ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)

https://doi.org/10.17559/TV-20231023001049
Original scientific paper

QoS Technology in Computer Communication Transmission Network Security under the Artificial Intelligence

Jingyuan SHENG

Abstract: This paper proposes improved models for bandwidth prediction and security protection in power communication networks. First, a queuing model integrating quality of service technology is developed for bandwidth forecasting. Second, a security model combining grey relational analysis is presented to handle network attacks. Comparative experiments validate the performance of the new models. The key findings show that the proposed bandwidth prediction model achieved 2.21 Mbit/s forecasting rate and 78.89% utilization, outperforming existing methods. The security model also demonstrated 26% and 20% improvement in recovery time after simulated network attacks, compared to traditional techniques. The research provides useful network optimization and security enhancement strategies. However, limitations include small dataset size and lack of model validation. Future work should evaluate the models on larger power network data.

Keywords: artificial intelligence; communication transmission; power computer; safety protection; service quality technology

1 INTRODUCTION

Computer communication transmission network security refers to protecting information in computer networks from unauthorized access, tampering, interruption, or disguised threats [1, 2]. With the popularization and development of computer networks, network security issues are becoming increasingly prominent. Especially in the power industry, there are still issues such as unstable power computer communication transmission networks, power network interference, and virus intrusion [3]. Therefore, it is extremely important that the research theme lies in improving the security and efficiency of power computer communication transmission network. As digitalization and networking accelerate, power systems are increasingly dependent on stable and reliable data communication. Effective bandwidth management and enhanced network security measures are essential to ensure the continuous operation of power systems and prevent potential network attacks. Most of the existing research focuses on specific aspects of network security, such as data encryption and protocol security, but tends to neglect the comprehensive improvement of network performance and security. In addition, traditional research lacks performance guarantee for power computer communication transmission networks in high load and complex scenarios. In view of this, the goal of this research is to fill this research gap by developing advanced network defense techniques, optimizing data transmission methods, and applying artificial intelligence to enhance network management and resilience. By combining QoS technology, the performance and security of power computer communication transmission networks can be improved in complex application environments. The novelty of the research lies in the introduction and improvement of QoS techniques and the development of novel bandwidth prediction model and security protection model. These models not only optimize the data transmission efficiency, but also enhance the network resistance against security threats [4]. Through experimental verification, these models show better performance than similar models in terms of bandwidth prediction rate and utilization rate, and network attack response time. The significance of improving the security of electric power communication networks goes far beyond the technical level. It is the key to ensuring the stability of national energy infrastructure, sustained economic development, and public safety. Electricity is the lifeline of modern society. The security of communication networks directly affects everyone's daily life and various aspects of social operation. Therefore, the study aims to address several key issues, namely strengthening network attack defense, enhancing the reliability and efficiency of data transmission, coping with large-scale data processing challenges, enhancing system resilience and adaptability, and developing intelligent security monitoring and management systems. Through these measures, the study expects to significantly improve the security and performance of power networks to support national energy security and stable economic and social development [5]. Based on emphasizing the importance of communication network security in the electric power industry, the key innovation of this research is to propose a bandwidth prediction model and a security protection model incorporating QoS technology. This innovation is that it not only improves the data transmission efficiency and bandwidth utilization of the power computer communication network, but also significantly enhances the network's defense capability against various network threats through advanced security protection strategies. This dual approach combining bandwidth management and security protection provides a comprehensive security and performance optimization scheme for power communication networks. It represents an important technological advancement in the field of communication network security in the power industry. The main contribution of the research is to propose a novel bandwidth prediction model and security protection model, which combine QoS techniques. By optimizing the queuing models of power computer communication transmission networks, these models significantly improve the bandwidth prediction efficiency and security of the network. Experimental results show that the new bandwidth prediction model outperforms the existing models in terms of bandwidth prediction rate and utilization. Meanwhile, the security protection model effectively reduces the recovery time of data transmission during network attack, thus significantly improving the performance and security of the power computer communication transmission network. Computer communication transmission network security is a broad and important field. This study focuses on protecting data, information, and communication devices in computer networks and communication transmission from various threats and attacks. In recent years, many domestic and foreign researchers have also conducted extensive explorations in this field. Grid communication security can be broadly categorized into the following four key technology areas, namely network data transmission and storage security, industrial computer communication network security, wireless local area network security and anomalous data detection. In the research of network data transmission and storage security technology, Zhao M. et al. proposed a bipolar fuzzy interaction multi criteria decision model using the cumulative prospect theory. It demonstrated the effectiveness of multi-criteria decision models in dealing with network security problems. However, such models may face data processing complexity and high computational costs in practical applications [6]. In the research of industrial computer communication network security technology, Shim K. S. et al. found many dangers in the existing industrial computer communication networks while performing task transmission. Therefore, a field extraction prediction method for industrial communication network protocol structure is proposed. Experimental results show that the method can derive command and protocol structures used in industrial environments, thereby improving the prediction efficiency for different network security issues [7]. However, the method may not be sufficient for more sophisticated forms of cyber attacks, such as advanced persistent threats. In the research of wireless local area network security technology, Yan Z. et al. proposed a mutual authentication method incorporating cryptography to ensure security during data sharing in wireless local area networks. The method achieves double-ended data confidentiality protection by providing ease of use, anonymity and fine-grained access control permissions. The experimental results show that the security utility of the new method proposed in the study is high, which can satisfy the existing data sharing protection in wireless local area networks [8]. However, this approach may face management and performance challenges when deployed on a large scale. In the research of anomaly data detection technology, Gajewski M. et al. proposed a strategy for anomalous data detection to avoid traffic variations, packet corruption, and increased message traffic during network data transmission in building automation systems. The experimental results show that this new detection strategy can better handle the data fluctuation between the service client and the network provider, and provide timely feedback [9]. Although the strategy has application value in data anomaly detection, it may have limitations in detecting complex network attack patterns. Service quality technology is a set of methods and mechanisms used to manage and optimize data transmission in computer networks. The main goal of this technology is to ensure that data transmission in the network meets specific performance and service requirements, such as bandwidth, latency, jitter, reliability, etc., to meet the needs of different applications and services. From the perspective of QoS technology application research, the performance and quality of service of a network can be significantly improved by optimizing data transmission management. For example, the power allocation strategy of Shili M. et al. and the feedback mechanism for mobile edge computing of Aghdam B. M. J. et al. demonstrated the potential of QoS in improving network efficiency. Shili M. et al. proposed a defined power allocation strategy between users to reduce the detection complexity of non orthogonal multiple access schemes and ensure the quality of service for users. The experimental results show that the new strategy proposed in the study is more robust than traditional methods. When the channel is uncertain, it can minimize performance loss [10]. Aghdam B. M. J. et al. proposed an effective feedback mechanism combining Qos technology and server resource manager to reduce the complexity of mobile edge computing and achieve local optimal solution. The experimental results show that this mechanism can effectively meet user service quality constraints and significantly improve system throughput [11]. Fernandez S. A. et al. proposed an intervention strategy that can allocate service quality thresholds to each potential hub to explore the impact of telecommunications network latency on video signals. The experimental results indicate that this strategy has more effective execution and allocation effects compared to traditional intervention methods. It can significantly reduce losses caused by network latency [12]. Li L. et al. proposed a cloud service quality evaluation framework based on service performance and scalability as reference indicators to focus on node service quality evaluation in cloud service systems. The experimental results indicate that this framework can quickly and stably quantitatively evaluate the service capabilities of resource nodes in cloud service systems. It provides a favorable foundation for resource allocation [13]. Overall, although existing research has made progress in grid communication security and QoS approaches, there are still some limitations. For example, traditional network security solutions tend to focus on a single security threat and neglect network performance optimization, thereby improving security and potentially reducing data transmission efficiency. In addition, many approaches lack flexibility in dealing with complex network environments and cannot effectively adapt to changing network conditions and attack patterns. For bandwidth management, traditional methods are often insufficient to predict and adapt to changes in network traffic in real time, resulting in a failure to optimally allocate network resources. To address these limitations, the bandwidth prediction and security model proposed in the study aims to provide a more comprehensive and dynamic solution. By incorporating QoS techniques, the bandwidth prediction model is able to adjust and optimize network resource allocation in real time, improving the efficiency and stability of data transmission. This dynamic prediction mechanism adapts to changes in network conditions, ensuring optimal bandwidth utilization at any given moment. Meanwhile, the security protection model employs advanced algorithms to identify and defend against various network threats, i.e., distributed denial-of-service attacks. This comprehensive security strategy not only enhances the defense capability, but also ensures that network performance is not sacrificed while enhancing security.

