Research On Intelligent Application of Machine Learning in Next Generation Computer Network

Yixiang Wang

ICC International Department, Changchun New Oriental School, Changchun, China

wyx052566@qq.com

Abstract. As a branch of AI, machine learning (ML) provides a new idea of intelligent management for the next generation computer network with its powerful data processing and pattern recognition capabilities. ML monitors and dynamically adjusts the traffic allocation strategy in real time by establishing a model in network traffic management to avoid congestion. In terms of network security protection, ML realizes anomaly detection, attack behavior identification and adaptive protection, which improves the response ability to unknown threats. In the allocation of network resources, ML predicts traffic changes, supports personalized service recommendation, and enhances user experience and resource utilization efficiency. Although ML has a broad application prospect, the problems it faces, such as data privacy and security, algorithm selection and optimization, and interpretability, cannot be ignored. Therefore, this paper puts forward some countermeasures, such as ensuring data security, optimizing algorithm performance and improving algorithm transparency, to promote the effective application of ML in complex network environment, so as to build a more secure, stable and efficient next-generation computer network, which has important theoretical and practical significance.

Keywords: Intelligent application; Machine learning; Computer network; Network traffic management; Network security protection; Network resource allocation.

1. Introduction

From the initial local area network to today's global Internet, the computer network has undergone earth-shaking changes, not only connecting people all over the world, but also greatly promoting the progress in many fields such as economy, culture, science and technology. However, with the emergence of emerging technologies such as big data, cloud computing and Internet of Things, computer networks are facing unprecedented challenges [1]. The continuous expansion of network scale, the surge of data traffic and the increasingly severe security threats all put forward higher requirements for traditional network technology and management methods.

In this context, machine learning (ML), as an important branch of AI, with its powerful data processing and pattern recognition capabilities, provides a new idea and method for the intelligentization of computer networks [2]. ML can automatically extract the characteristics and laws of the network by learning and analyzing historical data, so as to realize the functions of real-time monitoring of the network state, intelligent management of traffic, and active protection of security. This can not only greatly improve the performance and efficiency of the network, but also effectively reduce the cost of network management and maintenance.

Therefore, it is of great theoretical and practical significance to study the intelligent application of ML in the next generation computer network. Through in-depth study on the application of ML algorithm in network traffic management, network security protection and network resource allocation, more efficient and intelligent network management methods and technologies are explored, which provides strong support for building a safer, more stable and more efficient computer network. This paper discusses the intelligent application of ML in the next generation computer network, focusing on the analysis of the principle and practical application effect of ML in network traffic management, network security protection and network resource allocation.

2. Application principle

2.1. Network traffic management

In the next generation computer network, network traffic management is a crucial link. With the expansion of network scale and the surge of data traffic, how to effectively monitor, analyze and control network traffic has become an urgent problem [3-4]. ML, with its powerful data processing and pattern recognition capabilities, provides new ideas and methods for network traffic management.

In terms of network traffic monitoring, ML can establish a network traffic model by learning historical traffic data. This model can capture the changes of network traffic in real time, including the size, direction, speed and other key indicators of traffic. By comparing the difference between real-time traffic and model predicted traffic, network administrators can find abnormal traffic in the network in time and take corresponding measures to intervene.

In the aspect of network traffic analysis, ML can deeply mine the hidden information and laws in traffic data. For example, through the clustering analysis of traffic data, similar traffic can be classified into one category, so as to better understand the composition and structure of network traffic. In addition, ML can also analyze the traffic data in time series, predict the changing trend of future traffic, and provide decision support for network planning and management [5].

In the aspect of network traffic control, ML can dynamically adjust the traffic allocation strategy according to the network status and traffic demand. By learning historical data and network status, ML algorithm can automatically identify bottlenecks and congestion points in the network, and optimize traffic paths to avoid network congestion and improve transmission efficiency. At the same time, ML can intelligently allocate network bandwidth according to users' priorities and service quality requirements to ensure the smooth operation of key services.

