A Network Security Approach based on Machine Learning

1st Kai Yun
State Grid Xinjiang Information & Telecommunication Company
Xinjiang, China
liukaihrj@yeah.net

2nd Yang Jin
State Grid Xinjiang Information & Telecommunication Company
Xinjiang, China
mhjin246@163.com

3rd Qiang Huang
State Grid Xinjiang Information & Telecommunication Company
Xinjiang, China
zezhouhuang@yeah.net

4th Qingpeng Wang
State Grid Xinjiang Information & Telecommunication Company
Xinjiang, China
lipengweihh@163.com

2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS) | 979-8-3503-9846-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICICACS57338.2023.10100204

***Abstract*—Network security is the main content of network management, but in the process of network security management, it is vulnerable to hacker intrusion and communication interference, which reduces the level of network security, and causes the loss of crucial communication data and the wrong results of security assessment. Based on this, this paper proposes a machine learning method to machine study network communication data, enhance network communication data, and shorten network communication time. The network communication data is then analyzed by messages. Finally, the machine learning method is used to judge the security of communication data and output the final security assessment results. The results show that the machine learning method can accurately carry out network security analysis, reduce the interference of hackers and communications, and the security level is greater than 9 to 5%, which is better than the online security monitoring method. Therefore, the machine learning method can meet network security requirements and is suitable for network management.**

Keywords—network, communications, security, machine learning.

I. INTRODUCTION

Some scholars believe that network security is a comprehensive analysis process of network management [1], and it is necessary to conduct a comprehensive analysis of network communication data and encrypted data. It is prone to problems such as wrong transmission and incomplete network communication data [2]. Currently, network security often has the problems of low-security level [3], long security judgment time, and redundancy of network communication data of different servers in network management [4]. Therefore, some scholars propose to apply intelligent algorithms to network security judgment, identify interference factors such as hackers and communications, and analyze convex analysis to assess network security [5]. However, the data transmission between the central server and the local server is still not ideal [6], and there is a problem of low-security level. To this end, some scholars have proposed a machine science method through the convex analysis of critical values, identifying the more significant probability and prominent values in the key values [7], and conducting approximate analysis of key network communication data to achieve practical judgment of network security [8]. Therefore, based on the machine method, this paper analyzes the key values in network management and verifies the safety judgment results of the method.

II. RELATED CONCEPTS

Network security analysis makes security judgments on the probability features in key values, and detects the changing characteristics of critical values [9], which has high anti-hacker interference ability and can effectively make security judgments. , is a commonly used network security method. Network security analysis mainly calculates the peak value of network communication data based on network communication messages and the probability of approximation between messages [10]. The machine science method uses statistical theory to approximate the key points in the network communication data, calculate the probability, and complete the safety judgment and identification through the cross-calculation of key values [11]. Among them, the eigenvalue's convex and concave direction represents the key value's safe change direction. The machine method requires two definitions, which are as follows.

Definition 1: Any network communication data is P_i, the approximation result is x_{i}, the set of safety judgments is $k(x_i, y_i)$, and the number of machine learning is set_{i} . c_{i} Well, the $k(x_i, y_i)$ calculation process is shown in (1).

$$k(x_i, y_i) = \frac{\sum x_i \cdot P_i \left| set \right.}{c_i} \tag{1}$$

Definition 2: The probability function of the machine method is the overall probability, the security probability $f(x,P)$ A, and the B hacker intrusion probability ξ. Well, the $f(x,P)$ calculation process is shown in (2).

$$f(x,P) = \frac{x_i}{A \cdot B} + \xi \tag{2}$$

Definition 3: Convex function, security judgment $C(x_i)$ change to, hacker intrusion set is Δx_{i}, Δset_{i} security judgment number is Δc_{i}. Well, the calculation process is shown in (3).

$$C(x_i) = \Delta c_i \cdot \sum set_i \cdot \frac{x_i}{\Delta x_i} \tag{3}$$

979-8-3503-9846-5/23/$31.00 ©2023 IEEE

Definition 4: The statistical function is $f(x,r), C$ is the statistical threshold, and τ is the statistical error. Well, the calculation process is shown in (4).

$$f(x,r) = \sum C \cdot x_i + \tau \tag{4}$$

III. THE JUDGMENT OF NETWORK SECURITY BY MACHINE LEARNING

In the process of network security, the acceptance probability of network communication information should be calculated to reduce the error rate of security judgment. According to the principle of statistics [12], it is necessary to identify the network communication messages and encrypted data with differences, calculate the approximate value of the network communication data so as to identify the security judgment network communication data, and calculate the security judgment integrity after network security [13]. Therefore, it is necessary to extract random eigenvalues of the critical values after mining.