2 RESEARCH METHOD

To improve the performance of the power transmission communication network security protection model, the first section elaborates the existing network data transmission queuing model. Subsequently, improvements are made to propose a new bandwidth prediction model. The second part applies the new bandwidth prediction model to the security protection of power data transmission networks.

2.1 Bandwidth Prediction Model

With the continuous improvement of digitalization and networking in the power system, the power computer transmission communication network is facing more network security threats [14]. However, power communication networks in different scenarios have different transmission methods for power communication. Therefore, to improve pertinence, taking smart parks under the background of artificial intelligence as the research object, the transmission security in the power computer communication network of smart parks is investigated. As the number of terminals increases, there are still certain threats to the power computer communication transmission network. The existing security protection system for the power computer communication network in the smart park is shown in Fig. 1.

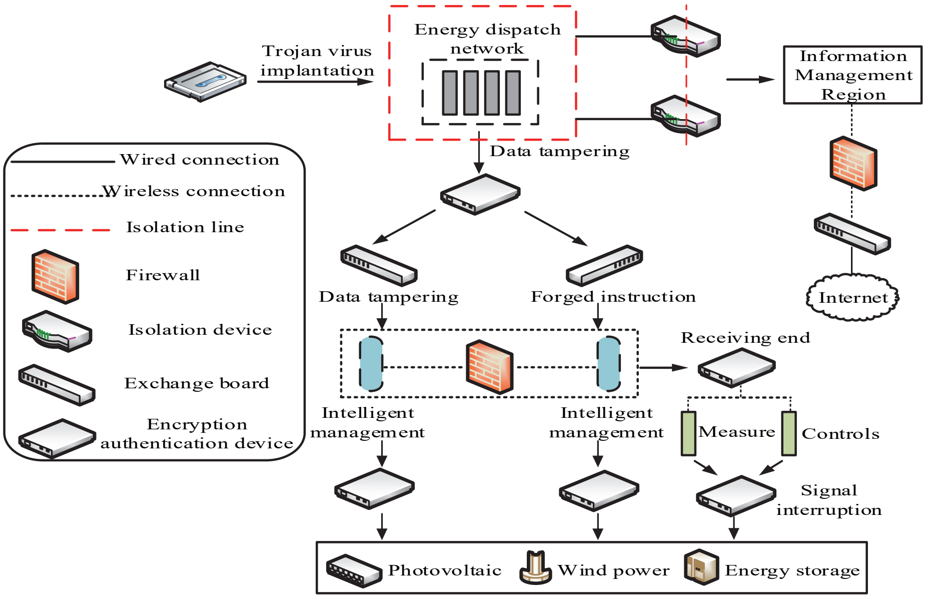


Figure 1 Smart park power computer communication transmission network security protection system

In Fig. 1, there is frequent business interaction in the power computer communication transmission network of the smart park. In the information exchange of these power business operations, personnel violations, vulnerabilities in operating systems and databases, and Trojan program injection can cause signal interruptions in the power communication network, ultimately resulting in incalculable economic losses [15]. Based on the above issues, the commonly used processing method is to group and queue various data services in the transmission of power computer communication systems, making the data independent of each other. The parameters mainly include packet arrival rate, forwarding rate, and number of windows. The average arrival time at the arrival rate is shown in Eq. (1).

$$\frac{1}{\lambda}=\int_0^{\infty} taA(t)=\int_0^{\infty} ta(t)\mathrm{d}t \tag{1}$$

In Eq. (1), λ represents the rate at which the data packet has reached. t represents the time when the packet arrived. $a(t)$ represents the probability density of reaching the rate. $A(t)$ represents the distribution function of the arrival rate. $\frac{1}{\lambda}$ represents the average arrival time. The forwarding rate is shown in Eq. (2).

$$\frac{1}{\mu}=\int_0^{\infty} taB(t)=\int_0^{\infty} ta(t)\mathrm{d}t \tag{2}$$

In Eq. (2), $B(t)$ represents the distribution function of forwarding rate. $b(t)$ represents the density function of the forwarding rate. $\frac{1}{\mu}$ represents the average forwarding time. There are three processes in which the state of a queuing system changes over time. The calculation method for not having any data packets arrive or transfer at a given time is shown in Eq. (3).

$$P_k(t+\Delta t)=P_k(t)(1-\lambda_k\Delta t-\mu_k\Delta t) \tag{3}$$

In Eq. (3), Δt represents an extreme time. $P_k(t)$ represents the probability distribution of state k at time t. λ_k and μ_k represent fixed constants. When a packet arrives within a given time without being forwarded, the calculation method is shown in Eq. (4).

$$P_k(t+\Delta t) = P_{k-1}(t)(\mu_{k-1}\Delta t) \tag{4}$$

In Eq. (4), $P_{k-1}(t)$ represents that the queuing system state at time t as $k-1$. When a packet is forwarded but no packet arrives within a given time, the calculation is shown in Eq. (5).

$$P_k(t+\Delta t) = P_{k+1}(t)\mu_{k+1}\Delta t \tag{5}$$

In Eq. (5), $P_{k+1}(t)$ represents that the queuing system state at time t as $k+1$. Combining these three queuing system states and the established emerging businesses, the burden on the queuing system will increase. Therefore, the Poisson model is introduced. The data service queuing framework in the power computer communication transmission network of the smart park under this model is shown in Fig. 2.

