Mobile Ad-Hoc Network (MANET): Security Issues Regarding Attacks

Nikhil Shukla
Deptt. Of Computer Science,
Vsgoi,Unnao.

Shalini Gupta
Deptt. Of Computer Science
Vsgoi,Unnao.

Amit Virmani
Deptt. Of Computer Science
U.I.E.T.Kanpur.

ABSTRACT

In this paper, we discuss the mobile ad hoc Network:Security issues regarding attacks. Owe to the vulnerable nature of the mobile ad hoc network, there are numerous security threats that disturb the development of it.In the history of communication, the present time period has advent the mobile computing which has changed our information society. Applications of ad-hoc network have a wide range of applications such as in military operations, emergency disaster relief and many other several commercial based works (community networking, interaction between attendees at a meeting or students during a lecture).we survey the current security solutions for the mobile ad hoc network.

Keywords

Mobile Ad Hoc Network, Security, Intrusion Detection, Secure Routing

1. INTRODUCTION:-

The applications and services run by mobile devices such as network connections and corresponding data services are the most demanding [1].The connections among the wireless devices are achieved via fixed infrastructure-based service provider, or private networks. For example, two cell phones are connected by BSC (Base Station Controller) and MSC (Mobile Switching Center) in cellular networks. When we talk about laptops these are connected to Internet via wireless access points. On the other hand infrastructure-based networks provide a great way for mobile devices to get network services; it takes time and sometime potentially high charges to set up the required infrastructure[3]. But except all this there are, some situations where network connections are not available in a given geographic area. So without any physical connection set up providing the needed connectivity and network services in these situations become a real challenge. For all the above reasons, we make advancement in technology and standardization, new alternative approach in mobile connectivity. These are dependent on the mobile devices which are also called nodes, connected to each other in the communication range by any automatic relationship. So setting up an ad-hoc mobile network is flexible as well as powerful.

There are two different types of wireless networks; the easiest network topology is, where each node is able to reach all the other nodes with a traditional radio relay system with a big range. There is no use of routing protocols with this kind of network because all nodes "can see" the others. The second kind uses also the radio relay system but each node has a smaller range, therefore one node has to use neighboring nodes to reach another node that is not within its transmission range. Then, the intermediate nodes are the routers.

2. Characteristics, Complexities and Design Constraints:-

Mobile ad-hoc networks eliminate the constraint of infrastructure set up and enable devices to create and join networks on the fly, anywhere, any time and virtually for any application. Mobile ad-hoc networks inherit the common problems of wireless networking in general, and add their own constraints specific to ad-hoc routing. Some of the notable characteristics, complexities and design constraints of MANETs are presented below:

2.1. Wireless medium: In an ad-hoc environment, nodes communicate wirelessly and share the same media (radio, infrared etc.). The wireless medium has neither absolute, nor readily observable boundaries outside of which the stations are unable to receive network frames. Thus the channel is unprotected from outside signals and hence it is significantly less reliable than wired media.

2.2 Autonomous and infrastructure less: MANET does not depend on any established infrastructure or centralized administration. Each node operates in distributed peer-to-peer mode, acts as an independent router and generates independent data. Network management has to be distributed across different nodes, which brings added difficulty in fault detection and management.

2.3. Dynamic and changing network topology: In mobile ad-hoc networks, because nodes can move arbitrarily, the network topology, which is typically multi-hop, can change frequently and unpredictably, resulting in route changes, frequent network partitions, and possibly packet losses**.**

2.4 Limited availability of resources: Because batteries carried by each mobile node have limited power supply, processing power is limited, which in turn limits services and applications that can be supported by each node. This becomes a bigger issue in MANET because; since each node is acting as both an end system and a router at the same time, additional energy is required to forward packets.

All the above discussed unique characteristics of ad-hoc networks present many research areas related to security, such as, key management models, secure routing protocols, instruction detection systems and trust based models. This thesis work is based on the research done in the area of secure structured model.In our thesis work we will use the term attacks and threats interchangeable.

3. SECURITY ISSUES OF EXISTING ROUTING PROTOCOLS:-

Any routing protocol must encapsulate an essential set of security mechanisms. These are mechanisms that help prevent, detect, and respond to security attacks. There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. They are mainly:

3.1. Confidentiality

Protection of any information from being exposed to unintended entities. In ad-hoc networks this is more difficult to achieve because intermediates nodes (that act as routers) receive the packets for other recipients, so they can easily eavesdrop the information being routed.

3.2. Availability

Services should be available whenever required. There should be an assurance of survivability despite a Denial of Service (DOS) attack. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g. key management service.

3.3. Authentication

Assurance that an entity of concern or the origin of a communication is what it claims to be or from. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

3.4. Integrity

Message being transmitted is never altered[2].

3.5. Non-repudiation

Ensures that sending and receiving parties can never deny ever sending or receiving the message.

Broadly there are two major categories of attacks when considering any network Attacks from external sources and attacks from within the network. The second attack is more severe and detection and correction is difficult. Routing protocol should be able to secure themselves against both of these attacks. Ad-hoc network have wide range of research issues among which security is particularly more challenging and important due to the unique topology and lack of infrastructure support. Till now many security mechanisms has been developed and proposed, but still it is difficult to ensure that whole network is free from any malicious attack.

In our work we have concentrated on the security issues associated with the existing attacks. In this thesis work first we discuss about existing attacker approaches and their attacking methods. Then here will be the new approach, developed with the potential based method of attackers. Also propose an approach in which all attacking potential will be incorporated. This approach will be based on the message-passing & functionality of attacks. The new proposed work represents a technique by which the group of attacks can be dissolved easily.