Definition 5: The one-way security judgment function is that when the $F(x_i|k)$ security judgment value occurs, the $k(x_i, y_i) < 1$ communication sales are normal; $f(x,P) \neq 1$, the information encryption is normal. The calculation $F(x_i|k)$ is shown in (5).

$$F(x_i|k) = \frac{k(x_i, y_i)}{f(x,P)} \wedge k \tag{5}$$

If the $F(x_i|k)$ output result is a positive number, the network security is reasonable [8], otherwise the value should be excluded. If it $F(x_i|k)$ is less than 0, the feature value does not meet the safety judgment requirements, and the safety judgment parameters should be adjusted.

Definition 6: The comprehensive judgment function of two-way safety judgment is calculated $F(dou|x_i)$ as shown in (6).

$$F(dou|x_i) = \sum_{o=1}^{2} E_o \Leftrightarrow \frac{k(x_i, y_i)}{f(x,P)} \wedge k \tag{6}$$

To reduce the occurrence of outliers, network security needs to sample and analyze critical numerical security judgments, including network communication messages, network communication, and large probability value ranges. In addition, according to the machine method, the security judgment of key network communication data is carried out, and the statistical theory is used to approximate the analysis and calculation of different network communication messages and network communication. At the same time, the interference analysis of key values of different complexity is carried out to eliminate the influence of key-value interference on the calculation results and reduce the difficulty of calculation, as follows.

Step 1. Collect network communication data, determine the security judgment rules, and perform machine analysis on the collected data, and then determine the threshold and weight of the calculation.

Step 2. Approximate calculation according to the network communication data and network communication in the key values, and compare the approximation of the results, finally determine the characteristic values of network communication messages and network communication, and mine the causes of abnormal network communication messages and network communication.

Step 3. Compare the abnormal network communication messages and network traffic, verify the security level, predictability and integrity of the results, and store the results in the network communication log.

Step 4. Accumulate the calculation of key-value network communication messages and network communication. If the preset capacity of key values is exceeded or the maximum number of iterations is reached, the analysis is terminated, otherwise the calculation is continued.

IV. PRACTICAL EXAMPLES OF NETWORK SECURITY

A. Parameters of Key Network Security Values

In order to verify the effect of the security judgment calculation method on network security, the security judgment effect of network communication data is judged, and the specific parameters are shown in Table I.

TABLE I. PARAMETERS OF KEY NETWORK SECURITY VALUES

Parameter	Key values	Safety judgment criteria
Degree of encryption (level)	2.56	Level 3
Hacking (times)	4.32	6
Safety judgment conditions (level)	6.51	10
Complexity (level)	4.25	5
Server Data (M)	3.68	4M
Probability Center (%)	5.66	6
Approximation value (%)	98.4	100

According to the parameters in Table I, there are no significant differences in probability centre, encryption degree, hacker intrusion, security judgment conditions, complexity, server data, probability centre and approximation value, indicating that there is no significant difference between the key value and the security judgment standard, which meets the statistical analysis requirements and can be analyzed by network security. The distribution of the different data is shown in Fig. 1.

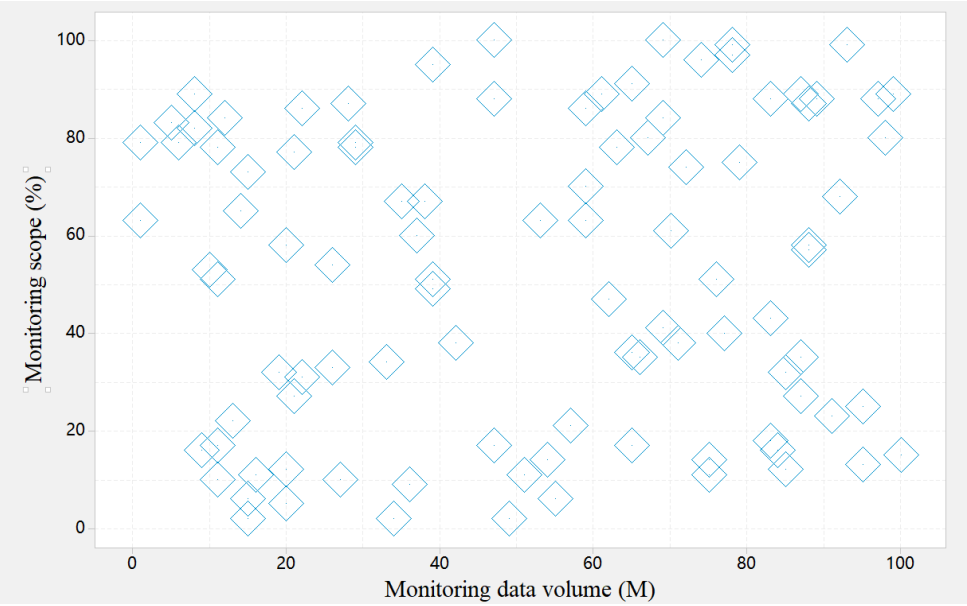

Fig. 1. Distribution of network communication messages

It can be seen from Fig. 1 that the distribution of network communication messages is relatively discrete, and the data is independent of each other, which meets the requirements of key numerical analysis, so it can be analyzed later by machine learning.

