Evaluation of Attacks using different Parameters based on their performance

Monica[1], Lalita Luthra[2]

Department of Information Technology, Northern India Engineering college, New Delhi

[1] monica.batra88@gmail.com
[2]lalita.luthra@gmail.com

***ABSTRACT* - The objective of this paper is to analyze, simulate and perform comparative study of three attacks based on various parameters namely, denial of service attack, wormhole, black hole attack for wireless ad hoc networks based on the performance, and comparison has been made on the basis of their properties like throughput, Packet Delivery Ratio (PDR) and End to End Delay with respect to the number of nodes. These three attacks have different properties and based on the way they are designed, they behave differently in different environments. Therefore it becomes essential to analyze each attack by simulating it in an ideal environment and find out how it performs, so that appropriate methodologies could be followed in the future research works to improve on the areas where a protocol is lacking.**

***Keywords* - Manets, Networking, Attacks, Performance, delay.**

I. INTRODUCTION

Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free to move in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile[3]. A mobile adhoc network (MANET) is a spontaneous network that can be established with no fixed infrastructure. It implies that all the nodes work as routers and take part in its discovery and maintenance of routes to other nodes in the network i.e. nodes which are in one another's radio range communicate directly via wireless links, while those that are further apart use other nodes as relays. It is an infrastructure less IP based network of mobile and wireless machine nodes connected with radio. While operating, the host of a MANET have no centralized administration mechanism. It is known for its routable network properties where each node act as a "router" to forward the traffic to other specified node in the network, power supply. All these challenges have created new demands on MANET routing protocols [1].

A. MANETS

A MANET is collection of autonomous mobile users that communicate over relatively bandwidth constrained wireless links. Mobile Ad-hoc Networks (MANETs) are new future wireless networks comprising entirely of moving nodes which can communicate on-the-move without base stations. In this type of networks nodes will generate both user and application traffic to carry out control of and routing protocols. Connectivity change, highest rate of error, partitions in the network ,collision interference, bandwidth and constraints on power combined together to pose newer problems in the entire network control—particularly in the design of higher level protocols such as routing and in implementing applications with Quality of Service requirements

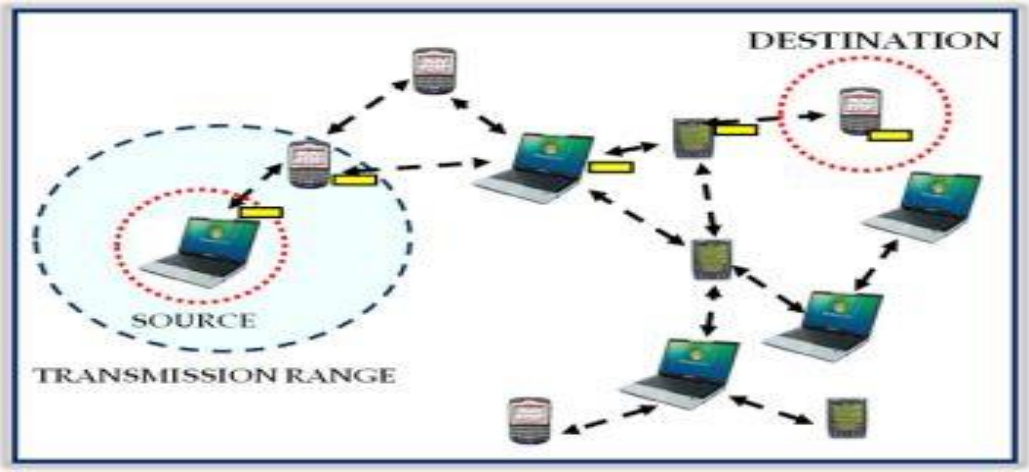

Fig. 1.1: Mobile Ad-hoc Network (Manet)

II. CHARACTERSTICS OF MANETS

MANETs have several salient characteristics namely[2][7]:

- **Dynamic topologies**:

Nodes can move arbitrariliy; thus, the network topology—having multi-hop may change randomly and frequently in unpredictable times, and may consist of both bidirectional and unidirectional links.

- **Bandwidth-constrained,variable capacity links**

Wireless links will be having muchg lower capacity as compared to their hardwired counterparts. In this context , the throughput of wireless communications which has been realized --after accounting for the effects of multiple access, fading, noise, and interference conditions,etc.--is often much less than a radio's maximum transmission rate.

