Journal of Electronics and Information Science (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/jeis.2024.090210
ISSN 2371-9524 Vol. 9 Num. 2

Utilization and Security Protection of Computer Communication Technology in the Information Age

Dongyuan Ge[1,a,*], Qianyi Fang[2,b], Qi Han[1,c]

[1]State Grid Heilongjiang Information & Telecommunication Company Ltd, Harbin, Heilongjiang, China
[2]Faculty of Science, Northeast Forrstry University, Harbin, Heilongjiang, China
[a]2914756@qq.com, [b]2834300729@qq.com, [c]389025758@qq.com
[*]Corresponding author

Keywords: Network Security, Computer Communication Technology, CNN Model, Safety Protection

Abstract: With the advent of the information age, computer communication technology has been widely applied, promoting the development of various industries. However, the accompanying information security issues have attracted widespread attention. This article explored the current application status of computer communication technology in different fields, analyzed its potential threats in information security, and explored protective measures using CNN (Convolutional Neural Networks) models, aiming to provide guidance and suggestions for industry practitioners. The research structure showed that the average accuracy of the CNN model was 94.8%, significantly better than the 89.5% of the SVM (Support Vector Machine) model. The average response time of the CNN model was only 20.5 milliseconds. The average false alarm rate of the CNN model on the false alarm rate indicator was 7.2%. In the final system overhead experiment, the CNN model required a significant amount of system resources in high traffic environments. From the above data conclusions, it can be seen that the CNN model exhibited higher efficiency and accuracy in network communication security, despite the high resource demand under high load conditions.

1. Introduction

With the rapid development of information technology, computer communication technology has become the core of modern society. However, the accompanying cybersecurity threats are also constantly increasing, which is a major challenge for individuals, businesses, and even national security. Therefore, it is urgent to strengthen the security protection of network communication technology. However, traditional security measures often seem inadequate in dealing with complex and constantly changing security threats. The introduction of CNN algorithm models in this situation is crucial for improving the accuracy and response speed of threat detection.

This article provides a detailed evaluation of the performance of CNN models in network security, and finds that CNN has high performance in detection accuracy, response speed, and false alarm rate. Especially when dealing with large amounts of network traffic, CNN performs better in

system resource management. Experimental evaluations are also conducted on the system resource consumption of CNN algorithm models under different network traffic load conditions, which provides valuable data support and some practical strategy suggestions for future practical deployment and application.

The article first introduces the background and significance of the research. In the methodology phase, detailed descriptions are provided for network traffic monitoring, behavior pattern modeling, and real-time threat detection. The experimental section presents the results of various experiments, compares the performance differences between CNN and SVM models in detail, and discusses the results. The final conclusion summarizes the research findings and provides suggestions for future research directions.

2. Related Works

Many researchers have recognized the importance of this issue and are actively exploring solutions. For example, in the face of unstable cybersecurity situations, combining deep learning with intrusion detection has become a hot topic in cybersecurity today. In this context, accurately detecting abnormal traffic has become an important task in intrusion detection. Yin Shenglin proposed an intrusion detection model based on residual dual routing deep capsule network [1]. In order to solve the problems of inability to recognize new types of attacks and limited flexibility in Internet of Things (IoT) network intrusion detection systems, Wu Hao proposed a network intrusion detection system based on honey field, which can effectively identify abnormal traffic and has continuous learning ability [2]. Intrusion detection systems play a crucial role in network security. Therefore, Mallampati S B developed a new fusion based feature importance method aimed at reducing high-dimensional feature space, which helped to accurately identify attacks while reducing false alarm rates [3]. With the emergence of Industry 4.0, water treatment system is considered as one of the typical industrial network physical systems connected to the open Internet. In order to deal with network attacks on controllers widely used in water treatment systems, Liu K proposed an entropy-based intrusion detection method [4]. With the increase of Internet usage, a large amount of information is exchanged between different communication devices. Therefore, the research proposed by Thakkar A can serve as a foundation for novice researchers in the field of community and network security to understand and develop efficient intrusion detection system models [5]. Xie Zhongyang elaborated on the characteristics, integration, and application of artificial intelligence and computer network technology, covering areas such as solving system problems, ensuring network information security, intrusion detection technology, network proxy management services, network monitoring, creating computer network models, and improving firewalls [6]. Modern life is increasingly influenced by the internet, making network security an important research field. Therefore, Siva Shankar S designed a unique intrusion detection system that optimizes artificial intelligence methods to effectively identify intrusions [7]. However, currently these solutions still have limitations. For example, protective strategies are often too complex, leading to a decrease in user experience; The anomaly detection model may generate false positives, increasing management costs.

