Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2021 SCPE. Volume 22, Issues 2, pp. 161–170, DOI 10.12694:/scpe.v22i2.1881

NETWORK VIRUS AND COMPUTER NETWORK SECURITY DETECTION TECHNOLOGY OPTIMIZATION

ZHIFENG HU [*], FENG ZHAO [†], LINA QIN [‡], AND HONGKAI LIN[§]

Abstract. With the advancement in communication technology, computer network will become important for information exchange. However, the network has the potential therefore the strong security policy is needed for network security ensuring. To prevent the computer network from the virus invasion, the computer network security technology is ensured, having a clear network virus understanding. In this paper, the structural model of network security detection and monitoring system is established in a proactive way, the function of each component is described, and the design model is introduced to conduct comprehensive and effective automatic security detection on the client and each layer of the network, so as to find and avoid the system from being attacked.Result: The observed example shows that the flow rate of information in and out of the network is relatively stable, with few changes, and the rate of change is close to zero per unit time. In the case of network attack, the amount of data flowing into the target network is far more than the amount of data flowing out of the network.Computer security technology is used to improve the security of the network and prevent network virus from attacking the computer network.

Key words: Network Virus; Computer Network; Safety Technology; Automatic Security Detection; Monitoring System

AMS subject classifications. 68M25

1. Introduction. With the rapid advancement of computer field, significant changes have taken place in network security technology. As a virtual space, computer network has the unique language, behavior and social communication modes of the computer, and its space is borderless and open. The emergence of the network has changed the behavior of human beings and gradually made the society have the characteristics of information [1]. In recent years, the computer network virus attacks the network wantonly, has caused the great threat to the computer network security operation. In the face of computer malicious attack, in addition to passive defense, we should also be active defense. Computer network security detection system is an important network security defense technology, its implementation principle is on the basis of the known security vulnerabilities database, item by item to the target host of the leak detection, inspection, switch and server can be a database of target object, after the test results, the system will automatically provide detailed and reliable analysis report to administrator, this for the improvement of overall level of computer network security provides a reliable basis [2, 3].

A certain system is required to protect the security of computer network information and the users also take reasonable protective measures. Various kinds of strategies are used together in the protection process of computer information security. In this way, the probability of infringement of information security is minimized [3-5]. Figure 1.1 shows the firewall network security connection.

At present, in our country most of the computer networks are installed with the firewall software to scan the network access resources and to deal with the hidden security problems [6-8]. It supervises and controls the access between various networks efficiently. Network information is closely monitored by the firewall when the network is running. Generally, to find the data information, IP address of network users are used by the firewalls. The IP address of users can be converted by the control function [9-11]. An effective way to ensure the information security of computer network is protective wall technology. For the operation of computer network, the utilization of protective wall or security system need to be strengthened [12]. The topological structure

[*] Modern Education Technology Center,Wuhan Business University, Hubei Wuhan 430056, China.(zhifenghu87@outlook.com).
[†] Modern Education Technology Center,Wuhan Business University, Hubei Wuhan 430056, China.(fengzhao877@hotmail.com).
[‡] Modern Education Technology Center,Wuhan Business University, Hubei Wuhan 430056, China.(linaQin67@outlook.com).
[§] Modern Education Technology Center,Wuhan Business University, Hubei Wuhan 430056, China (hongkailin262@gmail.com).

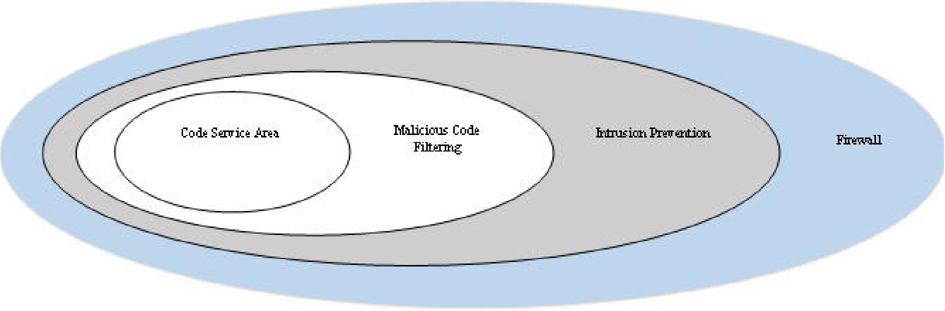

Fig. 1.1. *Firewall Network Security Connection*

can efficiently improve the security of computer network operation and for isolating viruses; Protective wall technology has an effective role. The viruses characteristics are becoming more diverse which requires relevant Internet technical managers [13].

