ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

A Detail Review on Mobile Ad Hoc Networks Attacks

Nikhil Verma[1], Jaspal Kumar[2]

M.Tech Student, Department of ECE, B. S. Anangpuria Institute of Technology & Management, Alampur, Ballabgarh-Sohna Road, Faridabad, Haryana, India[1]

Head of Department, Department of ECE, B. S. Anangpuria Institute of Technology & Management, Alampur, Ballabgarh-Sohna Road, Faridabad, Haryana, India[2]

ABSTRACT: Mobile ad hoc networks (MANET) have risen as a major next generation wireless networking technology. This network is a network of mobile nodes with dynamic structure. Here each node acts as a router for forwarding data to other nodes. Due its dynamic nature, security has become a primary concern to provide protected communication between different nodes in ad hoc networks. There are a number of challenges in security design *a*s ad hoc network is a decentralized network. There are five layers in MANET and each of these layers is vulnerable to various attacks. In this paper we discuss about various attacks and their protection mechanisms.

KEYWORDS: MANET, Black Hole Attack, Gray Hole Attack, DoS Attacks; Wormhole AttacK

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a collection of wireless mobile nodes which have the ability to communicate with each other without having fixed network infrastructure or any central base station. Since mobile nodes are not controlled by any other controlling entity, they have unrestricted mobility and connectivity to others. Routing and network management are done cooperatively by each other nodes. Due to its dynamic nature MANET has larger security issues than conventional networks. AODV is a source initiated on-demand routing protocol. Every mobile node maintains a routing table that maintains the next hop node information for a route to the destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table.

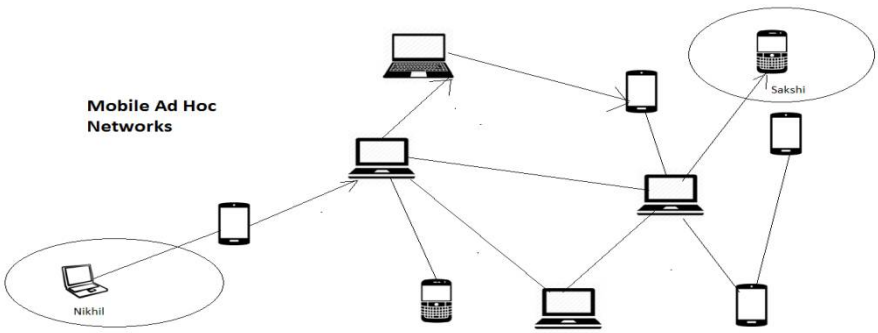

Figure 1: MANET

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

If not, it starts a route discovery process by broadcasting the Route Request (RREQ) message to its neighbors, which is further propagated until it reaches an intermediate node with a fresh enough route to the destination node specified in the RREQ, or the destination node itself. Each intermediate node receiving the RREQ, makes an entry in its routing table for the node that forwarded the RREQ message, and the source node. In the mobile ad hoc network security is the basic concern for network functions work properly. This can be achieved network services available, and the confidentiality and integrity of data ensure that it has been met security issues. Often exposed to security attacks because of the open medium, dynamic topology, and the lack of central monitoring and management, and any cooperative algorithms and functions clear defense mechanism, such as the Declaration of the ad-hoc mobile networks. These factors may change the situation on the battlefield MANET security threats. In Manet there is no any centralized administration and management, the nodes communicate with each other on the basis of mutual trust. This feature allows the ad hoc mobile networks within the network easier for an attacker to exploit. Wireless link also makes mobile ad hoc networks more vulnerable to attack, making it easier to attack the internal network, and access to ongoing contacts [11]. There can be a range of wireless link overhear a mobile node, or even participating in the network. MANET must be a safe way to transport and communications, mobile network attacks a growing threat, which is very difficult issues and important, Sound safe from today. In order to provide secure communications and transport, that the expert must understand the different types of network attacks. Sybil attack, Gray hole attack, Blackhole attacks, attack floods, directing attacks over the table, denial of service attacks (DoS), and misconduct of the contract selfishness. MANET is open to these kinds of attacks, since the communication between nodes on the basis of mutual trust phenomenon. There is no central point for network management, and unauthorized facilities, and strongly change the topology and limited resources.