However, relevant research also provides reference for further improving information security. In recent years, the development of cloud computing technology has driven the commercialization of remote outsourced storage services. Huang Y proposed a specific construction that utilizes an efficient and retrievable verifiable delay function, and demonstrated the security of this scheme in a random oracle model [8]. With the rapid development of cloud computing, cloud storage services have also experienced rapid growth. Han H proposed a series of requirements for evaluating existing blockchain based data integrity audit schemes and evaluated them accordingly [9]. Almost

all existing data integrity verification schemes require users to upload both outsourced files and label sets to cloud service providers simultaneously. Therefore, Yuan Y proposed a new approach to build integrity verification schemes through blockchain. This scheme is based on identity based encryption, avoiding the complex certificate management brought about by public key infrastructure [10]. However, these methods also have their own shortcomings. The complexity of blockchain technology may result in higher system deployment and maintenance costs, while there is still room for improvement in user friendliness through multi factor authentication. Therefore, this article proposed an intelligent network protection method based on CNN algorithm model, aiming to identify potential security threats in a timely manner by analyzing network traffic and behavior patterns in real-time.

3. Methods

3.1 Network Traffic Monitoring

This article provides an in-depth analysis of the effectiveness of CNN algorithms for network traffic monitoring, with the aim of enhancing timely identification of potential security threats through precise analysis. The article first outlines the methods for collecting network traffic data, including how to intercept data packets from various data sources. Next, the data preprocessing process is elaborated, which includes data cleaning and feature extraction to ensure that the data is suitable for subsequent deep analysis. The features taken are not limited to conventional packet header information, such as source IP address, destination IP address, port number, and protocol type, but also extend to the specific content of the packet, such as key information such as packet length and timestamp. The learning process of CNN can be represented by Formula (1):

$$w_{i+1} = w_i - \eta \nabla L(w_i) \tag{1}$$

In Formula (1), w_i and w_{i+1} represent the weights in the i-th and $i+1$-st iterations, respectively; η is the learning rate; $\nabla L(w_i)$ is the gradient of the loss function L over the weight w_i.

This article further discusses how to use CNN to process specific network features for identifying abnormal behavior. In recent projects, a new network traffic monitoring technology is implemented. Specifically, the focus is on monitoring and distinguishing between normal and abnormal traffic - abnormal traffic is often associated with network attacks such as malware intrusion and DDoS attacks. By deploying this technology in the company's network environment, its performance in different attack scenarios is recorded in detail. The results show that this technology not only responds quickly, but also efficiently and accurately identifies and alerts various network threats, greatly enhancing network security protection capabilities [11-12].

3.2 Behavioral Pattern Modeling

In this study, the current behavior pattern is compared with the normal behavior pattern library, and two methods are found to determine whether the program's behavior is abnormal. The first method is to compare the behavior pattern of the currently running program with the behavior pattern of the normal behavior pattern library to see if it is in the normal behavior pattern library. Short sequences that do not appear in the normal behavior pattern library are considered mismatched. The degree of program anomalies is determined by recording the number of mismatched short sequences. A threshold based on the normal operating conditions of the system is set, and programs with mismatched short sequences exceeding the threshold are considered abnormal. Obviously, since the number of inconsistent short sequences is related to the length of the

considered system call sequence, it is reasonable to use the ratio of mismatched short sequences as a percentage of the total number of short sequences in the behavior pattern. In theory, when a program runs normally, two numbers must be zero. If an exception occurs, both numbers have an important jump [13].

The second method is to compare the behavior patterns generated by running the program with normal behavior patterns. Here, CNN algorithm technology can be used to enhance the accuracy of behavior pattern recognition through deep learning models. CNN analyzes a large number of data samples to learn and identify complex behavior patterns that may indicate anomalies, which not only improves recognition efficiency but also significantly improves the accuracy of anomaly detection. Through this technology, even in complex and rapidly changing data, potential abnormal behaviors can be effectively monitored and warned.

