ISSN:0975-9646

Security Threats in Mobile Ad Hoc Networks - A Survey

Sanjeev Gangwar

Assistant Professor
Department of Computer Applications
VBS Purvanchal University Jaunpur (U.P.) India

Abstract- Mobile Ad Hoc networks (MANETs) is a class of wireless networks that have been researched extensively over the recent years. The security challenges arise due to MANET's self-configuration and self-maintenance capabilities. In comparison to wired network the mobile ad hoc network is more exposed to being attacked. Because of its fundamental Properties, such as dynamic topology, limited power and limited bandwidth, it is very hard to achieve absolute security in the mobile ad hoc network. This paper presents a thorough overview of security issues in Mobile Ad hoc Network.

Keywords: Mobile Ad hoc Network, Security issues, Attacks

1. INTRODUCTION

In recent years, the increasing popularity of mobile device, like laptops, PDAs and handled digital devices, has impelled a revolutionary change in the computing world. We need to acquire information and connect to other device whenever and wherever we want. So it is necessary to adopt wireless as the interconnection method. That is how MANET rises. A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies [1]. A set of wireless mobile hosts dynamically establish their own network on the fly, without relying on any preexisting communication infrastructure. But this open network architecture and dynamic network topology [2] are prone to be attacked internally and externally. So the ultimate goal of the security solutions for MANET is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. The mobile ad hoc network has the following typical features [3].

(i) Unreliability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.

(ii) Dynamic Network Topology: In MANETs, nodes can join and leave the network dynamically and can move independently. Due to such type nature there is no fixed set of topology works in MANETs. The nodes with inadequate physical protection may become malicious node and reduce the network performance

(iii) Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad ho networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol.

Because of the above features, the mobile ad hoc networks are more inclined to suffer from the malicious behaviors than the traditional wired networks. Therefore, we need to focus more attention to the security issues in the mobile ad hoc networks.

2. VULNERABILITIE OF THE MOBILE AD HOC NETWORKS

Because mobile ad hoc networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in the mobile ad hoc network than in the wired network. In this section, we discuss the various vulnerabilities that exist in the mobile ad hoc networks.

(i) No central infrastructure: The lack of such infrastructure makes it impossible for the distribution of centralized host relationships [5]. Instead any security solution should rely on a distributed cooperative scheme Instead of a centralized scheme.

(ii) Unreliability of wireless links: First of all, the use of wireless links makes the network susceptible to attacks such as eavesdropping and active interference. Unlike wired networks, attackers do not need physical access to the network to carry out these attacks. Furthermore wireless networks typically have lower bandwidths than wired networks. Attackers can exploit this feature, consuming network bandwidth with ease to prevent normal communication among nodes.

(iii) Multi-hop: Given that the lack of central routers and gateways, the source node need to route himself to the destination node. Thus, packets need to go through different mobile nodes before arriving at their final destination. Possibility of malicious nodes may lead to a serious vulnerability.

(iv) Constantly changing topology: MANET nodes can leave and join the network, and move independently. As a result the network topology can change frequently. It is hard to differentiate normal behavior of the network from anomaly/malicious behavior in

this dynamic environment. For example, a node sending disruptive routing information can be a malicious node, or else simply be using outdated information in good faith. Moreover mobility of nodes means that we cannot assume nodes, especially critical ones (servers, etc.), are secured in locked cabinets as in wired networks. Nodes with inadequate physical protection may often be at risk of being captured and compromised.

(v) Device limitation: The limitation of device in terms of power and memory and computation power poses great challenge in design a security protocols which calls for low complexity computation and memory. And the low power device may be selfish to provide normal services. The attacked may target on some nodes and try to flooding bunch of trash messages to running out of the device's power as DoS(Denial of Service) attack.

3. SECURITY SERVICES

The aim of a security service is to secure network before any attack happened and made it harder for a malicious node to breaks the security of the network. Due to special features of MANET, providing these services faced lots of challenges. For securing MANET a trade-off between these services must be provided, which means if one service guarantees without noticing other services, security system will fail. Providing a trade-off between these security services is depended on network application, but the problem is to provide services one by one in MANET and presenting a way to guarantee each service. We discuss important security services and their challenges as follows:

(i) Availability: Ensures that the desired network services are always available whenever they are expected, in spite of the presence of attacks. To achieving high availability we need to overcome denial of Service and energy starvation attacks, as well as node misbehavior such as node selfishness in packet forwarding [5].

