Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.417 – 424

RESEARCH ARTICLE

SECURITY ISSUES: THE BIG CHALLENGE IN MANET

Sneha U. Agalawe[1], Nitin R.Chopde[2]

[1]Department of Computer Science & Amravati University, India

[2]Department of Computer Science & Amravati universities, India

[1] sneha.agalawe@gmail.com; [2] nitin.chopde@raisoni.net

Abstract*— In recent years Mobile ad-hoc network (MANET) is one of the most promising fields for research and development of wireless network. As the popularity of mobile device and wireless networks significantly increased over the past years, wireless ad-hoc networks has now become one of the most vibrant and active field of communication and networks. Due to severe challenges, the special features of MANET bring this technology great opportunistic together. Owe to the vulnerable nature of the mobile ad hoc network, there are numerous security threats that disturb the development of it. We first analyze the main vulnerabilities in the mobile ad hoc. In this paper, we discuss security issues and their current solutions in the mobile ad hoc network. Networks, which have made it much easier to suffer from attacks than the traditional wired network. Then we discuss the security criteria of the mobile ad hoc network and present the main attack types that exist in it. Finally we survey the current security solutions for the mobile ad hoc network. Owe to the vulnerable nature of the mobile ad hoc network, there are numerous security threats that disturb the development of it. We first analyse the main vulnerabilities in the mobile ad hoc. In this paper, we discuss security issues and their current solutions in the mobile ad hoc network. Networks, which have made it much easier to suffer from attacks than the traditional wired network. Then we discuss the security criteria of the mobile ad hoc network and present the main attack types that exist in it. Finally we survey the current security solutions for the mobile ad hoc network.

***Keywords*— Mobile Ad Hoc Network; Security; IDS; Secure Routing; Authentication**

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) has become one of the most prevalent areas of research in the recent years because of the challenges it pose to the related protocols. MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an infrastructure less network. The proliferation of cheaper, small and more powerful devices make MANET a fastest growing network. An ad-hoc network is self-organizing and adaptive. Device in mobile ad hoc network should be able to detect the presence of other devices and perform necessary set up to facilitate communication and sharing of data and service. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. Due to nodal mobility, the network topology may change rapidly and unpredictably over time. The network is decentralized, where network organization and message delivery must be executed by the nodes themselves.. The set of

applications for MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. MANET is more vulnerable than wired network due to mobile nodes, threats from compromised nodes inside the network, limited physical security, dynamic topology, scalability and lack of centralized management. Because of these vulnerabilities, MANET is more prone to malicious attacks.

II. **MANET VULNERABILITIES**

Vulnerability is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows

A. Lack of centralized management

MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad-hoc network. Lack of centralized management will impede trust management for nodes.

B. Resource availability

Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.

C. Scalability

Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

D. Cooperativeness

Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.

E. Dynamic topology

Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.

F. Limited power supply

The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply.

G. Bandwidth constraint

Variable low capacity links exists as compared to wireless network which are more susceptible to external noise, interference and signal attenuation effects.

H. Adversary inside the Network

The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behavior of the node is malicious. Thus this attack is more dangerous than the external attack. These nodes are called compromised nodes.

I. No predefined Boundary

In mobile ad- hoc networks we cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network. As soon as an adversary comes in the radio range of a node it will be able to communicate with that node.

III. SECURITY GOALS IN MANET

We have discussed several vulnerabilities that potentially make the mobile ad hoc networks insecure in the previous section. However, it is far from our ultimate goal to secure the mobile ad hoc network if we merely know the existing vulnerabilities in it. As a result, we need to find some security solutions to the mobile ad hoc network [1]. In this section, we survey some security schemes that can be useful to protect the mobile ad hoc network from malicious behaviors. 3.1. Security Criteria Before we survey the solutions that can help secure the mobile ad hoc network, we think it necessary to find out how we can judge if a mobile ad hoc network is secure or not, or in other words, what should be covered in the security criteria for the mobile ad hoc network when we want to inspect the security state of the mobile ad hoc network. In the following, we briefly introduce the widely-used criteria to evaluate if the mobile ad hoc network is secure.

