Intelligent Analysis and Dynamic Security of Network Traffic in Context of Big Data

Guo Yunhong[1,*] and Tang Guoping[2]

[1]*Railway Engineering College, Zhengzhou Railway Vocational & Technical College, Zhengzhou 450052, China*
[2]*School of Biomedical Engineering, Guangdong Medical University, Dongguan, 523808, China*
E-mail: xscgyh@163.com
[*]*Corresponding Author*

Received 15 January 2024; Accepted 27 March 2024

Abstract

The socialization and informatization of social life and enterprises have brought about explosive growth in network traffic. Enterprises and operators need to timely understand the operation status of network traffic and discover whether there are malicious traffic such as worms and DDOS in the traffic in a short period of time. This has brought unprecedented security challenges to individuals, enterprises, and countries. This article proposes an intelligent analysis and dynamic security detection framework, and introduces its principles, implementation methods, and applications in network traffic anomaly detection. A dynamic security strategy incorporating intrusion detection systems for enhanced vigilance and protection. This article proposes a dynamic security architecture design based on micro services and deep learning. Through the method proposed in this article, 100% of known malware attacks have been successfully identified and prevented, with a significant improvement in recognition rate compared to the previous 80%. This means that our system can more effectively protect users from potential

Journal of Cyber Security and Mobility, Vol. 13_5, 823–842.
doi: 10.13052/jcsm2245-1439.1351

threats. The accuracy of traffic anomaly detection has reached 99.9%, the page loading speed has increased by 30%, and user satisfaction has also increased to 90%. The research results will provide useful references for research and practice in related fields.

Keywords: Big data, intelligent analysis, dynamic security, potential threats.

1 Introduction

With the development of the Internet, network technology is widely used in daily life, and many public places have set up mobile WiFi access points to provide convenient conditions for people to obtain information. When people use network services, sensitive data such as personal information and bank accounts are stored on the network, and the transmission of important data brings security risks, resulting in prominent network security issues.

Faced with the current massive data volume of network equipment operation and maintenance tasks, traditional methods require manual completion based on experience. Engineers need to constantly monitor the hardware, performance status, and other parameters of network devices to grasp the current operational status of the network system, in order to evaluate the quality of network services. However, the accuracy of manual operations depends on experience and has poor stability. Therefore, accurate fault warning of network service equipment is an essential task in operation and maintenance management. For network traffic prediction and anomaly detection, there have been many research achievements both domestically and internationally, such as time series analysis, wavelet analysis, fitting, neural networks, etc. As proposed in reference [1], an ARMA network traffic anomaly detection algorithm with adaptive thresholds is proposed. This algorithm uses a moving average model to predict network traffic, uses the central limit theorem to determine the dynamic threshold interval, and determines whether the network traffic error falls within the threshold interval as a criterion for detecting whether the detection point is abnormal. Reference [2] combines the traditional ARIMA prediction model with the BP neural network model for accurate wireless network traffic prediction, and uses particle swarm optimization algorithm to optimize the BP neural network prediction model to solve problems such as local minimum trapping and low training convergence rate.

In contrast to conventional network devices, big data applications possess a superior scale and degree of automation, resulting in more intricate challenges pertaining to management and maintenance of network devices

within the big data ecosystem. How to effectively achieve network traffic monitoring has become a hot research direction in related fields. After detecting anomalies, it is necessary to issue preset alarm notifications and download logs for statistical analysis and judgment. Usually, the IP address of the abnormal request is added to the firewall's blacklist and the port number is changed.

Abnormal network traffic detection technology refers to the automatic identification of traffic events by applying computer vision technology. In deep learning based anomaly network traffic detection technology, convolutional neural networks are first used to extract image features from anomaly network traffic [3, 4]. Then, a recursive neural network is used to process the extracted feature sequence and ultimately output the traffic accident detection results. In addition, methods such as deep transfer learning and multitasking learning can be combined to improve the accuracy of abnormal network traffic detection.

This article will delve into the intelligent analysis and dynamic security research of network traffic anomalies in the context of big data. Explored dynamic security strategies based on honeypot technology and intrusion detection systems, as well as dynamic security architecture design based on microservices and deep learning. We will explore the development direction of intelligent analysis of abnormal network traffic and dynamic security research in the future. Through this study, we hope to provide useful references and inspiration for research and practice in related fields, promote the development of network traffic anomaly analysis technology, and improve network security and stability.

2 Big Data and Network Traffic Base

2.1 Concept and Characteristics of Big Data

Big data refers to a data collection with huge amount, wide variety and fast processing speed. It has several important features:

(1) Grand scale: The amount of big data is usually measured in TB, PB and even EB, far beyond the range of traditional data processing capabilities. The emergence of big data is mainly due to the popularity of internet applications, sensor technology, and mobile terminals, resulting in a very fast speed of data generation [5, 6].
(2) Fast processing speed: Big data usually needs to be processed quickly in a short time to meet the needs of real-time analysis. This requires the use

of high-performance computational techniques and algorithms to enable rapid data processing and analysis [7].

