Research on the Identity Authentication Mechanism of Computing Node in Medical High Performance Distributed Parallel Computing Model

Yanmei Hu[1, a] and Mu Yang[2, b *]

[1] Chengdu Medical College, Chengdu, Sichuan, 610083, China

[2] Chengdu Medical College, Chengdu, Sichuan, 610083, China

[a]13965808@qq.com, [b]udjtrt@126.com

Keywords: Parallel computing; Identity authentication; 802.1X; Protocol extension

Abstract. This paper analyzes the existing Ethernet authentication technology, build open ring hash table as a data structure for storing user information. Through the efficiency analysis, the simulation and the realization of the system, the validity of the 802.1X protocol extension and the improved parallel computing authentication mechanism is verified. By modifying the authentication mechanism based on port control to user based authentication mechanism, it can effectively solve the problem that the parallel computing node is not fixed to the node in the parallel computing architecture. The method simplifies the structure of the identity authentication in the parallel computing model, improves the accuracy of the authentication, and ensures the safety and stable operation of the parallel computing platform.

Introduction

Parallel computing is relative to the serial computation. It is an algorithm that can execute multiple instructions at one time, the goal is to improve the computing speed, and to solve the problem of large and complex computation by expanding the scale of the problem solving[1]. Parallel computing can be divided into temporal parallelism and spatial parallelism. Parallel in time is the pipeline technique, and the parallel in space is the computation of the execution of the concurrent execution of multiple processors. With the combination of computational science and medicine, many medical research and medical experiments can be carried out by computer simulation. Distributed computing model, to take full advantage of the school of existing computer resources, will all the scattered single computer using distributed calculation principle of connecting the become a high performance parallel computer, provide the necessary hardware support for the teaching and scientific research of the school.

Parallel computing usually adopts multi node parallel computing architecture to improve computing power. Identity authentication among the computing nodes is parallel calculation model is an important part of, and parallel computing is normal operation, between the nodes of the safe and accurate collaborative work is a necessary mechanism and parallel computing whether the normal operation of the key.

Working Principle of Authentication Mechanism in Ethernet

Ethernet technology uses Carrier Sense Multiple Access Collision detect (CSMA/CD) technology, in a shared medium environment, to achieve a higher transmission rate[2]. Due to the high forwarding efficiency and the relatively low price, the switch in Ethernet has become the basic equipment to build the Ethernet. Using the switch, adding to the user's authentication management function, can carry on the identity authentication management from the physical access level to the parallel computing node[3].

There are three commonly used authentication technology: WEB certification, PPPOE certification and 802.1X certification. As far as the Ethernet environment is concerned, it is more suitable to choose 802.1X authentication.

802.1X protocol architecture consists of three parts, they are the client, authentication system and authentication server. Client is a user terminal system, the client is mainly to complete the start of the authentication process, and user input user name and password and authentication system for authentication process information interaction. After the success of the certification, the response to the certification system certification system. Certification system to start the process of certification. After the authentication status information is out of time, the client is re authenticated, relay or Extensible Authentication PPP (Protocol EAP) frame[4]. When the user through the certification, the certification server will notify the certification system, users are already through the authentication, to open the port controlled. Thereafter, the user can normally through the access port authentication system to provide services.

In the 802.1x protocol, client and the authentication system by carrying on the Ethernet protocol EAP protocol (eapol) for communications, authentication system and authentication server between the bearing on the radius protocol EAP protocol for communications. EAP protocol stack is showed as the Fig. 1.

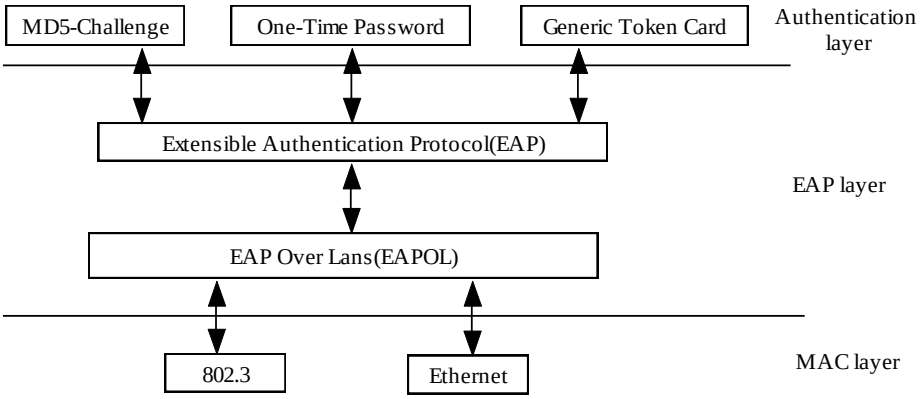

Figure 1. EAP protocol stack

Extended and Improved Parallel Computing Identity Authentication Mechanism Based on 802.1X Protocol

We use the switch to achieve the identity authentication of parallel computing nodes, first of all can be distinguished between the legitimate users and illegal users, the user for effective authentication and management. Increasing the management function of the user should not have too much impact on the exchange efficiency of the switch. So we use 802.1X protocol as the authentication technology of Ethernet switch.In view of the characteristics of parallel computing, we change the port based control in the 802.1X protocol to the user based control[5].