(ii) Integrity: Ensures that a message sent from node A to node B was not modified by any malicious node in the middle during its transmission. Integrity can be compromised mainly in two ways[6]:

- Malicious altering
- Accidental altering

A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.

(iii) Confidentiality: According to this service, each node or application must have access to specified services that it has the permission to access. Most of services that are provided by data confidentially use encryption methods but in MANET as there is no central management, key distribution faced lots of challenges and in some cases impossible. Authors in [14] proposed a new scheme for reliable data delivery to enhance the data confidentially. The basic idea is to transform a secret message into multiple shares by secret sharing schemes and then deliver the shares via multiple independent paths to the destination. Therefore, even if a small number of nodes that are used to relay the message shares, been compromised, the secret message as a whole is not compromised. Using multipath delivering causes the variation of delay in packet delivery for different packets. It also leads to out-of-order packet delivery.

(iv) Authenticity: The goal of this service is to provide trustable communications between two different nodes. When a node receives packets from a source, it must be sure about identity of the source node. One way to provide this service is using certifications, whoever in absence of central control unit, key distribution and key management are challengeable. In [13] the authors presented a new way based on trust model and clustering to public the certificate keys. In this case, the network is divided into some clusters and in this clusters public key distribution will be safe by mechanisms provided in the paper. Their simulation results show that, the presented approach is better than PGP. But it has some limitations like clustering. MANET dynamic topology and unpredictable nodes position, made clustering challengeable.

(v) Nonrepudiation: By using this service, neither source nor destination can repudiate their behavior or data. In other words, if a node receives a packet from node 2, and sends a reply, node 2 cannot repudiate the packet that it has been sent. Authors in [16] presented a new approach that is based on grouping and limiting hops in broadcast packets. All group members have a private key to ensure that another node couldn't create packets with its properties. But creating groups in MANET is challengeable. In previous part a brief discussion on security services and their challenges in MANET was provided. Detecting and eliminating malicious nodes, is another aspect of the MANET security. In the next section, important attacks in MANET and existing detection and/or elimination approaches to secure network against them is discussed.

(vi) Authorization: Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to different level of users. For instance, we need to ensure that network management function is only accessible by the network administrator. Therefore there should be an authorization process before the network administrator accesses the network management functions.

(vii) Anonymity: Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software. This criterion is closely related to privacy preserving, in which we should try to protect the privacy of the nodes from arbitrary disclosure to any other entities.

