Distance Vector (SAODV), Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks (SEAD), SRP [6][10][29][31][37][40][47].
vii) Authentication	vii) Man in middle	vii) Secure Socket Layer (SSL) and Transport Layer Security (TLS) is used.
viii) Authentication and Non-repudiation	viii)Sybil	-Suggestions provide for impersonation attacks are also applicable here. -Strong authentication scheme for nodes can be used [10][31][40][47]. viii) Random key distribution between nodes can be used. Key validation for random key distribution avoids this attack.
ix)Availability and Authentication	ix) Fabrication	-One-way pseudo random hash function can be used. -A single node may know the IP address of others.
x) Availability	x)Blackhole	-Radio resource testing can be used. -Strong authentication for node will protect from this attack [2][6][31][56]. ix) Digital signature is one of the solutions.
xi)Availability	xi)Greyhole	-Various protocol like: ARIADNE, ARAN, SAR, SAODV, SEAD, SRP defend fabrication attacks [6][10][31]. x) Authentication mechanism is one approach.
xii)Authentication	xii)Rushing	-Key validation for random key distribution avoids this attack. -Confirm Route Request (CREQ), Confirm Route Reply (CREP) is used to avoid this attack. -SAR, SAODV protect from blackhole [2][37][40][47][53]. xi) Dynamic Source Routing (DSR) and Ad hoc On-Demand Distance Vector (AODV) protocols detect this attack [6].
xiii)Availability	xiii)Resource Consumption	xii) Secure neighbor detection by any IDS mechanism and randomly forward the route request to avoid duplicate route request. -Use DSR and ARIADNE to limit the route request. -Rushing Attack Prevention (RAP) protocol handles secure neighbor detection, secure route delegation and randomized route request forwarding [6][29][31]. xiii) AODV monitors RREQ of neighbor that will not exceed from threshold. -SEAD protect from this attack [29][40]. xiv) SEAD based on the Destination Sequenced Distance Vector protocols (DSDV) prevents malicious nodes from decreasing the
xiv) Availability and Authentication	xiv) Route Table Poisoning	
xv) Availability and Authentication	xv) Route Cache Poisoning	
xvi) Availability	xvi) Route Table Overflow	
	xvii) Modification	

xvii) Integrity and Authentication		hop count value or increasing the sequence number. -ARAN provide end-to-end authentication [47][68]. xv) This type of attacks are not easily identifiable. IDS is required to detect such malicious node/s [4][6]. xvi) This type of attacks are also not easily identifiable. IDS is required to detect such malicious node/s. -Most of the security mechanism applied for flooding attack can also be applied for routing table overflow attacks [4][6]. xvii) Source node authentication avoids modification [73]. -By using one way hashed Message Authentication Code (MAC). -Using Digital Signature to prevent modification. -ARAN with authentication also prevents modification. -Using certification SEAD with one-way hash function to provide authentication. -SAR by verifying digital signature. -Protocols that defend modification are: ARIADNE, ARAN, SAR, SAODV, SRP [6][10][31][47]. xviii) This attack is part of modification and can be protected from above mentioned defense line [31]. xix) This attack is also part of modification. Best-effort Fault Tolerant Routing (BFTR) based on DSR detects this attack [36]. xx) Node authentication will avoid such attacks [73]. -Using time stamp and asymmetric encryption. -Digital signature with data prevents replay attacks. -One-way hash function can be used. -Message Authentication Code (MAC) and Hashed MAC can also be used. -AODV uses destination sequence number to limit replay [29][31][37][47][53][68]. xxi) It is an example of message replay attack. Major defense lines are same as message replay attack. xxii) Packet leashes can be used. -GPS and directional antenna is also one of the approaches but not suitable for MANETs. -Timed Efficient Stream Loss-tolerant Authentication (TESLA) with instant key disclosure can be used. -Authentication of node is also applicable [73]. -Trust based secure routing decision is used. -Secure Tracking of Node Encounters in Multi-hop Wireless Networks (SECTOR) mechanism can also be used. -Various protocols like ARIADNE, OLSR prevent this attack [2][10][29][31][36][40][47][53][64]. xxiii) Robust source routing can be used. -On Demand Secure Byzantine Routing (ODSBR) protocol can be used in presence of byzantine [29][36]. xxiv) SRP can be used [40]. xxv) Data Authentication is one of the approaches [2]. xxvi) Cryptographic techniques can be used. -Distributed firewall avoids flooding. -Exponential back off algorithm also avoid packet flooding. -AODV use to detect RREQ flooding. -Zone Routing Protocol (ZRP) can also be used to protect from packet flooding [2][6][31][36][40][47][53][64]. xxvii) Pretty Good Privacy (PGP) provides periodic exchange of
xviii) Integrity	xviii) Detour	
xix) Authentication and Integrity	xix) Misrouting	
xx) Authentication and Integrity	xx) Message Replay	
xxi) Availability	xxi) Tunneling	
xxii) Availability	xxii) Wormhole	
xxiii) Availability	xxiii) Byzantine	
xxiv) Privacy	xxiv) Location Disclosure	
xxv) Authentication and Integrity	xxv)Packet Replication	
xxvi) Availability	xxvi) Packet Flooding	
xxvii) Availability	xxvii) Misbehaving	
xxviii) Availability	xxviii) Sleep Deprivation	
	xxix)Packet Dropping	

