



### ATTACKS ON MOBILE AD-HOC NETWORKS

Chander Diwaker<sup>1</sup>, Sunita Choudhary<sup>2</sup>, Poonam Dabas<sup>3</sup>

<sup>1,3</sup>Faculty of Computer Sc. & Engineering, <sup>2</sup>Research Scholar,

Department of Computer Science & Engineering, University Institute of Engineering & Technology,  
Kurukshetra University, Kurukshetra -136 119, Haryana, INDIA.

**Abstract:** MANET became a popular research area among researchers due to their flexibility and independence of network infrastructures. Routing in MANET is a challenging issue due to dynamic network topology, limited bandwidth, and limited battery power. Early work in MANET research has mainly focused on various kinds of attacks to find and remove malicious nodes. In MANET, routing attacks are particularly serious issue. In this article, we have examined certain routing attacks in MANET.

**Keywords:** MANET, Security, Attack

## I. Introduction

MANET is a collection of mobile nodes connected by wireless links. Mobile nodes are self configured and can move in any direction freely. Each mobile node acts like a host and as well as a router. Mobile nodes within the range of each other can communicate with each other without the need of any base station. Mobile nodes which are not within the range of each other can communicate with each through multi hop relaying. For example, when node A want to communicate to node C, then message will go through A-B-C- as shown in the fig1. Here, a node B acts as router.

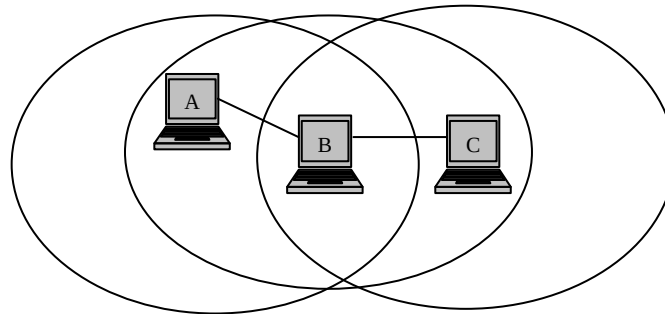


Fig 1 Routing in MANET

Mobile ad hoc networks are more vulnerable to attacks than wired networks because of its inherent characteristics such as dynamic topology, no central authority, limited resources, insecure operational environment etc. Due to these characteristics, security requirements such as integrity, authentication, confidentiality, availability etc are difficult to achieve. Thus security is primary concern in Mobile ad hoc networks. In this paper, we will describe various types of attacks which occur in different layers of MANET.

## II. TYPES OF ATTACKS

Attacks can be classified on the basis of the domain of attacks and behaviour of attacks is described in fig. 2:-

### A. ON THE BASIS OF DOMAIN

On the basis of domain, attacks can be classified as external and internal attacks. **External attacks** are caused by the nodes which are not a part of the network. External attacker wants to gain access to the network to disrupt the network functionality, to cause congestion in the network. These attacks can be prevented by implementing security measures such as firewalls. **Internal attacks** are caused by the nodes which are a part of the network. They want to gain access to the network either by compromising a current node in the network or by entering in the network as a new node. Internal attacks are more severe than the external attacks [4].

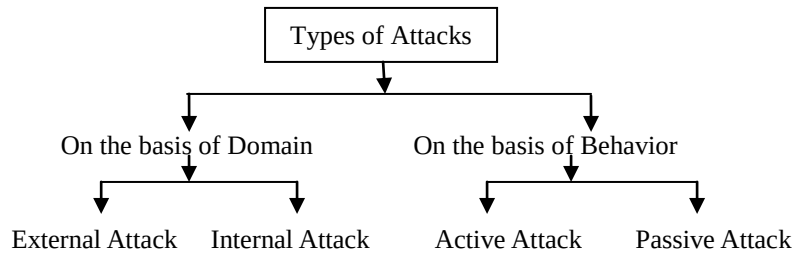


Fig 2 Types of Attacks

### B. ON THE BASIS OF BEHAVIOUR

On the basis of behaviour, attacks can be classified as active and passive attacks. Attackers in **passive attack** in the network do not disrupt the operation of the network. In order to attack a network, attack must have complete information about the network. Thus they simply listens the network in order to get complete information about the network such as how the nodes are located in the network, how they are communicating to each other etc. Passive attacks are difficult to detect because they do not make any changes in the network operations. Attackers in active attacks disrupt the network operations. They steal the important information about the network operations and then try to change the important data during the information exchange. Active attacks can be caused either by internal or external nodes [4].