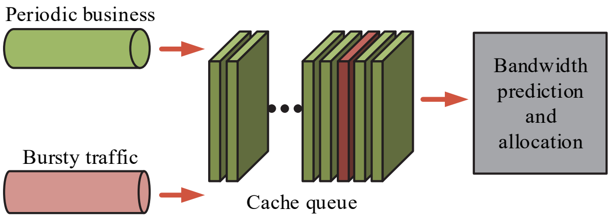


Figure 2 Data service queuing framework

From Fig. 2, two representative business data are transmitted through the loose mooring process and the interrupted loose mooring process, respectively. After reaching the queuing cache stage, the operation is performed by bandwidth prediction and bandwidth allocation. To better predict each business bandwidth and achieve the business data resources adaptation in the power computer communication transmission network of the smart park, Qos technology is introduced. The system forwarding rate during the service process is set to a fixed value. The data flow is analyzed. The state transition of the queuing system in the business data transmission network integrating Qos technology is shown in Eq. (6).

$$P_0 = \sum\nolimits_{k=0}^{c-1} \frac{(cp)^k}{k} + \frac{(cp)^c}{c} + \frac{(1-\rho^{n-c+1})}{1-\rho} \tag{6}$$

In Eq. (6), c represents the number of edge network associations in the system. λ represents the rate at which business data packets arrive. μ represents the packet forwarding rate of a single edge network for business data. n represents the maximum value of the configuration node. k represents the system status. ρ represents the ratio of data arrival rate to forwarding rate. The probability of state transition overflow in this system, i.e. the packet loss rate of data packets, is shown in Eq. (7).

$$P_{loss} = \sum\nolimits_{k=\gamma}^{n} P_e P_k = \sum\nolimits_{k=\gamma}^{n} \frac{k}{n} P_0 \tag{7}$$

In Eq. (7), γ represents the group cache threshold. P_e represents the data transfer status of business e. P_k represents the data transfer status of the business k. After the data packet arrives, the average queuing time is shown in Eq. (8).

$$T_s = \frac{L_s}{\lambda_e} \tag{8}$$

In Eq. (8), L_s represents the time when the business data arrived. λ_e represents the rate at which business packet packets arrive. The bandwidth prediction, i.e. the system utilization rate, is shown in Eq. (9).

$$\eta = \frac{\lambda_e}{c\mu} \tag{9}$$

In Eq. (9), μ is the forwarding rate. In summary, the study proposes an improved queuing model for accurately predicting the bandwidth requirements of power computer communication networks. This model takes into account key parameters such as packet arrival rate, forwarding rate, and number of windows. In particular, the model employs deep learning techniques to analyze historical data and predict future bandwidth demand, thus achieving more efficient network traffic management. The flow of the model is shown in Fig. 3.

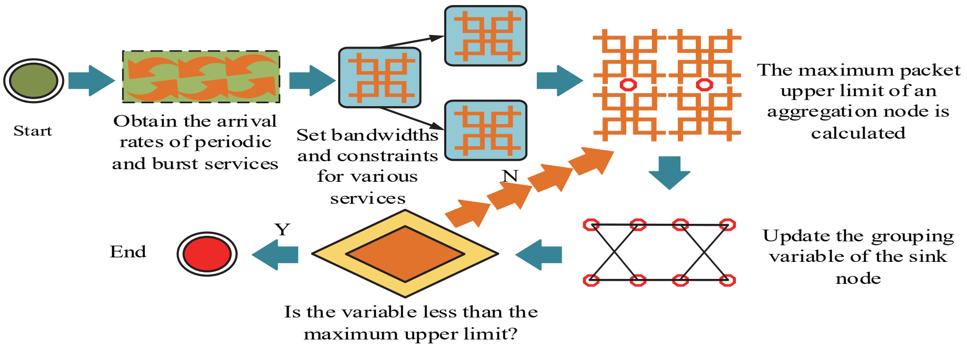

Start
Obtain the arrival rates of periodic and burst services
Set bandwidths and constraints for various services
The maximum packet upper limit of an aggregation node is calculated
Update the grouping variable of the sink node
N
Y
End
Is the variable less than the maximum upper limit?

Figure 3 Power computer communication transmission network bandwidth prediction process

In Fig. 3, the arrival rate of each type of power service is first obtained. The transfer probability of each state is calculated and determined. Then the packet loss rate and delay rate of each service are calculated respectively. The sampling interval and constraints for bandwidth prediction are set. The maximum upper limit of the packet cache variable value is adjusted. Then the bandwidth utilization rate and bandwidth prediction value for each service combination are calculated separately. The packet variable of the aggregation node is updated. If the variable is smaller than the maximum cached packet limit, the calculation is repeated again to determine the bandwidth utilization and bandwidth prediction value. If the variable is greater than the cached maximum packet limit, it is directly output. In addition, the main key parameters of this novel bandwidth prediction model include a packet arrival rate of 20 packets per second, a service rate of 25 packets per second, a queue length of 50 packets, and a 5 - minute time window. The model training process includes collecting historical network traffic data, performing data preprocessing and feature selection, and constructing a time series prediction model using neural networks. Cross validation is used for training and validation, followed by parameter adjustments based on the validation results. Finally, model performance is validated on an independent test set. For the bandwidth prediction model, important parameters include data arrival rate, forwarding rate and cache window size. These parameter adjustments should be based on an in-depth understanding for historical data and current trends in network traffic. Specifically, the data arrival rate needs to be set to reflect the actual situation of network traffic. The forwarding rate should take into account the network carrying capacity and historical performance. The cache window size adjustment aims at balancing the delay and data packet loss rate to optimize the efficiency and stability of the overall network transmission.

2.2 Construction of Power Grid Security Model

Combined with the above queuing model optimization design of the power computer communication transmission network, it optimizes the resource adaptation to a certain extent. The bandwidth prediction efficiency of the power business has been improved, ensuring the safe operation of the power computer network in the intelligent park. To implement network security protection more accurately, it is difficult to realize the correlation analysis of abnormal network attack events based on a single Qos technology. Therefore, based on bandwidth prediction, the Grey Relational Analysis (GRA) algorithm is introduced for auxiliary analysis [16]. The algorithm is mainly used to identify and analyze the correlation of abnormal events in the network. It is also effective in analyzing and assessing the relationship strength between different factors in complex datasets. In the field of network security, it is used to identify abnormal behaviors or potential network attack patterns. Specifically, the GRA algorithm first preprocesses the collected anomalous event data, including normalization to eliminate the effects of different data scales and ensure that the data is compared on the same benchmark. The algorithm measures the similarity or correlation between data sequences by establishing a Gray correlation. A high grayscale correlation indicates a greater similarity or correlation between two sequences. The application of the GRA algorithm in the security protection model of the electric power computer communication transmission network can be interpreted as first collecting and standardizing data on network attack events. Then, the GRA algorithm is applied to establish a correlation analysis model to identify abnormal events in the network by calculating the correlation between the data. Once potential security threats are identified, appropriate security measures are taken for response and prevention, such as strengthening firewalls, updating security policies, or implementing network isolation. The correlation analysis framework for abnormal events in the power computer transmission network of a conventional smart park is shown in Fig. 4.