2.2. Network security protection

In the next generation computer network, network security protection is facing increasingly complex and changeable threats. Traditional rule-based security protection methods are difficult to deal with new attack methods, while ML technology brings new opportunities for network security protection with its powerful data processing and pattern recognition capabilities.

(1) Abnormal flow detection

Collect a large amount of network traffic data from network devices, servers, etc., including data packet size, direction, source IP address, destination IP address, port number, protocol type and other information. These raw data are preprocessed, such as cleaning, denoising and feature extraction, for subsequent analysis. Using the preprocessed data to train the ML model, the common models include decision tree, support vector machine (SVM), random forest, neural network and so on [6-7].

Through SVM algorithm, normal network traffic is marked as positive and abnormal network traffic is marked as negative, so that the model can learn the characteristics and patterns of normal and abnormal traffic. Figure 1 shows the abnormal traffic detection using SVM algorithm. The blue dots in the figure represent normal flow, while the red dots represent abnormal flow. The SVM model distinguishes these two kinds of data by finding the optimal decision boundary. This decision boundary is learned by the model in the training process, which can maximize the interval between the two types of data.

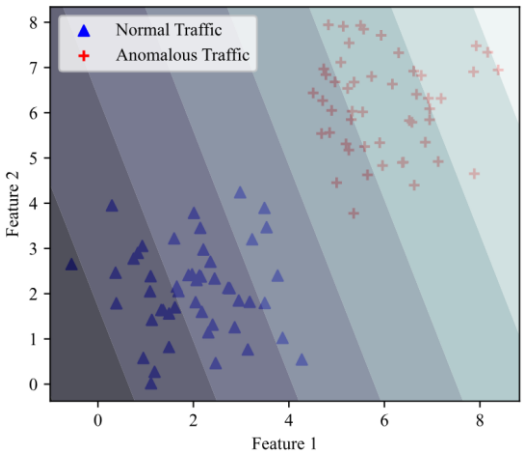

Figure 1 Abnormal traffic detection based on SVM algorithm

The trained model is applied to real-time network traffic monitoring. When new network traffic enters the system, the model will judge whether it belongs to abnormal traffic according to its characteristics. Once abnormal traffic is detected, an early warning signal is sent out immediately, so that the network administrator can take timely measures, such as blocking suspicious connections and limiting bandwidth.

(2) Attack behavior recognition

In addition to traffic characteristics, ML can also analyze the normal behavior patterns of network users and devices. Through the study and analysis of user login time, access frequency, operating habits and other data, the behavior model of users and equipment is established [8]. When users or devices in the network do not conform to the normal behavior pattern, such as accessing sensitive resources suddenly and frequently, downloading a lot of data during off-hours and so on, ML model can identify these abnormal behaviors and judge whether they are potential attacks. If a user usually only logs into the system during the daytime on weekdays, but suddenly tries to log in and transmit a large amount of data in the middle of the night, it is likely to be a sign that the account has been stolen or attacked.

Table 1 Types of network attacks and their descriptions

Attack Type	describe
Malware Attack	Including viruses, Trojans, worms, etc., by infecting computer systems, they perform malicious tasks, such as stealing information and destroying systems.
Phishing	Trick users into providing sensitive information, such as account numbers and passwords, through forged emails and websites.
Man-in-the-Middle Attack (MITM)	Intercept, tamper with or forge communication data, and obtain or tamper with sensitive information.
SQL Injection Attack	Using Web application vulnerabilities, data in the database can be obtained, modified or deleted through SQL statements.
Cross-Site Scripting Attack (XSS)	Inject malicious scripts into Web pages, execute malicious scripts and steal information when other users visit them.
DoS/DDoS Attack	A large number of requests consume the resources of the target system, making it unable to respond to normal requests, resulting in service interruption.
APT (Advanced Persistent Threat)	Long-term cyber attacks against specific targets, stealing a large amount of commercial or confidential data.
Zero-Day Vulnerability Attack	Attack by exploiting undisclosed security vulnerabilities in software.
Watering Hole Attack	Infect or set up websites that a specific user group may visit, and wait for the target to "fall into the water" to be infected.
Cryptocurrency Hijacking	Secretly use the processing power of other people's computers to mine cryptocurrencies.
DNS Attack	Use the loopholes in DNS protocol to carry out attacks such as DNS tunneling and DNS spoofing.

