ISSN 2522-6398 Vol. 3, Issue 1: 104-107, DOI: 10.25236/FER.2020.030115

Security Analysis and Strategy of Ad Hoc Network in Mobile Education Network

Cao Guihong

Hunan Institute of Engineering, Hunan 411101, China

ABSTRACT. *Ad Hoc network is composed of a group of mobile terminals with wireless transceivers. The mobile terminal has a routing function and can form an arbitrary network topology through wireless connection technology, so that timely communication can be performed in scenarios without fixed technical warfare. This paper first briefly describes the characteristics of the Ad Hoc network, then analyzes the security of the Ad Hoc network from the perspectives of usability, confidentiality, integrity, security authentication, and non-repudiation, and finally proposes a security strategy for the Ad Hoc network.*

KEYWORDS: *Ad hoc network; Network security; Security strategy*

1. Introduction

Ad Hoc networks are generally called MANET (Mobie Ad Hoc Networks) internationally. Initially, the Ad Hoc network was applied in the military field. Nowadays, Ad Hoc network is expanding from the military field to the civil field, such as earthquake rescue, fire rescue, forest communication, security communication, etc.. Ad Hoc network has several obvious characteristics: (1) independence, Ad Hoc wireless network does not need the support of hardware infrastructure network facilities at any time and anywhere[1]; (2) flexible, Ad Hoc network has flexibility. It can work independently, and it is already connected to the wireless network and the Internet; (3) there is no center, there is no central node in the Ad Hoc network, and the nodes are connected in a peer-to-peer manner. The network uses an authentication process to verify the identity of the newly joined node[2]; (4) self-organization, all nodes of the Ad Hoc network form a self-organized network through a distributed algorithm; (5) multi-hop, nodes in Ad Hoc networks usually communicate with nodes that are farther away through forwarding by intermediate nodes; (6) dynamic topology, nodes in the Ad Hoc network can move at any speed and pattern. In addition, the network path formed by the wireless network between nodes will also change at any time; (7) low security, compared with wireless networks and Internet networks, Ad Hoc networks have low security. Only one node is intercepted by criminals, and the entire network is easy to crack.

2. Ad Hoc Network Security Analysis

Security is critical for Ad Hoc networks. Compared with other networks, Ad Hoc is more vulnerable to security threats such as eavesdropping, spoofing and denial of service. The following is an analysis of Ad Hoc network security from the perspectives of availability, confidentiality, integrity, security authentication and anti-repudiation.

In terms of usability, Ad Hoc network has few "constraints" on nodes due to its features of centrless and dynamic topology. Because of this, when Ad Hoc network is attacked by security, the nodes can still provide effective services. An intruder can attack any level in Ad Hoc network, either the physical layer or the data link layer. Take data link layer intrusion as an example.   Because Ad Hoc topology changes frequently, it does not use the routing protocols in the traditional Internet network, but uses DSDV, WRP, AODV, DSR, LMR and other routing protocols. Intruders can make Ad Hoc networks unavailable or services unavailable by disrupting these routing protocols. In addition, because Ad Hoc network topology changes frequently, once there are dangerous channels between nodes, it will inevitably threaten the security of the network.

In terms of confidentiality, Ad Hoc networks, like other networks, also need to ensure that specific information is not leaked to unauthorized users. With the widespread popularity of online payment today, confidentiality is an important requirement for Ad Hoc network security. In the Ad Hoc network, the user's various private information must be transmitted to ensure that the information is not stolen. In addition, because the topology of the Ad Hoc network changes frequently, it is necessary to pay great attention to the security of routing protocols, and in some cases, to ensure the confidentiality of routing information. Similar to other networks, we can use encryption algorithms to provide the confidentiality of Ad Hoc networks.

Integrity includes two contents: one is data integrity, which refers to data changes in the Ad Hoc network that require specific changes and authorization methods, that is, the network needs to ensure that the information is not maliciously tampered with during the transmission of information (rewrite, rewrite, Reordering, etc.) or replication, and the second is the integrity of the system, which means that the Ad Hoc network prevents unauthorized manipulation. Integrity ensures that messages are sent and received consistently.