- **Energy-constrained operation**

We can say that some or all of the nodes in a MANET may depend on batteries or other exhaustible means for their energy. Energy conseravtion is the most important factor for these nodes..[7]

- **Limited physical security**

Mobile wireless networks are generally more prone to physical security threats than are fixed-cable nets. There is great possibility of eavesdropping, spoofing, and denial-of-service attacks so it should be considered carefully . All the characteristics set an underlying bases for assumptions and performance concernd issues for protocol design which extend beyond those guiding the design of routing within the higher-speed, semi-static topology of the fixed Internet

III. CLASSIFICATION OF ATTACKS

Categorization of attacks can be done based on source of the attacks i.e. Internal or External, and on the behavior of the attack i.e. Passive or Active attack. This classification is of much use because the attacker can ruin the network either internaly, externaly..

A. External and Internal Attack

Attacks that directly leads to the attacks on nodes presents in network and links all the interface between them. This type of attacks may broadcast wrong type of routing information to other nodes [5,6]. Congestion in the network can be caused by external attcaks, denial of services (DoS), and advertising wrong routing information etc [6]. External attacks are designed to prevent the network from different type of normal communication and restrict it from producing additional overhead over the network.

B. Attacks on Routing :

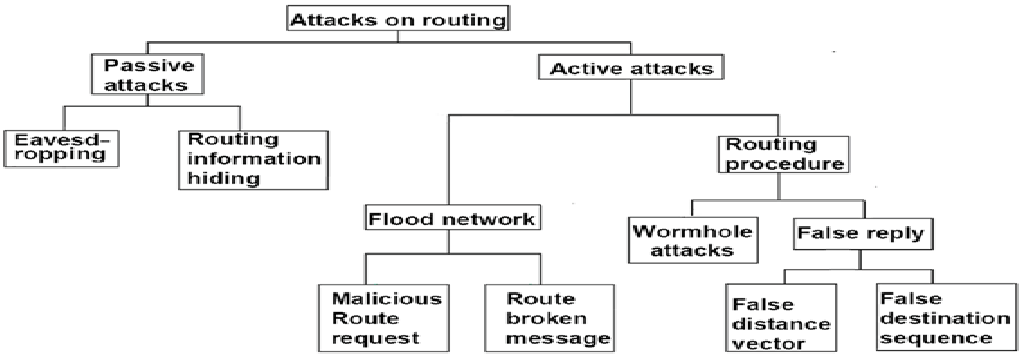

Figure1.2: Categorization of attacks

Figure 1.2 shows categorization of different attacks on routing.,showing seoerate classification for active and passive attacks.

C. Active and Passive Attack

MANETs are more susceptible to Active Attacks which are very severe on the network that prevent flow of messages between the nodes. Attacks can be internal or external.[8]Active external attacks can be performed by outside sources which do not belong to the network .A passive attack does not alter the data transmitted within the network. But due to inclusion of unauthorized “listening” to the network traffic or accumulation of data from it. Passive attacker never tries to disrupt the operation of a routing protocol but ries to attempts to discover the important information from the routed traffic [5, 9]. Detecting these type of attacks is very difficult as the operation of network itself doesn’t get affected.

IV. ATTACKS COMPARED

A. Denial of Service

In this type of attack, an attacker attempts to prevent legitimate and authorized users from the services offered by the network. A denial of service (DoS) attack can be performed in many different ways.[10] The classic way is to flood packets to any centralized resource present in the network so that the resources are no longer available to all the nodes in the network, as a result of which the network no longer operating in the manner it was designed to operate. This may lead to a failure in the delivery of guaranteed services to the end users. [13]which would not be possible in wired . The server or host in network will not be able to locate the return address of all the attacker while sending the authentication approval, causing the server to wait before closing the connection. When the connection is closed by the server , more authentic messages are sent by the sender with invalid return addresses.

