Design of Network Security Management System Based on K-Means Algorithm

Aiping Liu
Quanzhou University of Information Engineering, Quanzhou, China

Keywords: K-Means Algorithm, Network, Safety Management.

Abstract: The conventional network security management system focuses on the security of network data storage, and does not establish a network management architecture according to the actual needs of the system, which makes the network management always have security risks. Therefore, a network security management system based on K-Means algorithm is designed. In terms of hardware, S9300 switch and RJ45 port connector are designed. In terms of software, establish the function module of the network security management system, establish the network management architecture according to the actual needs of the system, and make the whole management process more reasonable. Optimize the density parameters of network security management based on K-Means algorithm, analyze the initiative and enthusiasm of network defense according to the network management architecture, and improve the network security defense capability to the greatest extent, so as to achieve network security management. The system test proves that the system has better performance and can be applied in real life.

1 INTRODUCTION

In the era of the Internet for All, Internet, big data, cloud computing and other technologies have gradually become essential technologies for people's life, office and learning(Jiang C-Zhao D). All kinds of financial services, such as payment and settlement, financial investment, and life payment, can be realized in the network environment. People can buy, earn money, and pay fees online without leaving home, which greatly improves the quality of life of people. In addition, the network can also provide people with travel route planning, hotel restaurant reservation, food reservation and other businesses. People only need to log on to relevant websites to obtain the materials they need, which plays an important role in optimizing people's travel and life(Vajjha H-Al-Haija Q A). In terms of functions, various network terminals can realize various functions such as communication and shopping; In terms of management, all kinds of network terminals can carry out business management, data management, data analysis, etc., which plays an important role in the development of social economy.

At present, social enterprises have also begun to develop network terminals to provide guarantee for higher management of enterprises. The use of network terminals can achieve efficient management of enterprises and improve their operational efficiency (Zhi and Li J). The threat of the network is also great, similar to hackers, Trojan attacks, network vulnerabilities and other security risks. Hackers can steal deposit information in network terminal software, damage the financial market, and attack the servers of large government and enterprise units through blackmail viruses, resulting in the information of units being stolen, or unable to work normally. The network can only be unlocked by paying ransom(Wang M - Huang J). From this point of view, network viruses pose a great threat to society, spread widely and have a long hiding period. It is urgent to design a security management system to ensure the safe use of the network. Therefore, this paper designs a network security management system based on the function of K-Means algorithm.

2 HARDWARE DESIGN

2.1 S9300 Switch

According to the actual requirements of the system, the management system designed in this paper divides the hardware structure of the system into

Liu, A.
Design of Network Security Management System Based on K-Means Algorithm.
DOI: 10.5220/0012275400003807

In *Proceedings of the 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (ANIT 2023)*, pages 104-109
ISBN: 978-989-758-677-4

sharing, connection and other modes, and the sharing end is divided into device sharing and data transmission sharing; The connection end is divided into device connection and data connection(Chao H C - Yuan T). In order to ensure the security of the network security management system, this paper designs the S9300 switch at the network management end, which forms the system sharing structure together with the out of band network management server and the network security firewall. As shown in Figure 1 below.

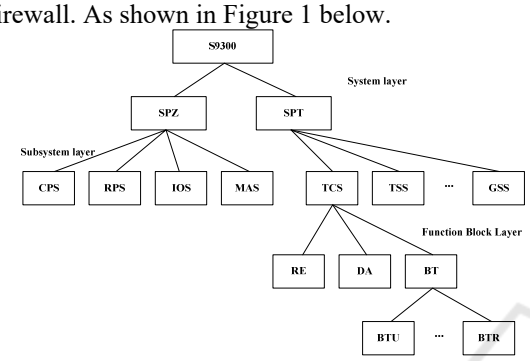

Figure 1: Functional Structure of S9300 Switch.

As shown in Figure 1, the S9300 switch designed in this paper is a fully digital centralized control switch that can run on mobile networks and public networks(Zhang N - Li R). SPZ and SPT are the control parts of S9300 switch, which control the security environment for storage, analysis and management of various network data. CPS, RPS, IOS, MAS, etc. are the network data processing subsystems of SPZ, which have the functions of maintenance, processing, input and output, and play an important role in improving the security performance of the network management system.

2.2 Rj45 Port Connector

The RJ45 port connector designed in this paper is mainly used to work with the S9300 switch. During the operation of the network security management system, the RJ45 port connector has the IEEE802.3 standard, and the maximum effective working distance can reach 100m, thus ensuring the effectiveness of the entire network management environment (Zhang, 2021). Relevant parameters of RJ45 port connector are shown in Table 1 below.

