Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey on Network Attacks in Mobile Ad Hoc Networks

Vivek Richhariya,
Ph. D Scholar, Department of Computer Science & Engineering,
AISECT University, Bhopal, India

Praveen Kaushik
Assistant Professor, Department of Computer Science & Engineering, MANIT, Bhopal, India

Abstract: A Mobile Ad hoc Network (MANET) is a collection of wireless nodes than can form of dynamically topologies without aid of any pre-existing infrastructure connected to fixed network or centralized administration. Security is an primary concern in mobile ad hoc network (MANETs). MANETs are more vulnerable to security attacks due to mobility of nodes. Attacks in ad hoc networks can be categorized as passive and active attacks, depending on whether the connectivity of the network is disrupted or not. In this paper, we give an overview of attacks on the network layer according to the protocols.

Keywords: MANET, Survey, Security attacks

I. INTRODUCTION

Wireless mobile system has been in use since 1980's. In the wireless networking system, the mobile devices communicated with access point like base station, connected to the fixed infrastructure (e.g. GSM. UMTS,WLL, WLAN, etc.). Mobile nodes in MANET are dynamically located and communicated at anywhere & any time without using pre-existing network infrastructure [2].

There are some characteristics of MANET.

- The communicating medium is broadcast.
- The topologies between the nodes are changing continuously (i.e. dynamically).
- Nodes are free to move anywhere.
- In the presence of selfish node or malicious nodes, the performance is decrease [3].

There are some security goals of MANET.

- Authentication: The authentication means that a user has the access right to use the resource. It is an assurance that the traffic you receive is sent by the authenticated user [7].
- Integrity: Integrity is an ensure that the data which is received by the receiver has not been change or modified after the send by the original user.
- Confidentiality: It means that the data is not examined by the unauthorized party.
- Non-repudiation: This is an authentication service. It ensures that the sender and receiver of message can not deny, they have ever sent or received such message. In other words, someone can not deny something.
- Access control: It is the prevention to use resource by unauthorized user.

Routing in MANETs

Routing is the act of moving information from a source to a destination in an internetwork. Throughout this process, at least one intermediate node within the internet work is encountered. The problem in routing is due to the dynamically topology of the nodes and the devices[14]. The type of routing are namely proactive and reactive.

In Table-Driven Routing Protocols (Proactive), Each and every node in the network maintains routing information to every other node in the network. Information of routing is generally kept in the routing tables and is periodically updated as the network topology changes. Certain proactive routing protocols are Destination-Sequenced Distance Vector (DSDV), Optimized Link State Routing (OLSR).

In On Demand Routing Protocols (Reactive), These protocols take a lazy approach to routing. In reactive, routing paths are searched for when demanded. When a source wants to send to a destination, it finds the path to the destination with the help of route discovery mechanisms. The route remains valid till the destination is reachable or until the route is no longer needed. Some reactive protocols are Ad hoc On-Demand Distance (AODV), Dynamic Source Routing (DSR) [12].

Vulnerabilities of MANETs

The vulnerabilities of MANETs are summarized below,

• **Wireless links***:* First of all, the use of wireless links makes the network susceptible to attacks such as active interference and eavesdropping. Attackers do not need physical access to the network to carry out these attacks unlike wired networks.

• **Dynamic topology***:* The nodes in MANETs can leave and join the network, and move independently. Due to this, the network topology can change frequently and trust may also be disturbed if some nodes are detected as malicious**.**

• **Cooperativeness***:* Routing algorithms for MANETs usually assume that nodes are cooperative and non selfishness. Therefore, a malicious attacker can easily become an important routing agent and disrupt network operations by disobeying the protocol specifications[6].

• **No pre defined boundary***:* In MANET, we can not precisely define a physical boundary of the network. As soon as malicious node comes in radio range of a node, it would be able to communicate with that node.

• **Limited resources***:* The node in MANET need to consider restricted power supply which will cause several problems. A node in MANET, behave in a selfish manner when it is finding that there is only limited power supply.