II. RELATED WORK

Fatima Ameza at. el. [1] - Here author present a simple method to detect Black hole attacks in the Ad hoc On Demand Vector (AODV) routing protocol. In their work author show the robustness of protocol which allows delivering a high ratio of data and consumes less route establishment delay. Author also define the approach of AODV-SABH (AODV Secured Against Black Hole attack) which hints to secure both the RREQ and the RREP packets. Securing RREQ packets: To secure the first field will be used to include the list of the addresses of all the transitional nodes between the source and the destination, in order to detect the address of the attacker. Securing RREP packets: If the address of the sender of RREP does not match any address recorded in its local table, then the receiving node concludes that the sender is a malicious node. So, it will reject the packet, and will alert the other nodes. For the simulations the Network Simulator 2 (ns-2) is used. Simulations consist of 20 nodes evolving in a region of (950 m ´ 950 m) during 100 seconds. Transmission range is set to 250 meters. Random waypoint movement model is used and maximum movement speed is 12m/s. Packets among the nodes are transmitted with constant bit rate (CBR) of one packet per second, and the size of each packet is 512 bytes.This parameter shows the time needed for the creation of a route by a source node, it is figured in milliseconds. Thus, when the destination node receives the RREQ packet, it checks if its sequence number is less than the one included in the packet. If it is, it will conclude to an attack and can find the address of the intruder by consulting the list of addresses in the RREQ packet. On the other hand, to secure RREP packets, every node sending RREQ must record the addresses of its receptors in a local table. So, when it receives a RREP packet it can check if the address of the sender is included or not in the table.

Nital Mistry at el [2]- Here author describe efficient and simple approach for defending the AODV protocol against Black Hole attacks and propagation of Mobile Adhoc Networks (MANETs) help to realize the nomadic computing pattern with universal access is proposed. Here author also prescribed attempt to focus on analyzing and improving the security of one of the popular routing protocol for MANETS viz. the Ad hoc On Demand Distance Vector (AODV) routing protocol. The main focus is on ensuring the security against the Blackhole Attacks. The solution that propose here is designed to prevent any alterations in the default operations of either the intermediate nodes or that of the destination nodes. The approach we follow, basically only modifies the working of the source node, using an additional function *Pre_Receive Reply (Packet P).* The proposed solution maintains the identity of the malicious node as Mali_node , so that in future, it can discard any control messages coming from that node. Now since malicious node is identified, the routing table for that node is not maintained. In addition, the control messages from the malicious node, too, are not forwarded in the network. Simulation Parameters having v Simulator Ns-2(ver.2.33), Simulation Time 100 s , Number of nodes 10 to 80,Routing Protocol AODV, Traffic Model CBR, Pause time 2s , Mobility 10 - 70 m/s, Terrain area 800m x 800m , Transmission Range 250m, No. of malicious node 1. To evaluate the packet delivery ratio,

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

End-to-End Delay and Normalized Routing Overhead; simulation is done with nodes with the source node transmitting maximum 1000 packets to the destination node. With the fact that the default AODV protocol is susceptible to the Blackhole attacks, in this research exercise, the author attempt at investigating the existing solutions for their capability.

Hoang Lan Nguyen et al [4] - Here author present a simulation-based study of the impacts of different types of attacks on mesh-based multicast in mobile ad hoc networks (MANETs).In this author also discussed the study how the number of attackers and their positions affect the performance metrics of a multicast session such as packet delivery ratio, throughput, end-to-end delay, and delay jitter. The simulation results show that a large multicast group with a high number of senders and/or a high number of receivers can sustain good performance under these types of attacks due to several alternative paths in the routing mesh results that show how a mesh based multicast session performs under various attack scenarios, identify several unique behaviors of a multicast network under attack , which have not been seen in unicast environments, the obtained results allow us to suggest some counter-attack measures (e.g., adding more senders and/or receivers to the multicast group to improve to the receivers, and builds a mesh of forwarding nodes. Simulation parameters value are ODMRP route refreshment interval 20 s, Channel capacity 2 Mbits/s , Packet size (excluding header size) 512 bytes ,Traffic model of sources Constant bit rate , Mobility model Random way-point , Path loss model Two-ray ,Queuing policy at routers First-in-first-out. Simulation results confirm an intuitive claim: the more attackers there are in the network, the more damage they inflict on a multicast session in terms of packet delivery ratio, or delay and delay jitter.

