Review on Attacks in Mobile Ad-hoc Networks (MANET)

Manju Sehrawat [1], **Praveen Sharma** [2]

M-Tech Student[1]*, Assit. Prof.* [2] *& Department of CSE & NGF College of Engineering &Technology*
Palwal, Haryana, India

ABSTRACT
Mobile ad-hoc networks (MANET) have grown as a major next generation wireless networking technology. This network is a network of mobile stations with dynamic nature. Here each node behaves as a router for routing the data to other nodes. Because of its dynamic structure, security has become a main concern to provide safe communication among various nodes in ad hoc networks. There are various challenges in security design *a*s ad hoc network is a not centralized network. MANET has five layers and each of these layers is susceptible to many attacks. In this paper we talk about large number of attacks and their security mechanisms.

I. INTRODUCTION

Wireless networks are categorised into two major categories: infrastructure based networks and infrastructure less networks. The infrastructure based networks uses the static base stations which are responsible for providing communication between two or more mobile nodes. Infrastructure less wireless networks is a kind of network in which mobile nodes communicates without any central coordinator. MANET (Mobile ad-hoc network) comes under the non-infrastructure or infrastructure less wireless networks. The word ad-hoc means temporary such that a mobile ad-hoc network is not a permanent network of different mobile nodes with no central coordinator [1]. These networks are not based on any hardware. A MANET is a autonomous network in which each node behave as a router to route message to another node that are not inside the same communication area. MANET follows a dynamic structure because in this every node can move randomly in the network [2]. Thus, a node often can change its connection to another node. Due to its dynamic configuration MANET has many applications i.e. in military area, natural disaster recovery, rescue operations etc. MANET can also used in the home, office or a small region of city. Though, MANET supports portability and mobility but is more susceptible and vulnerable to different types of security attacks. MANET not only acquires all the security attacks found in both wireless and wired networks, but also some unique security attacks are also introduced by itself. By the knowledge of some normally Authentic security measures for securing them [2]. The primary objective of this study is to enquire some of the significant issues that might be related to security attacks in MANET and various existing detection and mitigation methods [3].

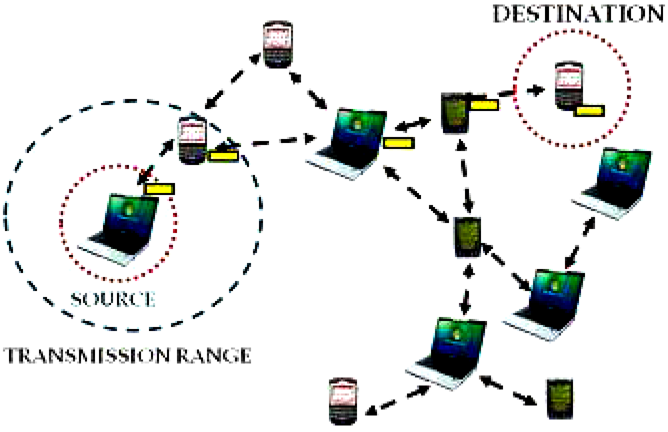

Figure1. Mobile Ad hoc Network

II. ATTACKS IN MANETS

Mobile ad-hoc networks (MANET) are susceptible to large number of attacks not only from outside but also within the network i.e. from inside. The attacks in MANET are classified into two broad categories:

A. *Active Attacks*

Active attacks interrupt the procedure of communication in the network. An active attack could cease the communication among the nodes. An active attack can change the data packet or lose the packet in the network. Thus active attacks interfere the general functionality of mobile ad-hoc network (MANET).

1. Jamming attack

Jamming attack is a kind of denial of service(DoS) attack. This attack uses a word jammer. Jammer means a single entity which deliberately blocks the methods of valid wireless communication. It is a active attack because of its actions. In this attack, a radio signal is interfered or jammed

ISSN: 2278 – 1323

which leads to the message to be corrupted or dropped. The attacker node having a strong transmitter cause that the produced signal will be strong enough to violate the communications and can easily break the directed signal [5]. This attack is developed after deciding the communication frequency.

