An Investigative Survey of different Security Attacks in MANETs

Naresh Dobhal

Devashish Pundir

ABSTRACT
MANETs (Mobile Adhoc Networks) are used to build up dynamic wireless networks which have no strictly defined infrastructure and no fixed topology with lucrative flexibilities to be used in various applications. Nodes with malicious intent or misleading behavior can join the adhoc network together with trustworthy nodes easily due to inherent characteristics of MANETs which makes them more prone to several attacks than wired networks. Conventional security policies and mechanisms designed for wired networks are mostly considered inadequate and ineffective for these highly dynamic and resource-constrained Adhoc networks. To design and develop security models for MANETs we must first be intriguing about the possible security attacks that may pounce upon different adhoc network scenarios. This paperwork focusses our attention on a comprehensive review to the various security threats and attacks prevalent in MANETs with the classification being done by taking into account the layered architecture of TCP/IP protocol suite underneath it.

General Terms
Adhoc networks, MANET, Routing, Target, Victim

Keywords
Internal attacks, External attacks, Active attacks, Passive attacks, Blackhole attack, Wormhole attack, Byzantine attack, Flooding attack, Colluding Misrelay attack.

1. INTRODUCTION
Adhoc networks are usually created on the fly for some specific purpose such as a single session or a temporary use only. MANET (Mobile Adhoc Network) is a wireless network which constitutes multiple wireless, autonomous nodes which can be dynamically organized to setup a network anytime, anywhere and without the use of any pre-existing network infrastructure facilities.

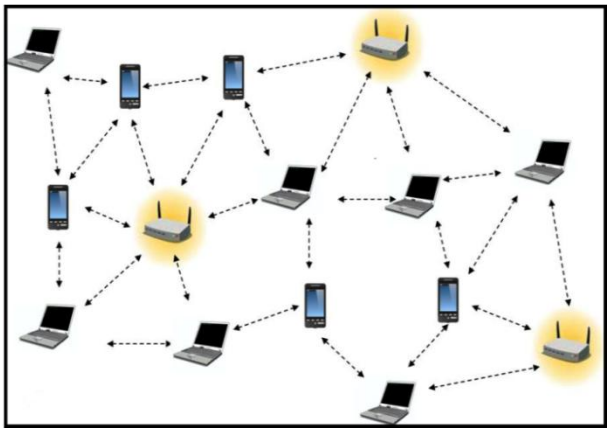


Figure 1:- Various wireless devices forming a MANET

Each node in a MANET is required to act as a HOST i.e. capable of receiving packets as well as a ROUTER i.e. capable of forwarding packets to other nodes in the network which cannot communicate directly with each other. Nodes in a MANET can be any device such as mobile phones or smartphones, laptops, PDA's, tablets etc. MANETs are self-configuring, self-healing and de-centralized adhoc network which are cost effective (unprofitable) to setup and operate.

2. CHARACTERISTICS OF MANET
Some of the basic characteristics of MANETs are:-

a) No fixed infrastructure
Nodes in a MANET do not rely on existing infrastructure which provides a very cost effective, flexible and dynamic network that can be used in remote (far flung) areas or even battlegrounds.

b) Dynamic topology
Nodes in a MANET are usually wireless devices that can join the network or leave the network owing to reasons such as not in coverage area of the network or they might terminate the connection etc.

c) Resource constraint
MANETs contain heterogeneous set of devices with varying processing power, varying storage speed, varying energy requirements etc.

d) Bandwidth constraints
The medium of communication among the nodes in a MANET is "wireless". It is already evident that the bandwidth of wireless networks is limited and also of variable capacity as if compared to wired networks.

e) Autonomous networks
MANETs are peer-to-peer, self-configurable, de-centralized networks which can be created on the fly by reducing/eliminating the complexities of setting up a physical infrastructure. Nodes can act either as a host or as a router as per requirements.

3. APPLICATION AREAS OF MANET
MANETs are of increasing use in areas where the ability to keep on move in vital in order to utilize time efficiently. MANETs find applications in battleground communications, connectivity in vehicles, natural or man-made emergencies, businesses, infotainment, mobile conferences, and virtual classrooms or in replacement of wired networks.

4. ROUTING STRATEGIES IN MANET
Nodes in MANETs have independent computational, switching (routing) and communication strategies due to their infrastructure-less nature. The topology of this network can change dynamically which requires the ability to discover

neighboring nodes & services to lie within the MANET node specifically.

Routing in MANETs require the discovery of most recent network topology in order to compute an optimal path from the source node to any destination node with minimum overhead, minimum bandwidth consumption and minimum delay in transmission.

The most arguable difference in MANET routing and conventional Internet routing is the "route discovery mechanism" used. The traditional Internet routing algorithms cannot be used due to mobility of nodes in MANETs. This has baffled the network scientists & engineers to design and develop various routing protocols to work optimally in different scenarios in today's mobile adhoc networks.

5. CLASSIFICATION OF ROUTING PROTOCOLS

Different routing protocols are differentiated on the basis of manner of creation of routing tables. This leads to classify protocols as Proactive routing protocols, Reactive routing protocols, Hybrid approach routing protocols and Hierarchical routing protocols.

a) Proactive routing protocols

These protocols maintain a routing table for entire nodes using the information present in the routing table of each individual node. Nodes periodically exchange topology information and maintain routes to various destinations even if they are not needed, which provides a minimal route selection time.

