Research on Wireless-Based Intrusion Detection in Mesh Network Security System

Kaifeng Wen

(School of Computer Science, Jiaying University, Meizhou 514015, China)

wenkaifeng2000@126.com

Keywords: MESH; intrusion detection; delay; characteristics

Abstract. There are many issues concerning security in existing MESH network. In response to this phenomenon, this paper presents a research on wireless-based intrusion detection in mesh network security system. By combining the characteristics of intrusion detection, it rearranged the system architecture and algorithms. In order to test the feasibility of this system, we used the error rate and delay to test it. Experimental results showed that this system is able to keep accurate data, and reduce delays at the same time.

Introduction

As the computer network technology continues to raise, the network security issues cannot be ignored now. Due to the special nature of the network caused by Mesh network vulnerable to malicious intrusion, routing attacks, and is denial of service [1-3]. Due to hacking and viruses, huge economic losses have been caused. Therefore, how to establish a secure network system attracts much attention. Intrusion Detection System is an initiative to protect themselves from attacks of a network security system. It can help the system to deal with cyber-attacks, expand security management capabilities, and improve the integrity of the information security.

Mesh network

Wireless Mesh Network is a self-organizing, multi-hop network. It is different from traditional wireless local area network, and also different from the mobile ad-hoc network[4-5]. It can be seen as an organic fusion of the WLAN and Ad-Hoc.

For a better description, we are comparing traditional wireless LAN, which is shown in Tab 1.

Tab 1. WLAN and MESH comparison table

	WLAN	MESH
Coverage area	250m	300m-3km
Mobility	Less than 50km/h	50km/h-350km/h
Network Performance	Have blind spots, long delays	No blind spot, a small delay

Wireless Mesh network architecture determines its inherent fragility and vulnerability [6].

a. Radio channel of insecurity. Compared with the wired network, wireless network has the nature of its scope, so that people can attack from any node. It can be destroying communication link, intercepted, and tampered with the message, even posing as legitimate users. Mesh network is more vulnerable to attack, and to protection problems.
b. Security threats of network structure. The principle of equality of wireless Mesh network makes the network not the central point, which is difficult to centralize network management and control. In this case, once a node is attacked, it will pose a threat to the entire network.
c. The threat of mistrust between nodes brought. Mesh network communication needs multi-hop to complete, so this requires synergistic node to complete a communication. If a malicious node invades, it will cause the entire network performance degradation and even denial of service.
d. Attacks for the routing. Multi-hop routing mechanism increases the coverage of Mesh network, but also provides a convenient attacker. If a node is compromised, the attacker could be mistakenly guided by modifying the routing information network transmission point. In this case, all nodes are affected, and the network also will be paralyzed.

Intrusion Detection Technology

Intrusion detection refers to the behavior, security logs, audit data or other network information can be obtained to operate, the system detected the intrusion or intrusion attempt[7]. Technically, it can be divided into misused detection and anomaly detection. Mistakenly detection is mainly for known attacks. It extracts the features and elements of attacks, and then follows the matching algorithm to find the attack. Anomaly detection, unlike misuse detection, can be found in an attack by unknown parameters and observed changes in the network node status. It cannot rely on signatures. In practical applications, intrusion detection is often divided into the following three processes: information collection, information analysis and results processing.

a. Collecting information on the network running

Collecting information on the network is the first step of intrusion detection technology, and it is the most critical step. This step is often determined after the results of the validity and reasonableness. The collected information includes network data, the system and network behavior.

b. Analyzing the information collected

The second aspect is use the collected information to conduct a comprehensive analysis which includes statistical analysis, complete analysis, and pattern matching analysis.

c. Real-time recording and corresponding counter-measures

Operation of the network will generate a lot of data, so we should use third step. It is the purpose to achieve this operational information in real-time recording. And it would accord records to determine whether the presence of the phenomenon of the invasion of network activity in the current network environment. And it will take appropriate counter-measures.

d. Processing analysis result

This step is treating the risk factor for the occurrence of or potential. The link is the network intrusion technology to run the last link, and it is a very critical part. Under normal circumstances, the action is divided into termination system or turn off a network connection.

System Framework

According to the main security risks existing in the wireless Mesh network[8], we designed the authentication server, firewall, intrusion detection systems, fault diagnosis and self-healing of the four-part security prevention and control system. It is shown in Fig. 1.

Firewalls are used to isolate the external network and internal network to prevent attacks from the Internet. Authentication service is to identify legitimate users and assign permissions. Intrusion detection systems, through malicious behavior of the attacker, has been successful across the network **boundary** which is detected, preventing the spread of damaging information.

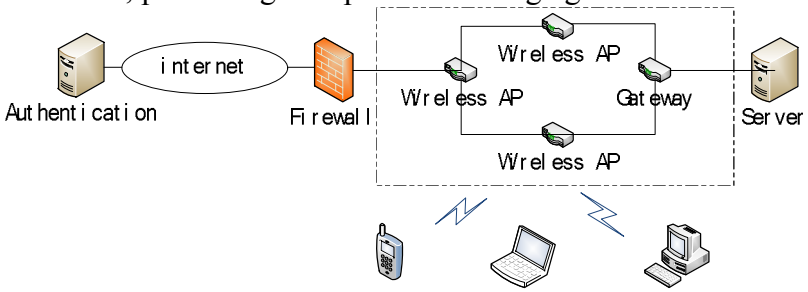

Fig. 1. wireless Mesh network security framework

Intrusion detection process

For the existing security problems, this article introduces intrusion detection process to make necessary adjustments, which is shown below.