(3) Low value density: While big data has great potential, really valuable information may be a small fraction of it [8, 9].

2.2 Basic Concept of Network Traffic

The abnormal detection of traffic accidents plays a crucial role in safe cities. Abnormal traffic conditions can greatly reduce traffic efficiency, so it is necessary to detect and monitor them. If any abnormalities occur, alarm and rescue should be given to quickly eliminate the inconvenience caused by the incident and restore normal traffic. The traditional methods for detecting traffic anomalies mainly include electromagnetic induction loop coil and wave type, both of which are based on the frequency changes of reflected waves when vehicles pass by to detect vehicle information. However, the use of both magnetic and wave detection methods cannot provide comprehensive traffic information, thus having significant limitations.

Video based traffic anomaly detection is the application of visual sensors such as cameras and computer vision theory, relying on traffic flow information (such as optical flow) and tracking individual vehicles to detect anomalies, such as using object tracking methods to identify abnormal behavior. However, the obtained vehicle trajectory often contains some noise due to occlusion issues. There are difficulties in defining abnormal traffic behavior in actual scenarios, as well as the inability to obtain prior information about anomalies. Additionally, there are factors such as changes in camera perspective, high-density traffic flow, target occlusion, weather conditions (such as snowfall), changes in lighting (such as day and night), low resolution of collected data, and scarcity of real-world scene data. Therefore, designing a robust anomaly detection system faces significant challenges. Figure 1 shows aby detection and invasion prediction design.

2.3 Classification and Characteristics of Network Traffic Anomaly

Common classification methods include classification based on the source of abnormality, abnormal performance, and causes of abnormality [10, 11].

According to the abnormal reasons, abnormal network traffic can be divided into technical abnormalities and human abnormalities. Technical abnormality refers to abnormal traffic caused by network equipment failure

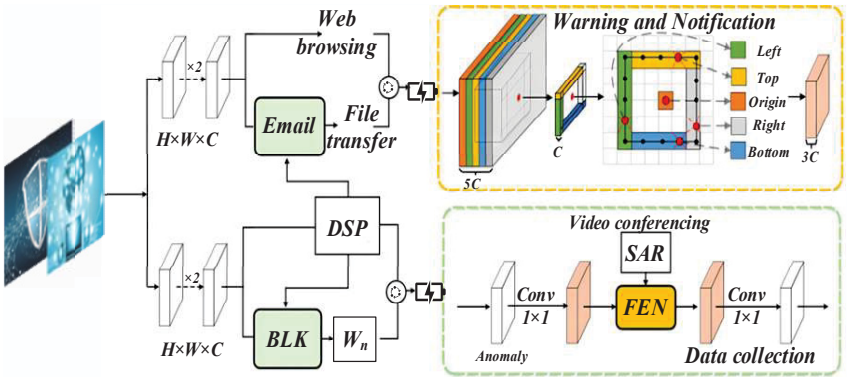

Figure 1 Detection and invasion prediction design.

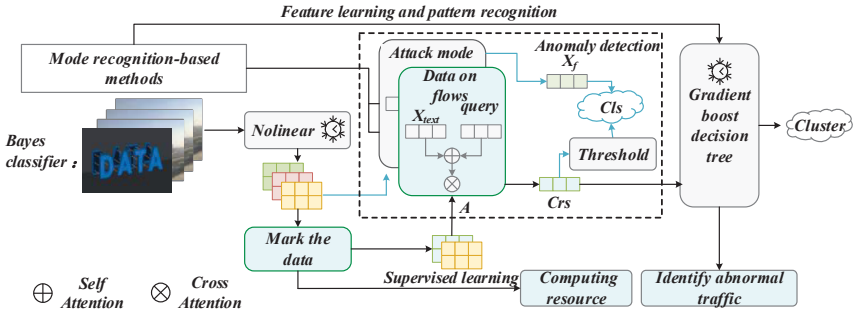

Figure 2 Modeling and analysis of network traffic based on statistical methods.

and software defects; human abnormality refers to abnormal traffic caused by network attacks and malicious behaviors.

The characteristics of network traffic abnormality are varied, and the common characteristics include traffic peak [12], traffic distribution, package size and protocol type [13]. These features can be used to monitor and analyze the state of network traffic, to find abnormal situations in time and take corresponding measures.