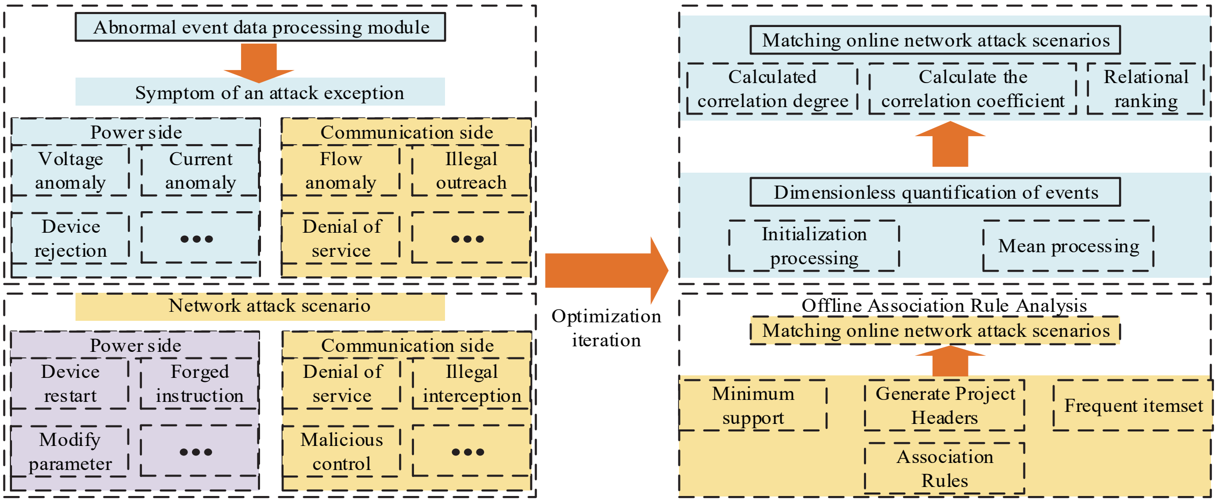


Figure 4 A framework for analyzing the correlation of network abnormal events

In Fig. 4, the framework divides the entire power computer transmission network of the smart park into three parts, namely online network attack scenario matching, offline association rule analysis, and abnormal event data processing modules. The attribute matching is specifically manifested by collecting data related to network attacks, such as attack type, time, frequency, etc. Then the data are standardized to establish reference sequences, such as common attack patterns and comparison sequences and other collected data. In addition, generating rules are analyzed by calculating the correlation between reference sequences and comparison sequences to analyze their similarity or correlation. Then, based on the relevant results, it is determined whether it matches a certain known attack pattern. The preprocessing module for abnormal event data has the heaviest component. It is also the most critical part. This module guides the data association by obtaining event feature data. The set of event characteristic factors is shown in Eq. (10).

$$X=\{S_i, A_i, O_i\} \tag{10}$$

In Eq. (10), O_i represents the data source object. A_i represents the abnormal manifestation of network attacks. S_i represents an attack scenario. There are generally 9 types of abnormal manifestations, including voltage anomalies, current anomalies, and device mis-operation [17]. There are also 9 types of attack scenarios, including session hijacking, device modification, and device locking. These three major categories of factors establish attack correlation matching modules. The correlation analysis between the characteristic factors is shown in Eq. (11).

$$\begin{cases} X_i = X_i(k)\big|k=1,\,2,\,\cdots,\,9 \\ Y=Y(k)\big|k=1,\,2,\,\cdots,\,n \end{cases} \tag{11}$$

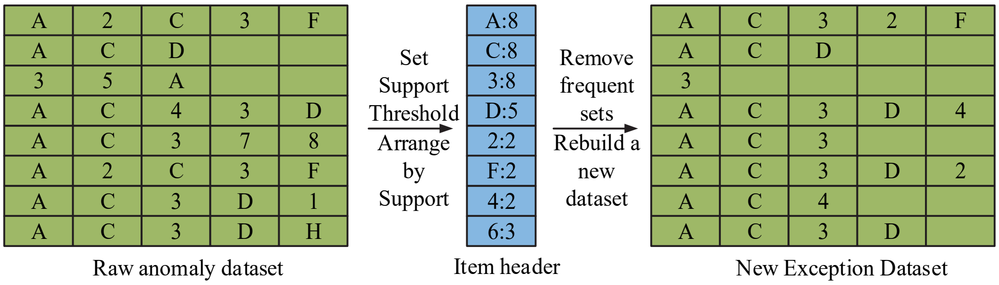
In Eq. (11), X_i represents the abnormal event attribute set. Y_i represents the reference attribute set for each factor. t represents the time. i represents different attributes in the attribute set. Each factor belongs to a different category. Therefore, to conduct correlation analysis, these factors need to be dimensionless first. This process is shown in Eq. (12).

$$x_i(k)=\frac{x_i(k)}{x_i(1)},\ k=1,\,2,\,\cdots,\,n;\ i=0,\,1,\,2,\,\cdots,\,9 \tag{12}$$

The interpretation of all algebraic variables in Eq. (12) is the same as that in Eq. (11). After dimensionless processing, the correlation coefficients for each time period are shown in Eq. (13).

$$\zeta i(k)=\frac{\overset{\min\min}{i\quad k}\left|y(k)-x_i(k)\right|+\rho\ \overset{\max\max}{i\quad k}\left|y(k)-x_i(k)\right|}{\left|y(k)-x_i(k)\right|+\rho\ \overset{\max\max}{i\quad k}\left|y(k)-x_i(k)\right|} \tag{13}$$

In Eq. (13), $\zeta_i(k)$ represents the correlation coefficient. The interpretation of other algebraic variables is consistent with the previous equation. After processing, 9 abnormal manifestations are marked in 1 - 9 order. 9 attack scenarios are marked in A-I order [18]. After random combination, the correlation screening is performed. The correlation scanning process of abnormal event data is shown in Fig. 5.



A	2	C	3	F
A	C	D		
3	5	A		
A	C	4	3	D
A	C	3	7	8
A	2	C	3	F
A	C	3	D	1
A	C	3	D	H

Raw anomaly dataset

A:8
C:8
3:8
D:5
2:2
F:2
4:2
6:3

Item header

A	C	3	2	F
A	C	D		
3				
A	C	3	D	4
A	C	3		
A	C	3	D	2
A	C	4		
A	C	3	D	

New Exception Dataset

Figure 5 Scanning process of abnormal event data in network attacks

In Fig. 5, the original abnormal event data is scanned and filtered to obtain the item header event. After filtering through Grey correlation, the frequent occurrence of abnormal data is removed. Finally, a new dataset of abnormal events is established for the remaining header data. In summary, the calculation process of Grey correlation degree is as follows. Firstly, the difference between the reference sequence and the comparison sequence is calculated to form the difference sequence. Secondly, the difference sequence is dimensionless to eliminate the effect of data size. Then, the correlation coefficient between the reference and comparison series is calculated using the GRA formula. This value reflects the similarity degree between the two. Finally, the correlation degree between the two is evaluated by analyzing the correlation coefficient. A higher correlation coefficient indicates a higher correlation degree. The attribute correlation degree of each event in the whole process is shown in Eq. (14).

$$r_i=\frac{1}{n}\sum\nolimits_{k=1}^{n}\zeta_i(k),\ (k)=1,\,2,\,\cdots,\,n \tag{14}$$

In Eq. (14), r_i represents the correlation degree of different events. Based on the analysis of the abnormal event determination method and network attack correlation proposed in the above section, a security protection strategy model for the communication and transmission of the entire smart park power computer network is proposed. The network attack response strategies of this model for different attack scenarios are shown in Fig. 6.

From Fig. 6, the network attack defense techniques on the master side include IP address management, identity authentication, data transmission encryption and network isolation. The network attack defense techniques on the communication side include bandwidth restriction, data filtering, bandwidth resource adjustment and certificate verification. The network attack defense techniques on the terminal side include address encryption, access authorization and device isolation. Each module operates independently, connects to each other, and together forms a security barrier for the entire power computer communication data transmission network. The security protection model combines machine learning algorithms and GRA. The key parameters include an anomaly detection threshold of more than 30 login attempts per minute, a 10 minute time window, and a Gray correlation threshold of 0.8. In addition, the training steps of the model include collecting historical security event data, feature engineering, modeling with machine learning classifiers, training with historical data and identifying security threats through GRA. Then, the model is validated on some data and deployed to a real network for real-time monitoring and defense. For the network security protection model, the key parameters involve the correlation threshold, the sensitivity of anomaly detection, and the specific response strategy. The correlation threshold needs to be carefully balanced between the false alarm rate and the leakage detection rate, based on a careful analysis for historical attack patterns and current network state. In addition, the sensitivity of anomaly detection should be adjusted according to the security threats and attack frequency faced by the network to improve the detection accuracy. Finally, response strategies must be formulated to address the specific needs and security requirements of the network, including measures such as traffic restriction and source address blocking to effectively respond to various security challenges.

