International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue IX, September 2017- Available at www.ijraset.com

Attacks on Manet Protocol Stack and Their Countermeasures

Saharsh Gaurav[1]
[1]*Centre of Computer Education, Institute of Professional StudiesOf Allahabad, Allahabad, India*

Abstract*: *A manet can be described as a group of random wireless nodes connected to each other forming a network with unrestricted mobility and no infrastructure. Mobile ad hoc networks (manet) are self configuring, wireless, dynamic and have no central administration. At a point where all these features make manet an awesome concept, they also create some loopholes in the security management of these ad hoc networks. This paper will primarily focus upon the security issues of the manet and their feasible solutions. The results enable us in risk minimization.
Keywords: Manet, attacks, dos, black hole, wormhole, byzantine, rushing, sinkhole, solutions

I. INTRODUCTION

As the advancements of the performance in wireless computer technology, MANETs have evolved as an advanced mobile wireless computing solution. A MANET is an infrastructure less, not centrally administered, self-organizing system of mobile nodes connected without wires. The key idea behind the development of the mobile ad-hoc networks is to provide a robust and efficient operation in a mobile wireless network. The devices of the MANET are free to move, enter and leave the network anytime which lets the MANET to have a dynamic topology, and hence the network becomes decentralized.The communication in MANET takes place by using multi-hops path i.e. the nodes that are in range of radio frequency of each other communicates directly and for communication with other nodes those are not in the range of radio frequency, intermediate nodes are being used. So to communicate with each other the nodes dynamically establishes a path from source to destination. Due to this feature of MANET and open communication medium makes them highly vulnerable. The main objective of this paper is to study the security attacks and vulnerabilities of the MANETs on different layers of protocol stack.

II. CHARACTERISTICS OF MANET

A .MANET has following characteristics some of which are

1) *Autonomous Terminal:* Every terminal in a MANET act as an autonomous node which may act as host and router in the same network i.e. beside of being a host, a node can also act as a router and perform switching functions also [6].
2) *Distributed Operations:* In MANET there is no central administration available i.e. a background network for central control of the network operations is not available, so the control and management of the MANET is distributed among the network nodes [3].
3) *Multihop Routing:*Routing algorithms in MANET are of basically two types Single Hop and Multi Hop. When the data packets are to be delivered from source to destination out of direct wireless transmission range then the packets are forwarded via many intermediate nodes
4) *Dynamic Topology:* The network topology of MANET changes rapidly and unpredictably because of the nodes which are mobile in nature.The mobile nodes in the network dynamically establish connectivity among themselves as they move about, forming their own network on the fly[3].

III. ATTACKS ON MOBIE AD-HOC NETWORKS

The attacks on Mobile ad-hoc networks can be classified into following categories:

A. Based on the Nature of Attacks

1) *Active Attacks: In* Active attacks the attacker attempts to change or destroy the data which is travelling through the network, hence creating a disruption in the network operations or some of the nodes by altering the data transmitted with their own data i.e. inserting their own data into the original data stream or by deleting the data from the data stream. [1]

2) *Passive Attacks:*In Passive attacks the attacker remains silent and only tries to read the confidential information that is transmitted over the network and tries to identify the patterns transmitted. The attacker doesn't tries to modify or corrupt the information but listens to it [5].

B. Based on the Location of Attacks

*1)External attacks:*External attacks are those attacks which are carried out by the nodes which are not the part of the network. External Attacks results in network congestion, unavailability of network services and also prevent the network from information interchange thus creating a network overhead [1, 5].

*2) Internal Attacks:*Internal Attacks are the attacks that are carried out by the compromised nodes that are the part of the network. From the point of an attacker internal attacks are more severe and harmful for the network as the attacker becomes the authorized part of the network through the compromised nodes. Internal attacks are very hard to detect as compared to the external attacks [1,5].