N.SHANTHI et. al. [6] – According to the author a simulation based study of the impact of different types of attacks in mobile ad hoc networks and study how these attacks affect the performance metrics of a multicast session such as packet delivery ratio, packet latency and packet-consumed energy is being described. The fundamental aspects of computer security like confidentiality, integrity, authentication and non-repudiation are valid when production of routing in the network is discussed here. Confidentiality ensures that classified information in the network is never disclosed to unauthorized entities. Integrity guarantees that a message being transferred between nodes is never altered or corrupted. Availability implies that the requested services are available in a timely manner even though there is a potential problem in the system. Authenticity is a network service to determine a user's identity. Non-repudiation ensures that the information originator cannot deny having sent the message. Simulation parameters values shows that the Channel capacity is 2Mbps, Packet size is 512bytes,Traffic model of sources is Constant bit rate, Mobility model is Random way point
Path loss model is Two – ray and Queuing policy at routers is First-in-first-out. The security issues have been left primarily ignored. The performance of a multicast session in a MANET under attack depends heavily on many factors such as the number of multicast receivers, the number of multicast senders, simulation results ensures that the more attackers there are in the network, they cause more damage on a multicast session from the view point of authentication, integrity and confidentiality. The operation of Gray hole attack and Worm hole attacks are different, they both cause the same degree of damage to the performance of a multicast group.

Irshad Ullah et. al. [7] – In this author proclaimed that the study of impact of Black Hole attack on the performance of MANET is evaluated exploring which protocol is more vulnerable to the attack and it was found that AODV is 10% more vulnerable to Black Hole attack as compared to OLSR. The measurements were taken in the light of throughput, end-to-end delay and network load. In this paper author analyzes Black Hole attack in MANETs using AODV and OLSR which are reactive and proactive respectively in nature. In this the attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. Detecting Black Hole attack is also one of the important issues in order to secure the network from such attacks. In a path based detection method is proposed, in which every node is not supposed to watch every other node in their neighborhood, but in the current route path it only observes the next hop. There is no overhead of sending extra control packets for detecting Black Hole attack. The stimulation parameters values are- Simulation time is 1000 seconds , Simulation area (m * m) is 1000 *1000 , Number of Nodes is 16 and 30, Traffic Type is TCP Performance Parameter are Throughput and delay and Network Load ,Pause time is 100 seconds, Mobility (m/s) is 10 meter/second, Packet Inter-Arrival Time (s) is exponential(1),
Packet size (bits) is exponential l(1024), Transmit Power(W) is 0.005, Date Rate (Mbps) is11 Mbps ,Mobility Model is Random. It was observed that when there is higher number of nodes and more route requests, it affect the network performance more. The percentage of severances in delay under attack is 2 to 5% and in case of OLSR, where as it is 5

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

to 10% for AODV. The throughput of AODV is effected by twice as compare of OLSR. From the research, it was found that AODV protocol is more vulnerable to Black Hole attack than that of OLSR protocol.

III. ATTACKS IN MANET

Mobile ad-hoc networks are vulnerable to numerous attacks not only from outside but also from inside i.e. within the network. The attacks in MANET are divided into two major categories:

A. Active Attacks

Active attacks disturb the operation of communication in the network. An active attack could stop the message flow between the nodes. An active attack can modify the data packet or drop the packet in the network. Hence active attacks disturb the normal functionality of a MANET.

B. Passive Attacks

A passive attack is an unauthorized listening to the network. It does not change the data transmitted within the network. A passive attacker obtains the data exchanged in the network without disturbing the operation of communication. Passive attack is difficult to detect because of the network operation itself does not get affected. These attacks can be controlled by using powerful encryption algorithm to encrypt the data which is being transmitted.

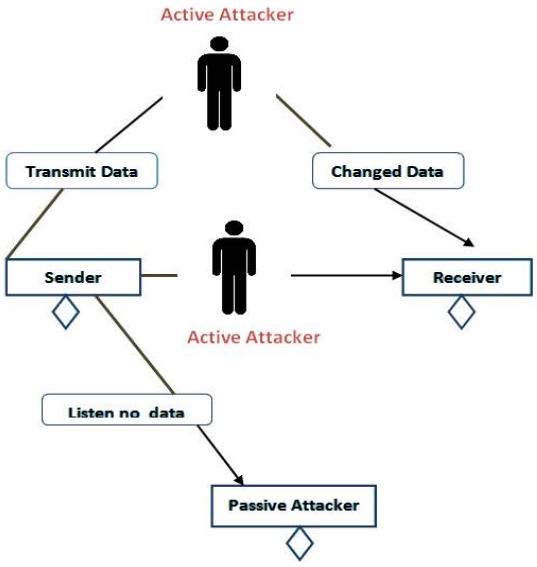

Fig: 2 Active - Passive attacks

Attacks at MAC Layer

1. Jamming attack: Jamming attack is a type of denial of service attack. Jamming attack uses the term jammer. Jammer can be defined as an individual entity which intentionally blocks the methods of legal wireless communication. It comes under active attack due to its actions. In jamming attack, a radio signal is jammed or interfered which causes the message to be lost or corrupted. The attacker node having a powerful transmitter causes that the generated signal will be strong enough to damage the communications and can easily crush the targeted signal [5]. This attack is originated after determining the communication frequency.