### C. TYPES OF ATTACKS IN VARIOUS LAYERS OF MANETS

Attackers can also attack on various layers of MANET. Thus attacks can also be classified according to at which layer the attack lies. These are described below:-

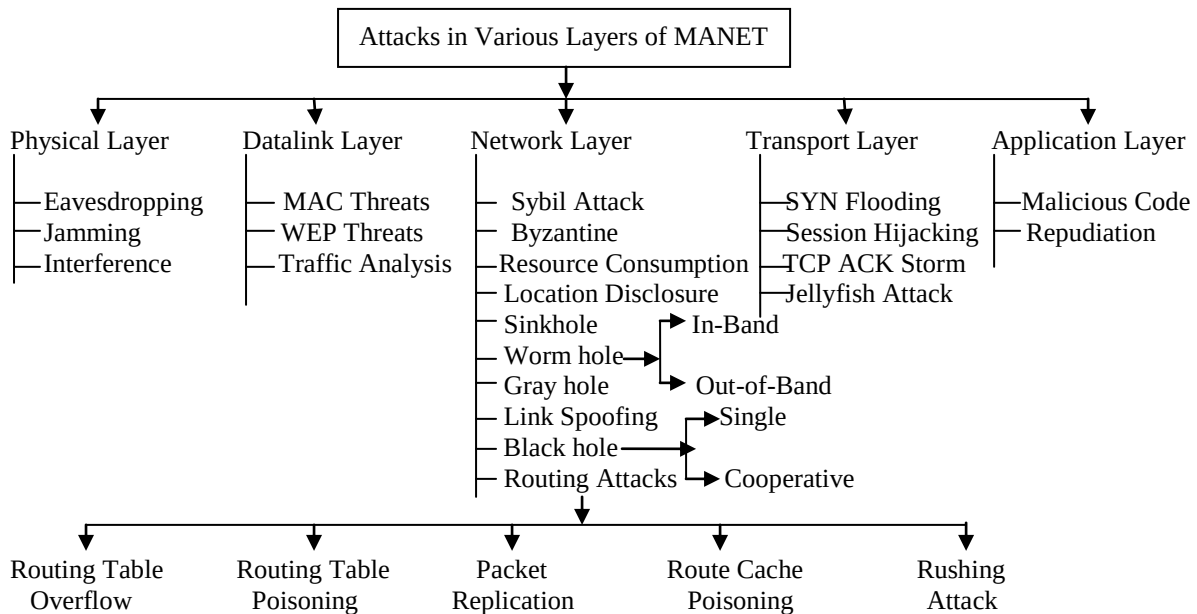


Fig 3 Attacks in various layers of MANET

### D. Physical layer Attacks

#### 1. Eavesdropping

Eavesdropping can be defined as reading of messages and conversation by the unintended receiver. In MANET,

Communication takes place on the wireless medium and usually use radio frequency spectrum for transmission and broadcast by nature. So any intruder having receivers tuned to proper frequency can intercept the messages and include duplicate messages during the transmission [1].

## 2. Jamming

Jamming is a special type of DOS attack. Once an attacker knows the transmission range of the communication, he/she can jam the network by sending too much messages. Due to jamming, the mobile nodes cannot receive the legitimate messages. Thus the network operation disrupts due to jamming [1].

## 3. Interference

Interference can block the wireless communication channel or disrupt the communication. An attacker can change the order of messages or can replay the old /stale messages. In this way, overall network operation is disrupted by the intruders [2].