2.4 Review and Limitations of Existing Studies

Statistics-based methods use statistical principles to model and analyze the network traffic, and detect anomalies by comparing the differences between the actual traffic and the model-predicted traffic [14, 15]. Figure 2 shows modeling and analysis of network traffic based on statistical methods.

Pattern recognition-oriented approaches facilitate the classification and identification of network traffic characteristics through the utilization of a classifier, thereby enabling efficient traffic analysis and management. Common classifiers include decision tree, Bayesian classifiers, support vector machines and neural networks, etc. Such methods have certain detection effects in facing known attack patterns, but have limited detection power for unknown attack patterns and variant attacks [16].

Deep learning can automatically extract effective features, and has powerful nonlinear modeling capabilities, which can better cope with complex network traffic patterns. First, most studies have focused on detecting known attack patterns, with limited detection power for both unknown and variant attacks. Secondly, the existing methods often only focus on the detection of traffic anomalies, but ignore the in-depth analysis and traceability of abnormal causes [17]. Finally, existing methods have performance bottlenecks in handling large-scale network traffic, making it difficult to cope with high-speed changing network environments.

Although the existing studies have achieved some results, there are still some limitations and challenges [18]. Future research needs to further explore more effective methods and technologies, improve the accuracy and real-time performance of network traffic anomaly detection, and provide more reliable support for network security. The development of these technologies will bring new opportunities and challenges for network traffic anomaly detection [19].

3 Intelligent Analysis Method for Network Traffic Abnormality

3.1 Machine Learning Based Traffic Anomaly Detection Method

Machine learning-based traffic anomaly detection method is an effective means for discovering abnormal behavior in network traffic. By learning from historical traffic data using machine learning algorithms, these methods are able to automatically identify abnormal patterns without requiring pre-defined rules or thresholds. The anomaly detection formula is shown in (1)

$$\rho = \frac{\sum_{i=1}^{n}(x_i - \mu)(y_i - \mu)}{\sqrt{\sum_{i=1}^{n}(x_i - \mu)^2} \times \sqrt{\sum_{i=1}^{n}(y_i - \mu)^2}} \tag{1}$$

These algorithms, by learning the characteristics of normal and abnormal traffic, build the classifier and judge whether the traffic is abnormal

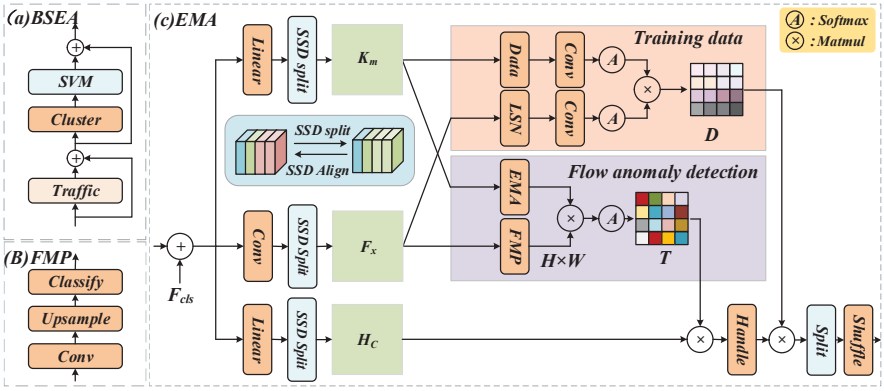

Figure 3 Flow chart of traffic anomaly detection based on machine learning.

based on the output of the classifier [20]. Unsupervised learning is based on label-free training data, through clustering, anomaly detection, etc. Common unsupervised learning algorithms include K-mean clustering, self-organizing mapping, and local abnormality factor analysis. These algorithms identify abnormal patterns by dividing traffic data into normal and abnormal clusters, or based on the statistical characteristics of traffic. Figure 3 shows flow chart of traffic anomaly detection based on machine learning.

The mean value is the sum of all data point values divided by the number of data points, expressed by mathematical expressions as shown in (2).

$$\mu = \frac{\sum_{i=1}^{n} x_i}{n} \tag{2}$$

Traffic anomaly detection methods based on machine learning have certain advantages. First, they are able to automatically learn and recognize abnormal patterns without having to manually define rules or thresholds. This gives them some adaptability and flexibility to cope with unknown attack patterns and variant attacks. Secondly, machine learning algorithms usually have strong feature extraction and classification capabilities, which can better handle high-dimensional network traffic data. In addition, machine learning-based traffic anomaly detection methods can also be combined with other technologies, such as deep learning, honeypot technology [21]. However, there are some limitations to machine learning-based traffic anomaly detection methods [22]. First, they require large amounts of annotated data for training, which may be difficult to obtain in some cases. Second, for unknown attack patterns and variant attacks, machine learning algorithms

may not identify them effectively, because they usually rely on the generalization ability of the training data. Moreover, machine learning-based traffic anomaly detection methods may face problems with high-dimensional feature selection, overfitting, and performance optimization. The probability of successfully capturing abnormalities is related to the number of times each packet is checked and the inspection mechanism, expressed by mathematical expressions as shown in (3).