Attacks at Network Layer

1. Black hole attack: In this attack, attacker node announces that it has an optimum route to the node whose packet it wants to use. On receiving side, attacker node sends a fake reply with extremely short route. If the node has been able to make its place between the communicating nodes, then it can do anything with the packets passing between them [1]. A black hole node acts as having a path with the highest sequence number to the destination. The black hole node falsely advertises the shortest path to the destination node in order to absorbs data packets and drops them [1].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

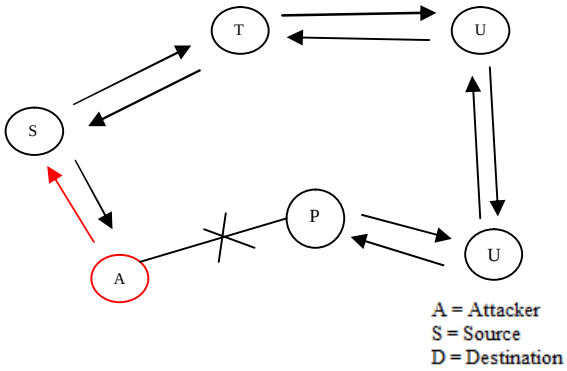

Fig. 3 Black hole Attack

2. Grey-hole attack: Grey-hole attack is a special kind of black-hole attack. In this attack, an attacker becomes the part of the routes in the network i.e. captures the route then drops data packets selectively [2]. One can't predict the probability of losing data packets. In grey-hole attack, attacker node first agrees to forward packets and then refuses to do so, which leads to dropping of data packets.

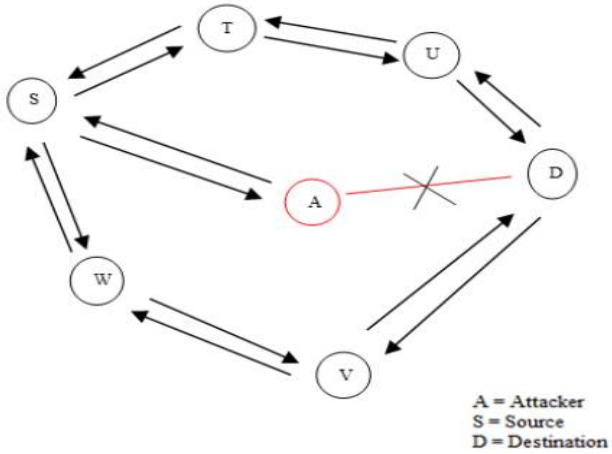

Fig. 4 Grey Hole Attack

The Gray Hole attack has two phases: In the first phase, an attacker node exploits the AODV protocol to act as having a valid route to the destination node, with the goal of interrupting data packets, even though the route is spurious. In the second phase, the attacker node drops the interrupted data packets with a certain probability. Grey-hole attack is more difficult to detect as compared to black Hole attack in which the attacker node drops the received data packets with certainty.

3. Wormhole: In this type of attack, two attacker nodes are present in the network which creates a tunnel. An attacker node receives the data packet at one point in the network and forwards it to another attacker node. The tunnel exist between two attacker nodes is called wormhole. Wormhole places the attacker nodes in a very powerful position compared to other nodes in the network. The attacker node could use this position in a number of ways. In wormhole attack, it copies the data packets at one location and replays them without any changes at different location or within the same network.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

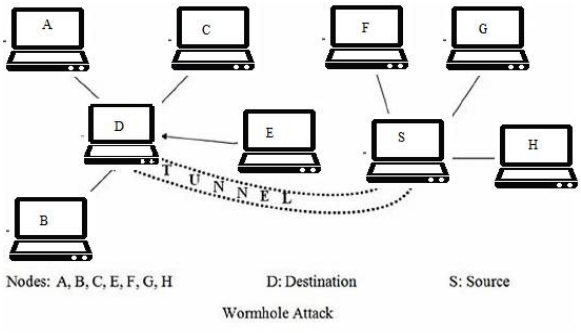

Fig. 5 Wormhole Attack

4. Sinkhole attack: In this attack, an attacker node provides wrong routing information in order to presents itself a specific node and hence receives the whole network traffic.