xxix) Availability		certificates. -BFTR also used that works in presence of mischievous nodes.
	xxx) Selfishness	-IDS can be used to detect misbehavior of node.
xxx) Availability and Integrity		-Cooperation of Nodes: Fairness In Dynamic Ad-hoc NeTworks (CONFIDANT) protocol can be used. -DSR which uses watchdog to detect it [2][19][31][36] [40][47][67].
	xxxi)Compromization	xxviii) Maintain priority RREQ by watching neighbor action.
xxxi) Authentication and Non-repudiation		-Link layer authentication protects sleep deprivation. -Anomaly based Intrusion Detection Protocol (AIDP) can be used. -DSR monitors neighbor's RREQ.
	xxxii) Session Hijack	-AODV isolates such attacks [2][6].
xxxii) Availability		xxix) BFTR, Ad hoc On-Demand Distance Vector State Transition Analysis (AODVSTAT) and DSR protocol detect it.
	xxxiii) SYN Flooding	
xxxiii) Availability	xxxiv) Repudiation	-AODV monitors the malicious node [2][6][31].
xxxiv) Authentication and Non-repudiation		xxx) CONFIDANT detect selfishness.
	xxxv) Denial of Service (DoS)	-Collaborative Reputation Mechanism to Enforce Node Cooperation (CORE) maintains cooperation among the nodes.
xxxv) Authentication and Availability		-Distributed IDS can be used. -Use cryptographic (Asymmetric or Symmetric) with authentication [10][40][47]. xxxi) Using Public Key Cryptography (PKI) and threshold cryptography it can be avoided. -IDS can be used to detect compromised node/s.
xxxvi) Availability and Privacy ***All attacks from (v) to (xxxvi) are active in nature.**	xxxvi) Virus / Worms / Trojan	-ARIADNE using one-way hash chain to avoid compromization [19][31][36][64]. xxxii) Securing transport protocol using public key cryptography and SSL and TLS can be used [3]. xxxiii) Firewall can be implement [47]. xxxiv) Cryptographic algorithms can be used. -ARAN can be used to avoid repudiation [6][10][31][40][47][68]. xxxv) Various techniques are available for authentication of a node ranging from one factor (password) to (Public Key Infrastructure) PKI. [73]. -Authentication and digital signature is prime solution. -Protocol ARAN can be used. -Techniques for Intrusion-resistant Ad hoc Routing Algorithms (TIARA) mitigate many of DoS attacks. -SEAD based on DSDV protect from this attack [6][36,37][40]. xxxvi) Antivirus and firewall are best solutions. -IDS) can also be used [3][37].

VI. Conclusion and Suggestions

MANET security issues include both attack and its countermeasures. Some specific type attack and their solution are presented in articles. Therefore, these topics attracted many researchers towards it. Some articles have common concepts like MANET characteristics, major types of attacks and their common solutions.

From this literature survey, it can be seen that some other issues of MANET are raised by authors like specific attacks, routing protocol, authentication problem, key management, trust management etc. due to their expertise or area of interest therefore some of the articles are diversified so their solutions are different for different problem domain. For security feature privacy, it has been suggested that encryption of data is best possible solution. On the other hand, for authentication feature, authors have suggested ARAN, SRP, SAR, SAODV and few other protocols. For other security features like integrity, availability and non-repudiation, a table was presented in work that clarifies which technique or protocol is suitable for a problem. An attack only affects one or two security features but not on all

features. Like eavesdropping affects only privacy factor, on the other hand Sybil affects authentication and non repudiation security features.