3.3 Real-time Threat Detection

In this article, the practical effects of applying Convolutional Neural Networks (CNNs) in network security management are explored through specific cases. By analyzing the performance of CNN in handling actual network traffic, some key findings are made. The performance of the system in identifying and responding to network threats, especially in detecting new complex attacks, demonstrates the importance of its deep analysis ability. How to improve the system's early warning capability and response speed is also discussed by comprehensively monitoring network data. This article provides practical suggestions on how to optimize network threat detection systems based on practical operational experience [14].

The decision engine uses Convolutional Neural Networks (CNN) as a tool to scientifically train models from core attributes to attack categories, and obtain the probability of various attacks occurring. The decision engine module is the core step in converting data features into the probability of attack occurrence. The decision engine uses learning algorithms to train classification models, and determines the type of attack and probability of occurrence of the data through the trained classification model. The decision engine fully utilizes the characteristics and core attributes of network traffic, extracts the information contained therein for attack discrimination, and provides a data foundation for multi-source fusion.

The collected data flow changes over time and arrives in real-time, with fast flow speed and short response time. However, there is a lack of a dynamic prediction model for network security situation in the big data environment, which cannot achieve real-time and accurate prediction of the global network security situation in the big data environment.

4. Results and Discussion

4.1 Testing Accuracy Experiment

The detection accuracy experiment compares the detection accuracy of CNN algorithm and SVM algorithm in network traffic classification tasks. Ten experiments are designed, and the accuracy values of the two models are recorded after the experiments. Among them, the accuracy can be represented by Formula (2):

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \tag{2}$$

In Formula (2), $\text{TP}, \text{TN}, \text{FP}, \text{FN}$ respectively represent the number of true positive examples, true negative examples, false positive examples, and false negative examples.

From Figure 1, it can be seen that in the comparison of 10 experiments, the average accuracy of

the CNN model is 94.8%, consistently maintained between 94.1% and 95.2%. The average accuracy of the SVM model is 89.5%, which remains within the range of 88.7% to 90.2% in 10 experiments, and the accuracy is significantly lower than that of the CNN model. From the above data conclusions, it can be seen that the CNN model has more advantages than the SVM model in network traffic classification tasks:

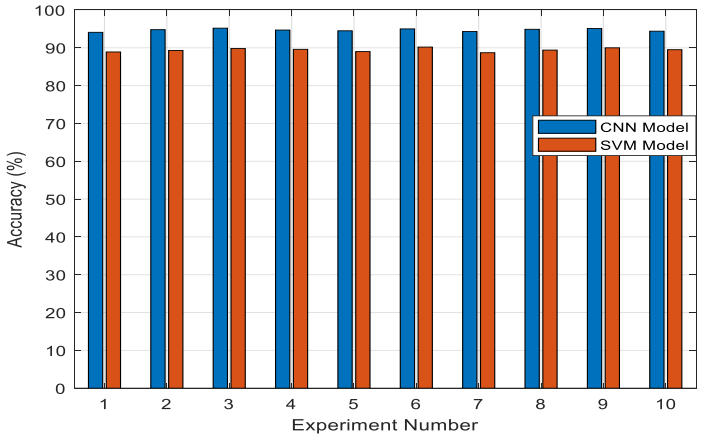

Figure 1: Evaluation of detection accuracy

4.2 Response Speed Experiment

In the response speed experiment, the time difference between CNN algorithm and SVM algorithm in threat detection and taking protective measures is compared by simulating malicious network traffic scenarios. 10 experiments are designed and the response time for each threat detection after each experiment is recorded. Then, the response time is plotted as a line graph to visually demonstrate the performance of the model's response speed. The specific data situation is shown in Figure 2:

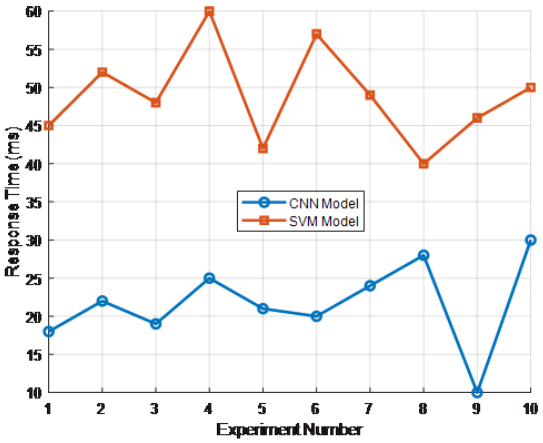

Figure 2: Response speed evaluation

From Figure 2, it can be seen that in 10 response speed experiments, the average response time of the CNN model is 20.5 milliseconds, with a response time range of 10 to 30 milliseconds. The average response time of the SVM algorithm model is 48.3 milliseconds, ranging from 40 to 60 milliseconds, significantly higher than that of the CNN model. From the data conclusion, it can be seen that the CNN model has obvious advantages in threat detection and response, and can take protective measures in a shorter time, thereby reducing the losses caused by potential threats.

4.3 False Alarm Rate Experiment

In the false alarm rate experiment, the false alarm situation of CNN algorithm and SVM model in network traffic classification is compared. The experiment designs 10 tests and records the ratio of misjudging normal network traffic as a threat each time.

From Figure 3, it can be seen that in 10 false alarm rate experiments, the average false alarm rate of the CNN model is 7.2%, fluctuating between 5% and 10%. The average false alarm rate of the SVM model is 19.3%, with a fluctuation range of 15% to 25%, which is much higher than that of the CNN model. From the data conclusion, it can be seen that CNN models have higher accuracy and lower false alarm rates in detecting normal and malicious traffic, providing more precise protection capabilities for network communication security and helping to reduce the interference of erroneous alarms on the normal operation of the system. The specific data situation is shown in Figure 3:

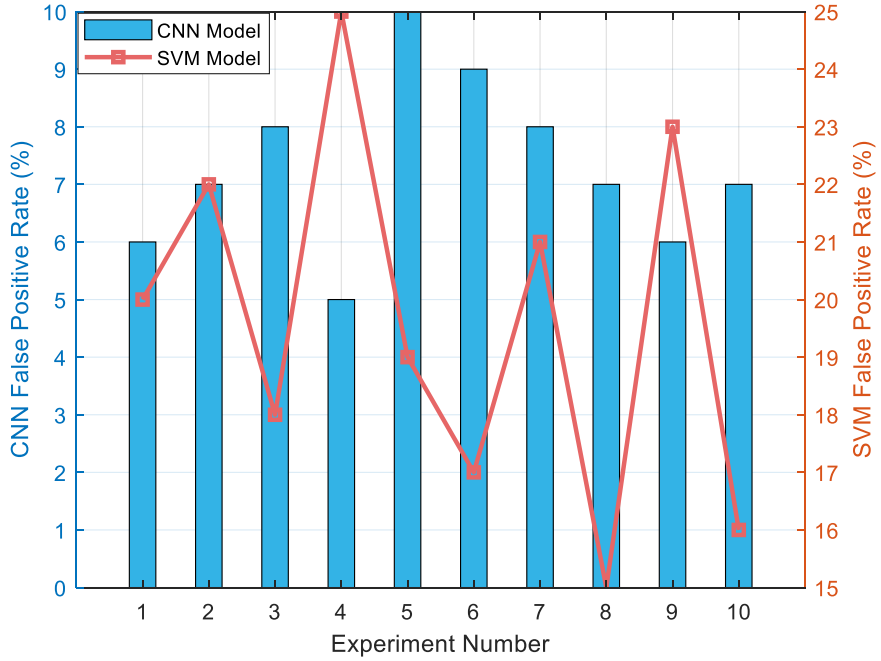

Figure 3: False alarm rate evaluation

4.4 System Overhead Experiment

The system overhead experiment involves running CNN models under different network traffic load conditions and measuring their consumption of system resources. The experimental design includes three different levels of traffic loads, aiming to evaluate the performance and resource requirements of the model in different network environments. The specific data details are shown in Table 1:

Table 1: System cost assessment

Traffic_Load	CPU_Usage	Memory_Usage	Bandwidth_Usage
Low	20%	2GB	100Mbps
Medium	50%	4GB	300Mbps
High	80%	8GB	500Mbps

From the data in Table 1, it can be seen that the CNN model increases CPU usage from 20% to

80%, memory usage from 2GB to 8GB, and bandwidth usage from 100Mbps to 500Mbps when handling low, medium, and high traffic loads. From the data conclusion, it can be seen that CNN models require significant system resources in high traffic environments and may require additional optimization or hardware support to ensure performance is not affected.

