Analysis of Network Layer Attacks and their Solutions in MANET

Abida Aslam[1], Mehak Abbas[2], Muhammad Yasir Adnan[3] and M. Junaid Arshad[4]
[1-4]University of Engineering & Technology, Lahore

***Abstract*– A temporary network of wireless mobile hosts without the assistance of standard administration form mobile ad hoc network (MANET). It has dynamic topology because mobiles can enter and leave the network continuously. As MANET are wireless, dynamic and have no central administration, maintaining security in this network is difficult. The major goal of this paper is to discuss the security threats in MANET and their solution. Security criteria and attack type in MANET is also included in this paper.**

***Keywords*– MANET, Infrastructure, Snooping, Replay Attack and Distributed Networks**

I. INTRODUCTION

Advancement in the Wireless network technologies have resulted many new applications in the internet discipline. Recently, due to the prestige of portable device and wireless networks Mobile ad Hoc network has become one of the most Vibrant and driving area of communication. A mobile ad Hoc network is an independent system of movable devices like smart phones, laptops and sensors. These devices can communicate and join each other at any time and any place through wireless links. Each device act as a router because each device forward traffic which is not related to it. MANET has some special characteristics like open network boundary, dynamic topology, distributed network, fast and quick implementation and hop-by-hop communication. These special features made the MANET popular for the military purpose and for the use of emergency relief situation. Due to these special features, MANET has to face a lot of security challenges. To understand these security challenges, one must understand the basic security parameter of MANET [1]. Without understanding them security approach is useless. These parameters are network overhead, processing time and energy consumption. Two essential concerns of security are security services and security attacks. Basic purpose of security service is protecting the network from the attack before it happened. As MANET is a dynamic, open boundary and autonomous network, in spite of security services, attack in this network is easy [2].

As infrastructure of MANET is not fixed, nodes are free to move. So they can enter into an area which is hostile and they will remain unmonitored. In this case physical attack is possible. Even without any physical access to network, different attacks such as replay attack, snooping and eavesdropping can easily be done. Battery issues and power consumption also lead to the problem in this network [3].

Due to dynamic topology, the network arrangement keeps on changing which makes it difficult to discern the route. It also makes the cryptographic protocols futile. Many other issues and their possible solutions are described in this paper.

The organization of the paper is as follows. Section II contains the security attacks in MANET. Section III discusses possible solutions for these attacks and section IV concludes this research.

II. NETWROK LAYER ATTACKS

There are different ways that can be used by malicious nodes to attack the network in MANET uses link layer protocol to provide connections between mobile nodes and it usually assumes that all of the nodes are cooperative but unfortunately it is not true. Cooperation between nodes is assumed and not enforced by MANET, so malicious nodes become the security attackers. Some current malicious routing attacks are discussed in following subsections in detail.

A) Flooding

Nodes that become attackers usually consumes all the networks resources as bandwidth, computational or battery power or more severely mess up with routing operations to a level where it severe degradation results in network performance [4]. This type of attack is also known as denial of services because attackers flood the network intentionally with meaningless Route Requests (PREQ) and Route Reply (PREP) messages [5].

Nodes usually sends a lot of PREQ's in no time to a node that actually does not exist in the whole network, and the node sending these PREQs says that it is a destination node to which it is sending messages. Because that destination node does not exist so there will be no reply to PREQs and these will flood the network [4]. Same is the case with route reply.

B) Blackhole

This attack occurs when attacking nodes claim that they have an ideal route to a node that is going to be affected by malicious nodes by the interruption in its packets. When malicious nodes get success in receiving the request, sends fake reply with extremely short route [6], [7]. When the malicious node succeeded in placing itself in the network of communicating nodes, now it can do anything with the

packets being passed in the network. Following figure depicts this behavior where node 4 which is malicious presents itself in the way discussed above i.e., it has shortest route to destination. Now in this network "S" which is a source node and wants to send data to "D" destination node, "S" starts discovering route, this is time when node 4 says it has shortest route. Node "S" finds node 4 best suitable node towards "D" and ignores all other nodes, this results in the loss of all packets at malicious node.