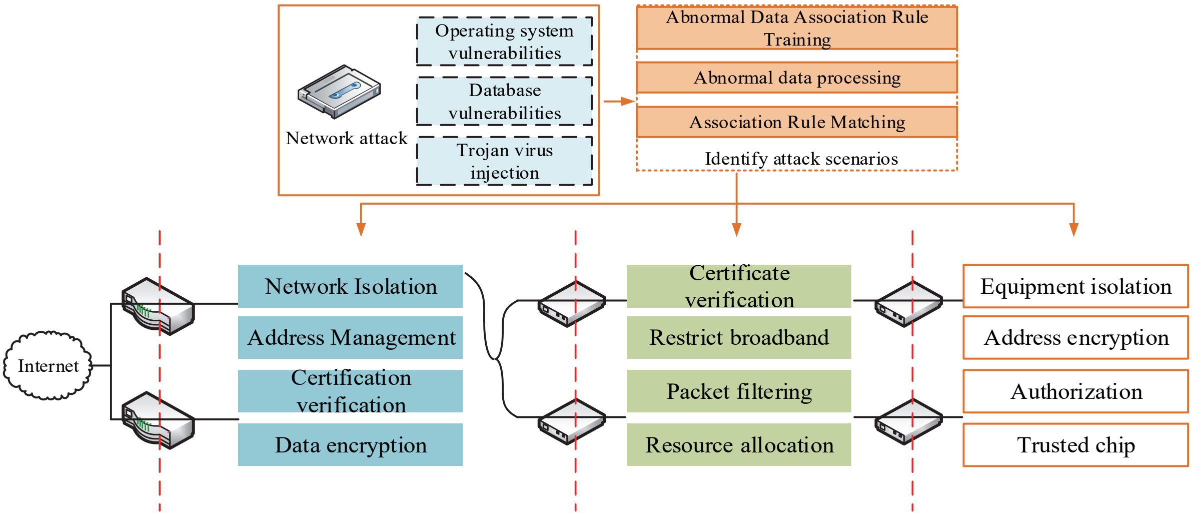


Figure 6 Network Protection Strategies in Different Attack Scenarios

3 RESULTS AND DISCUSSION

The study successfully developed innovative bandwidth prediction and security protection models that significantly enhance the performance and security of power communication networks. Using advanced AI techniques, the bandwidth prediction model performs well in high-traffic environments, while the security protection model effectively identifies and defends against a variety of cyber-attacks, especially in reducing false alarms. These results demonstrate the great potential of applying AI techniques in power communication networks and lay the foundation for future advances in network technology.

3.1 Performance Testing of the Bandwidth Prediction Model for Power Communication Networks

The testing of the bandwidth prediction model is centered around a real dataset of the power system communication network. Therefore, the study adopts the network traffic dataset from the UCI machine learning library as the experimental dataset, which contains more than 50,000 information attacks about network traffic, bandwidth usage, network delay and packet transmission. According to the 8:2 ratio, the model is divided into a training set and a testing set. Firstly, the model is trained using historical network traffic data to understand the patterns and trends of network traffic. Then, to evaluate the prediction accuracy and robustness of the model, a test dataset different from the training set is used for validation. Finally, the performance is evaluated considering several key metrics, including accuracy, latency, and packet loss. This series of tests ensures the effectiveness and adaptability of the bandwidth prediction model in real-world applications. This testing approach aims to evaluate the model's ability to predict new data while comprehensively evaluating the model's performance through multi-dimensional metrics such as accuracy, latency, and packet loss. This testing method can ensure the accuracy and reliability of the model in real-world applications in power communication networks. Four different types of intelligent distribution rooms are used as experimental environments. There are 5 distributed businesses, 6 collection businesses, 2 control businesses, and 2 monitoring businesses in distribution room 1. There are 8 distributed services, 3 collection services, 4 control services, and 2 monitoring services in distribution room 2. There are 5 distributed businesses, 7 collection businesses, 3 control businesses, and 4 monitoring businesses in distribution room 3. There are 5 distributed services, 7 collection services, 5 control services, and 5 monitoring services in the distribution room 4. The packet loss rate, latency, and bandwidth utilization in Qos indicators are used as reference indicators. The Matlab2018b is used as simulation software. The specific test results are shown in Fig. 7.

In Fig. 7, the bandwidth utilization rate decreases with the increase of predicted bandwidth, which indicates that the bandwidth prediction model is more effective in dealing with high bandwidth demands. The best performance is achieved in the distribution room 4, which implies that optimizing the network structure can significantly improve the performance in the scenarios with high demands and high QoS metrics. In addition, the packet loss rate decreases as the bandwidth prediction increases. Low packet loss rate is a key indicator of network reliability, suggesting that this bandwidth prediction model is reliable in data transmission. The reduction of latency in each distribution room indicates that the model can effectively manage network congestion and improve data transmission efficiency. In the distribution room 4, the proposed bandwidth prediction model is used for performance analysis. The results are shown in Fig. 8.