### E. Data Link Layer Attacks

#### 1. Attacks in IEEE 802.11 MAC

This attack is exposed in IEEE 802.11 MAC through NAV (Network Allocation Vector) field carried in the RTS/CTS (Ready to Send/Clear to Send) frames. During the RTS/CTS handshake, a small RTS frame including the time needed to complete the CTS, data and ACK frames is sent by the sender. All the neighbors of the sender and receiver update their NAV field according to the time that they overheard for transmission duration. The attacker is also aware of the duration of the ongoing transmission and he/she may transmit a few bits within this period to incur bit errors in a victim's link layer frame via wireless interference [3].

#### 2. Attacks in IEEE 802.11 WEP

WEP (Wired Encryption Privacy) is provided to enhance the security in the wireless communication. But this has also many weaknesses and is vulnerable to attacks [1].

- WEP protocol does not specify key management
- The reuse of IV and weakness of RC4 help to produce analytic attacks.

#### 3. Traffic Analysis and Monitoring

In this attack, the intruder continuously monitors the network traffic in order to get important information about the network such as location of the nodes, information exchanged during the communication. Confidential information about the network can be derived by analyzing the network. It can be passive or active [2].

### F. Network Layer Attacks

#### 1. Wormhole Attack

In this attack, a malicious node captures packet at one location of the network and tunnels them to another location in the network through a very high speed link where these packets are replayed back into the network. There are two types of wormhole attacks.

##### i. IN-Band Wormhole Attack

An in-band wormhole does not use external communication medium to develop a link between the colluding nodes. In-band wormhole is more harmful than out-of-band wormhole because it does not require any external hardware device and consumes existing communication medium to transmit the tunnelled traffic. Figure 4 shows an in-band wormhole developed over a wireless network between nodes C and H. The attracted traffic is forwarded with the help of a third colluder node E [5].

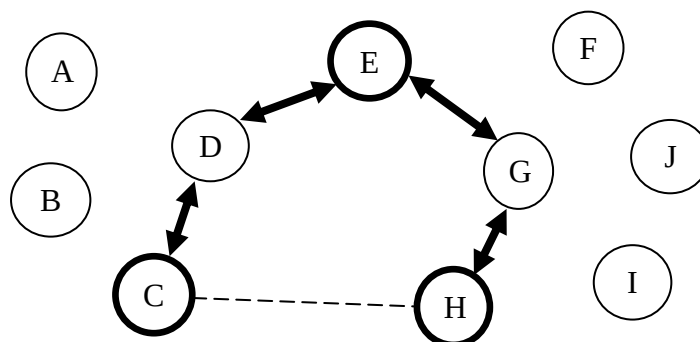


Fig 4 In-Band Wormhole between nodes C and H

## ii. Out-of-Band Wormhole Attack

In Out-of-band wormhole, the colluder nodes establish a direct high speed link between them using a wired link or a long range wireless transmission. Figure 5 shows an out-of-band wormhole established in a network by two colluding nodes [5].

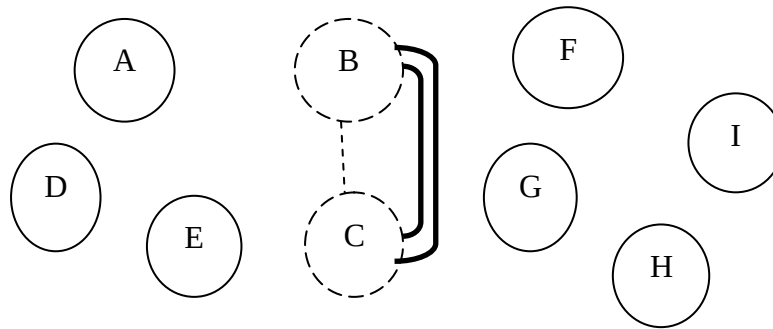


**Fig 5 Out-Of-Band link between attacker nodes B and C**

## 2. Black hole Attack

In this attack, the malicious node advertises fake routing information such as it has the shortest and stable path to reach the destination, and causes the other good nodes to establish the path through this malicious node. Once the path is established, then it either drops the data packets, or changes the routing updates packets. This creates unnecessary confusion in the routing process [10]. Black hole attack can be of two types [11]:

### i. Single Black Hole Attack

In this, a single node creates a black hole and disrupts the network operation. A single black hole attack can easily happen in the network [11]. This is shown in the fig 6:

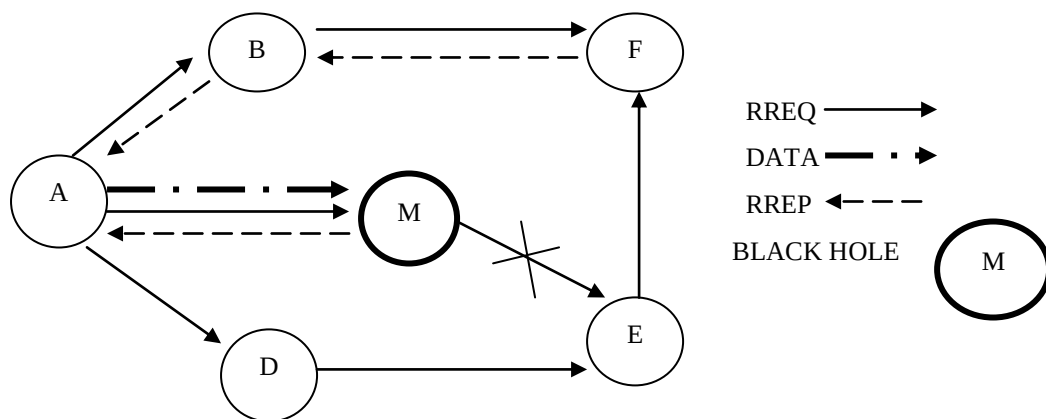


**Fig 6 Single Black hole Attack**

In this figure 6, node M is a malicious node. When node A broadcasts a RREQ packet, nodes B, D, and M receive it. Node M does not check its routing table whether it has route to node E or not. It immediately sends back a RREP packet, claiming that it has shortest path to node E. Node A receives RREP from node M ahead than RREP from node B and D. Thus, node A establishes path to node E through malicious node M and starts sending data packets. After receiving data packets from node A, malicious node M does not forward data packets; it simply drops them, and behaves like a black hole.

### ii. Cooperative Black Hole Attack

There can be more than one node which is cooperating with the single black hole, making them invisible from the other honest nodes [11]. The cooperative black hole attack is shown in figure 7.

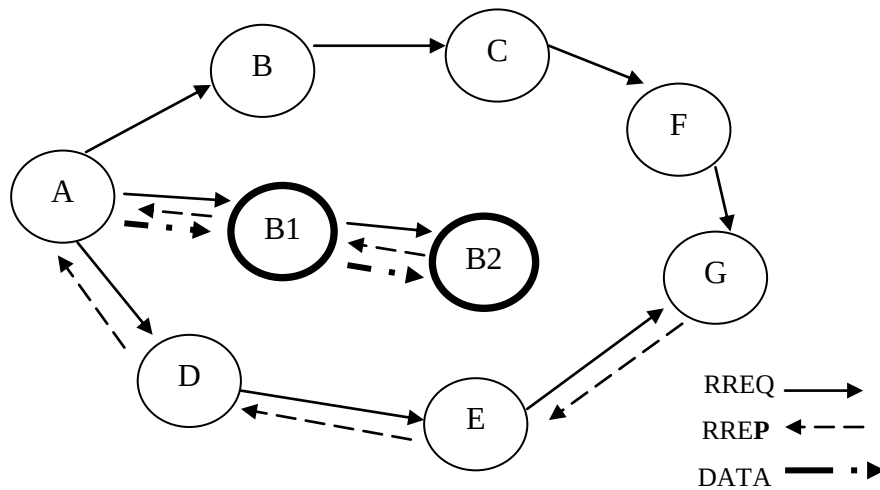


**Fig 7 Cooperative Black hole Attack**

When the source node A wants to send data to destination node G, it follows normal route discovery process. Here node B1 and B2 are colluding with each other. Hence, when B1 receives RREQ from node A, it further transmits it to node B2. B2 responds to RREQ with a RREP without checking whether it has route or not. Thus, B1 is first to respond to RREQ, source A believes that it has reliable route through B1 because B1 next hop B2 is also responding. Node A starts sending data through B1. B1 forwards data packets to B2, but B2 drops all the data packets. Cooperative black hole attacks are more difficult to detect than single black hole attack.