In terms of security authentication, each node in the Ad Hoc network not only needs to be able to confirm the identity of the node communicating with it, but also needs to be able to authenticate users who use the network without a global certification authority. Security authentication is very important for Ad Hoc networks. Ad Hoc has a non-central feature. Without security authentication, an intruder can easily capture a node in the network, and then use this as a breach to obtain the private information of authorized users in the network. Because Ad Hoc networks do not have a fixed management domain, it is difficult to use firewall technology for security authentication.

In terms of non-repudiation, in the Ad Hoc network, the sender of the information cannot deny the information it sends. Similarly, the recipient of the message cannot deny the information that has been received. In layman's terms, non-repudiation means “cannot be denied”. According to non-repudiation, when a message is sent, the receiver of the message can prove that the sender sent the message. Similarly, after the message is received, the sender of the message can prove that the receiver has received the message. In Ad Hoc networks, the non-repudiation of information is usually realized by some encryption algorithm.

3. Ad Hoc Network Security Strategy

According to the security characteristics of Ad Hoc network, the following security strategys are proposed.

3.1 Access Control

Setting up key distribution and authentication is a necessary means for Ad Hoc network access control. It can ensure at the application layer of the Ad Hoc network that legitimate users have access to the service and deny unauthorized access (intruders) to access the service. In some systems, although keys and authentication are not required, nodes in the network access the service through related security certificates. In practical applications, there are some differences in the implementation of access control according to different network structures and security levels of Ad Hoc networks. At present, common access control strategies in Ad Hoc networks include cluster-based access control, network resource classification-based access control, and reputation-based media access control.

3.2 Strengthening the Security of Routing Protocols

Due to the lack of defense procedures in the internal topology of the Ad Hoc network, it is vulnerable to security attacks, especially attacks from routing protocols[3]. Therefore, we need to further strengthen the security of common routing protocols in Ad Hoc networks. Take the AODV routing protocol as an example. This protocol is the most widely used routing protocol in Ad Hoc networks. Take the AODV routing protocol as an example. This protocol is the most widely used routing protocol in Ad Hoc networks. However, AODV routing protocols are also vulnerable to attacks, especially black hole attacks. There are many ways to strengthen the security of AODV routing protocols. For example, we can judge whether a node is a malicious node by comparing the trust value of the node in the Ad Hoc network. The specific principle is that if the responding intermediate node A is a malicious node, its next hop (destination) node B cannot receive data. This method can detect malicious nodes and effectively avoid black hole attacks. However, this method is time consuming in some large networks. In this regard, after the source node Y receives the data packet from A, we randomly select a node C between A and B, and then send a verification data packet to C, and at the same time send a data packet to B along this route. After receiving the data packet sent by Y, C sends a reply verification packet to Y. If Y continues to send data to B after receiving the verification packet of C, if it does not receive the verification packet of C within the specified time, it stops sending data to B. package. At the same time, Y issues a warning to the entire network, and then isolates C and abandons the route.

3.3 Optimize Network Intrusion Detection Algorithms

Based on the low security of Ad Hoc networks, researchers have proposed a chaotic immune clustering algorithm, which provides an effective means for Ad Hoc networks with detection and intrusion functions. Chaos immune clustering algorithm is a fusion of chaos optimization algorithm and immune clustering algorithm. This algorithm has the advantages of both chaos optimization algorithm and immune clustering algorithm. It has fast convergence speed and strong search ability. Features. Therefore, this algorithm can be embedded in the Ad Hoc network, and an Ad Hoc network with the function of detecting and removing intruders can be designed.

Acknowledgement

This project is a general youth project of Hunan University of Technology in 2015. The project number is xj1515. The project name is Ad Hoc Network Routing Security Protocol Research and Simulation.

References

[1] Xu Guiyue, Zhang Changjian, Gong Haimei (2019). Security strategy of wormhole attack in ad hoc wireless network. Electronic technology and software engineering, no.3, pp.169-170.

[2] Wang Haitao, Song Lihua, Zhang pengliang (2018). Security mechanism of wireless ad hoc network. Confidential science and technology, no.6, pp.27-31

[3] Sun Lvye, Jia Xiaozhu, Lai Wenjuan (2017). Research on AODV based secure routing protocol in ad hoc network. Journal of Qingdao University (NATURAL SCIENCE EDITION), vol.30, no.2, pp.74-76