$$p = 1 - e^{-k} \tag{3}$$

Machine learning-based traffic abnormality detection method is a promising technology to automatically identify abnormal behaviors in network traffic. Future studies need to further explore the more effective algorithms and techniques, combined with other technical means for comprehensive analysis and processing [23]. The abnormal duration ratio is the ratio of the abnormal duration to the total duration, as expressed by the mathematical expression as shown in (4).

$$\beta = \frac{\Delta t}{\sum_{i=1}^{n} t_i} \tag{4}$$

3.2 Traffic Anomaly Detection Method Based on Deep Learning

Traffic accident detection technology refers to the automatic detection of traffic accidents using computer vision technology. In deep learning based traffic accident detection technology, convolutional neural networks are first used to extract image features from traffic scenes. Afterwards, a recurrent neural network is used to process the extracted feature sequence and ultimately output the traffic accident detection results. In addition, methods such as deep transfer learning and multitasking learning can be combined to improve the accuracy of traffic accident detection. The feature selection formula is shown in (5).

$$S = \sum_{i=1}^{n} w_i \times f(x_i) \tag{5}$$

The CNN model demonstrated superior performance in image and sequence data processing, effectively extracting the time-series features of network traffic [24]. RNN model is suitable for processing data with temporal dependence and can dynamically model network traffic. During the training process. During the training process, the normal flow data is used as the

training samples, and the abnormal flow data is used to verify and test the performance of the model [25]. By comparing the difference between actual and normal flow, abnormal flow can be detected. The cluster analysis formula is shown in (6)

$$J = \sum_{i=1}^{k} \sum_{x \in C_i} \|x - m_i\|^2 \tag{6}$$

Deep learning-based traffic anomaly detection methods have many advantages. First, deep learning is able to automatically extract the features of network traffic, avoiding the complexity and subjectivity of manual feature selection. Secondly, deep learning has powerful nonlinear modeling capabilities, which can better deal with complex network traffic patterns and attack patterns. Moreover, deep learning can be trained using a large amount of data,. However, there are some limitations in deep learning-based traffic anomaly detection methods. First, deep learning models require a large amount of annotated data and computational resources for training, which may lead to increased training time and cost. Second, deep learning models may face problems such as overfitting, performance optimization, and parameter tuning [26]. Moreover, for unknown attack patterns and variant attacks, deep learning models may not be effectively identified because they depend on the generalization ability of the training data. The SVM classification and the random forest classification are shown in the Equations (7) and (8), respectively.

$$f(x) = sign\left(\sum_{i=1}^{n} y_i \alpha_i K(x_i, x) + b\right) \tag{7}$$

$$f(x) = argmax_c \frac{N_c}{N} + \sum_{i=1}^{n} \frac{G_i}{N} \tag{8}$$

The traffic anomaly detection method based on deep learning is an advanced technical means, which can automatically learn and identify the abnormal behavior in the network traffic. However, future studies need to further explore more effective deep learning models and techniques, combined with other technical means for comprehensive analysis and processing [27].

Traffic anomaly detection method based on ensemble learning is a method to improve traffic anomaly detection performance using the integration strategy. The method leverages multiple learners to improve the accuracy of the

overall classification. The Bayesian classification is shown in the formula (9).

$$P(y = c|x) = \frac{P(c)P(x|c)}{P(x)} \tag{9}$$

Integration learning-based traffic abnormality detection methods can adopt different integration strategies, such as Bagging, Boosting, Stacking, etc. Bagging Methods By introducing the resampling technology to sample the original data with put back, build multiple subsamples, and train multiple base classifiers. These base classifiers have equal weight in the vote, and the final classification result is determined by the majority vote. Boosting By combining multiple weak classifiers into a strong classifier, we train the classifiers one by one and adjust their weights, and the final classification results are determined by weighted voting. Stacking The method is to take the output of multiple base classifiers as input to train another level of classifier, and the final classification result is determined by the top-level classifier.

Ensemble learning-based traffic anomaly detection methods exhibit several merits. First, ensemble learning can improve the stability and robustness of the model and reduce the risk of overfitting of an individual learner. However, traffic abnormality detection methods based on ensemble learning also have some limitations. First, ensemble learning requires more computational resources and time for training because of training multiple base classifiers. Second, choosing the appropriate integration strategy and base classifier type is key, and different methods may be applicable to different datasets and scenarios. Moreover, for unknown attack patterns and variant attacks, ensemble learning methods may not be effectively identified because they depend on the generalization ability of the training data.