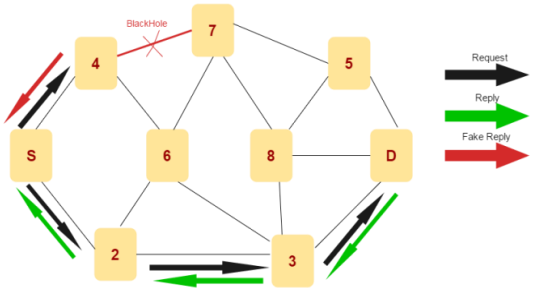

Fig. 1: Blackhole Attack

C) Link Spoofing

This type of attack occurs when malicious node does not represent its true identity in network like it may alter its IP or MAC. It basically allows loops resulting in portioning of network [8]. The malicious node does not broadcast any needed information which results in losing links.

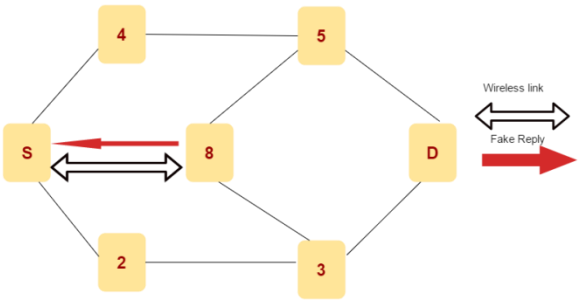

Fig. 2: Link Spoofing

D) Wormhole

Communication is between malicious nodes, that is malicious node at a point in network receives data packets and bridges them to another one which is also malicious. These bridges exists between two malicious are known as wormhole. These wormholes create severe extortions to routing protocols in MANET. The attackers which use wormholes are able to make their nodes more attractive to other nodes for sending packets [6].

The following Fig. 3 depicts that X and Y are forming tunnel that means these are malicious nodes in network. After initiation of PREQ from source node S to find route to destination D, nodes 1 and 2 transfers request to 5 and X. X which is malicious when finds PREQ, shares it with Y the other node of tunnel, so they start delivering PREQ through node 8 to D. Because it is a high speed link so it can force source node in selection of route to destination that can result in D ignoring PREQ that can arrive in later time and so it undermines the genuine route <S->2->5->7->D>.

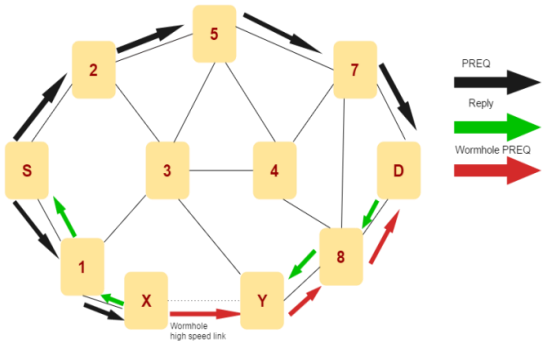

Fig. 3: Wormhole Attack

E) Sinkhole

One of the severe attacks in which attacking node presents an attractive, wrong routing link which is called a gateway, to attract all the network traffic towards it. When it receives whole traffic, it then alters the specific secret information, this malicious node tries to get the secure data from all neigh [9] boring nodes, because it make itself the best possible communicating route to destination [7].

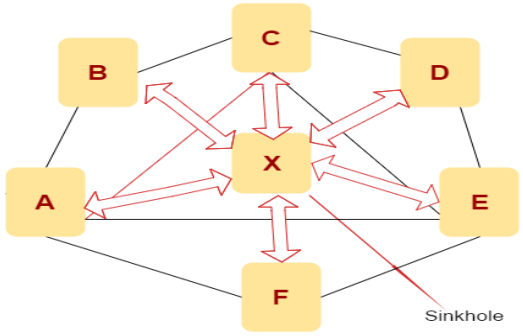

Fig. 4: Sinkhole

F) Session Hijacking

Attackers in this attack 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 [10].