C. Attacks Based on the Protocol Stack of MANET

1) Physical Layer Attacks

The execution of attacks on the physical layer of the protocol stack is very easier from an attacker's point of view. These types of attacks are hardware based attacks and they seek help from hardware source to occur [5].

a) *Eavesdropping:*Eavesdropping is the process of stealing and reading the messages by unintended receivers [5]. In this type of attack the sender and receiver of the messages or data doesn't come to know about the attack, the attacker silently listen all the messages and conversation between them without altering or deleting the data. These types of attacks are basically done to get the confidential information such as private key, public key, node password etc.

Fig (a): Eavesdropping

b) *Active Interference:*Active Interference is a kind of Denial of Services (DOS) attacks that blocks wireless communication channel. The consequences of such attacks depend on their routing protocol and duration of attack [7, 9 and 10]. The attacker after applying active interference is in a state of control of conversations that it can change the messages order or it can resend the older message.

c) *Jamming:*Jamming is a special class of DoS attacks which are caused by compromised nodes after determining frequency of communication. To create this kind of attack an attacker needs a powerful transmitter to generate a strong signal which has the capacity to thrash the targeted signal and infer the communication. Signal jamming could be in the form of random noise and pulse [10].

2) Data Link Layer Attacks

The data link layer protocols are very much exposed to DOS attacks [5]. These attacks change the behaviour of the nodes as an effect on the state of the network as a whole. The main effect of this kind of attack is route discovery failure, high energy consumption, link disruption etc. The misbehaviour of the nodes can be either malicious or selfish or the whole attack is done only for the traffic analysis purpose.

a) *Malicious behaviour of Nodes:*The nodes start effecting the network regular operations of routing protocol. When the number of communications between the neighbouring nodes increases, the effect of this becomes considerable. These types of attacks may fall into following categories:

*b) Denial of Service (DoS):*The main action of these types of attacks is to produce a malicious effect on the compromised nodes which has drastic security risks. It also effects the routing of the data packets if the compromised node is involved in it. The detection of the compromised node is also very difficult.

c) Attacks on Network Integrity: In case of secure communication and quality of service the integrity of network plays an important role. There are many attacks on the network which provides the wrong routing information.

*d) Selfish Behaviour of Nodes:*The behaviour of the nodes become selfish as they start dropping the packets or stop forwarding the packets just to conserve battery power or gain unwanted share of bandwidth. One of the major attacks of the selfish nodes are packet dropping as it creates network congestion. This attack takes the advantage of routing protocol as most of the routing protocol does not have mechanism to check whether the packet is forwarded or not [5].

*e) Traffic Analysis:*The main task of the attacker under this kind of attack is to analyse the traffic pattern to get the vital information about the network topology and then reveal the information about the nodes [5]. Information such as node location, topology used in communication, and roles of the nodes are mainly gathered.

3) Network Layer Attacks

*a) Black hole attack***:** In this kind of attack, the attacker uses the routing protocol and claims that it has having the most optimum path to the node whose packet it want to intercept. Once the attacker node successfully places itself between the communicating nodes it gains the ability to perform ant thing with the packets such as dropping the packets, sending the packet to the wrong node etc [1, 8].

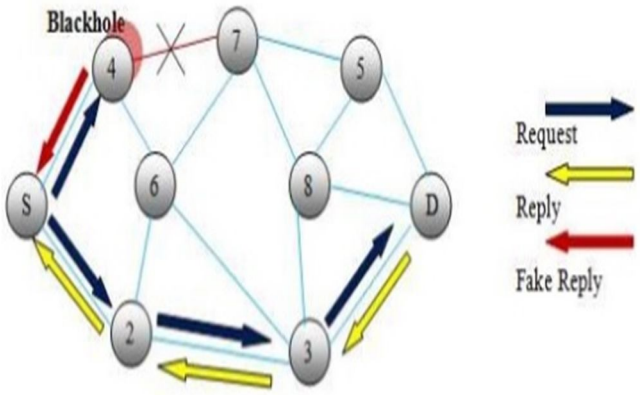

Fig (b): Black hole attack

As from the figure the source node (S) wants to send the data to the destination node (D). The source node (S) sends a route request message (RREQ). The malicious node (4) receives the RREQ message from the node S and immediately replies the node S with the claim of having the most optimum route to the node D. If the reply of the malicious node (4) reaches to the source node(S) before any other node's reply the source nodes (S) will start sending the data with the malicious path thus resulting the consumption of all data packets or loss of packets at malicious node (4).