2. Blackhole attack

In this type of attack, attacker node declares that it has an optimal route to the node whose data packet it wants to utilize. On receiver side, attacker node sends a fraud reply through a very short route. If the node has been capable to create its place between the communicating nodes, then it can do anything with the data packets which are passing between them [1]. A black hole node behave as having a route with the maximum sequence number to the destination node. The black hole node falsely publicizes the shortest route to the destination node with the objective to attract data packets and loss them [1].

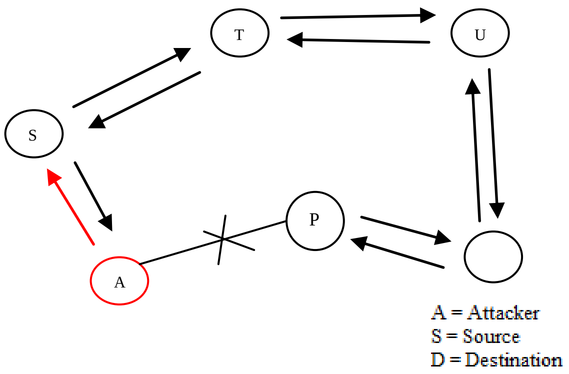

Fig 2: Blackhole attack

3. Greyhole attack

Greyhole attack is a particular type of blackhole attack. In this type of attack, an attacker acts as a part of the routes of the network such as gets the route and then drops data packets in a selective way [2]. One can't assume the probability of dropping data packets. In this attack, attacker node first agrees to route packets and then deny to do so, which leads to losing of data packets.

The Gray Hole attack has two stages: In the first stage, an attacker node manipulate the ad-hoc on demand distance vector (AODV) protocol to behave as having a legal route to the destination node, with the aim of disturbing the data packets, even though the route is false. In the second stage, the attacker node drops the disturbed data packets with a certain chance. This type of attack is more complex to find in comparison of black Hole attack in which the attacker node drops the obtained data packets with surety.

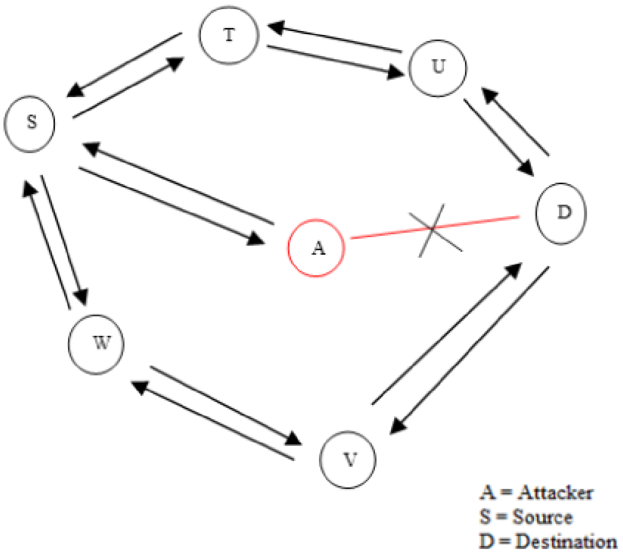

Fig 3: Grey hole Attack

4. Wormhole

Two attacker nodes are present in the network in this type of attack which generates a tunnel. An attacker node gets the data packet from one point in the network and route it to other attacker node. The tunnel live between two attacker nodes which is known as wormhole. Wormhole sets the attacker nodes in a very good situation as compared to other nodes. The attacker node could use this situation in many ways. In this attack, the attacker node obtains the data packets from one location and copies them without any modification at other location or inside the same network.