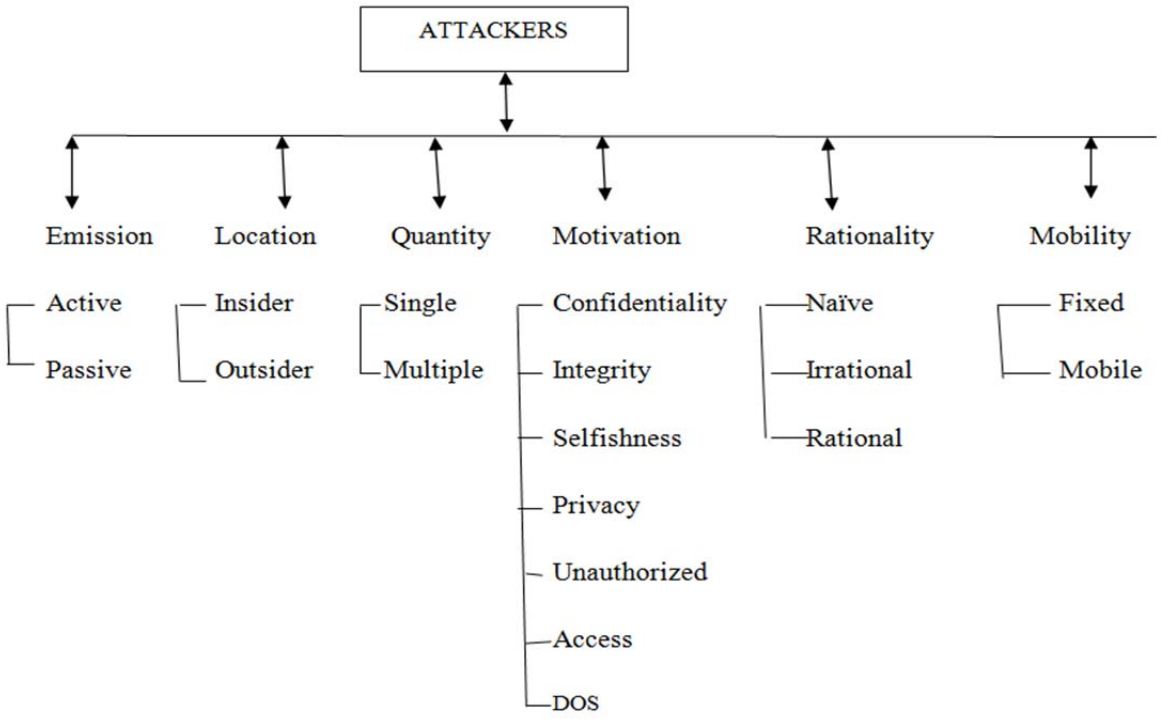

Figure 1

4. ATTACK TYPES IN MOBILE AD HOC NETWORKS

There are different types of attacker present in MANETs, which tries to reduce the performance of network which is classified in the figure 1

Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from within the network itself. Ad hoc network are mainly subjected to two different levels of attacks. The first level of attack occurs on the basic mechanisms of the ad hoc network such as routing. Whereas the second level of attacks tries to damage the security mechanisms employed in the network. The attacks in MANETs are divided into two major types.

(i) Passive attacks:

In a passive attack an unauthorized node monitors and aims to find out information about the network [8.9]. The attackers do not otherwise need to communicate with the network. Hence they do not disrupt communications or cause any direct damage to the network. However, they can be used to get information for future harmful attacks. Examples of passive attacks are eavesdropping and traffic analysis.

Eavesdropping Attacks, also known as disclosure attacks, are passive attacks by external or internal nodes [7]. The goal of eavesdropping is to obtain some confidential information that should be kept secret during the communication. The confidential information may include the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access.

Traffic Analysis: In MANETs the data packets as well as traffic pattern both are important for adversaries [10]. For example, confidential information about network topology can be derived by analyzing traffic patterns. Traffic analysis can also be conducted as active attack by destroying nodes, which stimulates self-organization in the network, and valuable data about the topology can be gathered. Traffic analysis in ad hoc networks may reveal following type of information. Traffic analysis in ad hoc networks may reveal:

- the existence and location of nodes;
- the communications network topology;
- the roles played by nodes;
- the current sources and destination of communications; and
- the current location of specific individuals or functions

(2) Active Attacks:

Active attacks [11] are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. Active external attacks can be carried out by outside sources that do not belong to the network. Internal attacks are from malicious nodes which are part of the network, internal attacks are more severe and hard to detect than external attacks [2, 4, 13]. These attacks generate unauthorized access to network that helps the attacker to make changes such as modification of packets, DoS, congestion etc. The active attacks are generally launched by compromised nodes or malicious nodes. Malicious nodes change the routing information by advertising itself as having shortest path to the destination. Active attacks are classified into four groups:

Dropping Attacks: Malicious or selfish nodes deliberately drop all packets that are not destined for them. While malicious nodes aim to disrupt the network connection,

selfish nodes aim to preserve their resources. Dropping attacks can prevent end-to-end communications between nodes, if the dropping node is at a critical point. It might also reduce the network performance by causing data packets to be retransmitted, new routes to the destination to be discovered, and the like. Unfortunately most routing protocols (DSR is an exception [12]) have no mechanism to detect whether data packets have been forwarded or not. However, they can be detected by neighboring nodes through passive acknowledgement or hop-by-hop acknowledgement at the data link layer. An attacker can choose to drop only some packets to avoid being detected; this is called a ***selective dropping attack***. Besides data packets or route discovery packets, an attacker can also drop route error packets, causing the source node to be unaware of failed links (thus interfering with the discovery of alternative routes to the destination).

Modification Attacks: Sinkhole attacks are the example of modification attacks. These attacks modify packets and disrupt the overall communication between network nodes. In sinkhole attack, the compromised node advertises itself in such a way that it has shortest path to the destination. Malicious node than capture important routing information and uses it for further attacks such as dropping and selective forwarding attacks [13].

Fabrication Attacks: In fabrication attack [14], the attacker send fake message to the neighboring nodes without receiving any related message. The attacker can also sends fake route reply message in response to related legitimate route request messages.

Timing Attacks: In this type of attacks, attackers attract other nodes by advertising itself as a node closer to the actual node. Rushing attacks and hello flood attacks uses this technique.

Rushing attack [15] on ad hoc networks which is carried out on on-demand routing protocols that keep a copy of packets at every node. In this attack, an attacker constantly spreads fabricated routing messages which suppress the legitimate routing messages as the nodes discard them as duplicate copies. Another type of attack is spoofing. In spoofing, a malicious node attempts to misrepresent its identity by changing its IP or MAC address in order to change the perception of a network by an incoming node.