B. Integrity and Level of Network Security

Network security should be maintained to a certain degree of stability; otherwise, it will affect the calculation results, and the integrity of network security results will be tested, and the specific results are shown in Table II.

TABLE II. COMPARISON RESULTS OF INTEGRITY AND SAFETY LEVEL (UNIT: %)

Algorithm	Mode	Parameter	Level of security	Completeness
Machine learning method	Probabilistic calculations	One-way network communication	92.22±4.01	98.22±4.02
		Two-way network communication messages	98.22±4.22	94.04±4.02
		Continuous communication	24.22~24.23	24.21~24.22
	Approximation analysis	Network communication	95.22±0.02	94.23±0.22
		Network communication messages	94.22±0.02	94.22±0.06
		Continuous communication	93.12±0.32	95.04±0.32
Online safety monitoring law	Probabilistic calculations	Network communication	74.82±4.32	78.22±0.02
		Network communication messages	78.32±4.92	74.02±2.82
		Continuous communication	75.22±4.32	73.14±2.88
	Approximation analysis	Network communication	75.12±4.42	74.29±0.32
		Network communication messages	74.23±4.12	74.22±0.92
		Continuous communication	74.23±4.12	74.22±0.08

It can be seen from Table II that the completeness and safety level of the machine learning method is greater than 90%, the mode change is less than 3, and the change approximation value of different methods is greater than 70%, which is significantly different. At the same time, the change range between network communication messages and communication is relatively small, so the overall result of the security judgment calculation method is better. The difference between network communication and network communication messages of the online security monitoring method is large, between 3~6, and the approximation value is less than 80%, which is relatively poor. The changes in the safety level and integrity of the different methods are shown in Fig. 2.