A. 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 [1]. This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack arget and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service.

B. Integrity

Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways 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[1], 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.

C. 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.

D. Authenticity

Authenticity is essentially assurance that participants in communication are genuine and not impersonators. 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[1]. 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.

E. Non repudiation

Non repudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message[2]. 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 rodeos, 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.

F. 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[2]. 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.

G. 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 [2]. 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. ATTACKS IN MANET

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

- External Attack: External attacks are carried out by nodes that do not belong to the network. It causes congestion sends false routing information or causes unavailability of services.
- Internal Attack: Internal attacks are from compromised nodes that are part of the network[3]. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyze traffic between other nodes and may participate in other network activities.

A. Denial of Service attack

This attack aims to attack the availability of a node or the entire network[3]. If the attack is successful the services will not be available. The attacker generally uses radio signal jamming and the battery exhaustion method.

B. Impersonation

Impersonation attack is a severe threat to the security of mobile ad hoc network. As we can see, if there is not such a proper authentication mechanism among the nodes, the adversary can capture some nodes in the network and make them look like benign nodes [3]. In this way, the compromised nodes can join the network as the normal nodes and begin to conduct the malicious behaviors such as propagate fake routing information and gain inappropriate priority to access some confidential information.

C. Eavesdropping

Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. The goal of eavesdropping is to obtain some confidential information that should be kept secret during the communication [3]. 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.

D. Routing Attacks

The malicious node makes routing services a target because it's an important service in MANETs. There are two flavors to this routing attack. One is attack on routing protocol and another is attack on packet forwarding or delivery mechanism. The first is aimed at blocking the propagation of routing information to a node. The latter is aimed at disturbing the packet delivery against a predefined path.

E. Black hole Attack

In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

F. Wormhole Attack

In a wormhole attack, an attacker receives packets at one point in the network, tunnel them to another point in the network, and then replays them into the network from that point[3]. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole.

G. Replay Attack

An attacker that performs a replay attack are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously[3]. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

H. Jamming

In jamming, attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered.

I. Man- in- the- middle attack

An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender[4].

J. Gray-hole attack

This attack is also known as routing misbehaviour attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.

V. MANET CHALLENGES

Regardless of the attractive applications, the features of MANET introduce several challenges that must be studied carefully before a wide commercial deployment can be expected.

A. Routing

Since the topology of the network is constantly changing, the issue of routing packets between any pair of nodes becomes a challenging task. Most protocols should be based on reactive routing instead of proactive[4]. Multi cast routing is another challenge because the multi cast tree is no longer static due to the random movement of nodes within the network. Routes between nodes may potentially contain multiple hops, which is more complex than the single hop communication.

B. Security and Reliability

In addition to the common vulnerabilities of wireless connection, an ad hoc network has its particular security problems due to e.g. nasty neighbor relaying packets. The feature of distributed operation requires different schemes of authentication and key management. Further, wireless link characteristics introduce also reliability problems, because of the limited wireless transmission range, the broadcast nature of the wireless medium (e.g. hidden terminal problem), mobility-induced packet losses, and data transmission errors.

C. Quality of Service (QoS)

Providing different quality of service levels in a constantly changing environment will be a challenge. The inherent stochastic feature of communications quality in a MANET makes it difficult *to* offer fixed guarantees on the services offered to a device. An adaptive QoS must be implemented over the traditional resource reservation to support the multimedia services.

D. Inter-networking

In addition to the communication within an ad hoc network, inter-networking between MANET and fixed networks (mainly IP based) is often expected in many cases[4]. The coexistence of routing protocols in such a mobile device is a challenge for the harmonious mobility management.

E. Power Consumption

For most of the light-weight mobile terminals, the communication-related functions should be optimized for lean power consumption. Conservation of power and power-aware routing must be taken into consideration.

F. Multicast

Multicast is desirable to support multiparty wireless communications. Since the multicast tree is no longer static, the multicast routing protocol must be able to cope with mobility including multicast membership dynamics (leave and join).