G) Rushing

In this attack, malicious node ensures that route should be established through it, which is why it always waits for route request PREQ, every time PREQ arrive this malicious node rushes the request to next intermediary node, to be hopeful to make a route through it [5].

Table 1: Solutions of Network Layer Attacks

Issues	Possible solutions	Shortcomings
Wormhole	Packet leashes : a simple and strong technique [11]	Includes the limitations of GPS technology, require loosely synchronized clocks [11]
	Time of flight: without CPU association ,it requires hardware to immediately reply [11]	Impractical approach as it requires hardware and MAC layer modifications [11]
	Directional Antennas: use of the directional antennas on all the nodes or several nodes [11]	Only applicable to networks which uses directional antennas to reply ,not applicable to other networks [11]
	Statistical Analysis: depends upon the previous records [11]	Good for networks which uses multipath on demand protocols [11]
Spoofing	Multi-copy routing protocol: Send multiple copies of a message so that it reaches its ultimate destination [12]	Increases network traffic [12]
	Encounter Bases routing(EBR): packet is replicated to a count which is set by the sender [12]	Requires extra overhead to count the replica [12]
Blackhole	Repeated next hop node [13]	Detect single blackhole attack in network [13]
	Real time monitoring: use of two variable fcount and rcount to detect the suspected node [13]	Threshold value identify the malicious node [13]
	Comparison of Sequence number: destination sequence number of all replying nodes is compared to detect suspected node [13]	It cannot detect the attack in the case when sequence number is not very large [13]
	Calculation of peak value : PREP sequence number, number of replies and routing table sequence number define peak value upon which routing decision is taken [13]	Overhead of peak value calculation [13]
	Check honesty of nodes: Honesty is checked by taking the opinion from neighboring nodes [13]	Only for the detection of single level blackhole [13]
Flooding	Neighbor suppression method: priority of nodes is set on the basis of number of PREP received [14]	A normal node can be suspected as malicious node due to the high mobility [14]
	Distributive Approach: use of the two threshold values to detect malicious node [14]	Takes extra time [14]
	DSR protocol: nodes are declared as friends, acquaintance and strangers on the basis of trust function [14]	This approach is not good in the network with high node mobility [14]
Rushing	Secure neighbor detection [15]	Sometimes a normal node can be detected as malicious node [15]
	Randomized Route Request Forwarding [15]	Increases network traffic and slows down the data sending rate [15]
	Secure route delegation [15]	
Session Hijacking	Securing user logins [9]	
	Secure password using encryption [9]	
	Limiting user's rights [9]	
Sinkhole	Encryption and decryption method [16]	Due to dynamic nature of MANET , encryption and decryption method is not much useful [16]

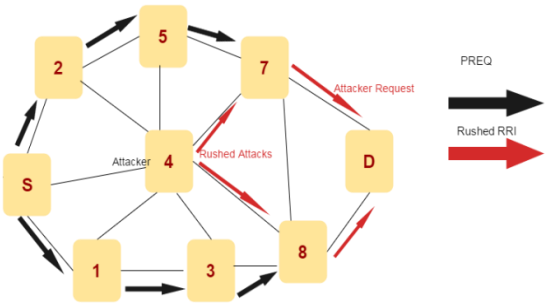

Fig. 5: Rushing

III. SOLUTIONS AND SUGESSIONS

Table 1 comprises the most suitable solution for each attack in a comprehensive way.

We have seen in each attack, there exist some malicious nodes that try to breach the security at network level. A proposed solution for this is we can add some protocol at source node that will be able to detect malicious node in the network at the time of sending PREQ and a routing table can be maintained in network to store the information of those malicious nodes so that all other nodes can consult that table before setting route to destination and also for future response.