2 NETWORK SECURITY ATTACKS

As we discussed earlier, securing wireless ad hoc network is a highly challenging issues. Since mobile ad hoc network is multihop in nature, it strictly depends upon the cooperation between the nodes. So the guarantee of cooperation of nodes is required. A variety of attacks have been identified and detected in the network. In order to provide a secure communication, we have to face the security challenges. Basically, we have two types of attacks [2].

2.1 Passive Attacks

A passive attack would not disturb the normal operation of mobile ad hoc network, while data have been exchanged from the network. The attacker do not damage to the network directly. However, they can get information for future harmful attacks. The types of passive attacks are eavesdropping and traffic analysis[2].

2.1.1 Eavesdropping Attack: Eavesdropping attack is the method of collecting information by snooping on transmitted data on legitimate network. This information may include the location, public key, private key or even password of the nodes. The attacker snoops the data interchanged in the network without modifying it. It is more vulnerable for MANET malicious nodes that can intercept the shared wireless medium.

2.1.2 Traffic analysis:-The main task of this attack is to monitor and analyze which type of the transmission is going on. Its aim is to engage in protocol or to provoke transmission between nodes. For this purpose, the attacker may use several methods such as time-correlation monitoring, traffic rate analysis, and etc[5].

2.2 Active Attacks

In this attack, an attacker always tries to alter or destroy the data or normal operation on MANET. Active attacks can be either internal or external. In external attack, the attacker focus on to cause congestion in the network. For this purpose, they propagates fake information or to disturb the nodes from providing services. In internal attacks, the attacker wants to get the normal access to participate in the network activities. The active attacks are namely dropping, modification, fabrication, etc[9].

2.2.1 Dropping attacks: The communication between two nodes outside the transmission range depends on intermediate nodes to forward the packets. But formerly these intermediate nodes does not work as expected i.e. they start to drop the packets during the communication in order to save their limited sources such as bandwidth, energy, etc. Such kinds of nodes are called misbehaving nodes or non cooperative nodes. Due to this, it might also reduce the network performance by causing data packets to be retransmitted and also new routes to the destination to be discovered [17].

2.2.2 Modification attacks: The attacker make some changes to the routing message. Due to movability of nodes in the network, the malicious node participate in the packet forwarding process and later on launch the message modification attacks. The example of message modification attacks are impersonation attacks and packet misrouting.

2.2.3 Fabrication attacks: In fabrication attacks, the attacker forges network packets. There are two types of fabrication attacks namely active forge and forge reply. The attackers send faked messages without receiving any related message in the case of active forge. In forge reply, the attacker sends fake route reply messages in response to related authenticate route request messages.

3. NETWORK LAYER ATTACKS

In ad hoc network routing mechanism works on three layers namely Physical, MAC and Network. As we discussed earlier, MANETs are more vulnerable to various attacks and all these three layers suffer from different attacks that cause routing disorder. These different types are attack are shown as follows[9].

3.1 Wormhole attack

An attacker receives packets at one position and tunnels them to another position in the network. In this way, routing can be disrupted when routing control messages are tunneled. Such tunnel between two colluding attackers is called as a wormhole. This attacks are severe threats to MANET routing protocols. When a wormhole attack is employed against an on-demand routing protocol (reactive protocol) such as AODV or DSR, the attack could prevent the discovery of any routes through the wormhole.

3.2 Blackhole attack

This is the most frequent attack that happens when packet are forwarded. The attacker uses routing protocol to advertise itself as having a authenticate route to a destination node. An attacker use the flooding based protocol for listing the request for a route from the source. Then attacker create a reply message having shortest path to the destination. As the result, the attacker reached to the source before the reply from the actual node and then source assume that it is the shortest path to the destination. Therefore a fake route is created. Once the attacker has been able to introduce himself between the communication node, then attacker may free to do anything with the packet which is send by source for the destination [2,3].

3.3 Byzantine attack

In this attacks, a compromised intermediate node operates only, or a set of compromised intermediate nodes operates in

connivance and carry out attacks such as forwarding packets through non-optimal paths, or selectively dropping packets, creating routing loops, which results in degradation or disruption of the routing services.