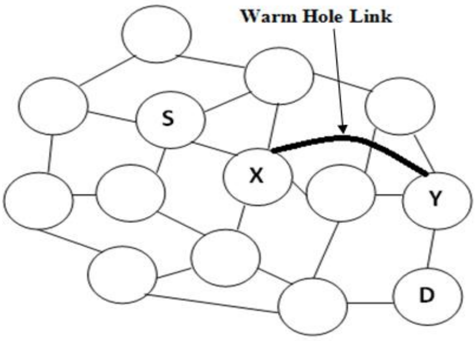

Fig 4: Wormhole Attack

5. Sinkhole attack

In this type of attacks, an attacker node gives false routing information in order to show itself a particular node and thus obtains all network traffic. Once obtaining the all network traffic complicated packet traffic, it alters confidential information i.e. drop the packet or modify the data to build network complicated. An attacker node tries to draw the safe data from all adjacent nodes.

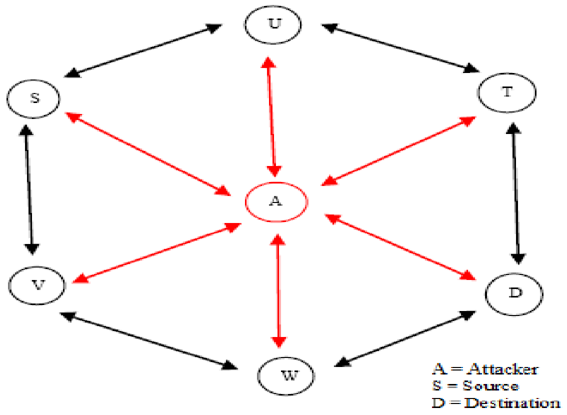

Fig 5: Sinkhole Attack

6. *Rushing Attack*

Rushing attack can also be called novel attack or denial of service attack. In this attack, an attacker node obtains a route request packet from the source node and directly floods it over the network before other nodes which also obtains the same route request packet. Rushing attacks are usually against the on-demand routing protocols.

7. *Sybil Attack*

In mobile ad-hoc network MANET, the medium for transmission of data packets is air and they don't have a centralized node to manage the network. Thus the routing depends on some unique node address. This feature of MANET can be utilized by the attacker for using fraud identities. This means the attacker can either use a identity of legal node or a random identity. This type of attack is called Sybil attack.

In Sybil attack, an attacker may generate multiple fraud identities. The attacker node may introduce itself as a large number of nodes rather a single node. These fraud identities are known as Sybil nodes.This attack may induce lots of data packets to be routed in the direction of fraud nodes.

8. *Jellyfish Attack*

Jellyfish attack is a type of denial of service attack and normally comes under the passive attack. Jellyfish attack creates delay during the reception and transmission of data packets in the network. This attack is not easy to find. Jellyfish attack is like the black hole attack, the only difference is, in black hole attack attacker drops all data packets while in jellyfish attack node creates delay during transmission of data packets.

I. Attacks at Transport Layer

1.) *Session Hijacking*

In this type of attack, the attacker node seeks to get confidential information which could be secret key, password etc. and other important data. An attacker produces a fraud ip address and gets the right sequence number. This attack objectives at gathering confidential data about the nodes.

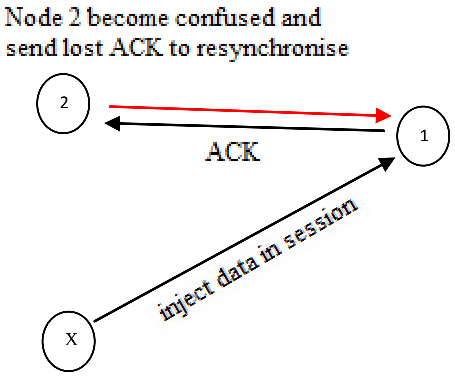

Fig: 6 Session Hijacking

II. Attacks at Application Layer

1.) *Repudiation attack*

Repudiation attack refers to denial of receiving or transmitting the data packet. In this type of attack, either a receiver refuse that he gets a data packet or a sender may refuse that he sends the packet.