IV. CONCLUSION

Studies to literature related to MANET shows that a lot of work has been done in this area by various institutes, about various domains of MANET. In this paper main focus was on attacks of network layer and solutions to these vulnerabilities to MANET. The solutions discussed in this paper and in other surveys are now well known to attackers and hackers, who are also working to breach these securities also so that they can easily dig into network. Therefore to avoid future attacks and abnormalities in MANET strict monitoring is required. An extra layer of security, having routing table which can keep track all the current and previous malicious nodes, can be added to all the aforesaid solutions to enhance their power to restrain vulnerabilities in the network. Moreover there should be a constant effort to explore literature and propose more solutions to improve the security of MANET.

REFERENCES

[1] A. .. Jayalakshmi .A, "A Study on Issues and Challenges in Mobile Ad hoc Networks," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 3, 2015.

[2] R. .G, "Mobile Adhoc Network(MANETS) :Proposed solution to Security Related Issues," *Indian Journal of Computer Science and Engineering (IJCSE)*, vol. 2, 2011.

[3] J. .. a. M. .. Anum .A, "Suggesting the Possible Solution of the Most Probable Security Attacks of MANETs," *International Journal of Computer Science and Telecommunications*, vol. 7, 2016.

[4] M. A. N. &. S. M. Rashid Hafeez Khokhar, "A Review of Current Routing Attacks in Mobile Ad hoc Netwroks," *International Journal of Computer Science and Security, volume (2) issue (3)*, pp. 18 - 29 , 2008.

[5] P. Berwal, "Security Issues in MANET: A Review," *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH AND TECHNOLOGY*, vol. 2, no. 12, pp. 3555-3557, 2013.

[6] A. P. K. Gagandeep, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 1, no. 5, 2012.

[7] H. K. Akanksha Saini, "Effect of Black Hole Attack on AODV Routing Protocol in MANET," *INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY*, vol. 1, no. 2, 2010.

[8] 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.

[9] A. A. Anum. A, "Possible Solutions of Different Security Issues and Challenges in Mobile Ad-Hoc Networks (MANETs)," *INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY SCIENCES AND ENGINEERING*, vol. 5, no. 6, 2014.

[10] S. S. Pradeep Rai, "A Review of 'MANET's Security Aspects and Challenges," *IJCA Special Issue on "Mobile Ad-hoc Networks" MANET*, 2010.

[11] N. S., "Defending Wormhole Attacks in Wireless ad-hoc Networks," *International journal of computer science & engineering survey (IJCSES)*, vol. 2, August 2011.

[12] H. .. Ankit .M, "A Review: Attacks and Its Solution over Mobile Ad-Hoc Network," *International Journal of Engineering Trends and Technology (IJETT)*, vol. 4, May 2013.

[13] 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.

[14] N. S. Shweta Y, "Flooding Attacks Prevention in Manet," *International Journal of Computer Technology and Electronics Engineering (IJCTEE)*, vol. 1, November 2011.

[15] S. S. P. Wilson, "Solution To Prohibit Rushing Attack In Mobile Ad-Hoc Network," *International Journal on Applications in Information and Communication Engineering*, vol. 1, September 2015.

[16] L. Sachin, "Security in MANET: Vulnerabilities, Attacks & Solutions," *International Journal of Multidisciplinary and Current Research*, vol. 2, Feb. 2014.

[17] B. K. e. al, "A Collusion Attack Against OLSR-Based Mobile Ad Hoc Networks," *IEEE GLOBECOM*.

[18] G. K. ,. P. .. Pravin. A, "Mobile Ad Hoc Networking: Imperatives and Challenges," *IJCA Special Issue on "Mobile Ad-hoc Networks"*, 2010.

[19] A. J. Prinkya. S, "A Study on Security Issues in Mobile Ad Hoc Networks," *International Journal of Innovations & Advancement in Computer Science IJIACS*, vol. 4, March 2016.