As shown in Table 1, this paper selects the parameters described in the table to ensure the storage and forwarding capability of network data management (Melad T-Humayun M) under half duplex, full duplex, self negotiation and other working modes. When used together with the S9300 switch, it can change the switching mode of the system to maximize the backplane bandwidth and forwarding capability, thus ensuring the overall performance security of the system.

Table 1: Parameters of RJ45 Port Connector.

classification	parameter
Fixed port	8 10/100/1000Base-T adaptive Ethernet ports
Fixed Port Properties	Connector type: RJ-45 Supports 10/100/1000Mbit/s transmission rate Supports half duplex, full duplex, and self negotiation working modes Supports MDI/MDI-X adaptation
Network cable type	10/100Base-TX : Category 3/4/5 twisted pair, supporting a maximum transmission distance of 100m 1000Base-T : Category 5 double line, supporting a maximum transmission distance of 100m
pilot lamp	Per Port: Link/Act , Speed Per device: Power
backplane bandwidth	16Gbps
Forwarding ability	11.9Mpps
Exchange mode	Store Forward Mode
MAC Address Table	Supports address automatic learning and aging (aging time is 5 minutes) Maximum support for MAC (Medium Access Control) addresses: 8K

3 SOFTWARE DESIGN

3.1 Establish the Function Module of Network Security Management System

In the network security management function module designed in this paper, each user is assigned an account. The account enters the system through the login terminal, connects to the network security data acquisition system function, and realizes data security management (Jiang L - Zhang Q). In this paper, with the help of K-Means algorithm, relevant business data is stored in the database, and Web logic business processing services are used to process, real-time transmission of network security data. The functional architecture of the network security management system is shown in Figure 2 below.

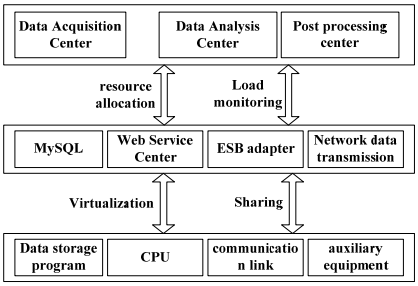

Figure 2: Functional Architecture of Network Security Management System.

As shown in Figure 2, this paper divides data acquisition, data analysis and post-processing into one functional module, which is mainly responsible for resource allocation, load monitoring and other functions. Then MySQL, Web service center, ESB adaptation center, information transmission, etc. are divided into a functional module, which is combined with storage center, CPU, communication link, auxiliary equipment and other functional modules to form a virtualized and shared operation service function. The ESB is used to monitor the data access request of each network software, send the relevant request to the big data center for analysis, and realize the storage and processing of network security video, image, voice and other data to ensure network security to the greatest extent.

3.2 Optimize Network Security Management Density Parameters Based on K-Means Algorithm

For the network security management system, the optimization of density parameters is effective in network security defense and plays an important role in network security management(Fang W, 2022). This paper mainly uses the K-Means algorithm, taking the network data object Xi as the center, and the average distance of the data object nearest to Xi is expressed as the density parameter of the network data object Xi. In this paper, m-dist is used to represent the optimized density parameter value. The larger the m-dist value, the smaller the density, and the more dispersed the data object Xi and the adjacent data objects are. This paper gives the network data sample Xi, which is expressed as:

$$X_i = \left\{ x_1^{(i)}, x_2^{(i)}, ..., x_n^{(i)} \right\} \tag{1}$$

In formula (1), X_i give network data samples for this paper; $x_1^{(i)}$, $x_2^{(i)}$, $x_n^{(i)}$ is of X_i discrete data of. This paper uses the K-Means algorithm, and the selection of k is determined according to the actual network demand X_i the ordered attribute distance from adjacent data objects is:

$$dist_k(X_i, X_j) = \left(\sum_{k=1}^{n} \left| x_u^{(i)} - x_u^{(j)} \right|^k \right)^{\frac{1}{k}} \tag{2}$$

In formula (2), $dist_k(X_i, X_j)$ is a data object$X_i$and adjacent data objects$X_j$ordered attribute distance; $x_u^{(i)}$、$x_u^{(j)}$by X_i and X_j sample data of. On this basis, analyze X_i and X_j the unordered attribute distance of is as follows:

$$m(x_u^{(i)}, x_u^{(j)}) = \sum_{n=1}^{k} \left| \frac{m_u, x_u^{(i)}, n}{m_u, x_u^{(i)}} - \frac{m_u, x_u^{(j)}, n}{m_u, x_u^{(j)}} \right|^k \tag{3}$$