B. *Passive Attacks*

A passive attack is an unauthorized hearing the information to the network. It does not alter the information which is transmitted within the network. A passive attacker gets the information exchanged in the network without interrupting the procedure of communication. Passive attack is not easy to find because communication operation itself does not get affected. Powerful encryption algorithm can be used to manage these types of attacks in which data is encrypted for transmission. Passive attacks can be further categorised into two categories:

1. *Eavesdropping*

Eavesdropping means preventing and reading the messages by an unauthorized person. The unwanted receiver can easily interrupt the communication which is on wireless medium by adjusting to appropriate frequency. The primary objective of eavesdropping is to steal the information which is kept hidden during the communication. This hidden information can be public key, private key or password.

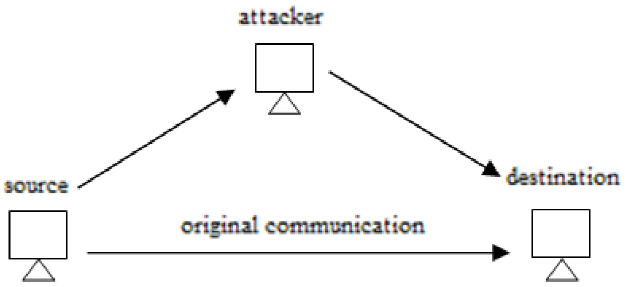

Fig 7: Eavesdropping

1.) *Traffic Analysis*

In this type of attack, traffic patterns and data packets both are significant for an attacker. The attacker can get the secret information about network topology by examining the traffic pattern. By using this attack, an attacker may determine about network topology, source and destination nodes and location of nodes.

CONCLUSION AND FUTURE WORK

The dynamic nature of MANET makes it vulnerable to attacks at different layers. One of the mostly attacked MANET layer is network layer. So, there is a need for secure environment for transmission of secure communications. In this paper, I have done a survey on network layer attacks and their possible detection mechanism. In future there can be several ways to defeat these protection mechanisms. So this is a further more potential area of research in which more powerful detection mechanisms can be invented.

REFERENCES

[1] Fatima Ameza, Nassima Assam and Rachid Beghdad, “Defending AODV Routing Protocol Against the Black Hole Attack”, International Journal of Computer Science and Information Security, Vol. 8, No.2, 2010, pp.112-117.

[2] Nital Mistry, Devesh C. Jinwala and Mukesh Zaveri, “Improving AODV Protocol against Blackhole Attacks”, International Multiconference of Engineers and Computer Scientists 2010, vol. 2, March 2010.

[3] Payal N. Raj and Prashant B. Swadas,”DPRAODV: A dynamic learning system against black hole attack in AODV based Manet”, International Journal of Computer Science Issues, Vol. 2, Issue 3, 2010, pp: 54-59.

[4] Hoang Lan Nguyen and Uyen Trang Nguyen, ”Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks”, International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, April 2006, pp. 149-149

[5] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah, “MANET Routing Protocols and Wormhole Attack against AODV”, International Journal of Computer Science and Network Security, vol. 10 No. 4, April 2010, pp. 12-18.

[6] N. Shanthi, Dr. Lganesan and Dr.K.Ramar, “Study of Different Attacks on Multicast Mobile Ad hoc Network”, Journal of Theoretical and Applied Information Technology, December 2009, pp. 45-51.

[7] Abhay Kumar Rai, Rajiv Ranjan Tewari and Saurabh Kant Upadhyay , “Different Types of Attacks on Integrated MANET-Internet Communication”, International Journal of Computer Science and Security, vol. 4 issue 3, July 2010, pp. 265-274.

[8] Jakob Eriksson, Srikanth V. Krishnamurthy, Michalis Faloutsos, “TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks”, 14th IEEE International Conference on Network Protocols, November 2006, pp.75-84.