The articles reviewed in this survey are from reputed transactions, journals, surveys, book chapter and some are from conferences. The author's not widespread knowledge and subject coverage area is the first limit of this survey. Articles of other language are not included and it is believed that these issues have also been addressed in other language articles.

SUGGESTIONS

i) Security issue is major issue in MANET. These networks are deployed for various situations. Most of the paper has not discussed the security features according to type of deployment. Future security issue related articles must consider situation related safety measures.

ii) MANET does not have clear picture of node's job in a network, when it starts. It creates chaos in network. It is suggested here that nodes of network at the time of deployment must have clear details of role and responsibility. It helps in authentication, that covers access control and later to judge the working of node.

iii) Security solutions in many articles are incorporated in existing routing protocol. Very few new protocols have been advised. It is here suggested that for security solutions, new algorithms must be device that solely work. These algorithms are mainly required for authentication, trust management and security level.

REFERENCES

[1] A. Dorri, S. R. Kamel, E Kheirkhah, "Security challenges in mobile ad hoc networks: a survey", International Journal of Computer Science & Engineering Survey (IJCSES), vol-6, no-1, February, 2015.

[2] R. D. Pietro, S. Guarino, N. V. Verde, J. Domingo-Ferrer, "Security in wireless ad-hoc networks–A survey", Journal of Computer Communications, vol-51, pp-1-20, 2014.

[3] N Islam. "Security Issues in Mobile Ad Hoc Network", In 19th IEEE International Conference on Networks (ICON2013) Singapore, Springer-Verlag Berlin Heidelberg, 2013.

[4] A. K. Abdelaziz, Nafaa M. Salim G., "Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks",. In 15th International Conference Computer Modeling and Simulation (UKSim), Cambridge University, 2013.

[5] E. M. Shakshuki, N. Kang, T. R. Sheltami, "EAACK—a secure intrusion-detection system for MANETs", IEEE Transactions on Industrial Electronics, vol-60, no-3, pp-1089-1098, 2013.

[6] A. Nadeem, M. P. Howarth, "A survey of MANET intrusion detection & prevention approaches for network layer attacks", IEEE Communications Surveys & Tutorials, vol-15, no-4, pp-2027-2045, 2013.

[7] G. J. Moses, P. S. Varma, N.Supriya, G. NagaSatish, "Security Aspects and Challenges in Mobile Ad Hoc Networks", International Journal Computer Network and Information Security, in MECS Press, June 2012.

[8] A. M. Kanthe, D. Simunic, R. Prasad, "Effects of malicious attacks in mobile ad-hoc networks", In IEEE International Conference on Computational Intelligence & Computing Research (ICCIC), pp-1-5, 2012.

[9] H. Aldabbas, T. Alwada'n, H. Janicke, A. Al-Bayatti, "Data Confidentiality in Mobile Ad hoc Networks", International Journal of Wireless & Mobile Networks (IJWMN) vol-4, no-1, 2012.

[10] J Karlsson, L. S. Dooley, G. Pulkkis, "Routing Security in Mobile Ad-hoc Networks", Informing Science and Information Technology Education Conference (InSITE'12), pp-22-27, Montreal, Canada, 2012.

[11] J. V. Mulert, I Welch, W. KG Seah, "Security threats and solutions in MANETs: A case study using AODV and SAODV", Journal of Network and Computer Applications, vol-35, no-4, pp-1249-1259, 2012.

[12] H. Ehsan, F. A. Khan, "Malicious AODV: implementation and analysis of routing attacks in MANETs", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp-1181-1187, 2012.

[13] A. M. Kanthe, D. Simunic, M. Djurek, "Denial of service (DoS) attacks in green mobile ad-hoc networks", In proceedings of the 35th IEEE International Convention MIPRO, pp-675-680, 2012.

[14] A. M. Kanthe, D. Simunic, R. Prasad, "A mechanism for greyhole attack detection in Mobile ad hoc networks", International journal of computer applications, ISSN-0975-8887, vol-53, no-16, 2012.

[15] S. A. Begum, L. Mohan, B. Ranjitha, "Techniques for resilience of denial of service attacks in mobile ad hoc networks", In proceedings of International Journal of Electronics Communication and Computer Engineering, no-1, 2012.