The organization of the paper is as follows. Section 2 gives exhaustive literature survey followed by a research method adopted in section 3. A discussion of obtained results is in section 4. Finally, Section 5 concludes the complete paper.

2. Literature Review. Network security detection technology is built on the basis of modern network security technology, in a long time, people do not take network security as a special problem. With the expansion of the scope of Internet use and the increase of commercial applications, the security problem of Internet is gradually paid attention [14]. In order to adapt to the current network security needs, major companies have developed their own network security detection and evaluation tools.For example, with the release of Microsoft's wsXp, Microsoft recently released version 3.2 of its latest network security detection program. This command line tool can help the system administrator to check the security status of the computer and timely find the unpatched vulnerabilities [15]. One of the UK's leading cyber security companies has developed an online tool to detect security vulnerabilities. It works by using artificial intelligence (Al) to simulate hackers' attacks. With the help of artificial intelligence principle, automatic Web proxy authority, special protocol program, defect confirmation and four levels of internal error correction, some Suggestions on how to repair the vulnerability are proposed [16]. At home, the development of network security technology is also going on like fire. In March 2018, the world's first network security online detection system (NetworkSeeurit, OnlineAuditSystem), developed and designed by shenzhen anluo technology co., LTD., was officially released by "China network security assessment center" and made available to the public. Shanghai jiao tong university, tsinghua university, zhejiang university and other universities, as well as China green alliance technology and other units, have invested certain research strength in expanding network security detection and evaluation technology, laying a solid theoretical foundation for the development of domestic security detection technology [17, 18].

Many researchers have worked on the various techniques on the network security in past few years. To solve the problem of computer information security, there are many technologies like cryptography technology, network security technology and so on [19]. To ensure the computer network information security by setting up computer detection, a special protection system has been established. The electronic products is faster and more severe with the rapid development of science and technology. In this paper, authors detail the network security for large organizational networks which is such a challenging task [20]. The basic aim is to reduce a successful large-scale attack and complex network architecture probability. The attack graphs are utilized to accurately assess the security of networked systems and to understand how vulnerabilities can be combined to stage an attack. It is the successful measurable model to measure the security risk.

The feasibility of computer networks against virus attacks is analyzed and the computer virus weapon characteristics is pointing out [21]. From the obtained results, it is notice that the computer spread the virus in the network speed and with time, the infected machines variation with time. Authors in this paper outline an software development that utilizes QoS and Cisco Catalyst parallel technologies [22]. For Network Intrusion

Detection performance increment , high-speed networks are designed. Authors detailed the network security situational awareness after an investigation. The logical analysis is done concerning the situational awareness network security from the data value chain [23]. Factor acquisition, model representation, measurement establishment, solution analysis, and situation prediction are the five different stages in this process. Authors aim to provide some references for the scientific research and engineering personnel in network security situational awareness. Authors analyses the types of security hidden dangers and the vulnerability detection technology Fuzzing technology [24]. Obtained results show that vulnerability detection technology protects network security efficiently. WS Fuzzer, Web Fuzz and Webvul are three vulnerability detection tools used for detection time of open source system analysis.

2.1. Contribution. The innovation of this paper is to analyze the important position and function of network security detection technology in maintaining network security. On the basis of the above analysis, a structural model of network security detection and monitoring system is proposed. In this paper, the design idea and key technologies of the network security detection and monitoring system are explained and discussed in detail.

3. Research Methodology. Network viruses are divided into mail viruses and vulnerability viruses according to the transmission route:

(1) Trojan is a backdoor program, including the client and server two parts. Generally used as a hacking tool, users in the unknown, the user's data stolen. Trojans do not have the ability to copy themselves. If the user USES the trojans, the hacker has the control of the whole machine. Because be controlled by hacker, so bring huge damage to the user. The way they usually do this is to upload the trojans to a server for users to download.

(2) The worm virus can be spread through MIRC scripts and HTM files. After the user's computer is infected, the worm virus automatically looks for local and network drives, looks for directories, searches for files, and then overwrites the original user files with virus code and changes the file's extension name to VBS. Now computer network security detection technology commonly used methods.