First, the normal behavioral characteristics of legitimate users were stored in a database IDS server. And then we used IDS information collection module captures data sent by abnormal. Intrusion

detection and analysis algorithms would be used to deal with the information and behavior of abnormalities. Then anything over baseline behavior would be considered as the invasion, activate response mechanisms, screening information source node.

Second, by establishing and gradually improving the invasion model library, we collected each of the fault code and intrusion model. When the similarity reaches a certain threshold value, the invasion could be determined.

Third, we installed appropriate number of focal point in the network, with real-time monitoring network traffic. If a node frequently issues the invalid packets, it should start early warning program. And listener should handle all aspects of the suspicious nodes.

```
void IntrusionDetection(node, rulerlibrary, modellibrary)
{  while(true)
     {package p;
     int l ;                    // l is the threshold
     p=node.controlInformation;     // Get control information sent by the node
     int tv=compare(p, rulerlibrary)   // Compared with the rule base
     if(tv> l )then
     kill(node);                  // Block this node
     if not(comparewith(p, modellibrary))
     modellibrary+=p; }           // Added model library
}
```

Simulation

In order to verify the feasibility of this, we used the MATLAB 2014a to simulation, and set the simulation time step are 60s. By constructing more than 100 data records, we marked out its normal and abnormal node. And by combining the abnormal rate and false alarm rate, we evaluated this algorithm. Wherein abnormal rate represents the proportion of checked exceptions accounted for the total. False alarm rate represents the proportion of a normal sample which was mistaken as anomalous samples. Its findings are as Tab 2.

Tab 2. Experimental data ratio table

	abnormal rate	false alarm rate
this algorithm	85%	4.30%

Through the above data it can be effectively demonstrated the feasibility of this paper system. For further analysis, we have to test the network communication delay in this system.

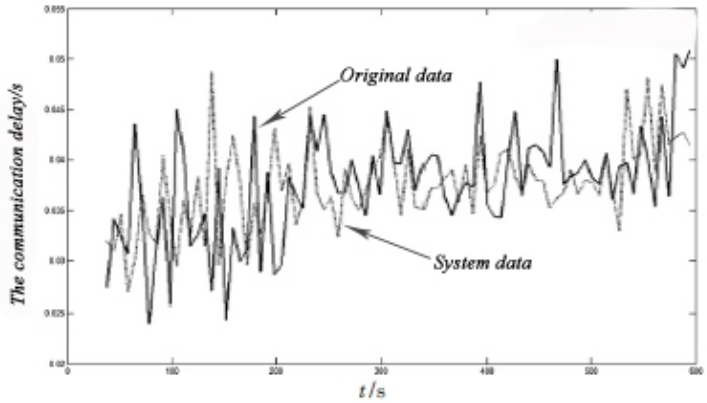

Fig. 2. System delay comparison chart

By observing the above comparison chart, it can be seen that after adding intrusion detection algorithm, the overall communications network latency slightly increased, but the range is not big. It can be effective to reduce the communication delay of original system.

Conclusions

This article presents a research on wireless-based intrusion detection in mesh network security system. The algorithm combining network features MSEH and intrusion detection, and combines with

the existence of security threats MESH. IIt is improve the structure and algorithm in the system. Through experiments, error rate can be controlled at 85%, and the false alarm rate can be controlled at 4.3%. And it can maintain a low latency at the same time.

References

[1]Karri Ganesh Reddy, Thilagam P. Santhi. Reputation-based cross-layer intrusion detection system for wormhole attacks in wireless mesh networks [J]. SECURITY AND COMMUNICATION NETWORKS. 2014,7(12): 2442-2462.
[2] Hassanzadeh Amin, Stoleru Radu, Polychronakis Michalis, etc. RAPID: Traffic-agnostic intrusion detection for resource-constrained wireless mesh networks [J]. COMPUTERS & SECURITY. 2014,46: 1-17
[3]Morais A, Cavalli A. A Distributed and Collaborative Intrusion Detection Architecture for Wireless Mesh Networks [J]. MOBILE NETWORKS & APPLICATIONS. 2014,19(1): 101-120.
[4]Chen J, Du RY Yu FJ, etc. Intrusion Detection Model Based on Incomplete Information Game in Wireless Mesh Networks[J]. CHINA COMMUNICATIONS. 2012,9(10): 23-32.
[5]Xiao Yang, Accountability for wireless LANs ad hoc networks and wireless mesh networks[J]. IEEE COMMUNICATIONS MAGAZINE. 2008,46(4): 116-126.
[6]Yi Ping, Wu Yue, Zou Futai,etc. A Survey on Security in Wireless Mesh Networks[J]. IETE TECHNICAL REVIEW. 2010,27(1): 6-14.
[7]Khan Shafiullah, Loo Kok-Keong, Din Zia Ud. Framework for Intrusion Detection in IEEE 802.11 Wireless Mesh Networks[J]. INTERNATIONAL ARAB JOURNAL OF INFORMATION TECHNOLOGY. 2010,7(4): 435-440.
[8]Deb Novarun, Chakraborty Manali, Chaki, Nabendu. CORIDS: a cluster-oriented reward-based intrusion detection system for wireless mesh networks[J]. SECURITY AND COMMUNICATION NETWORKS. 2014,7(3): 532-543.