[16] M. Stojanovic, V. Acimovic-Raspopovic, V. Timcenko, "The impact of mobility patterns on MANET vulnerability to DDoS attacks", Research Journal of Electronics and Electrical Engineering, vol-119, no-3, pp-29-34, 2012.

[17] A Annamalai, V Yegnanarayanan, "Secured system against DDoS attack in mobile ad hoc network", WSEAS Transactions on Communications, vol-9, 2012.

[18] E Lee, "Security in Wireless Ad Hoc Networks", Science Academy Transactions on Computer and Communication Networks, vol-1, no-1, 2011.

[19] S. Şen, J. A. Clark, J. E. Tapiador, "Security Threats in Mobile Ad Hoc Networks". Book Title: Security of Self-Organizing Networks: MANET, WSN, WMN, VANET. Auerbach Publications, CRC Press, 2011.

[20] K. Laeeq, "Security Challenges & Preventions in Wireless Communication", International Journal of Scientific and Engineering Research vol-2, Issue-5, pp-213-220, 2011.

[21] K. Konate, Abdourahime, G, "Attacks Analysis in Mobile Ad Hoc Networks: Modeling and Simulation", 2nd International Conference on Intelligent Systems, Modeling and Simulation (ISMS), Kuala Lumpur. 2011.

[22] J. Montero-Castillo, E. Palomar, "Cooperation in Ad Hoc Network Security Services: Classification and Survey", 5th International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies UBICOMM, 2011.

[23] P. Joshi, "Security issues in routing protocols in MANETs at network layer", Procedia Computer Science of World Congress on Information Technology Published by Elsevier, pp-954-960, 2011.

[24] F. Tseng, L. Chou, H. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Human-centric Computing and Information Sciences, Springer open journal, 2011.

[25] S. Agrawal, S. Jain, S. Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", Journal of Computing, NY, USA, ISSN 2151-9617, vol-3, Issue 1, 2011.