For the abnormal behaviors identified, ML model can further analyze their characteristics and determine specific attack types, such as DDoS attack, malware infection and phishing attack, so as to take more targeted protection measures. Different attack types are shown in Table 1.

(3) Threat intelligence integration and sharing

There are many sources of information about network security threats, including reports from security vendors, open source information, and sharing in network communities. ML can integrate and analyze these threat intelligence data from different channels, and mine the related information and potential threats. By analyzing the virus databases of several security vendors, we can find the spreading trends and characteristics of some emerging malware in different regions, so as to prepare for prevention in advance. ML algorithm is used to study and analyze the historical threat intelligence data, and to predict the new threats and attack trends that may appear in the future. At the same time, the threat intelligence database is constantly updated according to the new intelligence data, so that the network security protection system can adapt to the changing security situation in time.

(4) Adaptive protection mechanism

ML model can automatically adjust the network security protection strategy according to the change of network environment and the evolution of attack behavior. When a new attack means is detected frequently, the model can automatically increase the detection intensity and the strictness of protection rules for this type of attack; When the network traffic appears abnormal peak, the bandwidth allocation strategy is automatically adjusted to give priority to the normal operation of key services. Through continuous learning and feedback, ML model can self-optimize and evolve, and improve the detection ability and protection effect of unknown threats. With the passage of time, the model will gradually accumulate more experience and knowledge and better adapt to the complex and changeable network environment.

2.3. Network resource allocation

ML plays an important role in network resource allocation. It can predict the change of network traffic by analyzing historical data, so that resource scheduling and network optimization can be planned in advance, thus preventing network congestion. At the same time, it can also analyze users' online behaviors, such as browsing and shopping patterns, so as to provide personalized services and recommendations and enhance user satisfaction. In addition, different from the static traditional methods, ML supports dynamic resource allocation, which can be flexibly adjusted according to the real-time network environment and user demand changes, ensuring higher resource utilization efficiency and better user experience.

In the field of network resource allocation, ML algorithm optimizes resource allocation in different ways. Supervised learning uses historical data training model to predict future resource demand, such as dynamically adjusting resource allocation by analyzing the change of transmission data of resource blocks, so as to improve spectrum efficiency and system performance. Unsupervised learning focuses on the clustering and classification of network traffic, identifies different traffic patterns, and classifies users according to these patterns in order to allocate resources more reasonably. Reinforcement learning is to learn the optimal resource allocation strategy by interacting with the environment, such as using deep reinforcement learning to dynamically adjust bandwidth allocation in 5G network slice management to improve spectrum efficiency and service quality [9].

ML supports network resource optimization in various scenarios. In 5G network slicing technology, it helps build multiple logically independent virtual networks to meet diverse business needs, and dynamically adjusts network slicing configurations through decision tree models. For ultra dense networks (UDN), deep reinforcement learning is used to achieve efficient dynamic resource allocation, enhancing energy and spectral efficiency. In optical networks, improved semi supervised learning methods combined with deep packet detection techniques are used to create resource classifiers to improve the rationality of resource allocation.

3. Challenges and countermeasures

3.1. Data privacy and security

A large number of complex data processed may contain sensitive information, such as user identity, behavior habits and transaction records, which may easily lead to data leakage or malicious use without proper protection. At the same time, network attackers may also attack ML models to tamper with or steal data. In order to meet these challenges, we can take many countermeasures: including using advanced encryption algorithm and anonymous processing to ensure the security and privacy of data; Establish a strict access control and authority management system to ensure that only authorized persons can access sensitive data; And enhance the security design of the model, adopt tamper-proof technologies such as model encryption and watermarking, and set up monitoring and defense mechanisms to prevent network attacks.