These protocols can be used in scenarios with:-

(i) Networks with lesser mobility of nodes.
(ii) Small network size with few nodes.

List of Proactive protocols are:-

i) DSDV (Destination Sequenced Distance Vector)
ii) WRP (Wireless Routing Protocol)
iii) GSR (Global State Routing)
iv) STAR (Source Tree Adaptive Routing)
v) TBRPF (Topology Broadcast Reverse Path Forwarding)
vi) OLSR (Optimized Link State Routing)
vii) LANMAR (Landmark Routing)

Advantages of Proactive protocols are:-

(i) Considerably lower route determination latency.
(ii) QoS guarantee related to connection setup or other real time requirements.

Disadvantages of Proactive protocols are:-

(i) High overhead on routing tables due to frequent routing updates.
(ii) Consumption of bandwidth for periodic updates.
(iii) Maintaining of certain routes which may not be used even once.

b) Reactive routing protocols

These protocols are based upon the On-Demand Route Request approach in which nodes tend to find routes to destination nodes if there is a packet to be sent and its route is completely unknown at that time. The nodes using these protocols flood its neighbors with Route Request (RREQ) packets for computing a route to destination node.

These protocols can be used in scenarios with:-

(i) Networks with high mobility of nodes.

List of Reactive protocols are:-

i) AODV (Adhoc On-Demand Distance Vector)
ii) DSR (Dynamic Source Routing protocol)
iii) TORA (Temporally Ordered Routing Algorithm)
iv) ABR (Associativity Based Routing)
v) SSR (Signal Stability based Adaptive Routing)

Advantages of Proactive protocols are:-

(i) No overhead as routing information is obtained only when needed.
(ii) Scalability is possible as long as there is low mobility and less traffic.

Disadvantages of Proactive protocols are:-

(i) High route determination latency.
(ii) Flooding of RREQ packets can create congestion.

c) Hybrid Routing Protocols

Advantages of Proactive & Reactive protocols are combined in Hybrid routing protocol approach. In this approach initially the routes to nearby nodes are maintained through some Proactive protocols while later on Reactive protocols can be used to discover the routes for far-away nodes or additionally activated nodes.
Hybrid routing protocols may present an optimal choice of path in different network scenarios.

ZRP (Zone Routing Protocol) is a hybrid routing protocol.

Underlying disadvantages of Hybrid routing approach are:-

(i) Usefulness of this approach requires the knowledge of nodes activated at any time.
(ii) Reaction to traffic demand depends upon the gradient of traffic volume.

d) Hierarchical Routing protocols

Scalability of Proactive & Reactive protocols is limited due to their inherent designs. Enhancements made to these protocols improve performance but these enhancements still do not allow the protocol to scale well to larger networks.
Clustering protocols places the node into groups called Clusters and perform hierarchical routing between these clusters. This scheme increases the robustness of the routes by providing multiple possibilities for routing between clusters.

List of Reactive protocols are:-

(i) FSR (Fisheye State Routing)
(ii) CBRP (Cluster Based Routing Protocol)
(iii) ARC (Adaptive Routing using Clusters)
(iv) DCA (Distributed Clustering Algorithm)
(v) DMAC (Distributed & Mobility Adaptive Clustering)

Advantages of Hierarchical Routing protocols are:-

(i) Hierarchy of nodes remains stable during mobility of nodes.

(ii) Flooding of control messages across the network are reduced greatly and only thee cluster leaders needs to be flooded.

Disadvantages of Hierarchical routing protocols are:-

(i) The depth of nesting of clusters & addressing scheme reveals its advantages.

6. SECURITY VULNERABILITIES IN MANET

MANETs are more prone to wide variety of attacks than wired networks due to some weakness in their architecture. MANETs are de-centralized networks with the assumption that all nodes in the network are trustworthy & well-behaved and many of the routing protocols rely on the cooperation between these nodes.

Some of these existing vulnerabilities are:-

a) Medium of communication is Wireless
Wireless networks have less bandwidth as compared to wired networks, which encourages attackers to exploit this feature for network congestion and disruption of normal communication. Use of wireless medium makes the networks susceptible to issues like eavesdropping, active interference etc. Moreover in wireless networks a physical access is not required to carry out these attacks.

b) Frequently changing network topology
Nodes in a MANET can join & leave the network at any desired time. A node with inadequate security mechanisms may be targeted to work as a malicious (compromised) node and disrupt network performance.

c) Cooperation among nodes
MANETs are de-centralized networks in which a central administrator node ceases to exist. Each node carries the responsibility of acting as a host as well as a router. Routing algorithms assume that the nodes in the network are trustworthy and would cooperate for mutual benefit in carrying out network operations. This lays the basis for a node to get compromised without detection and disrupt network traffic.

d) Less secure and unclear network boundary
Attacks on MANETs can arise from every direction as there is no clear demarcation of the wireless network boundary. Compromised nodes can be present outside the network boundary as well as inside the network boundary too. Moreover non-existence of a central administrative node makes it difficult to deploy secured access control mechanisms.

e) Resource constraints
Lack of several vital resources in nodes of MANETs makes it even difficult to deploy certain security mechanisms applicable to wired networks, without deteriorating network efficiency & bandwidth.