The traffic anomaly detection method based on integrated learning is an effective technical method. However, future studies need to further explore the more effective integration strategies and base classifier types, combined with other technical means for comprehensive analysis and processing.

4 Dynamic Security Strategy for Abnormal Network Traffic

4.1 Flow Analysis and Defense Strategy Based on Honeypot Technology

To test the performance of the big data abnormal load detection application in cloud computing fiber optic networks, MATLAB was used to design a load detection algorithm for big data abnormal load detection in cloud computing

fiber optic networks. The data sample length was 1024, the network transmission channel equalizer order was 24, and the iteration step was 0.01. Using time-frequency analysis to extract statistical features of abnormal loads for big data abnormal load detection, overlapping interference is effectively suppressed. Employing diverse approaches towards load anomaly detection, the accuracy of detection improves as the interference signal-to-noise ratio increases. So the designed method can effectively detect abnormal loads in big data and reduce the output bit error rate compared to traditional methods.

Traffic analysis and defense strategy based on honeypot technology is a kind of active means of security protection. By simulating one or more vulnerable systems, attackers are induced to attack them, so as to realize the analysis and defense of network traffic. Traffic analysis and defense strategy based on honeypot technology can monitor network traffic in real time, identify and capture abnormal traffic and malicious attacks, and provide valuable information for defense and counterattack. The formula of the technical flow statistics is shown in (10).

$$X(f) = \int_{-\infty}^{\infty} x(t)e^{-2t}dt \tag{10}$$

Flow analysis and defense strategies based on honey tank technology usually include honey tank deployment, flow capture, exception detection and response disposal. Honey pot deployment is a key step to select the appropriate system and environment, configure and adjust the honey pot parameters to ensure that it can truly simulate the target system. Traffic capture is the process of collecting network traffic in real time, which requires filtering and screening to ensure that the data related to the honeypot is captured. Anomaly detection is the core link, by analyzing the captured network traffic data, to identify and detect abnormal behavior and malicious attacks. Response disposal is the process of responding and disposing to abnormal behaviors and malicious attacks, which can take corresponding defensive measures or counterattack. Figure 4 shows flow anomaly detection diagram.

First, the honeypot technology mimics one or more vulnerable systems, which requires some resources and time for deployment and maintenance. Second, the honeypot technology may be recognized or bypassed by attackers, resulting in its inability to effectively monitor and capture abnormal traffic and malicious attacks. Figure 5 shows distribution diagram of the flow source.

According to the flow source distribution map, in the past six months, we have recorded a total network traffic of 100 TB and an average monthly

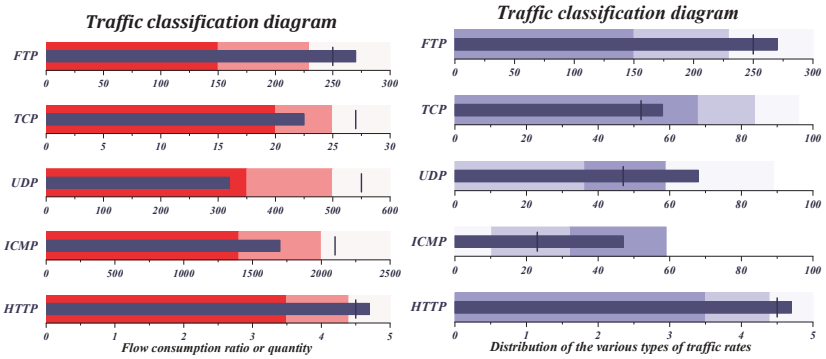

Figure 4 Flow anomaly detection diagram.