### 3. Byzantine Attack

In this attack, a compromised intermediate node or a set of compromised nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets to non-optimal paths or selectively drops data packets. This type of attack is hard to detect because the network seems to be worked as normal [6].

### 4. Resource Consumption

In this type of attack, an attacker tries to consume or waste away the resources of the nodes present in the network. An attacker tries to consume battery of victim node by unnecessarily sending route requests or forwarding excessive packets to the victim node. This attack is also known as sleep deprivation attack [2].

### 5. Location Disclosure

Location disclosure attack is a part of information disclosure attack. The malicious node wants to get information about the location of the nodes, status details of the nodes, public or private key. A compromised nodes present in the network can provide these information to the unauthorized nodes. Any confidential information exchange must be protected from these compromised nodes. They gather the node location information and plan the attack scenarios [7].

### 6. Gray hole Attack

A gray hole attack is a variation of black hole attack in which malicious node either selectively drops the packets or drops the packet for some time and then switches to its normal behaviour. Malicious node behaves as an honest node during the route discovery process and then silently drops some or all of the packets sent to it for further forwarding. Detection of gray hole attack is harder. It is also termed as node misbehaving attack [6].

### 7. Sybil Attack

In this attack, the Sybil attacker tries to act as several different identities/nodes. These additional identities achieved by malicious node are called Sybil nodes. The malicious node may fabricate new identities for itself or steal an identity of a legitimate node. Thus it makes difficult to identify the honest nodes in the network and prevent the fair allocation of resources among the network [2].

### 8. Sinkhole Attack

Sinkhole attack tries to attract all the traffic of its neighbouring nodes. Sinkhole attack can be implemented on ad hoc networks by using flows such as maximizing the sequence number or minimizing the hop count. In this way, path presented by the malicious node seems the shortest and fresh path and the source node establishes its path through the malicious node. By attracting the whole network traffic, it can change the confidential information such as make changes to the data packets or drops the data packets [9].

## 9. Link Spoofing Attack

In this attack, attacker sends fake link message to the non-neighbouring node. Thus it causes the target node to choose the attacker node as its multi point relay node. As an MPR node, attacker can intercept or drop the messages. Thus the network performance becomes worst [1].

## 10. Routing Attack

### i. Routing Table Overflow

In routing table overflow, an attacker creates routes to non-existent nodes in the network. The goal is to cause an overflow of the routing table which in turn prevent to create new routes to authorized nodes from being created [8].

### ii. Routing Table Poisoning

In route table poisoning, the compromised nodes present in the network send false routing updates or modify genuine route update packets sent to authorized nodes. Thus, routing table poisoning cause congestion in the network, or even make some part of the network inaccessible [8].

### iii. Packet Replication

In case of packet replication, the attacker replicates stale packets. This consumes additional bandwidth of the network and additional resources available to the nodes. It also causes unnecessary confusion in the routing process [6].

### iv. Route Cache Poisoning

In case of reactive routing, each node maintains a route cache which holds information of the routes that are used by the nodes in the recent past. Similar to the route table overflow, malicious node can also poison the route cache of the node [6].

### v. Rushing Attack

Reactive routing protocols are more vulnerable to this attack. A malicious node which receives the route request packet from the initiating node, immediately floods the packet throughout the network. When the nodes receive the original route request, they assume that it is duplicate route request and discards it. Thus, any route established by initiating node will contain the malicious node as one of its intermediate node. Hence, source node would not be able to establish secure route in the network [6].

## G. Transport Layer Attacks

### 1. SYN Flooding Attack

TCP connection between two communicating parties is established by completing three way handshakes. Thus SYN Flooding attack is performed by creating a large number of half-opened TCP connections with the target node. The intruder sends a large number of SYN messages to the target node, but does not send the acknowledgement to the target node. Thus, the target node becomes unavailable for some time [3].