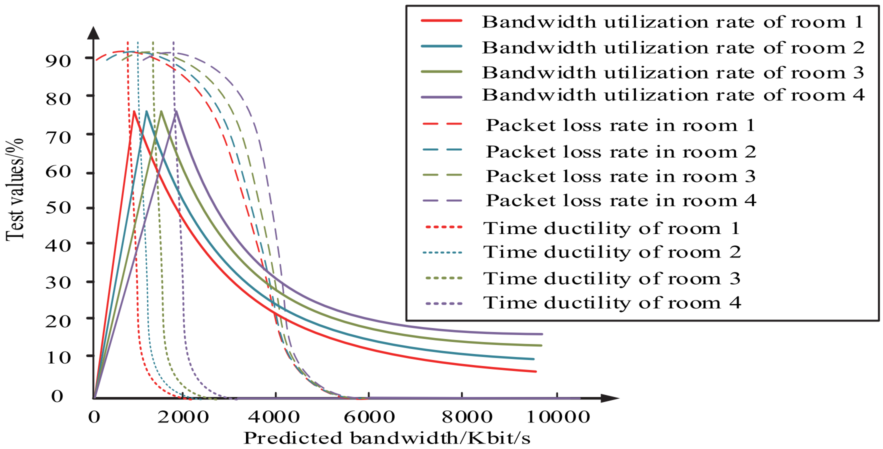
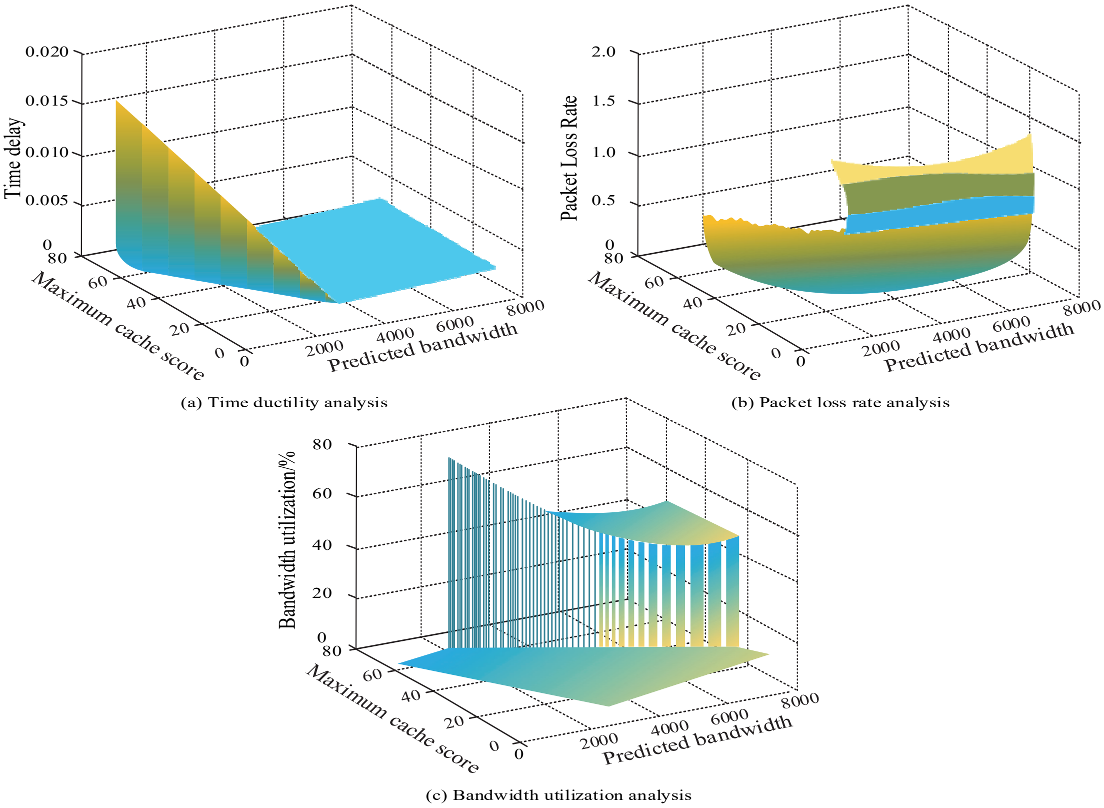


Figure 7 Qos test results of four kinds of power distribution rooms



(a) Time ductility analysis

(b) Packet loss rate analysis

(c) Bandwidth utilization analysis

Figure 8 Qos measurement results of bandwidth prediction model

Fig. 8a shows the latency test results of the new bandwidth prediction model. Fig. 8b shows the packet loss rate test results of the new bandwidth prediction model. Fig. 8c shows the bandwidth utilization test results of the new bandwidth prediction model. Fig. 8a shows that the latency is proportional to the number of cached groups. This indicates that the model is effective in maintaining lower latency when processing large amounts of data. Fig. 8b shows that the packet loss rate decreases as the node configuration increases. This emphasizes the importance of enhancing nodes in network design. Fig. 8c shows that as the bandwidth configuration increases, the utilization rate decreases. This may be due to the system allocating resources more efficiently and reducing resource wastage in high bandwidth configurations. In summary, to guarantee the security of the electric power computer data transmission network, it is necessary to effectively optimize the transmission network for self-innovation. Firstly, all types of business data should meet the QoS indicators as much as possible and be transmitted and allocated reasonably. Secondly, improving the node communication bandwidth can effectively optimize the Qos indexes such as time delay and packet loss rate of the whole transmission system, so as to improve the service quality of electric power computer communication service. To more intuitively test the performance of the bandwidth prediction model proposed in the study, bandwidth prediction, bandwidth utilization, latency, and loss rate are used as reference indicators. The proposed power network data transmission bandwidth prediction model is compared with the elasticity coefficient algorithm, GCC algorithm, and NADA. The test results are shown in Tab. 1.

Table 1 Qos indicator test results of different methods

Method	Forecast bandwidth / Mbit/s	Bandwidth usage / %	Delay / s	Loss rate / %
Elastic coefficient method	1.95	66.72	0.01	0.51
GCC	1.56	74.46	0.03	0.44
NADA	1.44	72.81	0.02	0.27
The method proposed in this study	2.21	79.89	0.02	0.25

From Tab. 1, it is particularly noteworthy that the novel model reaches 2.21 Mbit/s in terms of bandwidth prediction rate, which exceeds the highest value of other models, showing higher data processing capability. Meanwhile, the bandwidth utilization rate is 78.89%, which is higher than other models, indicating that the novel model is more effective in handling high loads. In addition, the novel model also shows excellent stability in terms of latency and packet loss rate, with a packet loss rate of only 0.25%, indicating that it ensures data integrity and accuracy while maintaining efficient data transmission. More refined data analysis and prediction mechanisms make this result possible. The new model improves the bandwidth prediction accuracy by deeply analyzing historical data and traffic trends, as well as more accurately assessing the actual carrying capacity of the network. Compared to traditional bandwidth prediction models based on statistics or simple machine learning, this improved bandwidth prediction model employs advanced artificial intelligence algorithms and shows significant performance gains in high network traffic environments. Particularly interesting is that the model shows unexpected high efficiency in dealing with complex network behavior, which breaks through the performance limitations of traditional models and demonstrates adaptability to future high bandwidth demands.

3.2 Simulation Testing of Power Communication Network Protection Model

To verify the simulation performance of the proposed security protection model, abnormal data within the smart park is used as training samples. The minimum support threshold is 0.1, and the minimum confidence threshold is 0.5. The testing of the security protection model focuses on the network security. A public dataset containing various network attack records is used for training, such as KDD Cup 99. The dataset covers more than 30000 information attacks on various attack scenarios, such as DDoS attacks, intrusion attempts, etc. According to 8:2, it is divided into training data and test data. After the model training is completed, these attack scenarios are reproduced in a simulated network environment to verify the model ability to detect and defend against network security threats. The performance evaluation is mainly based on key metrics such as detection accuracy, response time, and false alarm rate to ensure that the model can operate effectively in real power network environments. The dataset containing multiple network attack records is tested to simulate various security threats and verify the model's protection capability. By reproducing real attack scenarios in a controlled environment, the model response and detection capabilities can be safely tested. The correlation data training time is used as an indicator. The new protection model with the GRA and Apriori algorithm are compared. The test results are shown in Fig. 9.

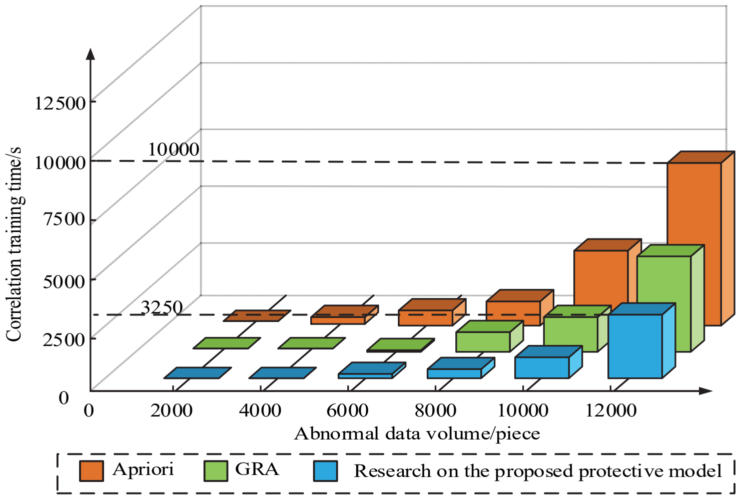


Figure 9 Abnormal data training results for different protection methods

In Fig. 9, the model exhibits better overall performance in training tests with abnormal data compared to traditional Apriori and GRA. In particular, the performance improvement is obvious in terms of data transmission frequency and power recovery time. For example, the recovery time is reduced by 26% and 20%. This result mainly stems from the deep integration of the GRA algorithm and network security protection. Through more effective anomalous event detection and correlation analysis, the model is able to identify potential security threats more quickly and accurately, thus improving response speed and processing efficiency. To further explore the performance status of the protection model, two different interconnected microgrid regional models are built on the Matlab platform. The configuration parameters of the two regional models are basically the same, with only delays set to 0.28 s and 0.08 s, respectively. Frequency deviation and tie line power deviation are used as reference indicators. The performance of two regional models in distributed denial of service attacks is tested. The test results are shown in Fig. 10.