7. CLASSIFICATION OF SECURITY ATTACKS ON MANET

Securing MANETs is a highly challenging issue owing to its existing architecture vulnerabilities. Attacks can be targeted at routing protocols or even at security mechanism s deployed in networks. Compromised nodes can be present outside as well as inside of the network. Attackers can disrupt normal network routing, isolate node(s), may consume vital resources such as bandwidth, computational speed or even battery.

Attacks can be classified on the basis of:-

(a) Location of attacker(compromised or malicious node)
- (i) Internal attack
- (ii) External attack

(b) Effects on system resources & network traffic
- (i) Passive attack
- (ii) Active attack

(c) Layer affected of TCP/IP protocol suite

Internal attacks
This type of attacks is initiated by authorized (legitimate) nodes within a network. An internal node may get compromised by an external attacker or it may behave selfishly in order to save its resources. Internal attacks are very hard to detect.

Ex: - Byzantine attacks

External attacks
This type of attack is initiated by non-authorized (non-legitimate) nodes which are not a part of the network. External compromised nodes can severely disrupt network routing and can cause congestion in various parts of the network.

Ex: - Eavesdropping

Passive attacks
Passive attack do not disrupt the network or alter traffic in the network, rather it indulges in the "stealing" of valuable information from the targeted networks. Malicious nodes whether internal or external, can gain entry into the network for their benefit. These attacks are hard to detect as the network itself does not get affected. They can be overcome by using methods such as strong security encryption mechanisms.

Ex: - Eavesdropping, Traffic monitoring & analysis

Active attacks
Active attacks tries to tamper the normal working of networks causing congestion, modification of data packets or routes. Attacks from internal compromised nodes tend to be more severe & hard to detect than attacks from external nodes.

Ex: - Spoofing, Denial of Services, Wormhole, Black hole, Sinkhole, Sybil etc.

Layers affected in the TCP/IP protocol suite
A wide range of attacks can be targeted at each specific layer of the protocol suite [7]. TCP/IP originally consisted of four layers: – Host-to-Network layer, Internet Layer, Transport layer, Application layer. For the sake of simplicity & clarity Host-to-Network layer can be broken into two layers: - Physical layer and Data Link layer [10].

TCP/IP layer		Possible attacks
Application layer		Repudiation, Data Corruption
Transport layer		Session hijacking SYN Flooding
Internet layer	(Network Layer)	Wormhole Blackhole Byzantine Routing attacks Sybil Sleep deprivation

		IP Spoofing Link Spoofing Link withholding Colluding miss-relay Flood rushing Gray hole
Host-to-network layer	Data Link layer	Traffic monitoring & analysis
	Physical Layer	Jamming Eavesdropping

8. ATTACKS ON PHYSICAL LAYER

Attacks such as Jamming, Eavesdropping are common on physical layer and are used in a generic sense.

8.1 Jamming

Jamming is a specific Denial of Service (DoS) attack that interferes with the communication link between the nodes present in the network [2]. The aim of jamming attack is to hinder (block) all the communication by authorized sender or receiver from transmitting or receiving packets in the network. Jamming can be conceived easily in MANETs as the adversary or malicious node can intercept the transmission as the communication link is wireless.

Jamming attack can be rendered in two different ways: -
(i) Physical or Radio Jamming
(ii) Virtual Jamming

Physical or Radio Jamming attack can be initiated easily by continuous emission of bogus radio signals so as to keep busy or deny complete access to any legitimate communication link. Malicious nodes can even use the fact that the strength of the radio signal weakens with the square of the distance between the nodes, thereby generating a strong signal that blocks or obstructs the legitimate signal between the interacting nodes which could result in packet corruption or packet loss. Malicious node can also be termed as Jammers.

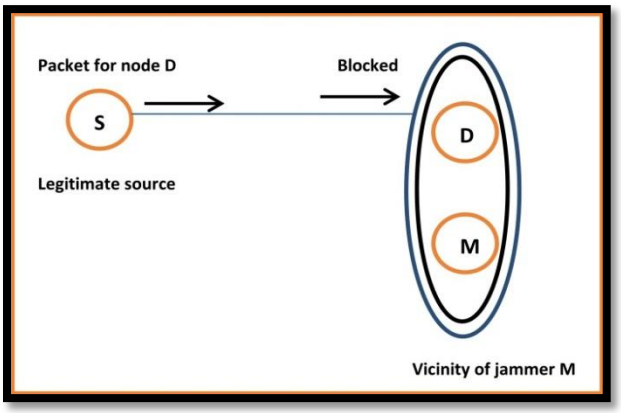


Figure 2:- Physical Jamming attack

Virtual jamming attacks are initiated at MAC layer by attacking the control/data frames. It is an active attack that disrupts the communication between nodes thereby degrading overall network throughput. This type of attack consumes less energy than the physical jamming attack.