In equation (3), $m(x_u^{(i)}, x_u^{(j)})$ by $x_u^{(i)}$ and $x_u^{(j)}$ the unordered attribute distance of; $m_u, x_u^{(i)}$ is the value of attribute u $x_u^{(i)}$ number of samples; $m_u, x_u^{(i)}, n$ is the value of attribute u in the nth sample cluster$x_u^{(i)}$number of samples; $m_u, x_u^{(j)}$ is the value of attribute u$x_u^{(j)}$number of samples; $m_u, x_u^{(j)}, n$ is the value of attribute u in the nth sample cluster $x_u^{(j)}$ number of samples. Take$dist_k(X_i, X_j)$ and$m(x_u^{(i)}, x_u^{(j)})$ is expressed as the optimized value of density parameter, and the formula is as follows:

$$m - dist(X_i, X_j) = \left(\sum_{u=1}^{n} \left| x_u^{(i)} - x_u^{(j)} \right|^k + \sum_{u=n+1}^{n} m(x_u^{(i)}, x_u^{(j)}) \right)^{\frac{1}{k}} \tag{4}$$

In equation (4), $m - dist(X_i, X_j)$ optimize values for density parameters. In the process of network security management, network data X_i is output, and the number of clusters is expressed as K. The output result is K clusters of data X_i. Select K objects in the high-density area from the output results as the cluster center, and execute the K-Means algorithm, $m - dist(X_i, X_j)$ the smaller the value, the greater the density of network data, the denser the data, and easier to implement the K-Means algorithm to ensure network security.

4 SYSTEM TEST

In order to verify whether the system designed in this paper has the security management performance, this paper tests the above system.

Ensure that the system is in stable operation under the environment where both hardware and software are in normal operation. The traditional network security management system and the management system based on K-Means algorithm designed in this paper are used to test the security management performance of the system. The test preparation process and the final test results are shown below.

4.1 Test Preparation

This paper analyzes the functional requirements of the system, designs the network security management process for the system functions, and uses Java language to develop the system. The system development tool is MyEclipse integrated platform, and the Tomcat operating system is Windows7. MySQL database is used for data storage. The database table is shown in Table 2 below.

Table 2: MySQL database table.

attribute	type	explain	Can be empty
SLP_PhoneNo	Char(11)	System login port	Yes
SLD_DevNo	Char(10)	System login device	No
C_Pwd	Varchar(10)	cipher	No
S_SimNo	Char(10)	Sim	No
AAP_Adr	Varchar(11)	APN Access Point	No
SLN_Name	Varchar(10)	System login name	No
APT_Type	Varchar(10)	Access point type	No
AT_IdentityType	Char(4)	Authentication Type	No
NSMMT_MsgNo	Varchar(10)	Network Security Management Message Types	No
NSMC_Content	Varchar(50)	Network security management content	No

As shown in Figure 2, the database in this paper follows the third normal form principle, and each data depends on transmission, which can solve the problem of network data redundancy, thus ensuring the effective management of the system. After the system environment is prepared, this paper completes the hardware installation of S9300 switch and RJ45 port connector according to the instructions, and debugs the hardware. The S9300 switch is powered on after all lines are connected. The voltage of each line of the switch is within the range of 3.0V~5.0V, which can ensure the normal use of the switch. After each line of RJ45 port connector is connected, the green indicator of the connector lights up to ensure the normal operation of the connector. After the hardware debugging is completed, this paper debugs the software, and the debugging code is shown in Figure 3 below.

```
Import java.utilArrayList,
import java.utilRandom;
public class KMeansRun {
private int kNum, //Number of clusters
private int iterNum = 10; /Iterations
private int iterMaxTimes = 10000://Maximum number of runs per iteration
private float disDiff = (float) 0.01://Termination condition for a single
iteration, distance difference between class centers in two runs
private List<float[]> original_data n=nl://Used to store raw network datasets
private DistanceCompute disC = new DistanceCompute();
/*moveK-Means*/
Public Set<Cluster> run() {
boolean iNeedIter = true;
while (iNeedIter) {
iNeedIter = calculateCenter(clusterSet); /* Calculate the center position of
each class! */
iterRunTimes ++ ; /*Record the actual number of runs*/
return clusterSet, 1*Assign a class to each point! */
}
```

Figure 3: Software Debugging Part Code.

As shown in Figure 3, in the process of software debugging, vulnerabilities were found in the software program, and K-Means algorithm was used to timely correct the code, make up for the vulnerabilities, and improve the running reliability of the software. After the debugging of hardware and software is completed, the system is in normal operation state. In this paper, enter the correct login name and password. After logging into the system, the interface shown in Figure 4 appears.