3.1. Use of firewall and detection technology. In the era of big data, firewall and security detection technologies are commonly used to effectively resist the risk of computer network. Firewall can usually be divided into hardware firewall and software fire-wall; can set up a protective barrier between the internal network and the external network. The establishment of a firewall can block external illegal programs from accessing user information, and by strengthening network management, such as setting access rights to data, the computer can be prevented from being infected by network viruses. Firewall as a filtering technology, has a strong anti-attack ability, can protect the user's computer information also can carry out real-time monitoring of network data [25-27]. Firewall solution schematic, as shown in Figure 3.1.

3.2. Access control technology. Access control technology is to define the user's identity, combined with the user's different rights to use the corresponding ability. Use the router to set the external access rights, can also use the permission software to set.

This technology is usually widely used in enterprises. Due to the privilege and confidentiality of computer access technology, if the authentication is not passed, the relevant information cannot be accessed, reducing the risk caused by malicious access. If it is an external access, the access will be directly denied, thus playing a role of security protection at a certain level. Of course, if a virus breaks into permission software or a computer has been monitored, the technology is not safe enough, mainly to prevent human accidents.

3.3. Data encryption and big data analysis. Data encryption technology is to ensure that data in the transmission process is not blocked, data encryption technology can be divided into keys and keys, like keys and locks. In the application of data encryption technology, the first to transfer the file for encryption processing, the information for digital trans-coding, containing a key decoding tool key, after the encryption packet is designated to receive IP, you can use the key decoding, the digital information into normal text again. Even if the encryption package is intercepted by hackers, there will only be a lot of Numbers and garbled code after forced open, unable to get the correct information data. Sometimes the data is exceeded in the typical storage, processing, and computing capacity of conventional databases which is referred by the big data. Many

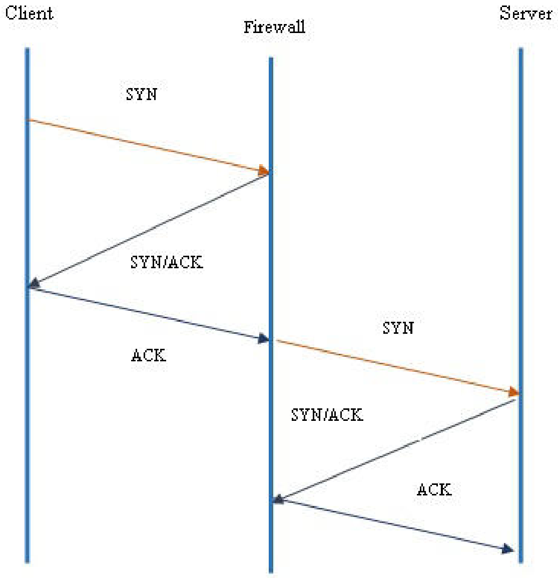

Fig. 3.1. *Firewall Solution Schematic*

tools and methods are needed for the analysis of the big data and to extract the pattern from the large scale data [28, 29]. Cause of big data is due to the increase in data storage capabilities and increased computational processing power providing more data than they have utilizing technologies to process [30, 31].

4. Results and Empirical Analysis. Because the purpose of network security detection system is to find the security holes in the system, we mainly use the existing security attack methods to carry out simulated attacks on the network system, in order to find the security holes and security Settings of the system defects. Network security detection system consists of two parts: security scanning and security analysis. The security analysis system carries out statistical analysis on the result information obtained by the security scanning system, classifies the security vulnerability according to the system, network, service and harm degree, and then queries the database through the vulnerability database control system, gives detailed information about the vulnerability, and suggests the patches to be adopted. The system structure of the entire network security detection system is shown in Figure 4.1.

4.1. Security scanning system. The security scanning system is composed of the following parts:

4.1.1. System configuration module. System configuration module is the manager of the entire system, can use gugong (graphical user interface) or HTML file and browser two ways to manage the system. The system configuration module is mainly used to configure the operation rules of each module of the system. That is, To determine the scope of the information collection. In other words, the information of a subnet or a specific host can be collected. If the information of a subnet is collected, the IP address range of the subnet can be set, such as: 202.118.179.1 – 202.118.179.254. In this way, security detection of subnet 202.118.179.0 can be conducted to collect necessary information. If you collect messages from a particular host, you can set the IP address of that host as 202,118.179.156.