*b) Link Spoofing:*Link Spoofing occurs when the true identity of the malicious node is not represented by the node, this can be done by changing the IP address or the MAC address. The link spoofers allows loops which results in losing the links to these nodes, It basically allows loops resulting in portioning of network [13]. The malicious node does not broadcast any needed information which results in losing links.

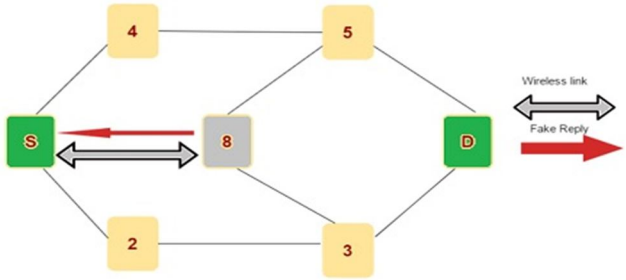

Fig (c): Link Spoofing

c) *Wormhole Attack:* Wormhole attack is one of the most sophisticated attacks on the Mobile ad-hoc Networks. In this kind of attack, a malicious node receives packet at one location and tunnels them to other location in the network. This tunnel between the two conspiring nodes is termed as wormhole [1]. An attacker uses the wormhole in the network to make their nodes more attractive so that more data packets are sent through them. The wormhole attack could be established between the two involved nodes or attackers through wired link or through a single long-range wireless link. In case of DSR and AODV routing protocol, the attackers can also prevent the discovery of the any routes which does not involve the wormhole attacked nodes or malicious nodes. And since radio channels are broadcast in nature the attackers can also create a wormhole for the data packets which are not addressed to them [9, 10, 15].As from the figure (d), we can see that nodes X and Yare malicious ones and form a tunnel in the network. Te source node (S) is willing to send some data to the destination node (D) and thus s initiates a route request (RREQ) message to the network to find the route to the node D. The neighbours of the node S, nodes 1 and 2 receives the RREQ message and forwards it to their respective neighbour node X and 5. On receiving of the RREQ message the node malicious node X send it immediately to the other malicious node Y with the help of a high speed link between X and Y, and later it initiate RREQ to its neighbour node 8, through which the RREQ is delivered to the destination node D. Due to high speed link, it forces the source node to select route <S-1-8-D> for destination. It results in "D" ignores RREQ that arrives at a later time and thus, invalidates the correct route <S-2-5-7-D>.As a result of selecting the wormhole route these malicious nodes can either drop all the packets or drop the packets selectively to avoid attack detection.

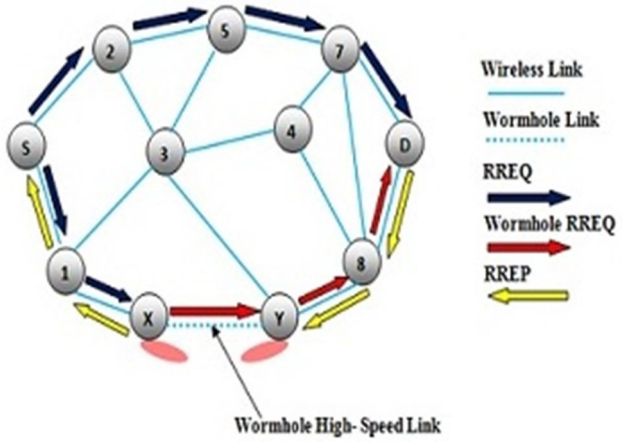

Fig (d): Wormhole Attack

d) *Sinkhole Attack:*In this attack, wrong routing information which is called gateway is presented in an attractive way by attacking node to attract all the network traffic towards it. When the whole network traffic is received by the maliciousnode then the information that is needed is extracted from the data packets. The malicious node tries to get all the secure information from all the neighbours because it makes itself the best possible communicating route to destination.