8.2 Eavesdropping

In this form of attack the malicious node intercepts the packets sent or received and it might reveal some confidential information such as location of sender/receiver, secret keys, passwords etc. which may be otherwise kept secret during communication between authorized users [8]. This is a passive form of attack which owes itself due to easy tapping of wireless nature of communication medium in MANETs.

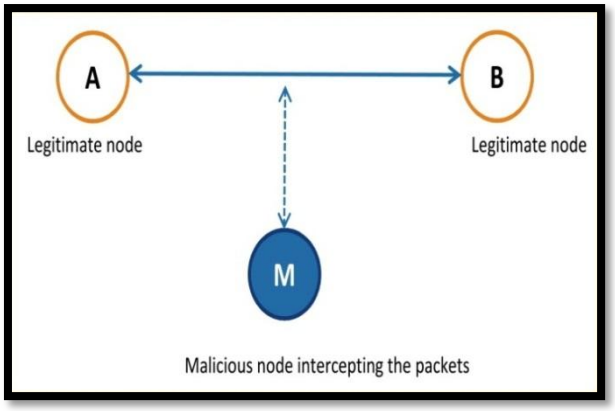


Figure 3: - Eavesdropping attack

9. ATTACKS ON DATA LINK LAYER

9.1 Traffic monitoring and analysis

In MANET literature it is also termed as ***Location Disclosure attack***. In this form of attack the malicious node monitors the broadcasted packets and analyses this traffic which might reveal information such as location of sender-receiver, sender-receiver pair, network topology, network routing structure, traffic rate, existence & location of other legitimate nodes etc. Several network tools exist in the internet which can be used for this purpose such as NetStumbler. Using this disclosed information other malicious nodes may also plan further attack scenarios in coordination.

The attacker can even record, alter and retransmit altered packets to other legitimate nodes remaining completely invisible. Leakage of such information can be devastating in security sensitive environments.

10. ATTACKS ON NETWORK LAYER

10.1 Impersonation

These attacks are also termed as IP Spoofing, Spoofing or Replay attacks. A malicious node acts as a genuine node if node authentication methods are not implemented properly or weak authentication methods are used. The malicious node can monitor traffic, send fake routing packets and even gain some confidential information.

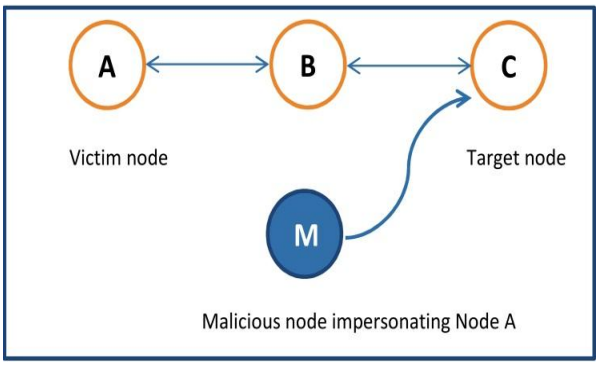


Figure 4: - Impersonation attack

10.2 Link Spoofing Attack

A malicious node can advertise (broadcast) FAKE routing links with non-neighbor nodes to disrupt normal routing operations [4]. It poses severe impacts on the routing protocols such as OSLR that uses link state link state information for discovering new nodes.

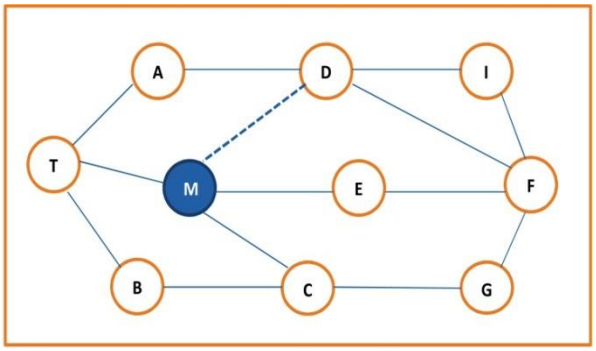


Figure 5: - Link spoofing attack

In the above network topology if we use routing protocol such as OSLR, malicious node **M** can advertise a fake link with the target's **T** two-hop neighbor **D**. Node **A** and **M** should be the multi-point relay (MPR) nodes for node **T**. MPR nodes are one-hop neighbors which covers all its two-hop neighbors. MPR strategy selects a set of nodes to retransmit its packet. Any node exclusive of MPR can read the packet but cannot retransmit it. It is used to minimize the size of the control messages and the number of broadcasting messages.

The fake link advertised by malicious node **M** causes the target node **T** to select only **M** as its MPR although **A** & **M** must be the MPR nodes. Now the malicious node **M** can reach node **E** and node **C** legitimately while it can also reach node **D** thorough its fake advertised link. Node **M** can plan future attack scenarios such as dropping packets or withholding the traffic generated by **T**.

10.3 Link Withholding Attack

In this type of attack a malicious/selfish node ignores the requirement of advertising the route of specific nodes or a certain part of the network. This behavior causes a link-loss to these nodes as they become isolated in the network. Malicious nodes disrupt normal network operations while selfish nodes can affect self-performance of the node itself due to several reasons such as battery power conservation.