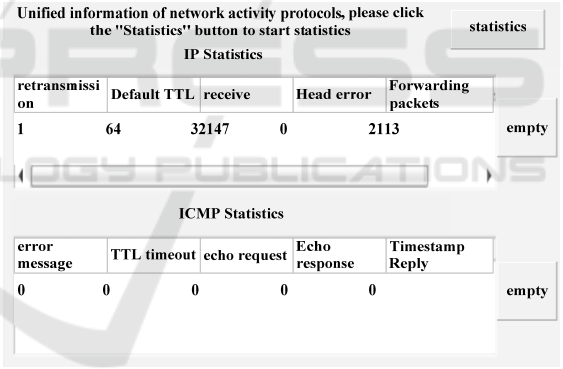

Figure 4: Network Security Analysis Interface of the System.

As shown in Figure 4, after clicking "Statistics" for network activity protocol statistics, network security management starts to run. Analyze the forwarding data, error data, time stamp and other data to determine the network environment, and extract the unreasonable and wrong network data to ensure the normal operation of the system.

4.2 Test Results

Under the above test conditions, this paper randomly selects 8 types of system operation information to analyze the system operation stability and operation standardization. Among them, the time spent in

system testing, the throughput of relevant operation information owned by the system during execution, the throughput of network security management system information, the number of hits of network security management system execution information, the number of hits of network security management system, and other operation information are the information to analyze the stability of system operation; Enter the user name admin and password admin, enter the non-existent user name abc, enter the password 123abb589, enter the IP address, and obtain the operation information such as data packets under the IP address, which is the normative information of the analysis system operation. The traditional network security management system was used to test with the network security management system based on K-Means algorithm designed in this paper. The test results are shown in Table 3 below.

Table 3: Test Results.

System operation information	Traditional management system performance	The performance of the management system designed in this article
Time spent on system testing	78s	32s
The throughput of relevant operation information possessed by the system during execution	106M	43M
Network Security Management System Information Throughput	0.82M/s	1.34M/s
Number of clicks on network security management system execution information	2045 times	6025 times
Number of clicks in the network security management system	96.3 times	224.7 times
Enter username admin and password admin	After two failed login attempts, successfully log in and display the system homepage content	Successfully logged in and displayed the system homepage content
Enter a non-existent username abc and a password of 123abb589	Prompt for password error	Prompt that the username does not exist or the password is incorrect
Enter an IP address to obtain data packets under that IP address	After prompting for an IP address that does not exist 3 times, display information about the data packets related to the input IP address	Display information about input IP address related packets

As shown in Table 3, this paper randomly selects eight types of system operation information, including the time spent in system testing, the throughput of relevant operation information held during system execution, the throughput of network security management system information, the number of hits of network security management system execution information, the number of hits of network security management system existence, the user name admin and password admin enter the non-existent user name abc, enter the password 123abb589, enter the IP address, and obtain the operation information such as data packets under the IP address, which is the key information to reflect the system operation performance. It can be seen from the table that after using the traditional network security management system, the system performance is poor, the system operation interface is non-standard, and the system cannot be operated accurately, affecting the use of the system. After using the network security management system based on K-Means algorithm designed in this paper, the system performance is better, the system running interface is smoother, and the system can be operated accurately to ensure the effective management of the network.

5 CONCLUSION

In recent years, Internet technology has developed rapidly, and network terminals are used more frequently, which not only changes people's lifestyle, but also provides a more convenient living environment for people. The network business in the enterprise is applied on the network terminal. Only personnel inside the enterprise can change the network data in the terminal to ensure the safe storage of enterprise data. In addition, network business greatly saves time costs and improves the efficiency of managers. However, the emergence of the network has not only brought convenience, but also brought hidden information for people. The problem of malicious attacks on the network continues to appear, trojans, network vulnerabilities and other problems, making people fall into a network crisis. Therefore, this paper uses K-Means algorithm to design a network security management system. Combine the hardware and software of the system with the actual functional requirements of the system to truly improve the security of network management.

REFERENCES

Jiang C.Network Security and Ideological Security Based on Wireless Communication and Big Data Analysis[J]. *Wireless Communications and Mobile Computing*, 2022, 2022(3):1-6.

Liang W , Xie S , Cai J , et al. Deep Neural Network Security Collaborative Filtering Scheme for Service Recommendation in Intelligent Cyber-Physical Systems(J). *IEEE Internet of Things Journal*, 2021, PP(99):1-1.