### 2. Session Hijacking

All the communications are authenticated at the beginning of the session. The intruder spoofs the victim's address and the correct sequence number. The attacker behaves like the victim node and continues the session. Then intruder steals all the confidential information which is exchanged during the transmission [1].

### 3. TCP ACK Storm

TCP ACK Storm occurs after the malicious node hijacks the session. When node A hijacks the Node B, then he will inject the session data and node B sends the acknowledge packet to the node with which it is communicating (here node C). But the packet will not contain the sequence number which is expecting node B. Then node C will send the packet to node B to resynchronize the connection [2]. This process repeats over and over.

### 4. Jelly Fish Attack

In this attack, the attacker first gains access to the network and become a part of the network. The attacker needs to intrude the forwarding group. It delays the data packets for some amount of time before forwarding the packets. Thus attacker achieves the high end to end delay and performance of the network becomes worst [1].

## **H. Application Layer Attacks**

### **1. Malicious Code Attacks**

Malicious code attacks include viruses, worms etc. They can infect the operating system and application software installed on the mobile nodes [2].

### **2. Repudiation Attacks**

Repudiation is the participation in the whole or a part of the communication by the intruder. Then intruder can disrupt the operation of the network. Many encryption mechanism and firewall are installed, but these are not sufficient to prevent the communication from intruders [2].

## **III. Conclusion**

Security is an important aspect in MANETs. In this paper, different types of attacks based on different layers of MANET are studied. Studying of attacks on different layers of MANET makes it easy to understand the security attacks easily. After the study of attacks, it is concluded that network layer is more vulnerable to attacks. Thus, more attention is given to network layer attacks. In future, more attacks can be finding out which will affect the various layers of MANET.

## **References**

1. Mohammad Wajid, Rajesh Kumar Singh, R. H. Goudar, "A Survey of Attacks Happened at Different Layers of Mobile Ad Hoc Network & Some available Techniques" In Proceedings by International Journal of Computer Applications (IJCA), 2011
2. Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A- Review" In International Journal of Engineering and Technology (IJEAT), ISSN: 2249-8958, Volume -1, Issue-5, 2012
3. Kamanshis Biswas and Md. Liakat Ali, Master of Science in Computer Science, Thesis on "Security Threats in Mobile Ad Hoc Network" Submitted to Department of Interaction and System Design, 2007
4. B. Revathi, D. Geetha, "A Survey of Cooperative Black and Gray hole Attack in MANET" In International Journal of Computer Science and Management Research, Vol 1 Issue 2, ISSN 2278-733X, Sep 2012
5. Cong Hoan Vu, Adeyinka Soneye, Master Thesis on "An Analysis of Collaborative Attacks on Mobile Ad Hoc Networks" Submitted to Blekinge Institute of Technology, 2009
6. G. S. Mamatha, Dr. S. C. Sharma, "Network Layer Attacks and Defense Mechanisms in MANETs- A Survey" In International Journal of Computer Applications (0975-8887) Volume 9- No. 9, 2011
7. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks" In Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D. -Z. Du (Eds), 2006 Springer
8. Vikas Soloman Abel, "Survey of Attacks on Mobile Ad Hoc Wireless Networks" In International Journal of Computer Science and Engineering, Vol. 3, No. 2, 2011
9. Priyanka Goyal, Sahil Batra, Ajit Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks" In International journal of Computer Applications (0975-8887) Volume 9 – No. 12, 2010
10. N. Shanthi, Dr. Lganesan, Dr. K. Ramar, "Study of Different Attacks on Multicast Mobile Ad Hoc Network" In Journal of Theoretical and Applied Information Technology, 2005-2011 JATIT
11. Fan-Hsun Tseng, Li-Der Chou, Han-Chieh Chao, "A Survey of Black Hole Attacks in Wireless Mobile Ad Hoc Networks" in Human- Centric Computing and Information Sciences, 2011