Determine the object of vulnerability inspection module and network service vulnerability or operating system vulnerability. For network service vulnerability, Te1net service vulnerability, FTp, Finger, Http and other network service vulnerability can be detected. For operating system vulnerabilities, you can check file permissions, password file Settings, and system configurations. Finally, the system configuration files are generated based on various configuration information. Each other module initialization and normal operation, according to this configuration file [32-35].

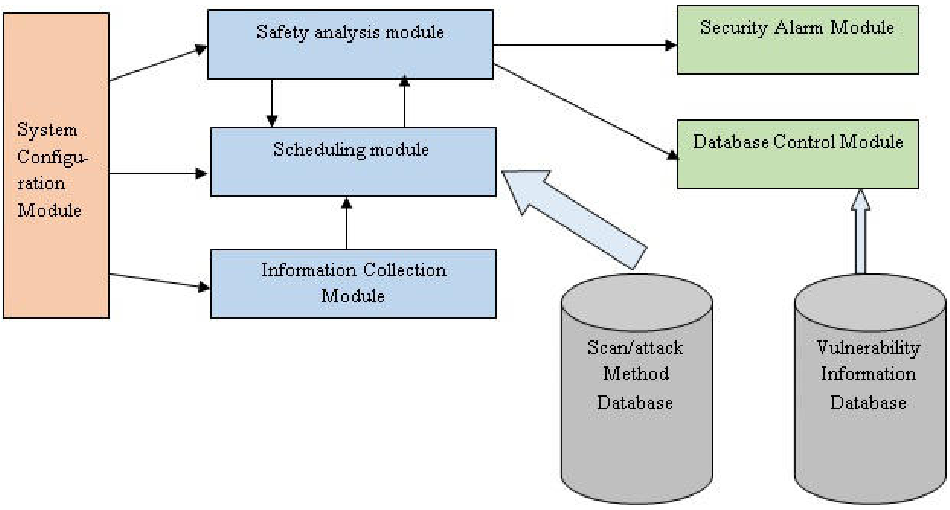
Safety analysis module
Security Alarm Module
System Configu-ration Module
Scheduling module
Database Control Module
Information Collection Module
Scan/attack Method Database
Vulnerability Information Database

FIG. 4.1. *Structure Model of Network Security Detection System*

4.1.2. Information collection module. Construct the topology diagram of the target network The network topology diagram reflects the interconnections among the network elements in the target network. For example, the connection between router, gateway and subnet, the connection between router and router and the connection between the internal hosts of the subnet can make the network administrator master the connection between various devices in the entire network. Different network topology structure itself has different security weaknesses, that is, the network security vulnerability determined by the network topology structure is different, so the corresponding security protection measures should be taken for different network topology structure.

Computer network topology can be divided into four types: bus network, star network and tree network, ring network and mesh network.

Determine the type and version number of the target host operating system In a network, different types of computers often coexist, different types of computers may run different operating systems, and each operating system has many versions, different operating systems may produce a variety of security vulnerabilities. For example, UNxI and sail N0DwS have published about 300 insecure points of the operating system, and there are nearly 50 kinds of known hacker attacks. For versions of the IX operating system, because they are written by different manufacturers or by different people, some versions may have certain vulnerabilities and some may avoid them. The possible security vulnerabilities of Windows operating system and t xI operating system are different.

4.2. Design of network security detection system. The purpose of network security detection system is to find the security holes in the system. However, for an attack method like DDOS (distributed denial of service attack), which attacks the network through ”simple” and ”normal” channels instead of exploiting the vulnerability of the system itself, network security detection system is difficult to detect. Therefore, we need to add monitoring function to the security detection system, timely detect abnormal network activities, repair potential attack vulnerabilities, and enhance the security performance of the network. We mainly implement the detection and monitoring of the network system from the following two aspects:

4.2.1. Monitor network traffic. From the most intuitive and natural point of view: all network services, data exchange, in the final analysis, are down to the host physical port of the bit flow, the normal service is so, illegal invasion is so. Therefore, starting from the underlying physical port, real-time monitoring of the state of bit-stream flow (direction, size, rate, rate of change, etc.) can help the system administrator to timely find network anomalies.