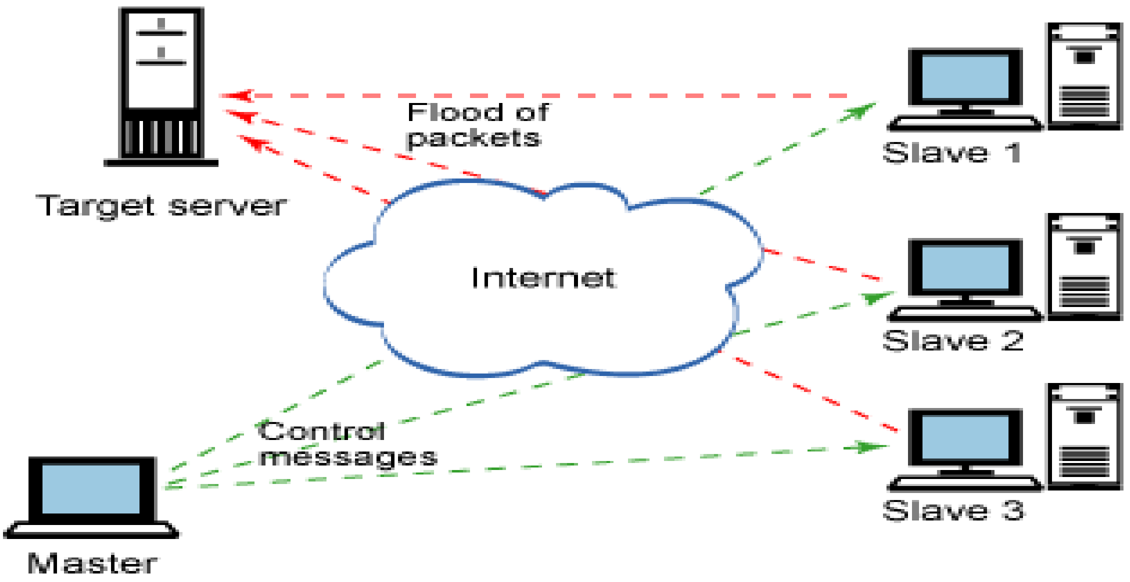

Figure 1.2: Denial of service attack

B. Blackhole attack

In this attack, the malicious node uses one of the routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This node advertises the availability of new routes without checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [4]. Some of the protocols which are based on flooding, the reply of the malicious node will be received by the requesting node before receiving the reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address [5].

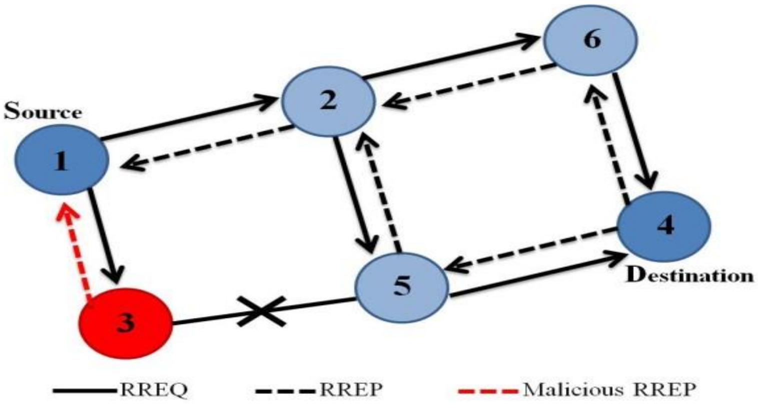

Fig. 1.3: Black hole Attack

C. Wormhole attack

Tunneling attack is also called wormhole attack. During a tunneling attack, an attacker gets the packets at one point in the network, and tunnels them to another point in the network, and then replays them into the network from that point. It is named tunneling attack as the colluding malicious nodes which are linked through a private network and is invisible at various higher layers [12]

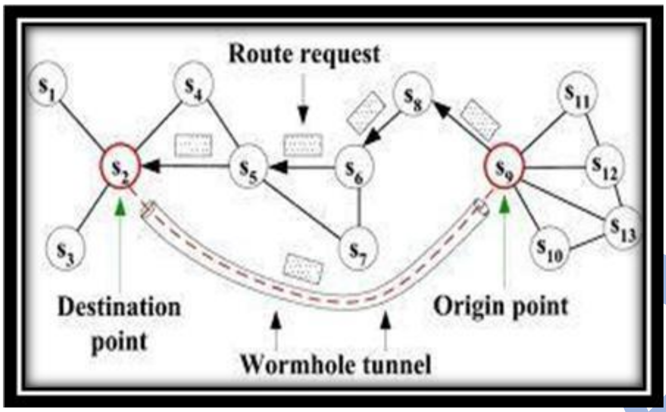

Fig. 1.4: Wormhole Attack

Three Step Procedure of Wormhole Attack Detection[11] :

The proposed scheme for wormhole attack detection consists of the following three steps:

1) Perform statistical analysis of the routes obtained from one route discovery. If anomalous patterns occur, go to step 2. Otherwise, choose several paths to feedback tothe source node.