[9] Mahdi Taheri, Dr. majid naderi, Mohammad Bagher Barekatain, “New Approach for Detection and defending the Wormhole Attacks in Wireless Ad Hoc Networks”, 18th Iranian Conference on Electrical Engineering,, May 2010, pp. 331-335.

[10] Dang Quan Nguyen and Louise Lamont, “A Simple and Efficient Detection of Wormhole Attacks”, New Technologies, Mobility and Security, November 2008, pp. 1-5.

[11] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, “Analysis of Wormhole Intrusion Attacks in MANETs”, Military Communications Conference, November 2008, pp.1-7.

[12] Maria A. Gorlatova, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano, ”Detecting Wormhole Attacks in Mobile Ad HocNetworks through Protocol Breaking and Packet Timing Analysis”, Military Communications Conference, October 2006, pp. 1-7.

[13] Mani Arora, Rama Krishna Challa and Divya Bansal, “Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks”, Second International Conference on Computer and Network Technology, 2010, pp. 102-104.

[14] Yih-Chun Hu, Adrian Perrig,and David B. Johnson, “Wormhole Attacks in Wireless Networks”, IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, February 2006, pp. 370-380.

[15] W. Weichao,B. Bharat, Y. Lu and X. Wu, “Defending against Wormhole

[16] Attacks in Mobile Ad Hoc Networks”, Wiley Interscience, Wireless Communication and Mobile Computing, January 2006.

[17] L. Qian, N. Song, and X. Li, “Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multipath,” IEEE Wireless Commuunication. and Networking Conference,

[18] I. Khalil, S. Bagchi, N. B. Shroff,” A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks”, International Conference on Dependable Systems and Networks, 2005.

[19] L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, “Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach”, IEEE Communication Society, WCNC 2005.

[20] L. Hu and D. Evans, “Using Directional Antennas to Prevent Wormhole Attacks”, 11th Network and Distributed System Security Symposium, pp.131-141, 2003.

[21] L.Lazos, R. Poovendran, “Serloc: Secure Range-Independent Localization for Wireless Sensor Networks”,ACM Workshop on Wireless Security, pp. 21-30, October 2004.

[22] W. Wang, B. Bhargava, “Visualization of Wormholes in sensor networks”, ACM workshop on Wireless Security, pp. 51-60, 2004.

[23] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, “Black Hole Attack in Mobile Ad Hoc Networks”, ACMSE, April 2004, pp.96- 97.

[24] Anu Bala, Munish Bansal and Jagpreet Singh, “Performance Analysis of MANET under Blackhole Attack”, First International Conference on Networks & Communications, 2009, pp. 141-145.

[25] Latha Tamilselvan and Dr. V Sankaranarayanan, “Prevention of Blackhole Attack in MANET”, The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007, pp. 21-26.

[26] Geng Peng and Zou Chuanyun,”Routing Attacks and Solutions in Mobile Ad hoc Networks”, International Conference on Communication Technology, November 2006, pp. 1-4.

[27] S. Lee, B. Han, and M. Shin, “Robust Routing in Wireless Ad Hoc Networks”, International Conference on Parallel Processing Wowrkshops, August 2002.

[28] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato1, Abbas Jamalipour, and Yoshiaki Nemoto1,” Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method”, International Journal of Network Security, vol..5 no..3, Nov. 2007, pp.338–346.

[29] Nadia Qasim, Fatin Said, and Hamid Aghvami, “Performance Evaluation of Mobile Ad Hoc Networking Protocols”, Chapter 19, pp. 219-229.

[30] G.S. Mamatha and S.C. Sharma, “A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS”, International Journal of Computer Science and Security, vol. 4, issue 3, Aug 2010, pp. 275-284.

[31] Preetam Suman, Dhananjay Bisen, Poonam Tomar, Vikas Sejwar and Rajesh Shukla, “Comparative study of Routing Protocols for Mobile Ad- Hoc Networks”, International Journal of IT & Knowledge Management, 2010.