[26] A. Abdullah S, "Rushing attack in mobile ad hoc networks", 3rd IEEE International Conference on Intelligent Networking and Collaborative Systems (INCoS), pp-752-758, 2011.
[27] D. Dong, M. Li, Y. Liu, X. Li, X. Liao, "Topological detection on wormholes in wireless ad hoc and sensor networks", IEEE/ACM Transactions on Networking (TON), vol-19, no-6, pp-1787-1796, 2011.
[28] Q. Jia, K. Sun, A. Stavrou, "CapMan: Capability-based Defense against Multi-Path Denial of Service (DoS) Attacks in MANET", In proceedings of IEEE 20th International Conference on Computer Communications and Networks (ICCCN), pp-1-6, 2011.
[29] Z. M. Fadlullah, T. Taleb, M. Schöller, "Combating Against Security Attacks against Mobile Ad hoc Networks (MANETs)", Security of Self-Organizing Networks MANET, WSN, WMN, VANET Auerbach Publications, Print ISBN: 978-1-4398-1919-7, 2010.
[30] R. Shrestha, K. Han, D. Choi, S. Han, "A novel cross layer intrusion detection system in MANET", IEEE 24th International Conference on Advanced Information Networking and Applications (AINA), pp-647-654, 2010.
[31] P. O. Mohammad, M. Cardei, J. Wu, "Routing security in ad hoc wireless networks", Network Security, pp-117-142. Springer US, 2010.
[32] A. H. Al-Bayatti, H. Zedan, A. Cau, "Security solution for mobile ad hoc network of networks (manon)", 5th IEEE International Conference on Networking and Services, ICNS'09, pp-255-262, 2009.
[33] M. Azer, S. M. El-Kassas, M. S. El-Soudani, "Security in Ad Hoc Networks: From Vulnerability to Risk Management", IEEE 3rd International Conference on Emerging Security Information, Systems and Technologies, SECURWARE'09, pp-203-209, 2009.
[34] L. Ertaul, D. Ibrahim, "Evaluation of Secure Routing Protocols in Mobile Ad hoc Networks (MANETs)", International Conference on Security and Management SAM'09, Las Vegas, 2009.
[35] M. Kargar, M. Ghodsi, "Truthful and Secure Routing in Ad Hoc Networks with Malicious and Selfish Nodes", International Journal of Security and its Applications, vol- 3, no- 1, pp-117-128, 2009.
[36] M. Nogueira, L,Aldri, L. Santos, G. Pujolle, "A Survey of Survivability in Mobile Ad Hoc Networks", IEEE Communications Surveys & Tutorials, vol-11, Issue-1, 2009.
[37] R. M. Savola, H. Abie, "On-line and off-line security measurement framework for mobile ad hoc networks", Journal of Networks, vol-4, no-7, pp-565-579, 2009.
[38] A. Hamieh, J. Ben-Othman, "Detection of jamming attacks in wireless ad hoc networks using error distribution", IEEE International Conference on Communications, ICC'09, pp-1-6, 2009.
[39] A. Mishra, "Security and Quality of Services in Ad Hoc Wireless Networks", Cambridge University Press, 2008.
[40] L. Abusalah, A. Khokhar, M. Guizani, "A survey of secure mobile ad hoc routing protocols", IEEE Communications Surveys & Tutorials, vol-10, no-4, pp-78-93, 2008.
[41] H. L. Nguyen, U. T. Nguyen, "A study of different types of attacks on multicast in mobile ad hoc networks", Ad Hoc Networks vol-6, no-1, published by Elsevier, pp-32-46, 2008.
[42] J. Ruiz, J. Friginal, D. de-Andrés, P. Gil, "Black Hole Attack Injection in Ad hoc Networks", Fault Tolerance Systems Group (GSTF), Valencia, Spain, 2008.
[43] J. Luo, M. Fan, D. Ye, "Black hole attack prevention based on authentication mechanism", IEEE International Conference on Communication Systems, ICCS 2008, pp-173-177, 2008.
[44] S. Choi, D. Kim, D. Lee, J. Jung, "WAP: Wormhole attack prevention algorithm in mobile ad hoc networks", IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, SUTC'08, pp- 343-348, 2008.
[45] I. Aad, J. Hubaux, E. W. Knightly, "Impact of denial of service attacks on ad hoc networks", IEEE/ACM Transactions on Networking, vol-16, no-4, pp-791-802, 2008.
[46] Y. Zhang, L. Lazos, W. Jr. Kozma, "AMD: Audit Based Misbehavior Detection in Wireless Ad Hoc Networks", IEEE Transactions on Mobile Computing, vol- X, no-X, 2008.
[47] B. Wu, J. Chen, J. Wu, M. Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks, Wireless Network Security Signals and Communication Technology, Springer USA, pp-103-135, 2007.
[48] F. Anjum, P. Mouchtaris, "Security for Wireless Ad Hoc Networks", John Wiley & Sons, Inc., Hoboken, New Jersey, 2007.
[49] J. Jeong Z. J. Haas, "An Integrated Security Framework for Open Wireless Networking Architecture", IEEE Wireless Communications, vol-14, Issue: 2, pp-10-18, 2007.
[50] J. C. Park, S. K. Kasera, "Securing ad hoc wireless networks against data injection attacks using firewalls", IEEE Conference on Wireless Communications and Networking, WCNC , pp- 2843-2848, 2007.
[51] Q. Gu, P. Liu, C. Chu, S. Zhu, "Defense against packet injection in ad hoc networks", International Journal of Security and Networks vol-2, no-1-2, pp-154-169, 2007.
[52] P-W. Yau, S. Hu C. J. Mitchell, "Malicious attacks on ad hoc network routing protocols", International Journal of Computer Research, vol-15, no-1, pp-73-100, 2007.
[53] B. Kannhavong, H. Nakayama, Y. Nemoto, N. K. A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", IEEE Wireless communications, vol-14, no-5, pp-85-91, 2007.
[54] F. Xing, W. Wang, "Understanding dynamic denial of service attacks in mobile ad hoc networks", IEEE Military Communications Conference, MILCOM , pp-1-7, 2006.
[55] P. Papadimitratos, "Secure ad hoc networking", 3rd IEEE Consumer Communications and Networking Conference, CCNC, pp-10-14, 2006.
[56] T. Roosta, S. Shieh, S. Sastry, "Taxonomy of security attacks in sensor networks and countermeasures", 1st IEEE international conference on system integration and reliability improvements, vol-25, pp-94-103, 2006.
[57] Y. Hu, A. Perrig, D. B. Johnson, "Wormhole attacks in wireless networks", IEEE Journal on Selected Areas in Communications, vol-24, no-2, pp-370-380, 2006.
[58] Jim P, A. Patwardhan, A. Joshi, "Cross-layer analysis for detecting wireless misbehavior", In proceedings of the IEEE Consumer Communications and Networking Conference (CCNC), pp-6-9, 2006.
[59] D. Djenouri, L. Khelladi, N. Badache, "A survey of security issues in mobile ad hoc networks", IEEE communications surveys, vol-7, no-4, pp-2-28, 2005.
[60] A. Chandra, "Ontology for MANET Security Threats", In proceedings of Second National Conference on Network Engineering. NCON, 2005.
[61] M. Denko, "Detection and prevention of Denial of Service (DoS) attacks in mobile ad hoc networks using reputation-based incentive scheme", Journal of Systemics, Cybernetics and Informatics, vol-3, no-4, pp-1-9, 2005.
[62] W. Yu, K. J. Liu, "Attack-resistant cooperation stimulation in autonomous ad hoc networks", IEEE Journal on Selected Areas in Communications, vol-23, no-12, pp-2260-2271, 2005.
[63] A. Mishra, K. Nadkarni, A. Patcha, "Intrusion detection in wireless ad hoc networks", IEEE Wireless Communications, vol-11, no-1, pp-48-60, 2004.
[64] H.Yang, H. Luo, F. Ye, S. Lu, L. Zhang, "Security in mobile ad hoc networks: challenges and solutions", IEEE Wireless Communications, vol-11, no-1, pp- 38-47, 2004.

