International Journal of Innovative Research in Science and Engineering
Volume 08, Issue 02, 2022
www.ijirse.com
ISSN: 2454-9665

Impersonation Attack in MANETS: A Review

J.Srinivasan

Assistant professor, Department of CSA, SCSVMV University.

ABSTRACT

Ad hoc networks are the special networks formed for specific applications. Operating in ad-hoc mode allows all wireless devices within range of each other to discover and communicate in a peer-to-peer fashion without involving central access points. Many routing protocols like AODV, DSR etc have been proposed for these networks to find an end to end path between the nodes. These routing protocols are prone to attacks by the malicious nodes. There is a need to detect and prevent these impersonation attacks in a timely manner before destruction of network services.

KEYWORDS

Network Protocols, Wireless Network, Mobile Network, Ad-hoc Networks, Routing Protocols, Security, and Attackers.

1. INTRODUCTION

Ad hoc Networks are the networks formed for a particular purpose. These networks assume that an end to end path between the nodes exists. They are often created on-the-fly and for one-time or temporary use. They find their use in special applications like military, disaster relief etc that are in a need of forming a new infrastructure less network with all pre-existing infrastructure being destroyed. Characteristics of Ad hoc networks include:

1) Lack of fixed infrastructure: An ad-hoc network is a collection of nodes that do not rely on pre-existing infrastructure for their connectivity. So these types of networks are flexible and easily reconfigurable.

2) Limited resources: Due to lack of fixed infrastructures, these networks have limited resources for their use. Resources like battery power, bandwidth, computation power, memory etc have to be used judiciously for the survival and proper functioning of the network.

3) Dynamic Topology: Nodes in the ad hoc networks are often mobile wireless devices like laptops, PDAs, smart-phones etc resulting in frequent change of their location, resulting in a dynamic topology.

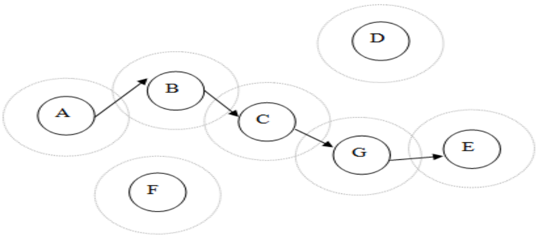

Figure 1 : An Example of Ad Hoc Networks

An example of ad hoc networks is shown in **Figure.1**. Here ad hoc network is being established by communication between wireless mobile nodes A, B, C, D, E, F and G. Node A wants to send a message to another node E in the network. Routing in the network for such a scenario takes place through multiple intermediate relay hops present in between A and E, assuming that all nodes in the network are trustworthy. Since A and B are in the wireless range of each other, A sends the message to B, B and C are in range of each other so message will get passed to C and so on till the message finally reaches E via the path A, B, C, G and E. The organization of this paper is as follows. Section I explores the various routing protocols in ad-hoc networks. Section II highlights the various Routing protocols involved. Network attacks are categorized in Section III. Section IV concludes the paper.

2. ROUTING PROTOCOLS IN MOBILE AD-HOC NETWORKS (MANETS)

The main goal of routing protocols in ad hoc networks is to find out the optimal path with minimum overhead, minimum bandwidth consumption and minimum delay between the source and the destination node. As most of the nodes in ad hoc networks are wireless mobile nodes, the topology of such type of a network does not remain fixed. As a result, it becomes the node's responsibility to regularly discover the network topology in order to route the messages properly.

Therefore, there is a need for various routing protocols to discover an optimal path from the source to the destination. A single routing protocol cannot work optimally in different network scenarios. A need is therefore felt for an appropriate protocol selection taking in consideration different network parameters such as density, size and the mobility of the nodes. On the basis of the network topology, the routing protocols in MANETS are broadly categorized as Proactive Routing Protocols and Reactive Routing Protocols which are discussed as follows:

1. Proactive Routing Protocols - In the proactive routing protocols, routing is done using the information present in routing tables maintained at each node i.e. table driven routing. These tables are exchanged on a periodic basis between the nodes. Each entry in the table contains the information of the next hop for reaching to a node or subnet and the cost of this route. Since information of the neighboring nodes is maintained at each node, the time for route selection becomes minimal.

2. Reactive Routing Protocols - In case of Reactive Routing protocols, the routing is done by the nodes only on demand i.e. only when the node needs to send a message. The sender floods its neighbors with Route Request (RREQ) packets to find route in the network. Any destination/intermediate node in the network having path to the destination will reply back with Route Reply (RREP) to the sender and the routing is accomplished.

These suffer from following disadvantages:

a) There is a time delay in finding the routes since a large number of control packets have to be exchanged before the exchange of actual data.

b) Network congestion may result due to excessive flooding of packets.

Reactive Routing find their applications in the following network scenarios:

c) High mobility networks.

d) Medium size networks.

Various Reactive routing algorithms are Ad Hoc On-Demand Distance-Vector (AODV)[10], Dynamic MANET On Demand (DYMO)[10], Admission Control enabled On demand Routing (ACOR)[10].

3. CATEGORIZING NETWORK ATTACKS

Attacks on the ad hoc networks can be broadly categorized as Passive Attacks and Active Attacks.