802.11 protocol is mainly to solve the wireless local area network user access authentication problem, after the authentication of the channel port is established, there is no other users to use the problem again. But the 802.1x protocol used in Ethernet and need to certified port can be connected to multiple users, when a user authentication is successful, open ports, there other illegal users can access and freedom to control problems, as shown in Fig. 2.

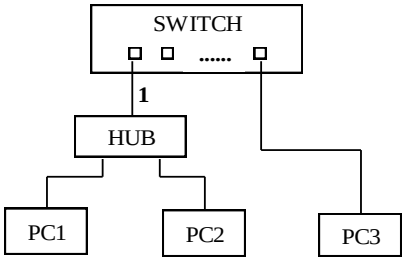

Figure 2. A network connection to a problem

In order to solve this problem, we extend the 802.1X protocol based on port control to user based control. In order to achieve this goal, the switch is often used in the flooding and address learning two functions, to achieve the user's control. We are in the certification switch to start the 802.1X authentication function of the port, the closure of the address learning and flooding function, the user through the authentication, the MAC address and connection of the port directly to the address forwarding table[6]. Only through the authentication of the user's MAC address as the destination address of the packet can be forwarded through the port, so as to achieve the user's control.

Commonly used authentication mechanisms are: static configuration of the way and automatic negotiation[3]. Because the standard 802.1x authentication mechanism is any of a product should be supported by standard authentication mechanisms, such as MD5Challenge and and static configuration compared, automated negotiation does not require authentication before the start of the designated by any authentication mechanism, improve the flexibility of the certification, simplifying the certification before the configuration. Automatic negotiation process of authentication mechanism is shown in Fig. 3.

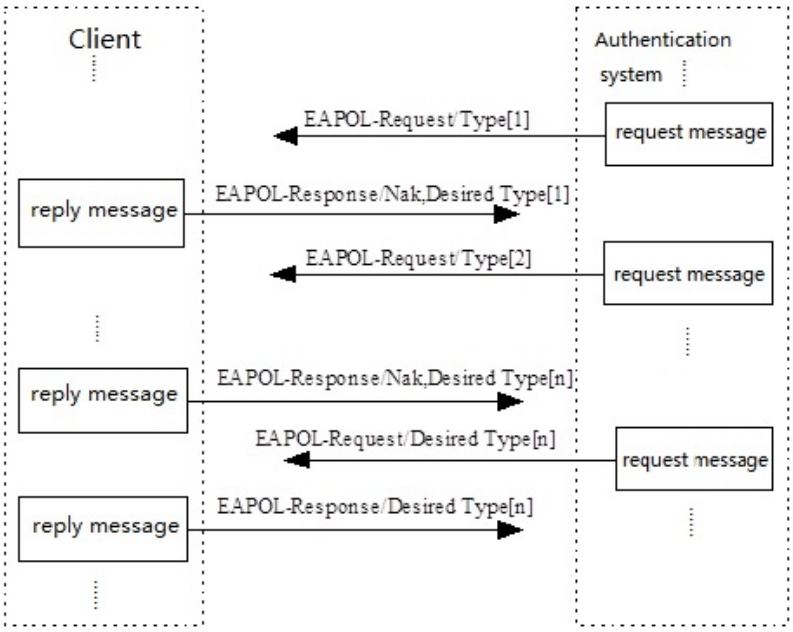

Figure 3. Automatic negotiation process of authentication mechanism

Definition of User Information Data Structure. The 802.1X protocol needs to store a large amount of user information. On the one hand, a single user itself needs to store the user name, MAC address, IP address, state machine control variables, billing control variables, etc.. On the other hand, the practical authentication system needs to support multi user authentication, and how to improve the spatial efficiency of the user information storage will directly affect the normal operation of the identity authentication mechanism in parallel computing model.

When searching the user information, how to improve the efficiency of the search is an important part of parallel computing authentication. Therefore, we use the open-loop hash table as a data structure for storing user information, can make full use of the open ring hash table to improve search efficiency for Mac, single hash chain is variable length, the user data structure of the large redundancy. The authentication data structure not only has high query efficiency, but also has the variability of structure.