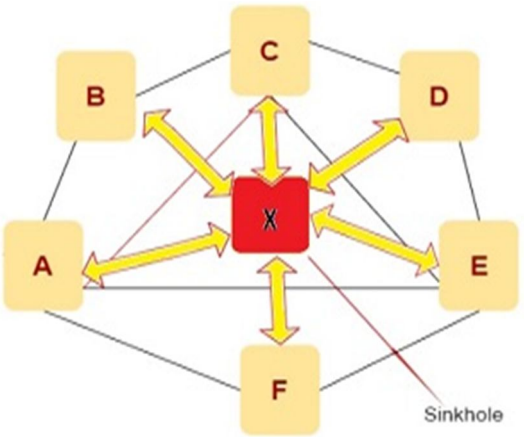

Fig (e): Sinkhole Attack

*e) Byzantine Attack:*In this attack, a single malicious intermediate node or a group of malicious intermediate nodes works in collusion to attack the network by creating routing loops, forwarding packets through other paths i.e. non-optimal paths, or selectively dropping packets resulting in degradation of the routing services. It is hard to detect as network views to be operate normally.

*f) Rushing Attack:*The malicious node in the network, tends to flood the network with its own Route Request Packets (RREQ) on receiving the route request message from the source node before any other node acts. Due to this kind of flooding, the other node which receives the RREQ packets from the source node discards the request of the source node treating it as a duplicate request. This attacks leads to the route which contains the contaminated node of the network. Finding any such route which does not contain the malicious node by the source node through the Routing protocol of the Manet is very hard or near about impossible in this attack situation and this attack is very hard to detect.

4) Transport Layer Attacks

a) Session Hijacking: In this attack, attackers try to take benefit to exploit unprotected session when the initial setup of session is done. Attackers try to spoof victim by getting its secure data that is password, secret key, login name etc. and other valuable information of the node. These attacks are also called address attacks.

5) Application Layer Attacks

*a) SYN Flooding:*The SYN Flooding is a kind of Denial of Services (DoS) attacks which leaves a large number of TCP connection half-opened, i.e. it never completes a handshake to open a complete connection [1]. In this attack the attacker sends a continuous pool of SYN packets to the target node. For communicating using the TCP, a three way handshake is needed which tells both the machines that they are ready to communicate with each other and agree on initial sequence numbers for the conversation. The target allocates memory on its connection queue to keep track of half-opened TCP connections and replies with a SYN-ACK. The attacker does not complete 3-way handshake by sending ACK to SYN-ACK to fully open the connection thus filling up all slots on connection queue of target node.

*b) Distributed DoS Attack***:** In this attack several foe that are distributed throughout the network collude and prevent legitimate users from accessing the services offered by the network, Distributed denial of service attack is more severe form of denial of service attack.

IV. COUNTERMEASURES TO THE ATTACKS

ATTACKS	SOLUTIONS
EAVESDROPPING	♦ HTTPS-ENCRYPTED CONNECTIONS
JAMMING	♦ FREQUENCY HOPPING SPREAD SPECTRUM [1] ♦ DIRECT SEQUENCE SPREAD SPECTRUM [1]
BLACK HOLE	♦ REPEATED NEXT HOP NODE [15] ♦ REAL TIME MONITORING [15] ♦ COMPARISON OF SEQUENCE NUMBER [15] ♦ CALCULATION OF PEAK VALUE [15] ♦ CHECK HONESTY OF NODES [15]