5. Conclusion

This article explored the application and security protection issues of computer communication technology in the information age, particularly using CNN models. It was compared with the SVM algorithm model, and the performance differences between the two in network security protection were analyzed in depth. Research found that CNN models were significantly superior to SVM models in terms of detection accuracy, response speed, and false alarm rate, especially in dealing with large-scale network traffic, showing higher efficiency and lower resource consumption. However, the study also pointed out that there is still room for improvement in the resource requirements of CNN models under extremely high network traffic, which may limit their application in larger scale systems. Future research can focus on exploring more efficient algorithm optimization methods to reduce resource consumption of CNN in high load environments, and consider how to combine other machine learning technologies or the latest artificial intelligence technologies to further improve the real-time and accuracy of network security protection. In addition, given the continuous evolution of network threats, continuously updating and training models to adapt to new security challenges can also be an important direction for future research.

References

[1] Yin Shenglin, Zhang Xinglan, Zuo Liyu. Intrusion detection system for dual routing deep capsule network [J]. Computer Research and Development, 2022, 59 (2): 418-429.

[2] Wu Hao, Hao Jiajia, Lu Yunlong. Research on Distributed Network Intrusion Detection System Based on Honey Field in IoT Scenarios [J]. Journal of Communications, 2024, 45 (1): 106-118.

[3] Mallampati S B, Hari S .Fusion of Feature Ranking Methods for an Effective Intrusion Detection System[J]. Computers, Materials, and Continuum (English), 2023, 76(8):1721-1744.

[4] Liu K, Wang M, Rongkuan M A, et al. Detection and localization of cyber attacks on water treatment systems: an entropy-based approach[J].Frontiers of Information Technology & Electronic Engineering, 2022, 23(4):587-603.

[5] Thakkar A, Lohiya R. A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions[J]. Artificial Intelligence Review, 2022, 55(1): 453-563.

[6] Xie Zhongyang. The application of artificial intelligence technology in computer networks [J]. Integrated Circuit Applications, 2023, 40 (1): 360-362.

[7] Siva Shankar S, Hung B T, Chakrabarti P, et al. A novel optimization based deep learning with artificial intelligence approach to detect intrusion attack in network system[J]. Education and Information Technologies, 2024, 29(4): 3859-3883.

[8] Huang Y, Yu Y, Li H, et al. Blockchain-based continuous data integrity checking protocol with zero-knowledge privacy protection[J]. Digital Communications and Networks, 2022, 8(5): 604-613.

[9] Han H, Fei S, Yan Z, et al. A survey on blockchain-based integrity auditing for cloud data[J]. Digital Communications and Networks, 2022, 8(5): 591-603.

[10] Yuan Y, Zhang J, Xu W, et al. Identity-based public data integrity verification scheme in cloud storage system via blockchain[J]. The Journal of Supercomputing, 2022, 78(6): 8509-8530.

[11] Lei N. Intelligent logistics scheduling model and algorithm based on Internet of Things technology[J]. Alexandria Engineering Journal, 2022, 61(1): 893-903.

[12] Deebak B D, Memon F H, Khowaja S A, et al. In the digital age of 5G networks: Seamless privacy-preserving authentication for cognitive-inspired internet of medical things[J]. IEEE Transactions on Industrial Informatics, 2022, 18(12): 8916-8923.

[13] Mahajan H B. Emergence of healthcare 4.0 and blockchain into secure cloud-based electronic health records systems: solutions, challenges, and future roadmap[J]. Wireless Personal Communications, 2022, 126(3): 2425-2446.

[14] Ramesh G, Logeshwaran J, Aravindarajan V. The Performance Evolution of Antivirus Security Systems in Ultra dense Cloud Server Using Intelligent Deep Learning[J]. BOHR International Journal of Computational Intelligence and Communication Network, 2022, 1(1): 15-19.