First, in order to monitor the data traffic in the whole network, the monitoring system must be placed on the switching node (e.g., router, switch, etc.) in the network system, because all data entering and leaving the

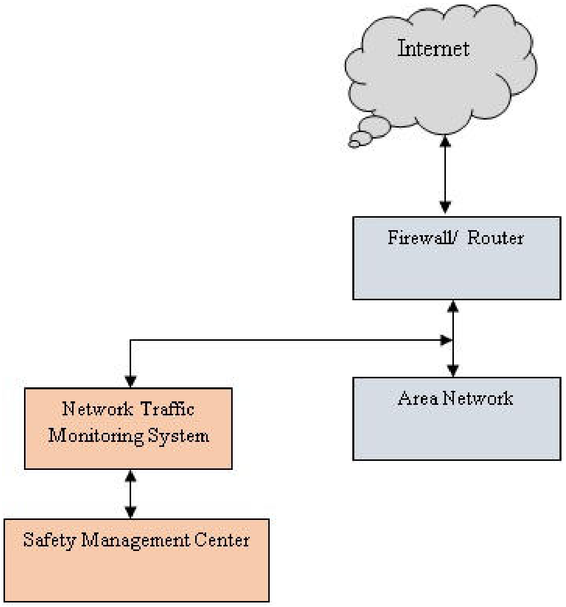

Fig. 4.2. *Location of Network Security Monitoring System*

network must flow through the switching node. In addition, the network card of the machine at the switching node is set to "promiscuous" mode so that all packets entering and leaving the network can be captured by the machine. Figure 4.2 shows the location of the traffic monitoring system in the network.

Secondly, in order to realize the real-time traffic monitoring of the network, it is necessary to obtain the changing rules of data traffic of various typical network visits and store them in the display system in the form of feature files. For example, typical network port information traffic has the following observed facts: There is a certain proportion and characteristics of the inbound and outbound flow in normal use mode as given in Eq. (4.1) to Eq. (4.4):

C_{out} represents the amount of traffic flowing out of the network;

C_r represents the traffic flowing into the network;

$$C_{out} << C_r \tag{4.1}$$

$$\frac{\theta_1 <= C_{out}}{C_r < \theta_2} \tag{4.2}$$

Changes of network port traffic under network attack:

$$C_{out} << C_{in} \tag{4.3}$$

$$\frac{C_{out}}{C_{in}} < \theta_1 \tag{4.4}$$

If the network traffic is displayed in the form of waveform, it can be seen that there is a significant difference in the waveform changes in two cases: in the case of normal network access, the waveform changes little, the waveform performance is relatively slow; However, in the case of similar DDoS attack, the waveform changes greatly and there are multiple data traffic peaks, indicating that a large amount of data flows into the monitored network. Different switching node hosts may not have the same characteristics for the above typical network access, so the characteristic files may not be the same. The monitoring system should be audited for different machines to obtain the characteristic parameters C_{out}/C_{in} and of the specified host. Also, the network port

Table 4.1
Same Speed Limit and Different Numbers of Packets

Packet Number (transmission interval 1 ms)	Packets Received	Packets Analysed	Packets Dropped	Packets Filtered	Packets Outstandings
100	100%	100%	0.00%	0.00%	0.00%
500	100%	49.38%	33.62%	0.00%	50.37%
1000	100%	28.83%	40.28%	0.00%	68.92%

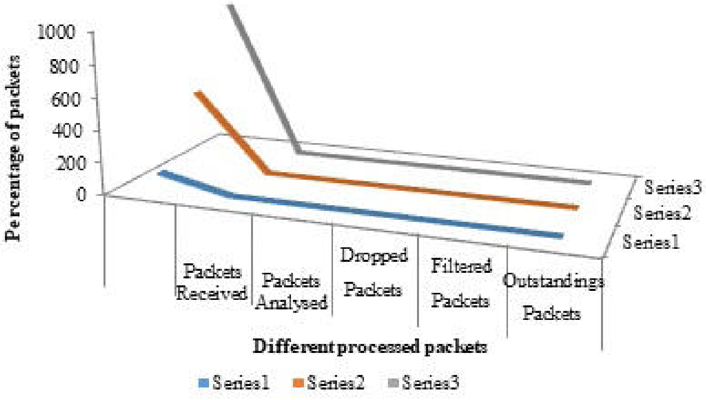

Fig. 4.3. *Same Speed Limit and Different Numbers of Packets*

information flow rate (Rout/Rout) and its rate in unit time rate of change (V_{in}/V_{out}) for identifying network normal or abnormal situation have important significance. Under the normal network access mode, there is a certain proportion and characteristics of the in-out rate as given in Eq. (4.5) and (4.6):

$$R_{out} \simeq R_{in} \tag{4.5}$$

$$V_{out} \simeq V_{in} \simeq 0 \tag{4.6}$$

Changes of data flow rate of network port under the circumstance of network attack as shown in Eq. (4.7) and Eq. (4.8).