[65] S. A. Razak, S. M. Furnell, P. J. Brooke, "Attacks against mobile ad hoc networks routing protocols", In proceedings of 5th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking & Broadcasting (PGNET'04), 2004.
[66] Y. Huang, W. Lee, "Attack analysis and detection for ad hoc routing protocols.: Recent advances in intrusion detection", Springer Berlin Heidelberg, pp-125-145, 2004.
[67] H. Luo, P. Zerfos, J. Kong, S. Lu, L. Zhang, "Self-securing ad hoc wireless networks", In proceeding of 7th International Symposium on Computers and Communications, ISCC 2002.
[68] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, E. M. B. Royer, "A secure routing protocol for ad hoc networks", In proceedings of IEEE 10th International Conference on Network Protocols, pp-78-87, 2002.
[69] L. Zhou, Z. J. Haas, "Securing Ad Hoc Networks", IEEE network, special issue on network security, vol-13, no-6, pp-24-30, 1999.
[70] A. B. Suryawanshi, B. K Saini, "Survey on Various Routing Protocols in Ad-hoc Networks", International Journal of Scientific Research in Network Security and Communication, Vol.5, Issue.3, pp.174-178, 2017.
[71] A.vani, "Detection and Elimination of Wormhole Attacks in a MANET ", International Journal of Scientific Research in Computer Sciences and Engineering, Vol.5, Issue.5, pp.35-40, 2017.
[72] P. Gupta, P. Bansal, "A Survey of Attacks and Countermeasures for Denial of Services (DoS) in Wireless Ad hoc Networks", In proceedings of 2nd International Conference on Information and Communication Technology for Competitive Strategies, (ICTCS-2016), p.25, ACM 2016.
[73] P. Gupta P. Bansal, "Authentication Process using Secure Sum for a New Node in Mobile Ad Hoc Network" International Conference on Data, Engineering and Applications (IDEA-2k17), Springer 2017.

Author's Profile

Praveen Gupta received his M.Sc. (Electronics), M.Tech (FS&P) and M.Tech. (Computer Science) degree from Devi Ahilya Vishvavidhyalaya Indore, India. He is pursuing his Ph.D. in Computer Engineering from Institute of Engineering and Technology (IET), Devi Ahilya Vishvavidhyalaya, Indore, India.

He is working as Associate Professor in computer engineering department of PITM, Indore. His research interests in Mobile Ad hoc Network and its security issues, Computer Networks. He is senior member of IEEE. He has 20 years of teaching experience and 8+ years of Research Experience.

Dr. Pratosh Bansal is a Professor, in Information Technology Department of Institute of Engineering & Technology (IET), a UTD of Devi Ahilya University, Indore (DAVV).
He has done his graduation in Mechanical Engineering from Govt Engineering College, Jabalpur He received his M.Tech. (Energy Management), M. Tech. (Computer Science) and Ph D in Computer Engineering from DAVV Indore. His areas of interest are-Enterprise Resource Planning, Knowledge Management, E-Commerce, Digital Forensics, Cloud Computing, Green IT and Energy Management.