Efficiency Analysis of Parallel Computing Authentication Mechanism Based on 802.1X Protocol Extension and Improvement. Usually the MAC address of the user is uniformly distributed, when there are n users, each hash chain is M=N/256 users, each user is searching probability for P=1/N, to MAC address index search users, a single hash chain on the average search length is:

$$ASLi = P1 \times 1 + P2 \times 2 + P3 \times 3 + \cdots + PM \times M \quad (1)$$
$$= \frac{1}{N} \times (1 + 2 + 3 + \cdots + M)$$

i=0,1， 2,3, ……,255

The average search length of the entire hash table is:

$$ASL = ASL0 + ASL1 + ASL2 + \cdots + ASL255 \quad (2)$$
$$= 256 \times \frac{1}{N} \times (1 + 2 + 3 + \cdots + M)$$
$$= 256 \times \frac{1}{N} \times \frac{(M+1) \times M}{2}$$
$$= \frac{N+256}{512}$$

It can be seen that the average search length is only related to the number of users, for a 12 port switch, allowing up to 3500 users on the line, the average search length is 7.3.

Test Environment and Authentication Test

The system by WinDriver company embedded real-time operating system (RTOS), as a separate environment, it with its good reliability and excellent real-time is widely application in the field of communications, military, aviation, aerospace and other sophisticated technology and real-time requirements of high. Tornado[4] is the WindRiver company provides an integrated development environment for program development under the VxWorks system. Support for the development language is C or C++. The device that uses Tornado to develop a program is called a host machine, the device that executes the program is called the target machine, where it is a switch. In order to facilitate the debugging, the debugging information is added in the coding of the 802.1X module, which can track the operation of the state machine.A complete authentication process, print information as shown in Fig. 4.

```
00:05:36: 802.1X: mac is 00 :0c:76:a1:30:c1
00:05:36: 802.1X: dot1x_hash_table_mac_create for mac 0: c:76:a1:30:c1
00:05:36: 802.1X: vlanId = 1
00:05:36: 802.1X: (c1)reAuth_SM enter BEGIN
00:05:36: 802.1X: txReqId:
00:05:36: 802.1X: port9 send EAPOL(len=27 vid=1)
00:05:37: 802.1X: mac is 00 :0c:76:a1:30:c1
00:05:37: 802.1X: port9 rx EAPOL-Packet
00:05:37: 802.1X: (c1)backAuth_SM enter RESPONSE
00:05:37: 802.1X: (c1)backAuth_SM enter SUCCESS
00:05:37: 802.1X: txCannedSuccess:
00:05:37: 802.1X: port9 send EAPOL(len=26 vid=1)
00:05:37: 802.1X: (c1)backAuth_SM enter IDLE
```

Figure 4. Authentication process debugging information

Conclusions

Practice has proved that the commonly used user authentication technology, WEB certification, PPPOE certification and 802.1X certification, each has its advantages and disadvantages, suitable for different application environment. After the improved 802.1X protocol, it can be implemented in the switch, which can achieve the goal of parallel computing node identity authentication management based on the user's control. Based on Ethernet environment of parallel computing in identity authentication of user management, is a personality price good choice, use of open-loop hash table as a data structure for storing user information, the Mac index improves the efficiency of searching, also a single hash chain is variable length, with good variable suitability.

Through experimental verification, the method is feasible. It simplifies the parallel computing model of identity authentication of the structure, improve the authentication accuracy and user information query efficiency, ensures that the parallel computing platform for the safe and stable operation.

Acknowledgements

This project was supported by Sichuan Education Department Science Project (No. 16Z084).

References

[1] Fox G C, Williams R D, Messina P C. Parallel computing works![J]. Florida State University, 2014:877–970.

[2] Chen F, Su L, Liu Y, et al. Confirming the Diversity of the Brain after Normalization: An Approach Based on Identity Authentication[J]. Plos One, 2013, 8(1):268-277.

[3] Feng Z. The research and implementation of a unified identity authentication in e-government network[J]. Physics Procedia, 2012, 24:2032-2038.

[4] Zhao X, Shang T, Li J, et al. A Secure Quantum Network Coding Scheme with Identity Authentication[J]. Sensor Letters, 2014, 12(2):460-465(6).

[5] Gupta A K, Gallasch G E. Equivalence class verification of the contract net protocol-extension[J]. International Journal on Software Tools for Technology Transfer, 2015:1-22.

[6] Akbar M S, Khaliq K A, Qayyum A. Vehicular MAC Protocol Data Unit (V-MPDU): IEEE 802.11 p MAC Protocol Extension to Support Bandwidth Hungry Applications[C]// Vehicular Ad-hoc Networks for Smart Cities Advances in Intelligent Systems and Computing. 2014:31-39.