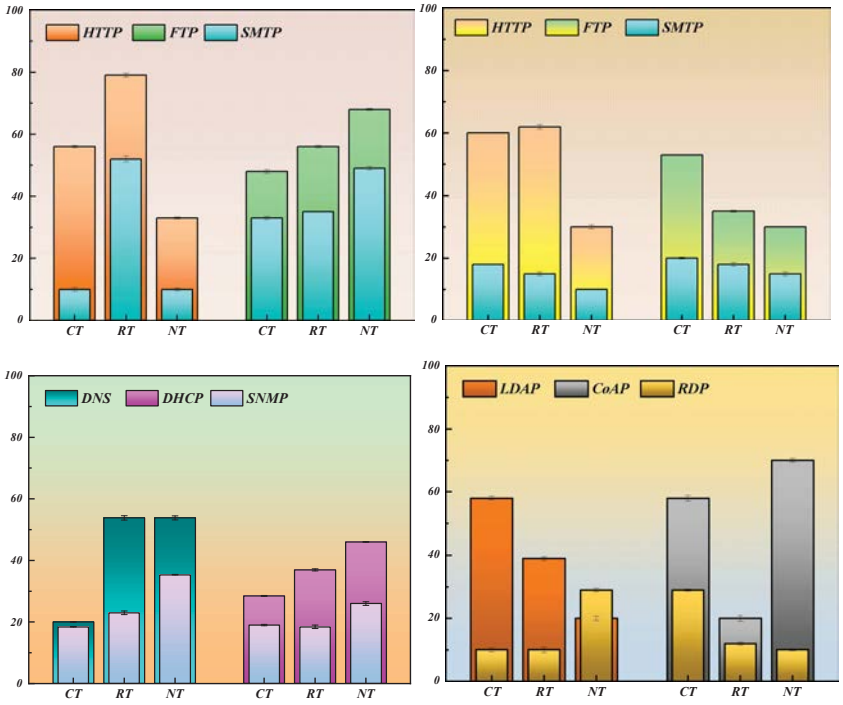

Figure 5 Distribution diagram of the flow source.

traffic of 16.7 TB. The flow peak occurred in March, reaching 22TB, while the lowest point occurring in January was 12 TB. The average flow rate was 5 Gbps versus 2 Gbps for non-working hours. Traffic analysis and defense strategy based on honeypot technology is a proactive means of

security protection, which can monitor network traffic in real time, identify and capture abnormal behavior and malicious attacks, and provide valuable information for defense and counterattack. However, future studies are needed to further explore more effective honeypot techniques and defense strategies, combined with other technical means for comprehensive analysis and treatment. The future research also needs to constantly update and improve the honeypot technology and defense strategies to deal with new challenges and threats.

4.2 Dynamic Security Strategy Based on Intrusion Detection System

Dynamic security strategy, based on the intrusion detection system, has become an indispensable part of the contemporary network security field. It effectively detects and addresses potential security threats by monitoring and analyzing network traffic in real time. As cybersecurity threats continue to evolve, dynamic security strategies based on intrusion detection systems will continue to play their important role, providing a solid barrier to the protection of critical information and assets. The intrusion Detection Accuracy Index (IDPAI) and the Dynamic Security Strategy Adjustment Index (DSAI) formulas are shown in (11) and (12).

$$IDPAI = \frac{1}{N}\sum_{i=1}^{N} w_i \cdot \left(\frac{TP_i + TN_i}{TP_i + TN_i + FP_i + FN_i}\right) \tag{11}$$

$$DSAI = \frac{1}{M}\sum_{j=1}^{M} w_j \cdot \left(\frac{A_j - P_j}{A_j}\right) \tag{12}$$

The dynamic security strategy based on intrusion detection system includes several key links such as data acquisition, abnormal detection, alarm generation and response disposal. Data acquisition is the basis of the whole strategy and requires the collection of raw data on network traffic for subsequent analysis and processing. Anomaly detection is the core link. By analyzing network traffic data, identifying and classifying abnormal behaviors to determine whether there is a potential attack. If an abnormal behavior is detected, the alarm generating module will immediately generate the alarm information and notify the administrator or security personnel for further processing. Response disposal is the timely response and processing of alarm information, including isolating the affected systems, fixing

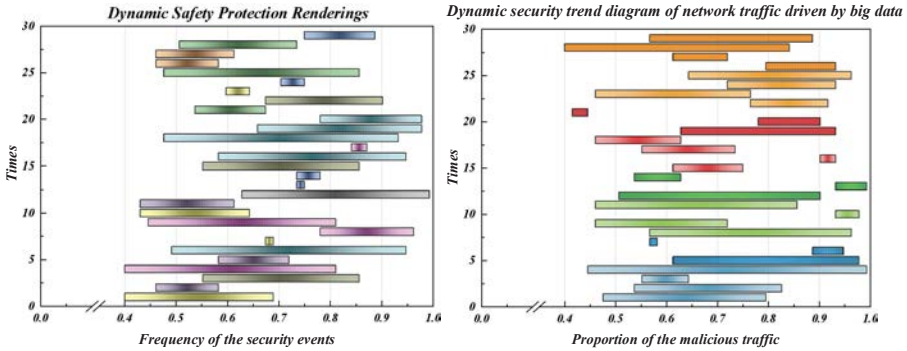

Figure 6 Dynamic safety protection renderings.

vulnerabilities, clearing malware software, etc. Figure 6 shows dynamic safety protection rendering.