G. Location-aided Routing

Location-aided routing uses positioning information to define associated regions so that the routing is spatially oriented and limited. This is analogous to associatively-oriented and restricted broadcast in ABR.

VI. SECURITY SCHEMES IN THE MOBILE AD HOC NETWORKS

In the previous subsection, we have introduced several well known attack types and challenges in the mobile ad hoc network. Therefore, it should be an appropriate time now to find some security schemes to deal with these attacks. In this part, we discuss several popular security schemes that aim to handle different kinds of attack listed in the previous subsection.

A. Intrusion Detection Techniques

Intrusion detection is not a new concept in the network research. According to the definition in the *Wikipedia,* an Intrusion Detection System (or IDS) generally detects unwanted manipulations to systems[4]. Although there are some differences between the traditional wired network and the mobile ad hoc network, intrusion detection technique, which is developed first in the wired network and has become a very important security solution for the wired network, has also gained some attentions from the researchers when they explore the security solution for the mobile ad hoc network. In the following, we discuss some typical intrusion detection techniques in the mobile ad hoc networks in details.

1) Intrusion Detection Techniques in MANET: the First Discussion: The first discussion about the intrusion detection techniques in the mobile ad hoc networks was presented in the paper written by Zhang et al. In this paper, a general intrusion detection framework in MANET was proposed, which was distributed and cooperative to meet with the needs of MANET. The proposed architecture of the intrusion detection system is shown below in Figure

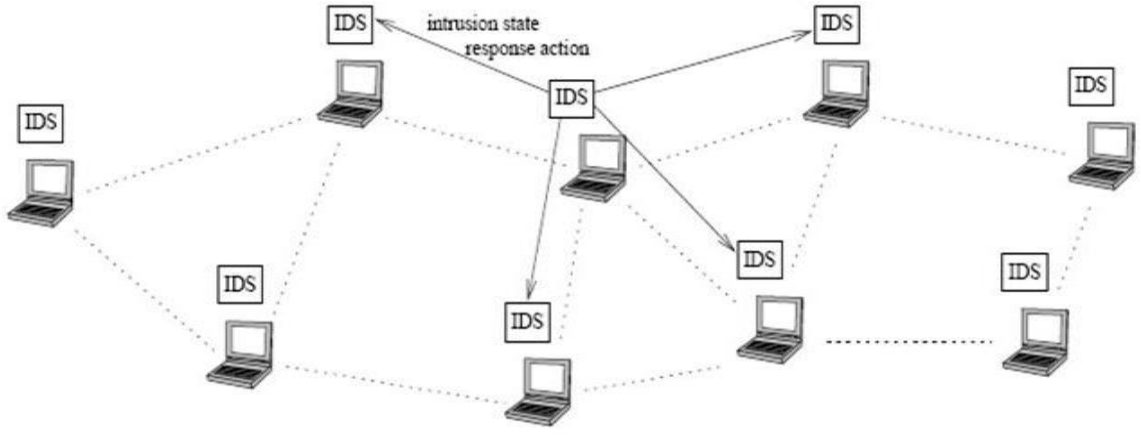

Fig. 1. IDS Architecture

In this architecture, every node in the mobile ad hoc networks participates in the intrusion detection and response activities by detecting signs of intrusion behavior locally and independently, which are performed by the built-in IDS agent. However, the neighboring nodes can share their investigation results with each other and cooperate in a broader range[4]. The cooperation between nodes generally happens when a certain node detects an anomaly but does not have enough evidence to figure out what kind of intrusion it belongs to[5]. In this situation, the node that has detected the anomaly requires other nodes in the communication range to perform searches to their security logs in order to track the possible traces of the intruder.