Zhao D , Song H , Li H . Fuzzy integrated rough set theory situation feature extraction of network security[J]. *Journal of Intelligent and Fuzzy Systems*, 2021, 40(1):1-12.

Vajjha H , Sushma P . Techniques and Limitations in Securing the Log Files to Enhance Network Security and Monitoring[J]. *Solid State Technology*, 2021, 64(2):1-8.

Tang C , Zhang J , Wang S , et al. Application and Implementation of Big Data Visualization Technology in Network Security System[J]. *Journal of Physics: Conference Series*, 2021, 1955(1):012002 (6pp).

Al-Haija Q A , Ishtaiwi A . Multi-Class Classification of Firewall Log Files Using Shallow Neural Network for Network Security Applications[J]. *Advances in Intelligent Systems and Computing*, 2021, 1370(1):1-15.

Zhi W W , Zhou X X , Yang L . Application of Fuzzy Comprehensive Method and Analytic Hierarchy Process in the Evaluation of Network Security Level Protection Research[J]. *Journal of Physics: Conference Series*, 2021, 1820(1):012187 (8pp).

Li S . Development Trend of Computer Network Security Technology Based on the Big Data Era[J]. *Journal of Physics Conference Series*, 2021, 1744(4):042223.

Li J , Yan L , Wang J , et al. Research on Network Security Risk Assessment Method Based on Improved AHP[J]. *Journal of Physics: Conference Series*, 2021, 1828(1):012115 (14pp).

Wang M , Zhang B . Analysis of Internet of Things Computer Network Security and Remote Control Technology[J]. *IOP Conference Series: Earth and Environmental Science*, 2021, 634(1):012035 (6pp).

Wang D , Fan H , Li G , et al. Research on Real-time Crawling and Marking Technology of Sensitive Access SQL Statements Based on Information Network Security Isolation Device[J]. *Journal of Physics Conference Series*, 2021, 1948(1):012059.

Huang J , Li J , Wang J , et al. Information Hiding Technology under the Background of Power System Network Security[J]. *Journal of Physics: Conference Series*, 2021, 1852(2):022064 (7pp).

Chao H C , Wu H T , Tseng F H.AIS Meets IoT: A Network Security Mechanism of Sustainable Marine Resource Based on Edge Computing[J]. *Sustainability*, 2021, 13(6):3048.

Einy S , Oz C , Navaei Y D.The Anomaly- and Signature-Based IDS for Network Security Using Hybrid Inference Systems[J]. *Mathematical Problems in Engineering*, 2021, 2021(9):1-10.

Yuan T , Niu Y , Lv L.Research on Optimization Strategy of Computer Network Security Technology under the Background of Big Data Era[J]. *Journal of Physics: Conference Series*, 2021, 1744(3):032237 (4pp).

Zhang N . Research on the Application of Data Encryption Technology Based on Network Security Maintenance in Computer Network Security[J]. *Journal of Physics Conference Series*, 2021, 1744(2):022060.

Ma J , Yu G , Ke H , et al. Network Security Management and Protection of Industrial Internet Equipment[J]. *Chinese Journal of Engineering Science*, 2021, 23(2):81.

Li R , Li F , Wu C , et al. Research on Vehicle Network Security Situation Prediction Based on Improved CLPSO-RBF[J]. *Journal of Physics: Conference Series*, 2021, 1757(1):012148 (8pp).

Zhang H , Kang C , Xiao Y.Research on Network Security Situation Awareness Based on the LSTM-DT Model[J].*Sensors*, 2021, 21(14):4788.

Melad T.Data Network Security Over The Horizon Radar[J]. *International Journal of Scientific and Research Publications (IJSRP)*, 2021, 11(7):730-746.

Humayun M , Hamid B , Jhanjhi N Z , et al. 5G Network Security Issues, Challenges, Opportunities and Future Directions: A Survey[J]. *Journal of Physics Conference Series*, 2021, 1979(1):012037.

Jiang L.On the Relationship between Computer Firewall Technology and Network Security[J]. *Journal of Physics Conference Series*, 2021, 1744(3):032137.

Ni Z , Zhao F.Research and Implementation of Network Security Management Based on Virtualization Technology[J]. *Journal of Physics Conference Series*, 2021, 1802(4):042070.

Zhang Q , Ma D. Discussion on Network Security of Information Retrieval Technology in Network Communication[J]. *Journal of Physics: Conference Series*, 2021, 1744(3):032200 (6pp).

Fang W , Zhao R , Zhu D.Study on Sparrow Search Algorithm Based on K-Means Clustering[J]. *Computer Simulation*, 2022, 39(9): 403-409.