The ***hello flood attack*** [16] is another attack that makes the adversary attractive for many routes. In some routing protocols, nodes broadcast Hello packets to detect neighboring nodes. These messages are received by all one-hop neighbor nodes, but are not forwarded to further nodes. The attacker broadcasts many Hello packets with large enough transmission power that each node receiving Hello packets assumes the adversary node to be its neighbour. It can be highly effective in both proactive and reactive MANET protocols.

A further significant attack on MANETs is the collaborative ***wormhole attack***. In worm hole attack, malicious node records packets at one location of the network and tunnels them to another location [17]. Fault routing information could disrupt routes in network [23]. Authors in [24] presented a way to secure MANET against this attack by using encryption and node location information. But as mentioned before, key distribution is a challenge in MANET.

5. CONCLUSION AND FUTURE WORK

The main concern in MANETs is security. Wireless ad hoc networks are exposed to being attacked or harmed because of its fundamental properties such as lack of central control, dynamic quality topology, limited resources and open communication. These features introduce new challenges to intrusion detection technology, so achieving security in ad hoc network is harder compared to wired networks. These attacks can classified as an active or passive attacks. Different security mechanisms are introduced in order to prevent such network. In future study we will try to invent such security algorithm, which will be installed along with routing protocols that helps to reduce the impact of different attacks.

REFERENCES

[1] Sanjeev Gangwar: Mobile Ad Hoc Network: A Comprehensive Study and Survey on Intrusion detection, in International Journal of Engineering Research and Applications, 2012.

[2] H.Nishiyama, T. Ngo, N. Ansari, and N. Kato, "On Minimizing the Impact of Mobility on Topology Control in Mobile Ad Hoc Networks," Wireless Communications, IEEE Transactions, 2012.

[4] Amitabh Mishra, "Security and Quality of Service in Ad Hoc Wreless Networks" (chapter 1, 3), ISBN- 13 978-0-521-87824-1 Handbook.

[5] Panagiotis Papadimitraos and Zygmunt J. Hass, Securing Mobile Ad Hoc Networks, in Book *The Handbook of Ad Hoc Wireless Networks (Chapter 31)*, CRC Press LLC, 2003.

[6] Y. Hu, A. Perrig and D. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, in Proceedings of ACM MobiCom Workshop - WiSe'03,2003.

[7] Vikrant Gokhale, S.K.Gosh, and Arobinda Gupta, "Classification of Attacks on Wireless Mobile *Ad Hoc* Networks and Vehicular *Ad Hoc* Networks *a Survey"*.

[8] Y. Hu, A. Perrig and D. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, in Proceedings of ACM MobiCom Workshop - WiSe'03, 2003.

[9] Y. Hu, A. Perrig and D. Johnson, Wormhole Attacks in Wireless Networks, IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, February 2006.

[10] N.Dixit, S. Agrawal, and V. K. Singh, "A Proposed Solution for security Issues In MANETs," International Journal of Engineering Research & Technology (IJE RT), vol. 2, 2013.

[11] Akanksha Saini, Harish Kumar, "Effect of Black Hole Attack on AODV Routing Protocol in MANET".

[12] Yau P.-W., Mitchell C.J., "Security Vulnerabilities in Ad Hoc Networks", In Proc. of the 7th Int. Symp. on Communications Theory and Applications, pp. 99-104, 2003

[13] Buchegger S., Tissieres C., Le Boudec J.-Y.,"A Test-Bed for Misbehaviour Detection in Mobile Ad-Hoc Networks –How Much Can Watchdogs Really Do?", Mobile Computing Systems and Applications (WMCSA '04), pp. 102-111, 2004.

[14] Ning P., Sun K., "How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols", In Proc. of the IEEE Workshop on Information Assurance, pp. 60-67, 2003

[15] Hu Y.-C., Perrig A., Johnson D.B., "Rushing Attacks and Defence in Wireless Ad Hoc Network Routing Protocols", In Proc. of the ACM Workshop on Wireless Security, 2003

[16] Yi P., Dai Z., Zhang S., Zhong Y., "A New Routing Attack in Mobile Ad Hoc Networks", Int. Journal of Information Technology, vol. 11, No. 2, pp. 83-94, 2005.

[17] M.A. Gorlatova, P. C. Mason, M. Wang, and L. Lamont, " Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis," Military Communications Conference, IEEE, MILCOM, 2006.