In the topology given below the malicious/selfish node **M** do not advertise the links with node **D** which is linked with node **I**. These types of attacks create serious damages when link state protocols such as OLSR are being used.

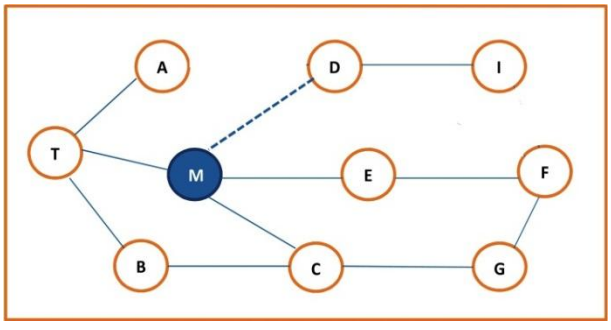


Figure 6:- Link withholding attack

10.4 Colluding Misrelay attack

These are active attacks initiated by internal malicious nodes. In this attack multiple malicious nodes act in coordination (colluding) to modify or drop packets so as to disrupt network routing operations.

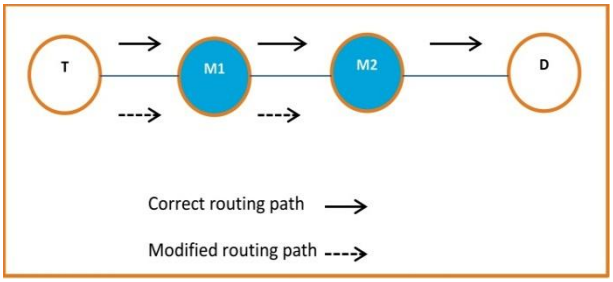


Figure 7: - Colluding Misrelay attack

Malicious node **M1** forwards routing packets from legitimate target node **T** which is being destined for node **D**, to avoid being detected by **T** as a malicious node dropping packets. However another malicious node **M2** can easily drop or modify these packets without being detected. This attack is difficult to detect by conventional methods and it has been researched that a pair of malicious nodes can disrupt 100% of packets in a MANET using OLSR protocol.

10.5 Sleep deprivation attack

It is a denial of service attack that can be targeted against either a legitimate single or legitimates multiple nodes whose vital resources need to be made exhausted [5]. Malicious node (s) force the legitimate nodes to use their vital resources such as battery power, bandwidth or computing power by sending false requests for existent or non-existent destination nodes.

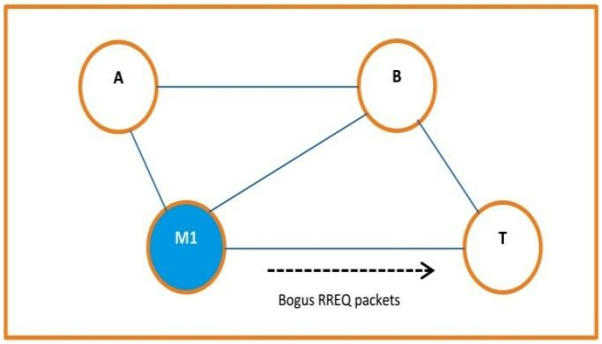


Figure 8: - Sleep deprivation attack

Sleep deprivation attack minimizes the expected lifetime of a genuine node by requesting a service over & over by a malicious node which deprives the legitimate node to go to its idle or power saving mode. In due time the legitimate node becomes incapacitated with no more ability to take part in network operations and can even become unreachable afterwards.

10.6 Gray Hole attack

In literature this type of attack is also termed as Routing Misbehavior attack which targets nodes particularly using AODV routing protocol. A malicious node exploits AODV protocol to advertise itself having a valid route to a destination node with the intention of intercepting packets even though the route may be spurious (faulty). If the packets are routed

through this malicious node they get dropped with a certain probability.

A grayhole node may exhibit its malicious behavior in several ways: -

(i) It can drop packets with certain probability coming from specific nodes while forwarding packets from other nodes correctly.

(ii) It can drop packets only for some time duration but may switch back to normal routing behavior later.

(iii) It can combine the latter two scenarios which is even more difficult to diagnose.

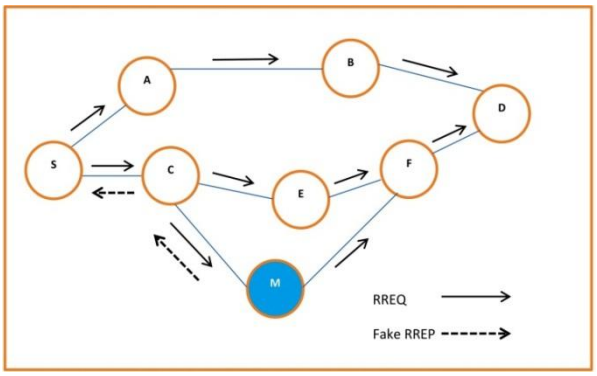


Figure 9: - Grayhole attack

Gray Hole attack is difficult to diagnose than Black hole attack as black hole nodes drops received packets certainly while grayhole nodes drops packets with only a certain probability.