$$R_{out} \ll R_{in} \tag{4.7}$$

$$V_{in} \gg V_{out} \simeq 0 \tag{4.8}$$

From the above observation examples, it is seen that under normal circumstances, the flow rate of incoming and outgoing network information is relatively stable with few changes, and the rate of change per unit time is close to zero. In the case of network attack, the amount of data flowing into the target network is far more than the amount of data flowing out of the network, and the rate of information flow in unit time changes obviously, indicating that there is a large amount of data pouring into the target network [36-38].

In the experiment, the packet transmission rate was remain to the similar speed (1 ms intervals) to get a fair analysis of numbers of packets (each packet carried 1 KB). We sent 100, 500 and 1000 packets batches at 1 ms intervals and the experimental results are shown in Table 4.1 and the Figure 4.3 shows its graphical representation.

Table 4.2
Speed and Values are same but Different Packet Size

Packet Number (speed 12,000 per 1 ms)	Packets Received	Packets Analyzed	Packets Dropped	Packets Filtered	Packets Outstanding
1 Byte	100%	100%	0.00%	0.00%	0.00%
400 Bytes	100%	42.09%	32.67%	0.00%	58.67%
800 Bytes	100%	23.67%	41.89%	0.00%	80.11%

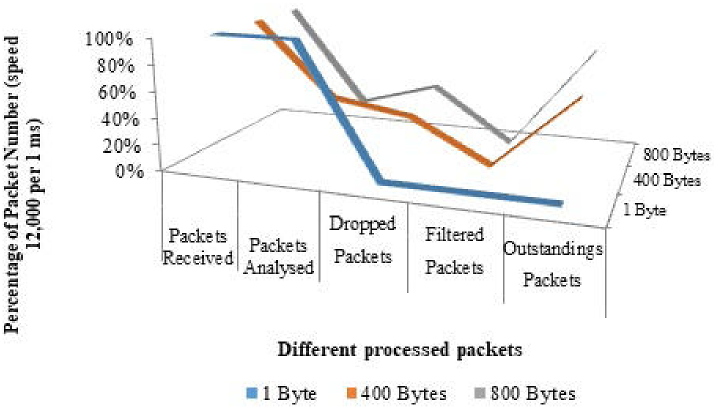

Fig. 4.4. *Same Speed and Value but Different Packet Size*

If we transfer 12,000 packets in interval of 1 ms then the packet size was increased to 400 bytes,the 35% of them are dropped.The Snort dropped more When the packet size was increased to 800 bytes. The Table 4.2 presents the experimental results.

The graphical representations of results are also shown in Figure 4.4. Experiment results shows that more packets will be dropped if there is increase in packet size.

4.3. Monitor network connections. Due to the initial design of TCP1-P protocol without too much consideration of security factors, there are many network attacks against the weak links of TCP work protocol. Here's how they work: They first choose to send SNY packet request to the service port of the target host to establish a connection with it, then the target host needs to assign the data structure needed for the connection, and the connection state becomes YSNRCVD. If the service port does not receive a response from the host after sending a SY-ACK packet to the host requesting the connection, the service port has to wait quite a long time, and if there are too many half connections, it may consume all the resources used to establish the half connection. The normal connection requests are not answered because there is no corresponding resource if the resource is exhibited. The main characteristics of these attack methods are: when launching an attack, as long as very little data traffic can produce significant results; The source of the attack cannot be located; There is no way to tell whether a TCP connection request is legitimate on the server side.