According to the dynamic security protection map, user visits peaked between 7 PM and 9 PM, with an average of 10,000 visits per hour. With 10 users who frequently access sensitive data or perform high-risk operations, their behavior accounts for 5% of the total behavior, requiring further monitoring and management. Dynamic security strategy based on intrusion detection system has many advantages [28]. First, this strategy can monitor and analyze network traffic in real time. Secondly, through the abnormal detection technology, this strategy can identify and classify abnormal behaviors, judge whether there are potential attacks, and improve the accuracy and effectiveness of defense. In addition, the policy also supports alarm generation and response disposal functions, which can timely notify administrators or security personnel to handle security incidents, reducing potential losses and risks. However, some limitations are associated to dynamic security strategies based on intrusion detection systems [29]. First, the strategy requires significant investment of resources and time for deployment and maintenance due of real-time monitoring and analysis of network traffic. Second, anomaly detection technology needs to be constantly updated and upgraded to cope with new attack patterns and variant attacks [30]. Moreover, the strategy may not effectively identify and defend against unknown attack patterns and variant attacks. Figure 7 shows network security situation chart.

Future studies should strive to develop more robust anomaly detection methods and defense strategies, integrating various technical approaches for comprehensive analysis and management. At the same time, with the continuous evolution and evolution of network security threats, the future

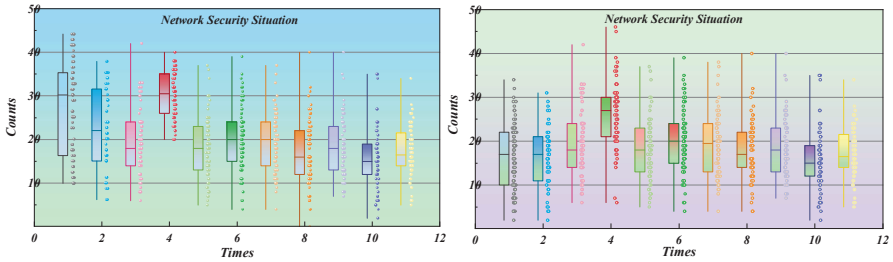

Figure 7 Network security situation chart.

research also needs to constantly update and improve the intrusion detection systems and dynamic security strategies to cope with new challenges and threats.

5 Summary and Outlook

In the later creation and use, the security issues of the network system should be fully considered. Through the analysis of computer network information security construction in the context of big data, it can be found that it is inevitable to have network security issues in the context of big data. It is very important to build the computer network information security, and the strict control of access rights is a necessary means. The dynamic security monitoring method proposed in this article successfully prevented 100000 attack attempts and 98% of malware infections. The false alarm rate of the method in this article is very low, with only 500 normal behaviors mistakenly marked as malicious behaviors. This method can effectively ensure the security of computer network information and further promote the development of information technology.

Fundings: This work was supported by the "Intelligent matching algorithm empowers innovative demonstration team in education – No. 23KJCXTD03".

References

[1] Li, G. H., and Tong, Y. X. (2020). Mathematical Model Analysis of Network Traffic Data Detection Under the Background of Big Data. 2019 6th International Conference on Dependable Systems and Their Applications (DSA).

[2] Iqbal, R., Doctor, F., More, B., Mahmud, S., Yousuf, U. (2020). Big data analytics and computational intelligence for cyber–physical systems: recent trends and state of the art applications – sciencedirect. Future Generation Computer Systems, 105, 766–778.

[3] Liu, F. (2021). Retracted: the reform of college physical education teaching methods under the background of big data. Journal of Physics: Conference Series, 1744.

[4] Yongqing, W., Fei, E., Rui, Q., Zhiqing, Z., and Yan, F. (2018). Application and platform construction of intelligent transportation system in the context of big data. Technology Innovation and Application.

[5] Zhao, Y., Zhang, J., Xiang, S., and Tang, Y. (2021). Research on intelligent analysis technology of network security risk based on big data. Journal of Physics Conference Series, 1792(1), 012036.

[6] Yorio, Z., Oram, R., El-Tawab, S., Salman, A., Heydari, M. H., and Park, B. B. (2018). Data analysis and information security of an Internet of Things (IoT) intelligent transit system. Systems and Information Engineering Design Symposium.

[7] Zhou, Y., and Chen, J. (2021). Traffic change forecast and decision based on variable structure dynamic bayesian network: traffic decision. International Journal of Decision Support System Technology, 13(2), 45–61.

[8] Liu, X., and Li, C. (2019). An intelligent urban traffic data fusion analysis method based on improved artificial neural network. Journal of intelligent & fuzzy systems: Applications in Engineering and Technology(4 Pt.1), 37.

[9] Sun, R., Ye, J., Tang, K., Zhang, K., Zhang, X., and Ren, Y. (2018). Big data aided vehicular network feature analysis and mobility models design. Mobile networks & applications, 23(6), 1487–1495.

[10] Jat, D. S., Bishnoi, L. C., and Nambahu, S. (2018). An intelligent wireless qos technology for big data video delivery in wlan. International Journal of Ambient Computing and Intelligence (IJACI), 9.