10.7 Flooding attacks

Flooding attacks paralyses the entire network by exhausting network bandwidth and vital resources of the legitimate nodes. Flooding attack can be classified as: -

(i) RREQ flooding

(ii) Data flooding

RREQ flooding initiates sending of massive bogus route requests (RREQ) packets that will be definitely be re-broadcasted by other nodes. Bogus RREQ packets imply that such destinations do not exist in the network. RREQ flooding attack consumes network bandwidth and nodes battery power which can be used otherwise for useful purposes.

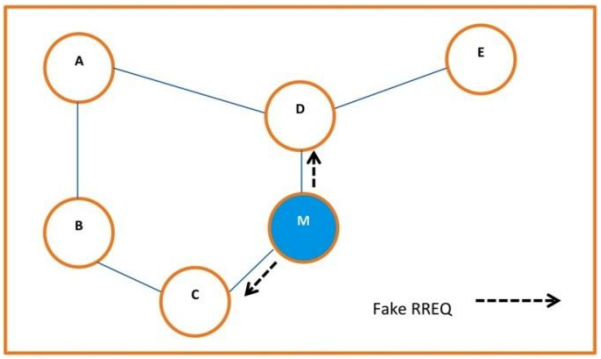


Figure 10:- RREQ flooding attack

Data flooding requires sending of useless data packets into the network after route to all destinations is being determined. This attack also consumes network & node resources.

10.8 Black Hole attack

In this attack a single malicious node sends out fake routing information claiming that it has optimum route (zero metrics path) for all destination nodes which causes other good nodes to route packets thorough this malicious node [1].

The malicious node acts like a black hole which drops all packets certainly received by it instead of forwarding those packets to their destinations. In some scenarios it can also impersonate itself as the destination node whenever it receives a RREQ packet for any particular destination. It sends back RREP packet with a modified higher sequence number back to the source node claiming it to be the destination node. The source node routes all data towards this malicious node thinking it is the required destination node.

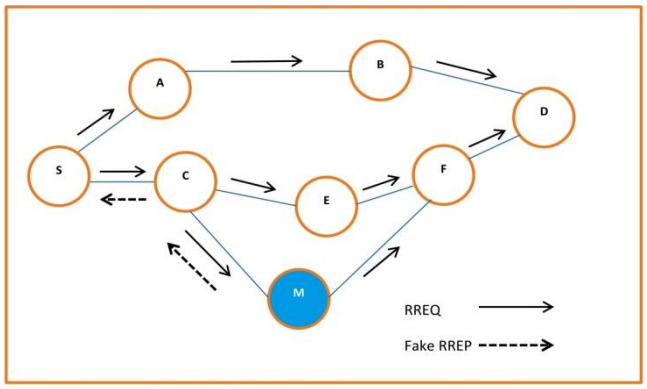


Figure 11: - Blackhole attack

10.9 Traditional Wormhole attack

Traditional Wormhole attacks are carried out by two or more external malicious nodes colluding together. A malicious node intercepts & records packets at one location in the network and tunnels them to another malicious node using some private communication link network and then replays (insert into network) them into the network from that point. The other nodes that receive the replayed packets are unable to distinguish them from legitimate routing packets which cause the nodes to become victim by accepting the fake tunneled routing packets instead of legitimate packets.

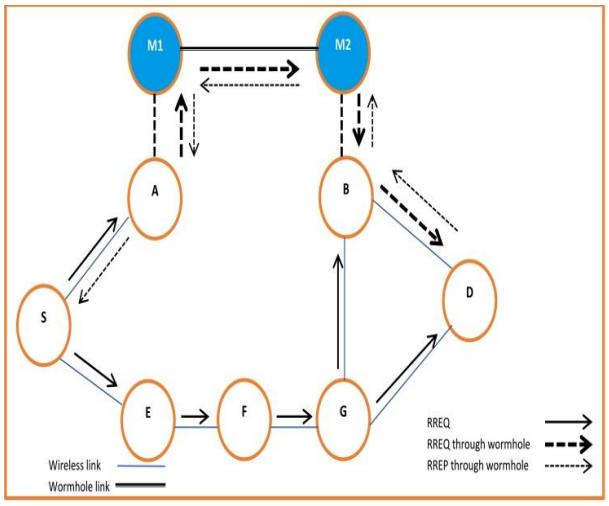


Figure 12: - Traditional wormhole attack

M1 and **M2** are the external malicious nodes with some private network link connecting them. The source node **S** broadcasts a RREQ packet for identifying a route from node **S** to destination node **D**, to its immediate neighbors **A** and **E**. Node **E** would forward the RREQ packets as usual to node **F**. Meanwhile the malicious node **M1** intercepts & records this RREQ packet at node **A** and tunnels this packet to its colluding node **M2**. Node **M2** re-broadcasts this recorded RREQ packet to nodes in its vicinity ex. Node **B**. Now node **B** replies RREP packet corresponding to this recorded RREQ packet as it knows the route to destination **D**. It should be made clear that this recorded RREQ packet has arrived earlier than the legitimate packet that follows the path **E-F-G**. Hence source node **S** will select a path that passes through the wormhole nodes i.e. **S-A-M1-M2-B-D**. The traffic passing through the wormhole link can be used by malicious nodes for their advantage too. Data packets can be modified or dropped; sometimes these packets can also be kept for further analysis. If wormhole nodes are present in a network using on-demand routing protocols, it could prevent the discovery of any distinct route other than through the wormhole.