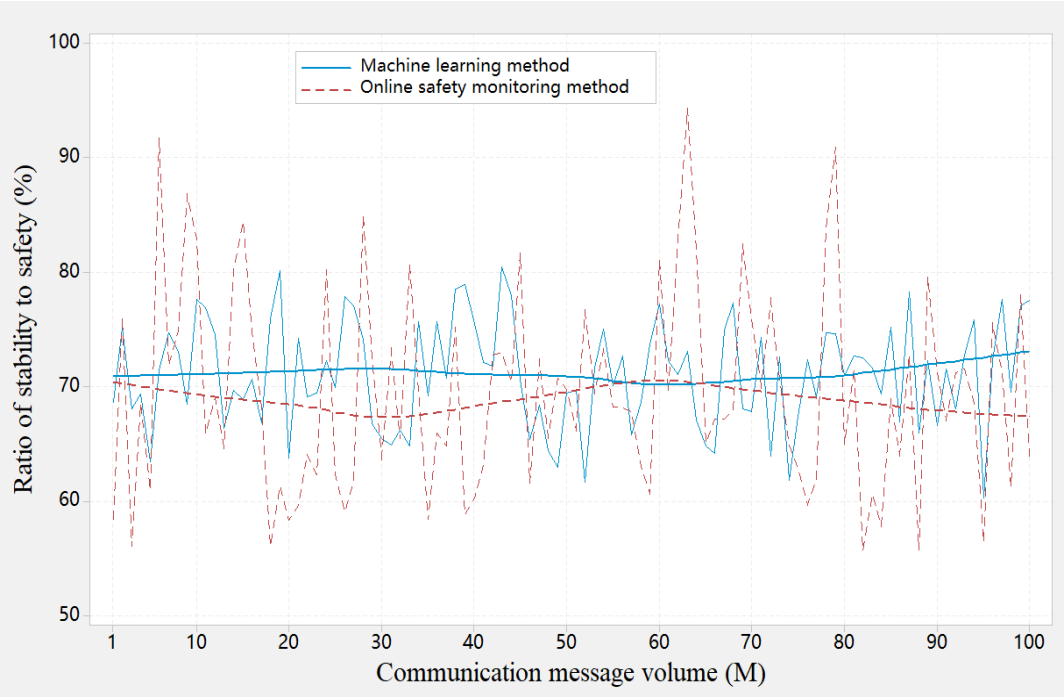

Fig. 2. Comparison of the integrity and security levels of different algorithms

It can be seen from Fig. 2 that in continuous sampling, the network security level and integrity of the machine learning method are more concentrated, while the security level and integrity of the machine learning method are more scattered, which is consistent with the research results in Table II. The reason is that the machine method analyzes the probabilistic data of critical numerical network communication data, network communication and other data and calculates the convex function values of different values to simplify the network communication length, network communication message location and other attributes. After discovering hackers and communications, the communication data is used to conduct an approximation analysis to determine the cause of abnormal transmission.

C. *Security Judgment Time of Network Communication*

Security judgment time is an essential indicator of network security effect, including accounting security judgment, proximity analysis security judgment, industry security judgment, etc. The specific results are shown in Table III.

TABLE III. SECURITY JUDGMENT TIME FOR NETWORK COMMUNICATION (UNIT: SECONDS)

Algorithm d	**Monitoring phase**	**One-way judgment time**		**Judge the time in both directions**	
		image	***text***	***image***	***text***
Machine learning method	1/2	1.75±0.72	1.27±0.22	1.25±0.42	1.77±0.27
	1/4	2.25±0.57	2.42±0.25	2.25±0.77	2.45±0.25
	1/6	6.47±0.27	6.27±0.47	7.47±0.47	8.07±0.72
variation	0.35~1.77				
Online safety monitoring law	1/2	2.75±0.72	2.22±0.42	2.25±0.42	2.27±0.27
	1/4	4.25±0.57	4.72±0.75	4.27±0.27	4.25±0.27
	1/6	9.47±0.27	8.77±0.27	12.27±0.77	6.27±0.22
variation	6.45~11.57				

According to Table III, in the machine method, the time of network security is relatively stable, and the change range is between 0.35~0.77. Among them, the safety judgment time of images, text, and audio in the safety judgment is between 1~2 second, the safety judgment time is between 22~27 seconds, and the overall safety judgment time is ideal. Compared with the machine method, the calculation time of the online safety monitoring method is relatively long, and the time variation range is 6.45~11.57. The reason is that the online security monitoring method is based on a small number of hackers and communications, iteratively analyzes the images, text, and audio, and determines the key numerical security judgment time. If the number of servers for security judgment is small, the later communication messages will decrease exponentially, thereby shortening the calculation time. Fig. 3 shows the security judgment time of the overall data in Table III.

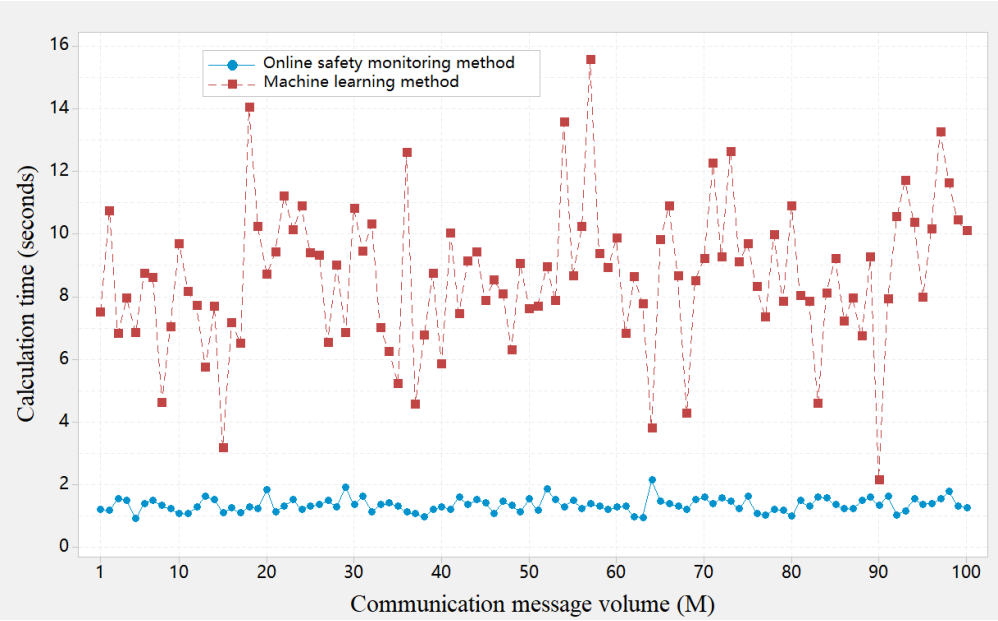

Fig. 3. Comprehensive comparison of different methods

Through the analysis of Fig. 3, it can be seen that the comprehensive analysis degree of the machine learning method is more significant, and the overall change is relatively stable, while the change range of the online security monitoring method is more extensive, which is inferior to the former. Therefore, the results in Fig. 3 further validate Table III.