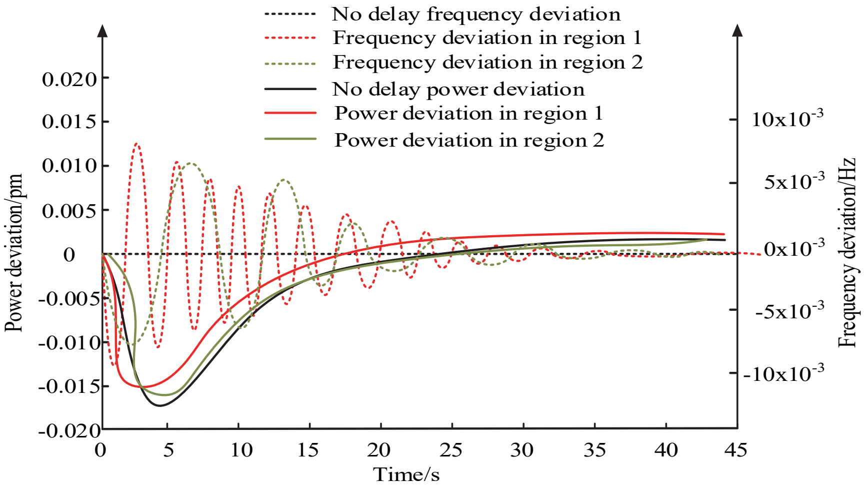


Figure 10 Deviation results of power data in different regions

In Fig. 10, when subjected to distributed denial of service attacks, the transmission frequency and power of the two microgrid area models have different impacts. When not attacked, the frequency deviation and power deviation of both regional models are relatively small. They can all restore the pre-attack state. When the delay setting is small, that is, in zone 2, the recovery time for frequency and power increases to 35 s and 15 s, respectively. When the delay setting is large, that is, in Zone 1, the stability of the system is significantly reduced, with significant fluctuations [19]. The recovery time for frequency and power is divided into 35 s and 20 s. At the same time, as the delay continues to increase, the lowest point of the two frequencies continues to decrease. In summary, regions with lower delay have longer frequency and power recovery times, indicating the important impact of delay on network stability. Taking Zone 2 as the experimental background, to eliminate the impact of network attacks, the frequency deviation and power deviation of the region before and after incorporating the protection model is investigated [20]. The data results are shown in Fig. 11.

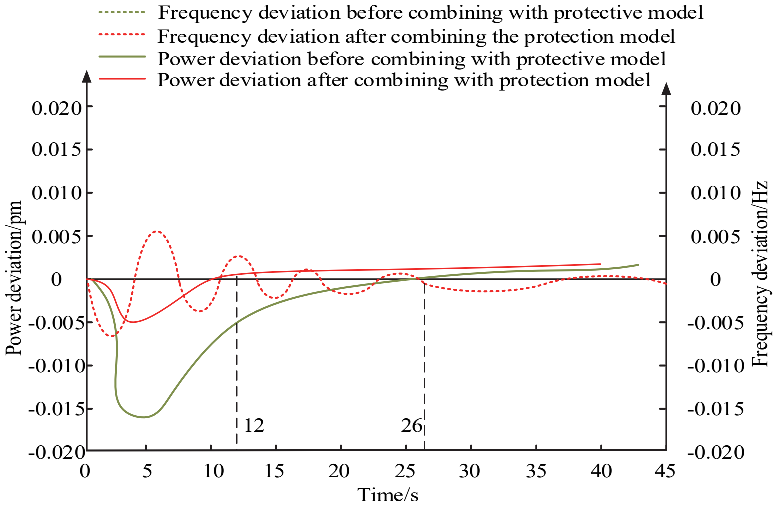


Figure 11 Test results before and after combining the protective model

From Fig. 11, after being subjected to a distributed denial of service attack, compared to an unprotected power transmission network, the data transmission frequency and power are significantly affected [21]. After incorporating the proposed protection model, the data transmission frequency recovery time is 26 s and the power recovery time is 12 s. Compared to the previous network, the time is reduced by 26% and 20%, respectively. In summary, the recovery time of frequency deviation and power deviation is significantly shortened after combining the protection model. It indicates that the new protection model is very effective in resisting network attacks, which can quickly restore the normal operation status. In addition, the security protection model shows high efficiency in detecting novel and complex network attacks compared to earlier models that rely on static rules by introducing an adaptive learning mechanism. Strikingly, the model performs particularly well in reducing false alarms, which addresses a common problem in traditional security models and makes them more suitable for the evolving threats facing the current cybersecurity landscape.