10.10 Flood Rushing attack

Flood rushing attack generally originates in the route discovery phase of routing protocol and are mainly targeted against on-demand routing protocols. A legitimate node requesting a route to a destination node would broadcast RREQ packet and each node forwards only the first arriving RREQ packet in order to limit the overhead of message flooding. On-demand protocols use duplicate packet suppression method to limit overhead.

Whenever a malicious node receives a RREQ packet; it forward this packet quickly throughout the network before other nodes could send them. Remaining legitimate nodes would receive the packet & forward it in their usual way but they would be suppressed because a RREQ packet has already been forwarded quickly by the malicious node. This causes the routing protocol to discover the route passing through the malicious node instead of a legitimate route.

A malicious node can initiate flood rushing attack in many ways: -

(i) The malicious node can enhance the forwarding speed by flooding the neighbors with bogus RREQ packets so as to slow down their processing capability.

(ii) The malicious node can enhance its forwarding speed by transmitting the packets at higher transmission power which effectively decreases the number of hops required to reach the destination.

(iii) The malicious node can ignore the delays caused at MAC sub-layer or Network layer.

10.10 Byzantine attacks

Byzantine attacks are the strongest attacks made on the MANETs by legitimate internal nodes which are well aware of the system behavior but have been compromised [6]. Byzantine is a term that describes the legitimate internal nodes whose actions cannot be trusted or do not conform to the protocol specifications. The aim behind the attacks is to block the normal functioning of the network and also to corrupt it.

The nodes that want to participate in network operations undergoes authentication procedure and after being authenticated as a legitimate node they are given full control and are able to take part in network operations. Any legitimate node can be turned into a byzantine node so as to disrupt normal network communications of other nodes but it participates in routing correctly. The byzantine node can work in isolation or colludes with other Byzantine nodes to initiate attacks such as: - Blackhole attack, Flood rushing attack, Byzantine wormhole attack, Byzantine overlay network wormhole, creation of routing loops, non-optimal path selection for packet forwarding etc.

Traditional Wormhole vs. Byzantine Wormhole

(i) In traditional wormhole attack, the malicious nodes can make the legitimate nodes to think of existence of a direct communication link between them [9]. In Byzantine wormhole attack there exist wormhole communication links between the malicious nodes and not between the legitimate nodes.

(ii) In traditional wormhole attack, the malicious nodes are generally external nodes which do not take part in network operations. In Byzantine wormhole attacks, the malicious nodes are internal nodes taking full participation in the network operations.

(iii) Traditional wormhole attack is an external attack which do not require authentication for external nodes & is initiated after a network is formed. Byzantine wormhole attack is an internal attack initiated by authenticated internal nodes.

10.11 Routing attacks

Routing is the most important service of any network and also the primary target of malicious nodes. Attacks can be initiated in routing protocols itself or on packet forwarding or delivery.

Attacks on routing protocols aim to block the propagation of the correct routing information to a victim node even if there exist some routes from victim to other nodes in the network by attacking the inherent flaws present in routing protocols.

Attacks on packet forwarding or delivery try to disturb the packet forwarding or delivery along a predefined path are initiated by selfish nodes or malicious nodes & are usually hard to detect. Nodes can show selfish behavior such as dropping of route packets to conserve its battery power that are assumed to be forwarded. Nodes can even show malicious behavior by using denial-of-service attack such as sending out overwhelming network traffic to any victim node so as to exhaust its battery power.

Some possible attacks can be: -

(i) Routing table poisoning attacks
The malicious node can corrupt the routing tables of other nodes in the network which would result in false routes, selection of non-optimal paths, routing loop formation and even congestion in some portion of the network.

(ii) Routing table overflow attacks
This type of attack is initiated at route discovery phase by a malicious node which sends a lot of route advertisements for non-existent nodes. The victim's routing tables are overflowed from these bogus requests and it prevents the discovery of new routes. Proactive routing protocols which update their routing information periodically are more affected than the reactive protocols.

(iii) Route cache poisoning attacks
A legitimate node can update its routing table with the vital routing information contained in the routing packets that it hears (receives through RREQ broadcasting) even if it is not an intermediate node. A malicious node can gain advantage of this situation to poison the route cache of a victim node by sending spoofed routing information packets causing the neighboring nodes to update their routing tables erroneously.

10.12 Sybil attacks
Sybil attack refers to the generation of several fake identities of non-existent nodes by a single malicious node which presents itself as a large number of malicious nodes conspiring together. The new fake identities generated are termed as Sybil nodes. Each Sybil node may generate a new identity for itself or may impersonate a legitimate node.

Sybil attack aims at disrupting network services such as fair allocation of resources because Sybil nodes may present themselves at various locations in the network. Moreover Sybil nodes make it difficult to identify the misbehaving nodes in the network.