V. Conclusion

For network security machine learning cannot accurately perform network security. Based on this, this paper proposes a machine learning method to set data for image and approximation analysis and uses an approximation to analyze the feature value of safety judgment. Network communication messages and network communication analysis are carried out through machine learning to reduce the mapping of hackers and industries in security judgment. The characteristic value is used as the node for safety judgment analysis to realize the safety judgment of critical values. The results show that the completeness and safety level of the machine learning method is greater than 90%, and there is no significant difference in the changes of image, text and audio, but the difference of the online safety monitoring method is more significant. In the machine method, the time of network security is relatively short, and it is not affected by the prediction level of images, proximity analysis and industry, and security judgment. In contrast, in the machine learning method. The safety judgment time is relatively long, and the time variation range is 6.45~11.57. Therefore, the machine learning method can meet network security requirements and is better than the machine learning method.

References

[1] M. F. Hyder, Waseemullah, M. U. Farooq, U. Ahmed, and W. Raza, "Towards Enhancing the Endpoint Security using Moving Target Defense (Shuffle-based Approach) in Software Defined Networking," Engineering Technology & Applied Science Research, vol. 11, no. 4, pp. 7483-7488, Aug 2021.

[2] S. Javanmardi, M. Shojafar, R. Mohammadi, A. Nazari, V. Persico, and A. Pescape, "FUPE: A security driven task scheduling approach for SDN-based IoT-Fog networks," Journal of Information Security and Applications, vol. 60, Aug 2021.

[3] Ramesh, G. P., & Gowrishankar, K. S. (2012). Enhancement of power quality and energy storage using a three-terminal ultra capacitor and CCM converter for regenerative controlled electric drives. Int J Emerg Res Manag Technol, 9(2), 56-61.

[4] O. O. Olakanmi and K. O. Odeyemi, "VerSA: Verifiable and Secure Approach With Provable Security for Fine-Grained Data Distribution in Scalable Internet of Things Networks," International Journal of Information Security and Privacy, vol. 15, no. 3, pp. 65-82, Jul-Sep 2021.

[5] A. Sharma and R. K. Jha, "A Comprehensive Survey on Security Issues in 5G Wireless Communication Network using Beamforming Approach," Wireless Personal Communications, vol. 119, no. 4, pp. 3447-3501, Aug 2021.

[6] H. Vargas, C. Lozano-Garzon, G. A. Montoya, and Y. Donoso, "Detection of Security Attacks in Industrial IoT Networks: A Blockchain and Machine Learning Approach," Electronics, vol. 10, no. 21, Nov 2021.

[7] Perveen, N., Roy, D., & Chalavadi, K. M. (2020). Facial expression recognition in videos using dynamic kernels. IEEE Transactions on Image Processing, 29, 8316-8325.

[8] R. Florea and M. Craus, "A Game-Theoretic Approach for Network Security Using Honeypots," Future Internet, vol. 14, no. 12, Dec 2022.

[9] D. Gupta, S. Rani, A. Singh, and J. L. V. Mazon, "Towards Security Mechanism in D2D Wireless Communication: A 5G Network Approach," Wireless Communications & Mobile Computing, vol. 2022, Jul 2022.

[10] T. Khan, K. Singh, M. Manjul, M. N. Ahmad, A. M. Zain, and A. Ahmadian, "A Temperature-Aware Trusted Routing Scheme for Sensor Networks: Security Approach," Computers & Electrical Engineering, vol. 98, Mar 2022.

[11] W. K. Ma et al., "Equilibrium Allocation Approaches of Quantum Key Resources With Security Levels in QKD-Enabled Optical Data Center Networks," Ieee Internet of Things Journal, vol. 9, no. 24, pp. 25660-25672, Dec 2022.

[12] Fathima, N., Ahammed, A., Banu, R., Parameshachari, B. D., & Naik, N. M. (2017, December). Optimized neighbor discovery in Internet of Things (IoT). In 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT) (pp. 1-5). IEEE.

[13] M. Ragheb, S. M. S. Hemami, A. Kuhestani, D. W. K. Ng, and L. Hanzo, "On the Physical Layer Security of Untrusted Millimeter Wave Relaying Networks: A Stochastic Geometry Approach," Ieee Transactions on Information Forensics and Security, vol. 17, pp. 53-68, 2022.