3.2. Algorithm selection and optimization

It is challenging to select and optimize ML algorithm in a specific application scenario, because different algorithms have their own advantages and disadvantages and applicable scope. Wrong selection or insufficient tuning may lead to poor model performance. In order to solve this problem, we need to know the principles and characteristics of each algorithm in detail, and choose the best algorithm by evaluating its performance in specific scenes through experiments. Subsequently, parameter tuning and cross-validation are carried out to enhance the model performance and generalization ability; In addition, the ensemble learning method can be used to fuse multiple models, and the advantages of different algorithms can be integrated to improve the overall performance and stability.

3.3. Interpretability

In the complex network environment, the decision of ML algorithm is lack of interpretability, which makes it difficult for network administrators and decision makers to trust and effectively supervise these algorithms, thus limiting its application scope. To meet this challenge, we can make the decision-making process easier to understand by improving the transparency of the algorithm, simplifying the structure and clarifying the logic; Develop visual and explanatory tools, provide intuitive display of algorithm decision path and intermediate results, and enhance user trust; At the same time, the interpretable evaluation standard is established to evaluate and promote the design and development of interpretable ML algorithm in a quantitative way.

4. Conclusion

ML has demonstrated its ability to optimize network performance and user experience in network traffic management, security protection and resource allocation. By establishing an accurate traffic model, ML can monitor and dynamically adjust traffic in real time and improve transmission efficiency. In terms of security, it can detect abnormal traffic, identify attacks and integrate threat intelligence, and enhance adaptive protection against unknown threats; For resource allocation, ML uses a variety of learning methods to achieve efficient dynamic scheduling, support personalized service, prevent congestion and improve system performance. Although there are challenges such as data privacy, algorithm selection and optimization, and interpretability, we can effectively deal with them through measures such as encryption, anonymity, access control and visualization tools. The application of ML has important theoretical and practical significance for building the next generation of more secure, stable and efficient computer networks.

References

[1] Li, X., Hu, Z., Wang, H., Fu, Y., & Liu, P. (2020). Deepreturn: a deep neural network can learn how to detect previously-unseen rop payloads without using any heuristics. Journal of Computer Security, 28(5), 499-523.

[2] Wang, H., & Chen, G. (2023). Improving computer network security evaluation with grey relational analysis and probabilistic simplified neutrosophic sets. International journal of knowledge-based and intelligent engineering systems, 27(4), 425-436.

[3] Shen, G., & Li, X. (2023). A fuzzy group decision-making framework for computer network security evaluation with probabilistic linguistic information. International journal of knowledge-based and intelligent engineering systems, 27(3), 355-365.

[4] Gorbett, M., Siebert, C., & Shirazi, H. R. I. (2023). The intrinsic dimensionality of network datasets and its applications 1. Journal of computer security, 31(6), 679-704.

[5] Yang, W. H. (2020). Security detection of network intrusion: application of cluster analysis method. Computer Optics, 44(4), 660-664.

[6] Zhang, Y., Wang, H., & Stavrou, A. (2024). A multiview clustering framework for detecting deceptive reviews. Journal of computer security, 32(1), 31-52.

[7] Xu, S., Qian, Y., & Hu, R. Q. (2020). Edge intelligence assisted gateway defense in cyber security. IEEE Network, 34(4), 14-19.

[8] Yu, J., Peng, K., Zhang, L., & Xie, W. (2024). Image encryption algorithm based on dna network and hyperchaotic system. The Visual Computer, 40(11), 8001-8021.

[9] Liu, X., Xia, C., Wang, T., Zhong, L., & Li, X. (2020). A behavior-aware sla-based framework for guaranteeing the security conformance of cloud service. Frontiers of Computer Science, 14(6), 1-17.