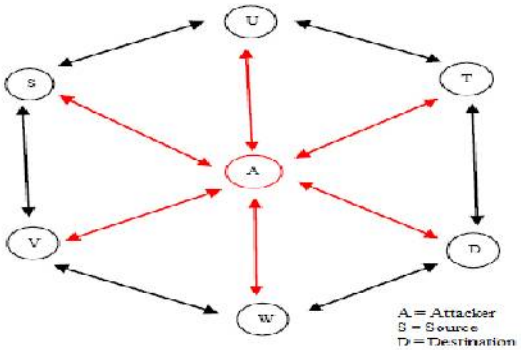

Fig. 6 Sinkhole Attack

Once receiving the whole network traffic complicated packet traffic it modifies secret information such change the data or drop the packet to make network complicated. An attacker node tries to attract the secure data from all neighbouring nodes.

5. Rushing Attack: Rushing attack can also be known as a denial of service attack or novel attack. In rushing attack, an attacker node receives a route request packet from the source node and immediately floods it throughout the network before other nodes which also receive the same route request packet. These attacks are generally against the on-demand routing protocols.

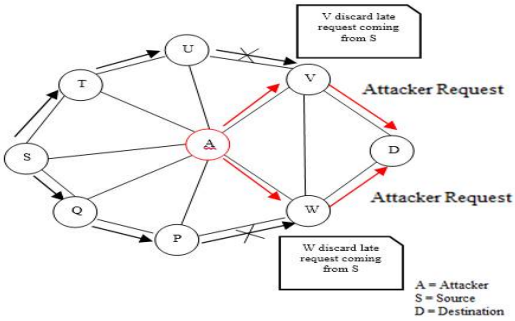

Fig. 7 Rushing Attack

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

6. Sybil Attack: In MANET the transmission medium for data packets is air and they don't have a centralized node to control the network. So the routing is based on some unique node address. This property of MANET can be used by the attacker for using fake identities. This means the attacker can either use a random identity or the identity of legitimate node. This type of attack is known as Sybil attack.

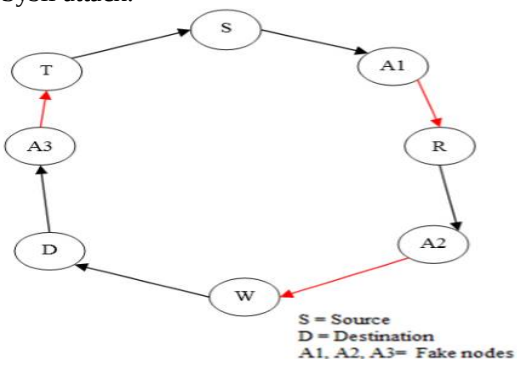

Fig. 8 Sybil attack

In Sybil attack, an attacker may create multiple fake identities. The attacker node may present itself as a large number of nodes instead of a single node. These fake identities are called Sybil nodes.This attack may cause a lot of data packets to be routed towards the fake nodes.

7. Jellyfish Attack: Jellyfish attack generally comes under the passive attack and also a type of denial of service attack. Jellyfish attack produces delay during the transmission and reception of data packets in the network. This attack is difficult to detect. Jellyfish attack is same as the black hole attack with the only difference that is in black hole attack attacker drops all data packets but in jellyfish attack node produces delay during forwarding of data packets.

Attacks at transport Layer

1. Session Hijacking: In this type of attack, the attacker node tries to obtain secure data which could be password, secret key etc. and other useful information. An attacker creates a fake ip address and obtains the correct sequence number. This attack aims at collecting secret data about the nodes.

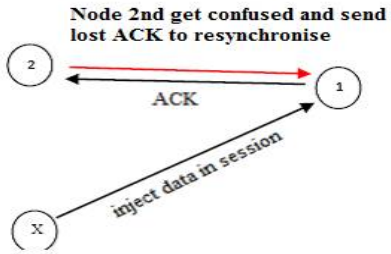

Fig. 9 Session Hijacking

Attacks at Application Layer

1. Repudiation attack

Repudiation means denial of transmitting or receiving the data packet. In this type of attack, either a sender may deny that he sends the packet or a receiver denies that he receives a data packet.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

I. PASSIVE ATTACKS

A passive attack is an unauthorized listening to the network. It does not change the data transmitted within the network. A passive attacker obtains the data exchanged in the network without disturbing the operation of communication. Passive attack is difficult to detect because of the network operation itself does not get affected. These attacks can be controlled by using powerful encryption algorithm to encrypt the data which is being transmitted.
Passive attacks are further classified into two categories:

1. Eavesdropping

Eavesdropping is an interception and reading of messages by an unauthorized receiver. The unintended receiver can easily intercept the communication which is on wireless medium by tuning up to proper frequency. The main aim of eavesdropping which is kept secret during the communication. The secret information can be private key, public key, and password.