Wireless mobile ad-hoc nature of MANET brings new security challenges to network design. Mobile ad-hoc networks, due to their unique characteristics, are generally more vulnerable to information and physical security threats than wired networks or infrastructure-based wireless networks.

4. ANALYSIS OF SECURITY ATTACK

Security is an essential service for wired and wireless network communications. The success of mobile ad-hoc networks (MANET) strongly depends on people's confidence in its security. However, the characteristics of MANET pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and non-repudiation. First, we give an overview of attacks according to the protocols stacks, and to security attributes and mechanisms. We present a different Types of Attacks Faced by Routing Protocols. Then we present preventive approaches following the order of the layered protocol stacks. We also put forward an overview of MANET intrusion detection systems (IDS).

There are a wide variety of attacks that target the weakness of MANET. For example, routing messages are an essential component of mobile network communications, as each packet needs to be passed quickly through intermediate nodes, which the packet must traverse from a source to the destination. Malicious routing attacks can target the routing discovery or maintenance [8] phase by not following the specifications of the routing protocols. There are also attacks that target some particular routing protocols, such as DSR, or AODV. Currently routing security is one of the hottest research areas in MANET.

4.1. Security attacks

The attacks in MANET can roughly be classified into two major categories, namely passive attacks and active attacks. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET. Examples of passive attacks are eavesdropping, traffic analysis and traffic monitoring[4]. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay.

The attacks can also be classified into two categories, namely external attacks and internal attacks, according the domain of the attacks. External attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows valuable and secret information, and possesses privileged access rights.

4.2 Types of Attacks Faced by Routing Protocols

Due to their underlined architecture, ad-hoc networks are more easily attacked than a wired network. The attacks prevalent on ad-hoc routing protocols can be broadly classified into passive and active attacks.

A Passive Attack does not disrupt the operation of the protocol, but tries to discover valuable information by

listening to traffic. Passive attacks basically involve obtaining vital routing information by sniffing about the network[7]. Such attacks are usually difficult to detect and hence, defending against such attacks is complicated. Even if it is not possible to identify the exact location of a node, one may be able to discover information about the network topology, using these attacks.

An Active Attack, however, injects arbitrary packets and tries to disrupt the operation of the protocol in order to limit availability, gain authentication, or attract packets destined to other nodes. The goal is basically to attract all packets to the attacker for analysis or to disable the network. Such attacks can be detected and the nodes can be identified.

5. ATTACKS USING DIFFERRENT CLASIFICATIONS:-

On the basis on network protocol stack, attacks can be classified into following categories (below is a classification of security attacks based on protocol stack; some attacks could be launched at multiple layers):

- Application layer :Repudiation, Data Corruption Attacks
- Transport layer :Session Hijacking, SYN Flooding Attacks
- Network layer:Wormhole, Blackhole, Byzantine, Flooding Attacks
- Data link layer :Resource Consumption, Location Disclosure Attacks
- Physical layer:Traffic Analysis, Monitoring, Disruption MAC (802.11)
- Multi-layer attacks :WEP - Weakness Attacks

6. Conclusion

In this survey paper, we try to inspect the security issues in the mobile ad hoc networks,

which may be a main disturbance to the operation of it[6]. Due to the mobility and open media nature, the mobile ad hoc networks are much more prone to all kind of security risks, such as information disclosure, intrusion, or even denial of service. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wired networks.First we briefly introduce the basic characteristics of the mobile ad hoc network. Because of the emergence of the concept pervasive computing, there is an increasing need for the network users to get connection with the world anytime at anywhere, which inspires the emergence of the mobile ad hoc network. However, with the convenience that the mobile adhoc networks have brought to us, there are also increasing security threats for the mobile adhoc network, which need to gain enough attention.Finally we introduce the current security solutions for the mobile ad hoc networks. We start with the discussion on the security criteria in mobile ad hoc network, which acts as a guidance to the security-related research works in this area. Then we talk about the main attack types that threaten the current mobile ad hoc networks. In the end, we discuss several security techniques that can help protect the mobile ad hoc networks from external and internal security threats.

During the survey, we also find some points that can be further explored in the future, such as some aspects of the intrusion detection techniques can get further improved. We will try to explore deeper in this research area.

7. REFERENCES

[1]M. G. Zapata and n. Asokan. Securing ad-hoc routing protocols. In *wise '02: proceedings of the acm workshop on wireless security*, pages 1–10, new york, ny, usa, 2002. Acm press.93

[2]Wenbo He, Achieving privacy and integrity of data aggregation in Wireless sensor networks, University of Illinois at Urbana-Champaign, 2008.

[3]wikipedia.org/wiki/Mobile_adhoc_networ.

[4]Ramachandran and A. Yasinsac. Limitations of On Demand Secure Routing Protocols. Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC, 2004

[5]M. Burrows, M. Abadi, and R. Needham. A Logic of Authentication. ACM Transactions on Computer Systems, 1990.

[6].Security Issues in Mobile Ad Hoc Networks-A Survey Wenjia Li and Anupam Joshi Department of Computer Science and Electrical Engineering University of Maryland, Baltimore County

[7]P. Papadimitriou and Z. Haas. Secure Routing for Mobile Ad-hoc Networks. In Proceedings of SCS communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), 2002.

[8]Yih-Chun Hu Adrian Perrig, Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, 2003 IEEE.