2) Test the suspicious paths by sending (test) data packetsand wait for ACK.

3) If attack is confirmed, report to security authority and/or notify the source and the neighbors of the attackers inorder to isolate the attackers from the network.

V. PERFORMANCE ANALYSIS

Parameters used are:

1) Packets Received: It refers to the no of packets that has been received in the network.

2) Packets lost: Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Loss of packet is identified differently as one of the main error types found in digital communications; the other two being bit error and spurious packets caused due to noise.

3)Bytes transferred: It mean how much amount of data has been transferred in terms of bytes.

4) Bit rate expected delay: Bit rate, as the name implies, describes the rate at which bits are transferred from one location to another. In other words, it measures how much data is transmitted in a given amount of time. Bit rate is commonly measured in bits per second (bps), kilobits per second (Kbps), or megabits per second (Mbps)

Table I
Parameter Evaluation

Sno	**Parameter**	**Wormhole Attack**	**Blackhole Attack**	**Dos attack**
1	packets transmitted	high	Very low	low
2	Packets lost	Very less	Very high	less
3	No of bytes transmitted	high	low	low
4	Bitrate	high	Less than wormhole	Less from both

VI. CONCLUSION

Mobile Ad-Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. Security of MANET is one of the important features for its deployment. In this paper, we have analyzed the behavior and challenges of security threats in mobile Ad-Hoc networks. In our study we analyzed that Black Hole attack ,denial of service attack ,wormhole attack with four different scenarios with respect to the performance parameters of end-to-end delay, throughput and packet lost packet transmitted and etc. We have compared the blackhole, wormhole, denial of service attack on the basis of their performance using different parameters. In the end we can conclude that rate of data loss is very less in wormhole attack as compared to black hole and denial of service attack.

REFERENCES

[1] Senthil kumar P., Baskar M. and Saravanan K., "A Study on Mobile Ad-Hock Networks (MANETS)", JMS, Vol. No.1, Issue No.1, September 2011.

[2] M. Ilyas, "The Handbook of Ad Hoc Wireless Networks," CRC Press, 2003.

[3] L. Zhou, Z.J.Haas,Cornell Univ., "Securing ad hoc networks,"IEEE Network, Nov/Dec 1999,Volume: 13, Page(s): 24-30, ISSN: 0890-8044

[4] Prof. Mohit Dua, Prof. Virender Ranga Ms. Krishma Mehra, Mr. Pawan Kardam, Ms. Snehal Mohan Bahsakhetre Department of Computer Engineering "Performance evaluation of AODV, DSR, DSDV Mobile adhoc protocols on different scenarios: An analytical review"

[5] Mohammad Ilyas, "The Handbook of Ad Hoc Wireless Networks",

[6] Amitabh Mishra, "SECURITY AND QUALITY OF SERVICE IN AD HOC WIRELESS NETWORKS" (chapter 1, 3), ISBN- 13 978-0-521-87824-1 Handbook.

[7] IETF MANET Working Group. "Mobile Ad Hoc Networks (MANET). Working

[8] Vikrant Gokhale, S.K.Gosh, and Arobinda Gupta, "Classification of Attacks on Wireless Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks a Survey".

[9] Panagiotis Papadimitratos and Zygmunt J. Haas "Securing Mobile Ad Hoc Networks".

[10] B. Awerbuch, D. Holmer, C. Nita Rotaru and Herbert Rubens. "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures". Proceedings of the ACM Workshop on Wireless Security 2002, Pages 21-30, September 2002.

[11] Y.C. Hu, A. Perrig, and D.B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols", Proceedings of ACM WiSe 2003, San Diego, CA, Sep. 2003.

[12] PRADIP M. JAWANDHIYA, MANGESH M. GHONGE "A Survey of Mobile Ad Hoc Network Attacks". International Journal of Engineering Science and Technology Vol. 2(9), 2010, 4063-4071

[13]L. Zhou and Z. J. Haas. "Securing Ad Hoc Networks". IEEE Network Magazine, Volume. 13, no. 6, Pages 24-30, December 1999

[14] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007