ISSN:0975-9646

Nanditha N et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3367-3369

Survey on Mobile Adhoc Networks

Nanditha N
M. Tech student
MVJ College of Engineering
Bangalore, India

Sreedevi N
HOD of Department of Computer Science
MVJ College of Engineering
Bangalore, India

Abstract—**A mobile ad hoc network is a self-configuring infrastructure-less network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger internet. In this paper, we have done a survey on MANETS, security issues in mobile ad hoc networks, IDS'S in MANET, Security solutions for MANETS.**

Keywords-MANET

I. INTRODUCTION

Ad hoc network are the temporary network. Ad hoc network short-range network and they are created when device uses the same protocol. Ad-hoc network does not need any subscription service. With the help of ad-hoc network it reduces the cost and improves the security. An ad hoc network is a local area network where messages flow from one node to another node instead of relying on a base station. Ad hoc networks give the ability to wireless devices to communicate with each other in local area network. Ad hoc networks decreased the dependence in infrastructure and increase the speed of deployment. Since nodes are not bound to any centralized control they are free to move about arbitrarily and hence the topology changes. Due to the noise, capacity of each link can vary. Ad hoc network nodes rely on batteries or some other exhaustive mean energy. For lean power consumption we tend to design these protocols .

MANET stands for Mobile Ad hoc network. Mobile ad hoc network is a self-organized network of mobile nodes, without base station support. In this the mobile nodes communicate with each other with the help of a shared wireless channel. The most significant characters of MANET are mobility. This means that nodes can join or leave the network in MANET dynamically. This leads to rapid change in topology. In order to keep the routing information available, all the nodes need to know the topological changes occurring anywhere in the network. When regular updates occur related to topology then the traffic of the network is rises.

MANET is a peer-to-peer network, which allows live communication between any two nodes, only if both nodes are within their radio range. Unfortunately, in large cases not all the nodes of network are in the radio range of each other to communicate directly i.e. not within one hop. So we can use multi-hop topology. These nodes are called Intermediate nodes through which the message is being sent by source relayed node to the destination node. A MANET is a decentralized system. A decentralized wireless system consists of free nodes. It is sometimes called mobile mesh network and is a self-configurable wireless network.

MANET consists of mobile nodes and a router. A router connects to multiple hosts and wireless communication devices. These wireless communication devices are transmitter or receivers. Receiver and transmitters will have smart antennas of various kinds and nodes (transmitter/receiver) can be fixed or mobile. In real life these node referred to those devices which are free to move in any direction such as a mobile phone, laptop, personal computer etc. All the nodes are also located in cars, airplanes or with people having small electronic devices etc. These nodes can connect each other randomly and forms topologies. These nodes communicate to each other and send packets to neighbour nodes as a router. Ability of self-configuration of these nodes makes them more suitable for instant network connection.

II. SECURITY ISSUES IN MOBILE ADHOC NETWORKS

In recent years, the explosive growth of mobile computing devices, which mainly include laptops, personal digital assistants (PDAs) and handheld digital devices, has impelled a revolutionary change in the computing world: computing will not merely rely on the capability provided by the personal computers, and the concept of ubiquitous computing emerges and becomes one of the research hotspots in the computer science society [1]. In the ubiquitous computing environment, individual users utilize, at the same time, several electronic platforms through which they can access all the required information whenever and wherever they may be [2]. The nature of the ubiquitous computing has made it necessary to adopt wireless network as the interconnection method: it is not possible for the ubiquitous devices to get wired network link whenever and wherever they need to connect with other ubiquitous devices. The Mobile Ad Hoc Network is one of the wireless networks that have attracted most concentrations from many researchers.

A Mobile Ad hoc network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension [3]. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas

nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication to automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network. The mobile ad hoc network has the following typical features

- 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.

- Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes.

- Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc 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 features listed above, the mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks. Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks.

III.TYPES OF ATTACKS IN MANETS

There are numerous kinds of attacks in the mobile ad hoc network, almost all of which can be classified as the following two types .

(i). External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services.

(ii). Internal attacks, in which the adversary wants to gain the normal access to the networkand participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

In the two categories shown above, external attacks are similar to the normal attacks in the traditional wired networks in that the adversary is in the proximity but not a trusted node in the network, therefore, this type of attack can be prevented and detected by the security methods such as membership authentication or firewall, which are relatively conventional security solutions. However, due to the pervasive communication nature and open network media in the mobile ad hoc network, internal attacks are far more dangerous than the internal attacks: because the compromised nodes are originally the benign users of the ad hoc network, they can easily pass the authentication and get protection from the security mechanisms. As a result, the adversaries can make use of them to gain normal access to the services that should only be available to the authorized users in the network, and they can use the legal identity provided by the compromised nodes to conceal their malicious behaviors. Therefore, we should pay more attention to the internal attacks initiated by the malicious insiders when we consider the security issues in the mobile ad hoc network.

III. SECURITY SOLUTIONS FOR MANETS

A) *Security criteria:*

i) Availability: The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it [4]. This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service [5].

ii). Integrity : Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways

- Malicious altering
- Accidental altering

iii) Confidentiality : Confidentiality means that certain information is only accessible to those who have been authorized to access it. In other words, in order to maintain the confidentiality of some confidential information, we need to keep them secret from all entities that do not have the privilege to access them.

iv) Authenticity: Authenticity is essentially assurance that participants in communication are genuine and not impersonators [4]. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is not such an authentication mechanism, the adversary could impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal network operations.

v) Nonrepudiation: Nonrepudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message. This is useful especially when we need to discriminate if a node with some abnormal behavior is compromised or not: if a node recognizes that the message it has received is erroneous, it can then use the incorrect message as an evidence to notify other nodes that the node sending out the improper message should have been compromised.

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.

IV. INTRUSION DETECTION SYSTEM FOR MANETS

Due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, an IDS should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at the first time. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches .

V.CONCLUSION

In this paper, survey on MANETS, Security issues in mobile ad hoc networks, security solutions for MANETS, IDS for mobile ad hoc networks is done.

REFERENCES

[1] Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.

[2]Amitabh Mishra 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.