3.4 Routing Attacks

There are several types of attacks in the routing protocol which are targeted at disrupting the normal operation of the network. These attacks on the routing protocol are given as follows:

- **Routing Table Overflow:** Here, the attacker seeks to generate routes to nonexistent nodes. The main purpose is to create enough routes to prevent new routes from being created.
- **Routing Table Poisoning:** In this attack, the compromised nodes in the networks send false routing information's updates or modify actual route update packets sent to other uncompromised nodes.
- **Packet Replication:** Here, an adversary node replicates stale packets. It consumes additional battery power and bandwidth resources available to the nodes.
- **Route Cache Poisoning:** In the reactive routing protocols (e.g. AODV), each node keeps a route cache which maintains routing information regarding routes that have become recognized to the node in the recent past.

3.5 Gray hole attack : This attack is also called as routing misbehavior attack which leads to dropping the message. Gray howl is a node that can switch from behaving correctly to behaving like a black hole[11].

3.6 Resource consumption attack

This attack is also called as the sleep deprivation attack. An attacker or a selfish node can try to consume battery life by requesting excessive route discovery.

4. Conclusion

In this survey paper, we try to explain the network security threats in the mobile ad hoc network. Due to movability of nodes in MANETs, the security needs are much higher than as comparison to traditional wired network. Our main aim of this survey paper is to detect and mitigate the malicious node, which is acting as a normal node in the network. During the survey, we discussed how the attack has been occurred in the network layer. To conclude, the security is mobile ad hoc network is a complex and challenging topic.

References

[1] Y.C. Hu, A. Perrig, and D.B.Johnson, "*Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad hoc Network*," Proc. 22 Annual Joint Conf. IEEE Computer and Communication Societies San Francisco, CA, April 2003.

[2] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , "*A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks* ,"

[3] Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp, @ 2006 Springer.

[4] Lidong Zhou, Zygmunt J. Haas:," *Securing Ad hoc Networks*",IEEE Network Magzine, 13, 6, Pages 24-30, 1999.

[5] Ping Yi, Yue Wu and Futai Zou and Ning Liu, "*A Survey on Security in Wireless Mesh Networks*", Proceedings of IETE Technical Review, Vol. 27, Issue 1, Jan-Feb 2010.

[6] Sukla Banerjee , "*Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks*", Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[7] Pradip M. Jawandhiya, Mangesh M. Ghonge, Dr. M.S.Ali, Prof. J.S. Deshpande, "A Survey of Mobile Ad Hoc Network Attacks ", International Journal of Engineering Science and Technology, Vol. 2(9), 2010, 4063-4071

[8] Nishu Garg and R.P.Mahapatra, "*MANET Security Issues* ," IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[9] 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.

[10] Wikipedia, "Mobile Ad Hoc Networks",:http://en.wikipedia.org/wiki/Mobile_ad_hoc_network, 8/2010.

[11] J. Lundberg, "*Routing Security in Ad-hoc NEtworks* ," http://citeseer.nec.com/400961.html.

[12] V. Madhu Viswanatham and A.A. Chari, "*An Approach for Detecting Attacks in Mobile Adhoc Networks* ," Journal of Computer Science 4 (3): 245-251, 2008 ISSN 1549-3636 © 2008 Science Publications.

[13] Hoang Lan and Uyen Trang Nguyen, "*Study of Different Types of Attacks on Multicast in Mobile Ad hoc Networks*", Proceedings of ICNICONSMCL'06, 0-7695-2552-0/06@ 2006 IEEE.

[14] S. Murphy, "*Routing Protocol Threat Analysis,"* Internet Draft, draft-murphy-threat-00.txt, Octomber 2002.

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

[16] P. Papadimitratos and Z.J.Haas, "*Securing the Routing Infrastructure*", IEEE Communications, vol. 10, no. 40. Octomber 2002, pp. 60-68.

[17] Amitabh Misgra and Ketan M. Nadkarni, "*Security in Wireless Ad hoc Networks*", in Book The Handbook of Ad hoc Wireless Networks(Chapter 30),CRC Press LLC, 2003.