2) Misbehaviour: Detection through Cross-layer Analysis: Multi-layer intrusion detection technique is another potential research area that Zhang et al. point out in their paper. However, they seem not to explore deeper in this area. In this part, we will discuss the cross-layer analysis method presented by Parker et al. This type of cross-layer attack will be far more threatening than the single-layer attack in that it can be easily skipped by the single-layer misbehaviour detector. Nevertheless, this attack scenario can be detected by a cross-layer misbehaviour detector, in which the inputs from all layers of the network stack are combined and analysed by the cross-layer detector in a comprehensive way[5]. First of all, it will be an important problem that how to make the cross-layer detection more efficient, or in other words, how to cooperate between single-layer detectors to make them work well. Because different single-layer detectors deal with different types of attacks, there can be some different viewpoints to the same attack scenario when it is observed in different layers. Therefore it is necessary to figure out the possible solution if there are different detection results generated by different layers. Second, we need to find out how much the system resource and network overhead will be increased due to the use of cross-layer detector compared with the original single-layer detector[5]. Due to the limited battery power of the nodes in the ad hoc networks, the system and network overhead brought by the cross-layer detection should be taken into account and compared with the performance gain caused by the use of cross-layer detection method.

B. Secure Routing Techniques in Mobile Ad Hoc Network

As we have discussed, there are numerous kinds of attacks against the routing layer in the mobile ad hoc networks, some of which are more sophisticated and harder to detect than others, such as Wormhole attacks and Rush attacks. In this part, we first discuss these two kinds of sophisticated attacks and then we introduce *Watchdog* and *Bathwater*, which are two main components in a system that aims to mitigate the routing misbehaviours in mobile ad hoc networks[6]. Finally we move to a secure ad hoc routing approach using localized self-healing communities.

C. Defence Method Against Wormhole Attacks in Mobile Ad Hoc Networks

Wormhole attack is a threatening attack again routing protocols for the mobile ad hoc networks. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and replays them there into the network.

VI. CONCLUSION

The future of ad- hoc networks is really appealing, giving the vision of anytime, anywhere and cheap communications. Before those imagined scenarios come true, huge amount of work is to be done in both research and implementation. At present, the general trend in MANET is toward mesh architecture and large scale. Improvement in bandwidth and capacity is required, which implies the need for a higher frequency and better spatial spectral reuse. Propagation, spectral reuse, and energy issues support a shift away from a single long wireless link (as in cellular) to a mesh of short links (as in ad- hoc networks). Large scale ad hoc networks are another challenging issue in the near future which can be already foreseen. As the involvement goes on, especially the need of dense deployment such as battlefield and sensor networks, the nodes in ad-hoc networks will be smaller, cheaper, more capable, and come in all forms. In all, although the widespread deployment of ad- hoc networks is still year away, the research in this field will continue being very active and imaginative.

ACKNOWLEDGEMENT

I would like to thank to all people those who have help me to give the knowledge about these research papers and I heartly thankful to my guide with whose guidance I would have completed my research paper and make it to published, finally I like to thank to all the website and IEEE paper which I have gone through and have refer to create my research paper successfully.

REFERENCES

[1] P.Visalakshi , S.Anjugam , " *Security issues and vulnerabilities in Mobile Ad hoc Networks (MANET)-A Survey",* International Journal of Computational Engineering Research (IJCER) ISSN: 2250-3005 National Conference on Architecture, Software system and Green computing

[2] Sakil Ahmad Ansari , Prof. Saoud Sarwar ," *An Analytical Approach for Security Measures Issues in MANET*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, February 2014

[3] Sevil Şen, John A. Clark, Juan E. Tapiador , "*Security Threats in Mobile Ad Hoc Networks*" .

[4] Priyanka Goyal, Vinti Parmar, Rahul Rishi ," MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011 ISSN (Online): 2230-7893

[5] 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.

[6] Reijo M. Savola and HabtamuAbie "On-Line and Off-Line Security Measurement Framework for Mobile Ad Hoc Networks" JOURNAL OF NETWORKS, VOL. 4, NO. 7, SEPTEMBER 2009

[7] 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.

[8] http:www.wikipedia.org/wiki/Mobile_ad_hoc_network

[9] http://pioneerjournal.in/conferences/tech-knowledge/12th-national-conference/3630-a-case-study-security-issues-in-mobile-ad-hoc-network.html

[10] www.csee.umbc.edu/~wenjia1/699_report.pdf