5. Conclusion. Reasonable use of the computer network security inspection system can realize the real-time monitoring of the computer network security, as well as the real-time identification of network intrusion behavior. Although it is an important component of computer network security, it focuses on finding that it cannot replace the firewall to adjust the access control of the entire network. However, firewall lacks the recognition function of unexpected intrusion behavior, so it needs security detection system to identify unexpected intrusion behavior. Therefore, the two need to supplement each other to ensure network security. With the gradual integration of the network into People's Daily life, people's requirements for network security are also getting higher and higher. The observed example shows that the flow rate of information in and out of the network is relatively stable, with few changes, and the rate of change is close to zero per unit time. Computer security technology is used to improve the security of the network and prevent network virus from attacking the computer network. The extensive application of network security detection technology can guarantee the security of people's network life.The hybrid technique can be designed in the future for network security which can result effectively.

Acknowledgement. Wuhan education and science project "Network Virus and Computer Network Security Detection Technology Optimization" in Applied-Oriented Universities Taking Wuhan Business University.

REFERENCES

[1] Li, S., Zhang, W., Li, G., Su, L., and Huang, Q. , *Vehicle detection in uav traffic video based on convolution neural network*, In 2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), pp. 1-6, April 2018.

[2] Zhang, H., Zhang, Y., Feng, P. R., Zheng, R. Y., Luo, Y. L., and Yang, Z. X.,*Establishment of RT-LAMP Detection Method for Bluetongue Virus*, In 2018 9th International Conference on Information Technology in Medicine and Education (ITME), pp. 789-793, October 2018.

[3] Butt, P. K., Shaikh, M. K., Pathan, M., Shahani, I. A., Tunio, S., and Qureshi, S., ,*Social Network Chatting Apps Network Traffic Optimization*, Indian Journal of Science and Technology, vol. 11, 2018.

[4] Junsheng, Y.,*Application of Virus Protection Technology in Computer Network Security in Big Data Environment* , Computer Fan, vol. 11, pp. 77-78, 2018.

[5] Ming, X., Chen, Y., and Guo, J.,*Analysis of computer network information security and protection strategy*, In MATEC Web of Conferences, vol. 267, 2019.

[6] Liebenberg, K., Smit, A., Coetzee, S., and Kijko, A.,*A GIS approach to seismic risk assessment with an application to mining-related seismicity in Johannesburg, South Africa*, Acta Geophysica, vol. 65, pp. 645-657, 2017.

[7] Li, W., Liu, Y., Qiao, W., Zhao, C., Yang, D., and Guo, Q.,*An improved vulnerability assessment model for floor water bursting from a confined aquifer based on the water inrush coefficient method*, Mine Water and the Environment, vol. 37, pp.196-204, 2018.

[8] Sang, Y., Shen, H., Tian, H., and Zhang, Z.,,*Achieving probabilistic anonymity in a linear and hybrid randomization model*, IEEE Transactions on Information Forensics and Security, vol. 11, pp. 2187-2202, 2016.

[9] Huaqiong, D., and Binhui, T. , *Prediction of data flow in computer network based on linear multi-scale model*, Journal of Shenyang University of Technology, vol. 39, pp. 322-327, 2017.

[10] Praude, C. C. , *Computer Art and Actor-Network Theory: Actants and Intersubjective Associations in Scene*, Leonardo, vol. 51, pp. 29-529, 2018.

[11] Cotroneo, D., Iannillo, A. K., and Natella, R. ,*Evolutionary Fuzzing of Android OS Vendor System Services*, Empirical Software Engineering, vol. 24, pp. 3630-3658, 2019.

[12] Wu, H., Ding, Y., Winer, C., and Yao, L., ,*Network security for virtual machine in cloud computing*, In 5th International Conference on Computer Sciences and Convergence Information Technology, pp. 18-21, November 2010.

[13] Ho, A., Maiga, A., and Aïmeur, E. ,*Privacy protection issues in social networking sites*, In 2009 IEEE/ACS International Conference on Computer Systems and Applications, pp. 271-278, May 2009.

[14] Yongquan, F., and Dongsheng, L.,*Application driven network latency measurement analysis and optimization techniques edge computing environment: a survey*, Journal of Computer Research and Development, vol. 55, 2018.

[15] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., and Stoddart, K. ,*A review of cyber security risk assessment methods for SCADA systems*, Computers and security, vol. 56, pp. 1-27, 2016.

[16] He, Q., Zhang, Q., Quek, T. Q., Chen, Z., Li, S. ,*Distributed optimization in fog radio access networks—channel estimation and multi-user detection*, In 2018 16th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt), pp. 1-8, May 2018.