11. ATTACKS ON TRANSPORT LAYER

11.1 Session Hijacking
Most of the routing protocols are protected only at session startup only but not thereafter and this fact can be used by malicious nodes to take advantage for some disruptive purposes. The malicious node can spoof (steal) the identity such as IP address of a victim node and may start a session with the target node.

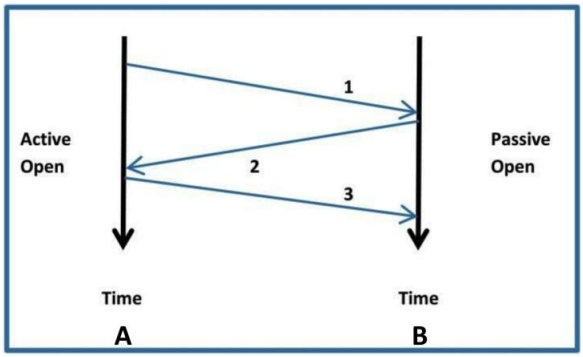
Session Hijacking is planned in two steps: -

(i) The malicious node snoops (steals) the victim's IP address so as to impersonate the victim node. It determines the correct sequence number expected by the target and starts a legitimate session with the target node.

(ii) The malicious node starts a denial-of-service attack on the victim node with a view to continue the session with the target node.

11.2 SYN flooding
SYN flooding attack is a denial-of-service attack targeted at Transport layer. The malicious node tries to keep multiple half-opened TCP connections with a legitimate node and keep these connections without providing them the chance to complete the whole phase of synchronization.

A normal TCP handshake: -



(1) Node **A** sends a SYN segment to node **B**. It only sets the SYN flag, no real data is transported.

(2) Node **B** sends a SYN + ACK segment to node **A**.

(3) Node **A** sends an ACK segment which acknowledges receipt of second segment.

Malicious node sends a large number of SYN segments to a legitimate node, pretending each of them is coming from a different node by faking the sender's IP addresses in the datagrams. The legitimate assumes that other legitimate nodes are issuing open request commands; it therefore allocates necessary resources for it. It sends SYN + ACK segments to nodes which pretend they to be legitimate and gets lost in the route itself. A lot of resources are consumed in this way.

The malicious node monopolizes a node by issuing a number of fake SYN requests, which causes it to run out of resources, then denying service to every request made afterwards and may even collapse.

12. ATTACK ON APPLICATION LAYER

12.1 Repudiation
A non-repudiation service policy grants that committed actions cannot be denied by sender or receiver. A receiver cannot deny that a message has not been received and sender cannot deny its participation in sending the message. Security measures implemented at Network layer & Transport layer do not solve the problem of authentication or non-repudiation in general.

Repudiation can also be seen as a malware whereas an attacker node keeps accessing the network as a selfish node and deny any participation in network operations thereafter.

13. CONCLUSION
Mobile adhoc networks are adding a new dimension in communication technology and currently an emerging research field in computer science. MANETs are lucrative to use owing to their flexibility which presents a tradeoff with its security. MANETs are soft targets for users with unfair intentions. MANETs present a host of security flaws which makes them more vulnerable to attacks than wired networks. Traditional techniques of detection & prevention of attacks cannot be easily integrated into MANETs. For designing efficient techniques for detection & prevention of attacks an in-depth study of various possible attacks is presented in this paper. From the literature presented it is crystal clear that MANETs are an easy host for numerous types of attacks. Proper security policies & measures should be considered or designed taking in consideration the features & applications of mobile adhoc networks.

14. REFERENCES
[1] Gurnam Singh, Gursewal Singh. "Detection & Prevention of Blackhole using Clustering in MANET using NS2". IJECS Volume - 3 Issue -8, August 2014.

[2] Arif Sari, Dr. Beran Necat. "Securing mobile ad-hoc networks against jamming attacks through unified security mechanism". IJASUC Volume - 3, Issue - 3, June 2012

[3] Wenjia Li and Anupam Joshi. "Security Issues in Mobile AdHoc Networks - A Survey". University of Maryland, Baltimore County.

[4] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato. "A survey of routing attacks in Mobile ad hoc networks". IEEE wireless communications, October 2007

[5] Shikha Jain. "Security threats in Manet: a review". IJIT, Vol.3, No.2, April 2014

[6] Mohammad Rafiqul Alam. "Detecting Wormhole and Byzantine Attacks in Mobile ad hoc Networks". Curtin University of Technology May 2011.

[7] Gagandeep, Aashima, Pawan Kumar. " Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review". IJEAT, Volume-1, Issue-5, June 2012.

[8] Upma Goyal, Mansi Gupta and Kiranveer Kaur. "Meliorated Detection Mechanism for the detection of Physical Jamming Attacks under AODV and DSR protocols in MANETs". IJAIEM, Volume 3, Issue 10, October 2014.

[9] R. Sivakami and G. M. Kadhar Nawaz. "Defending against security breaches of byzantine attacks in manets". ARPN, VOL. 10, NO. 8, MAY 2015

[10] Sevil Şen, John A. Clark, Juan E. Tapiador. "Security Threats in Mobile Ad Hoc Networks". University of York, YO10 5DD, UK