SPOOFING	♦ MULTI-COPY ROUTING PROTOCOL ♦ ENCOUNTER BASED ROUTING (EBR)
WORMHOLE	♦ PACKET LEASHING : A STRONG TECHNIQUE [14] ♦ DIRECTIONAL ANTENNAS ON NODES [14] ♦ STATISTICAL ANALYSIS ON DATA[14]
SINKHOLE	♦ ENCRYPTION AND DECRYPTION METHOD
BYZANTINE	♦ ATTACK DEFENCE SYSTEM USING GAME THEORY [16] ♦ ROBUST SOURCE ROUTING (RSR)[7]
SESSION HIJACKING	♦ SECURING USER LOGINS [8] ♦ SECURE PASSWORD USING ENCRYPTION [11] ♦ LIMITING USER'S RIGHTS [13]
SYN FLOODING	♦ ENCRYPTION AND DECRYPTION METHOD [1]
RUSHING ATTACK	♦ ROUTE DISCOVERY PROTOCOL (RAP) [17]

IV. CONCLUSION

In recent time, MANETs have emerged as one of the most promising device connectivity technology and gained tremendous attention from researchers. Since these networks can be rapidly deployed without the need of any defined infrastructure, they can be easily applied to various scenarios ranging from emergency operations and disaster relief to military services,etc. In this paper main focus was on attacks of network layer and solutions to these vulnerabilities to MANET. The paper discusses the most important attacks that breach the security of any Manet first and later their solutions in the next sections.

In Future, we will focus on some new attacks and will propose their possible solutions which the complete performance and security analysis.

REFERENCES

[1] Abhay Kumar Rai, Rajiv RanjanTewari, Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security (IJCSS), Volume (4): Issue (3).

[2] NishuGarg, R.P.Mahapatra. "MANET Security Issues". IJCSNS International Journal of Computer Science and Network Security, Volume.9, No.8, 2009.

[3] Jai Shree Mehta, ShilpaNupur, Swati Gupta, "An Overview of MANET: Concepts, Architecture & Issues," International Journal of Research in Management, Science & Technology, vol. 3 No.2,Apr. 2015.

[4] Hoang Lan Nguyen, UyenTrang Nguyen. "A study of different types of attacks on multicast in mobile ad hoc networks". Ad Hoc Networks, Volume 6, Issue 1, Pages 32-46, January 2008..
[5] Saritha Reddy Venna and Ramesh BabuInampudi, "A Survey on Security Attacks in Mobile Ad Hoc Networks," International Journal of Computer Science and Information Technologies, Vol. 7 (1) , 2016, 135-140.
[6] The IETF website. [Online]. Available at : https://www.ietf.org/rfc/rfc2501.txt
[7] Zubair Muhammad Fadlullah, TarikTaleb, and Marcus Schöller, "Combating against Security Attacks against Mobile Ad Hoc Networks (MANETs)"
[8] Gagandeep, Aashima& P. Kumar," Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Vol.1, Issue-5, June 2012.
[9] Vikrant Gokhale, S.K.Gosh, and Arobinda Gupta, "Classification of Attacks on Wireless Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks a Survey".
[10] ShefaliKhatri, Punit Sharma, PrashantChaudharyAnchitBijalwan, "A Taxonomy of Physical Layer Attacks in MANET," International Journal of Computer Applications (0975 – 8887) Volume 117 – No. 22, May 2015.
[11] Bing Wu, Jianmin Chen, Jie Wu, MihaelaCardei ,"A Survey on Attacks and countermeasures in Mobile Ad Hoc Networks ," Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z.Du (Eds.) pp107-139, @ 2006 Springer.
[12] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.
[13] M. K. R. Monika, "Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review," International Journal of Computer Applications (0975 – 8887), vol. 12, no. 2, November 2010.
[14] N. S., "Defending Wormhole Attacks in Wireless ad-hoc Networks," International journal of computer science & engineering survey (IJCSES), vol. 2, August 2011.
[15] S. .J, "Review of Prevention and Detection Methods of Black Hole Attack in AODV- based on Mobile Ad Hoc Network," International Journal of Information and Computation Technology, vol. 4, November 2014
[16] ChetnaGuntewar et al, A Review on Byzantine Attack Detection and Prevention Using Game Theory / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015, 749-752.
[17] Y. Hu, A. Perrig, and D. B. Johnson. "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols". Proceedings of the ACM Workshop on Wireless Security 2003, Pages 30-40, September 2003.