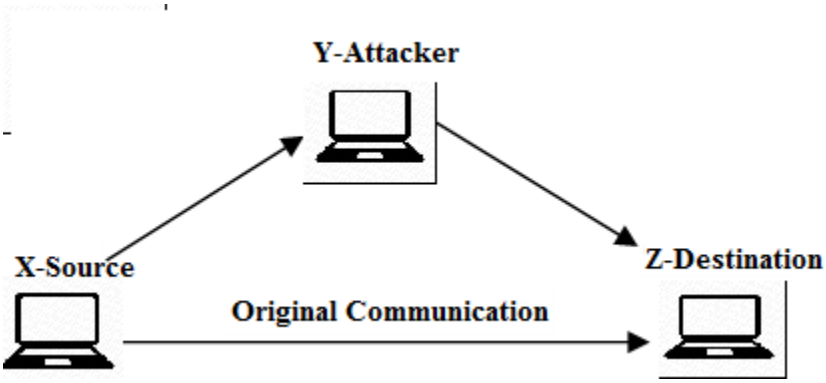

Fig. 10 Eavesdropping

2. Traffic Analysis

In this attack, for an attacker data packets and traffic patterns both are important. The attacker can obtain the confidential information about network topology by analysing the traffic pattern. Using traffic analysis attack, an attacker may find about network topology, location of nodes, source and destination nodes.

IV. 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, Dr. Lganesan and Dr.K.Ramar, "Study of Different Attacks on Multicast Mobile Ad hoc Network", Journal of Theoretical and Applied Information Technology, pp. 45-51, December 2009
[2] Nital Mistry, 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, pp. 265-274, July 2010.
[3] 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, pp.75-84, November 2006.
[4] Hoang Lan Nguyen, 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 , pp. 331-335, May 2010,
[5] Dang Quan Nguyen and Louise Lamont, "A Simple and Efficient Detection of Wormhole Attacks", New Technologies, Mobility and Security, , pp. 1-5, November 2008
[6] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, "Analysis of Wormhole Intrusion Attacks in MANETs", Military Communications Conference, pp.1-7, November 2008
[7] 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, pp. 23- 30, October 2006
[8] 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, pp. 102-104, 2010

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

[9] 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, pp. 370-380, February 2006
[10] W. Weichao,B. Bharat, Y. Lu and X. Wu, "Defending against Wormhole
[11] Attacks in Mobile Ad Hoc Networks", Wiley Interscience, Wireless Communication and Mobile Computing, January 2006.
[12] 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,
[13] 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.
[14] 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.
[15] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", 11th Network and Distributed System Security Symposium, pp.131-141, 2003.
[16] L.Lazos, R. Poovendran, "Serloc: Secure Range-Independent Localization for Wireless Sensor Networks",ACM Workshop on Wireless Security, pp. 21-30, October 2004.
[17] W. Wang, B. Bhargava, "Visualization of Wormholes in sensor networks", ACM workshop on Wireless Security, pp. 51-60, 2004.
[18] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE, pp.96- 97, April 2004
[19] Anu Bala, Munish Bansal and Jagpreet Singh, "Performance Analysis of MANET under Blackhole Attack", First International Conference on Networks & Communications, pp. 141-145, 2009
[20] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, pp. 21-26, 2007
[21] Geng Peng and Zou Chuanyun,"Routing Attacks and Solutions in Mobile Ad hoc Networks", International Conference on Communication Technology, pp. 1-4, November 2006
[22] S. Lee, B. Han, and M. Shin, "Robust Routing in Wireless Ad Hoc Networks", International Conference on Parallel Processing Wowrkshops, August 2002.
[23] 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, pp.338–346, Nov. 2007
[24] Nadia Qasim, Fatin Said, and Hamid Aghvami, "Performance Evaluation of Mobile Ad Hoc Networking Protocols", Chapter 19, pp. 219-229.
[25] 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, pp. 275-284, Aug 2010
[26] 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.