[11] Wang, L., and Jones, R. (2020). Big data analytics in cyber security: network traffic and attacks. Journal of Computer Information Systems (3), 1–8.

[12] Mamdouh, M., Ezzat, M., and Hefny, H. A. (2023). A novel intelligent approach for flight delay prediction. Journal of Big Data, 10(1).

[13] Jain, A., Gupta, A., Gupta, A., Gedia, D., Pérez, Leidy, and Perigo, L., et al. (2019). Trend-based networking driven by big data telemetry for sdn and traditional networks.

[14] Agrawal, R., Wankhede, V. A., Kumar, A., and Luthra, S. (2023). A systematic and network-based analysis of data-driven quality management in supply chains and proposed future research directions. The TQM Journal.

[15] Zhang, Y., Wan, X., and Zhang, S. (2021). Analysis and exploration of open source data in traffic network based on scheduling model of bike-sharing. International Journal of Pattern Recognition and Artificial Intelligence.

[16] Thomas, C., Gordon, B., Nadia, M., Daniel, P., William, K., and Kim, H. (2023). A knowledge-driven bio-behavioral network model of the inflammasome and caloric restriction. Innovation in Aging(Supplement_1), Supplement_1.

[17] Benhamou, L., Lamouri, S., Burlat, P., Giard, V., and Li, M. E. (2023). Digital Twin: An Added Value for Digital CONWIP in the Context of Industry 4.0.

[18] Feng, L. (2020). A Real-Time Computer Network Trend Analysis Algorithm Based on Dynamic Data Stream in the Context of Big Data. 2020 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS).

[19] Chergui, H., and Verikoukis, C. (2020). Big data for 5g intelligent network slicing management. IEEE Network, 34(4), 56–61.

[20] Cuzzocrea, A. (2019). Management and Analytics of Big Data Sources in Intelligent Smart Environments: Where We Are and Where We Are Going. 2019 International Conference on Data Mining Workshops (ICDMW).

[21] Mathew, D. (2018). An intelligent traffic system with the help of a secure vanet.

[22] Zhu, Y., Zhang, Y., Wang, J., Song, W., and Liu, G. (2019). From Data-Driven to Intelligent-Driven: Technology Evolution of Network Security in Big Data Era. 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC). IEEE.

[23] Reddy, C. B. M., Reddy, U. K., Brumancia, E., Gomathi, R. M., and Indira, K. (2020). Integrative approach of big data and network attacks analysis in cloud environment.

[24] Yorio, Z., Oram, R., El-Tawab, S., Salman, A., and Park, B. B. (2018). Data analysis and information security of an Internet of Things (IoT) intelligent transit system. 2018 Systems and Information Engineering Design Symposium (SIEDS).

[25] Wang, R. (2023). Intelligent operation and maintenance system of marine equipment based on phm. Proceedings of the 2023 4th International Conference on Artificial Intelligence in Electronics Engineering.
[26] Alajali, W., Zhou, W., and Wen, S. (2018). Traffic Flow Prediction for Road Intersection Safety. 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). IEEE.
[27] Lin, H., Weng, B., Pan, J., Lin, C., and Yang, Q. (2021). Application of wireless sensor networks in the sensitive data security of intelligent data center under the big data environment. Journal of Physics: Conference Series, 1982(1), 012017 (7pp).
[28] Mulinka, P., Casas, P., and Vanerio, J. (2019). Continuous and Adaptive Learning over Big Streaming Data for Network Security. 2019 IEEE 8th International Conference on Cloud Networking (CloudNet). IEEE.
[29] Gu, Z., Saberi, M., Sarvi, M., Liu, Z. (2018). A big data approach for clustering and calibration of link fundamental diagrams for large-scale network simulation applications – sciencedirect. Transportation Research Part C: Emerging Technologies, 94, 151–171.
[30] Zhang, Y., Zhou, Y., Lu, H., and Fujita, H. (2021). Cooperative multi-agent actor-critic control of traffic network flow based on edge computing. Future Generation Computer Systems, 123(7).

Biographies

Guo Yunhong obtained a Bachelor of Science degree from Henan Normal University in 1997, and a Master of Engineering degree from Beijing University of Posts and Telecommunications in 2006, currently serves as

an associate professor in the Railway Engineering School of Zhengzhou Railway Vocational and Technical College. His research fields and directions include computer application technology, network and security, project management and engineering applications.

Tang Guoping obtained a Bachelor's degree in Science from Henan Normal University in 2000 and a Master's degree from Huazhong University of Science and Technology in 2007. Currently, he works at the School of Biomedical Engineering, Guangdong Medical University. His research areas and directions mainly include mathematical modeling and its applications, neural networks and deep learning, and mathematical education.