1. Passive Attacks - The main aim of passive attackers is to steal the valuable information from the targeted networks. Attackers do not disturb the normal network functioning like inducing false packets or dropping packets. They simply become a part of the network but continuously keeps an eye on the network traffic thus in turn violating the message confidentiality constraint. Since they do not initiate any malicious activity to disrupt the normal functioning of the network, it becomes very difficult to identify such attacks. Examples of such types of attacks are traffic analysis, traffic monitoring and eavesdropping.

2. Active Attacks - Active attackers tamper with the network traffic like cause congestion, propagation of incorrect routing information etc. Due to their active participation, their detection and prevention can be done using suitable prevention algorithms. Examples of passive attacks include modification attack, impersonation, fabrication and message replay. Attacks can also be classified depending upon the position of the attacker in the network.

3.1 Impersonation Attack

There is no proper authenticated mechanism to join an ad hoc network. Impersonation Attack is caused when any adversary node joins and takes the identity of a trusted node in the network. It then starts damaging the authentication constraint of the network. In this the attacker node uses address (IP or MAC) of some legitimate node in the network for its outgoing packets resulting in receiving of the messages which are for that node. Such a malicious node can also spread fake routing knowledge and gains inappropriate access to confidential data of genuine nodes, and becomes an authorized entity in the network.

An attacker can impersonate an authorized node as follows:

1) By guessing the identity details of the authorized node or,

2) By disabling other node’s authentication mechanism.

Consider the network scenario in **Figure 2** where node D sends packets to its neighbors(C and G) with source address as E because of which any packet coming for E through C and G will now be directed to the malicious node D instead of E.

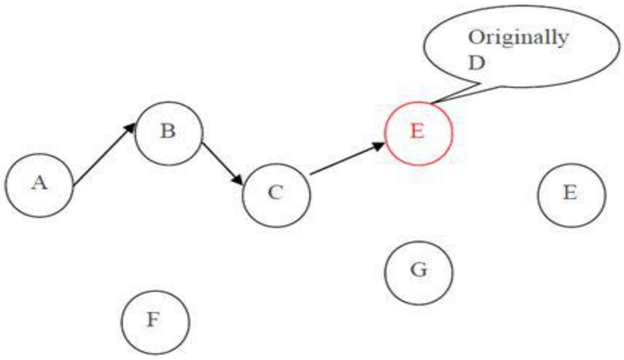

Figure 2: An Example of Impersonation Attack

4. CONCLUSION AND FUTURE WORK

This paper presented one of the popular attacks like impersonation attack in MANETs. The author had presented some of the methods to attack a network model along with one of the proposed solutions. Various issues that need to be addressed keeping in view the security of MANETS have also been highlighted. The need of the hour is to detect and prevent these impersonation attacks in a timely fashion. In the future work, the author would like to propose an integrated security system which will analyze the network for detecting the presence of these attack. After detection of a particular attack author will try to pinpoint the attacker nodes and then mitigate their affect by excluding those nodes from the system.

REFERENCES

[1]. S. Agrawal, S. Jain, and S. Sharma, "A survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks," Journal of Computing, Volume 3, Issue 1, January 2011, ISSN 2151-9617.

[2]. V. Balakrishnan, V. Varadharajan, U.K. Tupakula, "Fellowship: Defense Against Flooding and Packet Drop Attacks In MANET," Network Operations and Management Symposium, NOMS 2006, pp. 1- 4, 2006.

[3]. Y. Guo, S. Gordon, S. Perreau, "A Flow Based Detection Mechanism against Flooding Attacks in Mobile Ad Hoc Networks," Wireless Communications and Networking Conference, IEEE (WCNC 2007), pp.3105-3110, March 2007.

[4]. S. Desilva, and R.V. Boppana, "Mitigating Malicious Control Packet Floods In Ad Hoc Networks," Proceedings of IEEE Wireless Communications and Networking Conference 2005, vol. -4, pp. 2112- 2117, March 2005.

[5]. Y. Sasson, D. Cavin, A. Schiper, "Probabilistic Broadcast for Flooding in Wireless Mobile Ad hoc Networks," 2003 IEEE Wireless Communications and Networking, (WCNC 2003), New Orleans, LA, USA, vol.2, March 202003, pp.1124-1130.

[6]. Revathi Venkataraman, M. Pushpalatha, and T. Rama Rao, "Performance Analysis of Flooding Attack Prevention Algorithm in MANETs," World Academy of Science, Engineering and Technology 2009.

[7]. M.A. Shurman, S.M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks," ACM Southeast Regional Conference, pp. 96-97, 2004.

[8]. J. CAI, P. YI, J. CHEN, Z. WANG, N. LIU, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network," 2010 24th IEEE International Conference on Advanced Information Networking and Applications (AINA),Perth, Australia, April 20-23, 2010, pp.775- 780,.

[9]. Y.C. Hu, A. Perrig and D. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proceedings of the ACM Workshop on Wireless Security (WiSe), SanDiego, California, pp. 30-40, September 2003.

[10]. T.H. Clausen, G. Hansen, L. Christensen, and G. Behrmann, "The Optimized Link State Routing Protocol, Evaluation Through Experiments and Simulation," Proceedings of IEEE Symposium on Wireless Personal Mobile Communications 2001, September 2001.