[17] Lu, D., Liu, J., Zhang, Y., Liu, F., Zeng, L., Peng, R., and Zuo, J.,*Discovery and optimization of phthalazinone derivatives as a new class of potent dengue virus inhibitors*, European Journal of Medicinal Chemistry, vol. 145, pp. 328-337, 2018.

[18] Dasgupta, S., Banerjee, K., Dhumal, K. N., and Adsule, P. G.,*Optimization of detection conditions and single-laboratory validation of a multiresidue method for the determination of 135 pesticides and 25 organic pollutants in grapes and wine by gas chromatography time-of-flight mass spectrometry*, Journal of AOAC International, vol. 94, pp. 273-285, 2011.

[19] Ming, X., Chen, Y., and Guo, J. , *Analysis of computer network information security and protection strategy*, In MATEC Web of Conferences, vol. 267, pp. 02013, 2019.

[20] Wang, S., Zhang, Z., and Kadobayashi, Y., ,*Exploring attack graph for cost-benefit security hardening: A probabilistic approach*, Computers and security, vol. 32, pp. 158-169, 2013.

[21] Yang, P., *Radiation-based virus attack and defense reliability optimization design* , Chemical Engineering Transactions, vol. 51, pp. 793-798, 2016.

[22] Bul'ajoul, W., James, A., and Pannu, M. , *Improving network intrusion detection system performance through quality of service configuration and parallel technology*, Journal of Computer and System Sciences, vol. 81, pp. 981-999, 2015.

[23] Li, Y., Huang, G. Q., Wang, C. Z., and Li, Y. C.,*Analysis framework of network security situational awareness and comparison of implementation methods*, EURASIP Journal on Wireless Communications and Networking, vol. 1 2019.

[24] Wang, C., Ren, T., Li, Q., Wang, X., Guo, G., and Dong, J. , *Network computer security hidden dangers and vulnerability mining technology*, MS&E, vol.750, pp. 012155, 2020.

[25] Watanabe, Y., and Sugahara, H. , U.S. Patent Application No. 14/408,363, 2015.

[26] Meletis, E. I., Politis, C., and Schommers, W. ,*Selected peer-reviewed articles from the international conference (IC4N) on nanoscience/nanotechnology*, Quantum Matter, vol. 3, 287-289, 2014.

[27] Ijaz, S., Hashmi, F. A., Asghar, S., and Alam, M.,*Vector based genetic algorithm to optimize predictive analysis in network security*, Applied Intelligence, vol. 48, 1086-1096, 2018.

[28] Yan, F., Jian-Wen, Y., and Lin, C. ,*Computer network security and technology research*, In 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation, pp. 293-296, June, 2015.

[29] Orchier, J., Soriano, R., Salvaterra, L., Ardito, D., and Byreddy, A.,U.S. Patent No. 6,070,244. Washington, DC: U.S. Patent and Trademark Offic, 2000.

[30] Wenisch, T. F., Berard, S. R., and Smith, D. J,U.S. Patent No. 7,100,054. Washington, DC: U.S. Patent and Trademark Office, 2006.

[31] Bonnafous, L., Lall, U., and Siegel, J.,,*A water risk index for portfolio exposure to climatic extremes: Conceptualization and an application to the mining industry*, Hydrology and Earth System Sciences, vol. 21, pp. 2075, 2017.

[32] Nasri, Z., and Mozafari, M.,*Multivariable statistical analysis and optimization of Iranian heavy crude oil upgrading using microwave technology by response surface methodology (RSM)*, Journal of Petroleum Science and Engineering, vol. 161, pp. 427-444, 2018.

[33] Sang, Y., Shen, H., Tian, H., and Zhang, Z.,*Achieving probabilistic anonymity in a linear and hybrid randomization model*, IEEE Transactions on Information Forensics and Security, vol. 11, pp. 2187-2202, 2016.

[34] Prajapati, C. S., and Bhat, N.,*ppb level detection of NO 2 using a WO 3 thin film-based sensor: material optimization, device fabrication and packaging*, RSC advances, vol. 8, pp. 6590-6599, 2018.

Edited by: Pradeep Kumar Singh
Received: May 16, 2021
Accepted: Sep 20, 2021