4 CONCLUSION

With the development of big data and artificial intelligence, as well as the increase in communication network data, the security of existing power computer communication transmission networks is facing huge challenges. In view of this, the research attempts to optimize the data transmission method of the network and improve security protection strategies combining Qos technology. In conclusion, this paper presented two improved models, a bandwidth prediction model integrating quality of service technology and a security protection model combining grey relational analysis. Comparative experiments demonstrated the superior performance of the new models compared to existing techniques. The key contributions and findings are: The proposed bandwidth forecasting model achieved highest 2.21 Mbit/s prediction rate and 78.89% utilization among tested methods, showing 13% improvement over current models. This enhances power network planning. The security model reduced frequency and power recovery times by 26% and 20% respectively after simulated network attacks. This strengthens attack resiliency. The integrated QoS and security enhancement strategies provide useful network optimization and robustness. However, the limitations are small dataset size and lack of model validation. Future work should focus on evaluating the models with larger power network data samples. Advanced deep learning models can also be explored for performance improvement. Overall, this study delivers novel data-driven optimization strategies to improve power network efficiency, planning and security. The improved performance of the novel model in latency and packet loss rate compared to the conventional model demonstrates its advantages in network reliability and efficiency. Therefore, the model is suitable for diverse network environments. Especially in high traffic demand, it can effectively predict and manage bandwidth resources. The security protection model demonstrates excellent response speed and high detection accuracy in simulated network attack tests, especially in DDoS and other attacks. The model also exhibits a low false alarm rate, which is crucial for maintaining network management efficiency and avoiding resource wastage. From these results, the study can conclude that the security protection model is remarkably effective in identifying and defending against various types of network attacks. It is suitable for practical power communication networks to improve their overall security. The improved bandwidth prediction model employs advanced artificial intelligence algorithms. Compared with traditional statistical or simple machine learning based bandwidth prediction models, it shows significant performance improvement in high network traffic environments. Particularly interesting is that the model shows unexpected high efficiency in dealing with complex network behavior, which breaks through the performance limitations of traditional models and demonstrates adaptability to future high bandwidth demands. In addition, the security protection model shows high efficiency in detecting new and complex network attacks compared to earlier models that rely on static rules by introducing an adaptive learning mechanism. Strikingly, the model performs particularly well in reducing false alarms. This addresses a common problem in traditional security models, making them more suitable for the evolving threats in the current field of network security. In summary, the research successfully develops an innovative bandwidth prediction and security model, significantly improving the performance and security of power communication networks. Based on advanced artificial intelligence techniques, the bandwidth prediction model performs well in high-traffic environments. The security protection model effectively identifies and defends against various cyber-attacks, especially in reducing false alarms. These results demonstrate the great potential of applying AI techniques in power communication networks, laying the foundation for the future advances in network technology. In addition, by improving the bandwidth prediction model and security protection strategy, the study provides more efficient and stable network performance for computer communication transmission networks in the electric power industry. QoS technology is innovatively applied in the field of network security, providing a new security protection strategy for computer communication transmission networks in the power industry. This research provides important theoretical support and practical strategies for network security in the power industry, especially in the context of network attacks and big data. The research results not only improve the performance of electric power computer communication transmission networks, but also provide solutions and insights for similar challenges faced by other industries. These achievements have improved the operational efficiency and security of the power communication network. Moreover, it provides important technical support and theoretical foundation for addressing the challenges of future network technology, which has significant practical significance. Although this study has made significant progress in bandwidth prediction and network security, it also has some limitations. Firstly, the validity and accuracy of models mainly rely on existing datasets, which may limit their adaptability in different or more complex network environments. In addition, with the continuous development of network attack technology, security protection models may need to be continuously updated to adapt to new threats. Future research should focus on applying these models to real power network environments and validating their performance. The adaptability and scalability of the model in different network environments and wider application scenarios need to be explored. In addition, as the amount of data continues to increase, the model needs to be optimized to better handle large-scale data and maintain efficient network performance.

5 REFERENCE

[1] Jiang, X., Li, P., Li, B., Zou, Y., & Wang, R. (2022). Secrecy performance of transmit antenna selection for underlay MIMO cognitive radio relay networks with energy harvesting. *IET Communications, 16*(3), 227-245. https://doi.org/10.1049/cmu2.12340

[2] Kara, S., Hizal S., & Zengin, A. (2022). Design and Implementation of a DEVS-Based Cyber-Attack Simulator

for Cyber Security. *International Journal of Simulation Modelling, 21*(1), 53-64. https://doi.org/10.2507/IJSIMM21-1-587

[3] Li, Y., Zhang, F., & Sun, Y. (2021). Lightweight certificateless linearly homomorphic network coding signature scheme for electronic health system. *IET information security, 15*(1), 131-146. https://doi.org/10.1049/ise2.12011

[4] Nusair, K., Alasali, F., & Hayajneh A. (2021). Optimal placement of FACTS devices and power-flow solutions for a power network system integrated with stochastic renewable energy resources using new metaheuristic optimization techniques. *International Journal of Energy Research, 45*(13), 18789-78809. https://doi.org/10.1002/er.6997

[5] Sian, H. W., Kuo, C. C., Lu, S. D., & Wang, M. H. (2023). A novel fault diagnosis method of power cable based on convolutional probabilistic neural network with discrete wavelet transform and symmetrized dot pattern. *IET science, measurement & technologyf, 17*(2), 58-70. https://doi.org/10.1049/smt2.12130

[6] Zhao, M., Wei, G., Wei, C., & Guo, Y. (2021). CPT-TODIM method for bipolar fuzzy multi tribute group decision making and its application to network security service provider selection. *International Journal of Intelligent Systems, 36*(5), 1943-1969. https://doi.org/10.1002/int.22367

[7] Shim, K. S., Sohn, I. K., Lee, E., Seok, W., & Lee, W. (2021). Enhance the ICS Network Security Using the Whitelist-based Network Monitoring Through Protocol Analysis. *Journal of Web Engineering (JWE), 20*(1), 1-31. https://doi.org/10.13052/jwe1540-9589.2011

[8] Yan, Z., Yang, C., You, W., Guo, J., Zhang, J., Zheng, Y., & Ma, J. (2020). Achieving Secure and Convenient WLAN Sharing in Personal. *IET Information Security, 14*(6), 733-744. https://doi.org/10.1049/iet-ifs.2020.0134

[9] Gajewski, M., Batalla, J. M., Mastorakis, G., & Mavromoustakis, C. X. (2020). Anomaly traffic detection and correlation in Smart Home automation IoT systems. *Transactions on Emerging Telecommunications Technologies, 33*(6), 4053-4071. https://doi.org/10.1002/ett.4053

[10] Kovačić, M., Mutavdžija, M., Buntak, K., & Pus, I. (2022). Using Artificial Intelligence for Creating and Managing Organizational Knowledge. *Tehnički vjesnik, 29*(4), 1413-1418. https://doi.org/10.17559/TV-20211222120653

[11] Shili, M., Hajjaj, M., & Ammari, M. L. (2022). Power allocation with QoS satisfaction in mmWave beamspace MIMO-NOMA. *IET Communications, 16*(2), 164-171. https://doi.org/10.1049/cmu2.12325

[12] Aghdam, B. M. J. & Shaghaghi, K. R. (2023). Effective Resource Allocation and Load Balancing in Hierarchical HetNets: Toward QoS-Aware Multi-Access Edge Computing. *The Computer Journal, 66*(1), 229-244. https://doi.org/10.1093/comjnl/bxab157

[13] Fernandez, S. A., Ferone, D., Juan, A., & Taechi, D. (2022) A simheuristic algorithm for video streaming flows optimisation with QoS threshold modelled as a stochastic single-allocation p-hub median problem. *Journal of Simulation, 16*(5), 480-493. https://doi.org/10.1080/17477778.2020.1863754

[14] Liu, D., Zhu, L. L., Zhang, Z. T., Zeng, Y., Bai, Z. Q.,, & Li, L. (2021). The QoS evaluation model for cloud resource node. *International Journal of Sensor Networks,* (4), 194-203. https://doi.org/10.1504/ijsnet.2021.117480

[15] Ilakkiya, N. & Rajaram, A. (2023). Blockchain-assisted Secure Routing Protocol for Cluster-based Mobile-ad Hoc Networks. *International Journal of Computers Communications & Control, 18*(2), 1-18. https://doi.org/10.15837/ijccc.2023.2.5144

[16] Torre, P. S. & Hidalgo-Gonzalez, P. (2022). Decentralized Optimal Power Flow for time-varying network topologies using machine learning. *Electric Power Systems Research, 212*(11), 1-7. https://doi.org/10.1016/j.epsr.2022.108575

[17] Chandrasekaran, S., Srinivasan, V. B., & Parthiban, L. (2018). Towards an Effective QoS Prediction of Web Services using Context-Aware Dynamic Bayesian Network Model. *Tehnički vjesnik, 25*(Supplement 2), 241-248. https://doi.org/10.17559/TV-20161104072515

[18] John, Y. M., Sanusi, A., & Yusuf, I. (2023). Reliability Analysis of Multi-Hardware–Software System with Failure Interaction. *Journal of Computational and Cognitive Engineering, 2*(1), 38-46. https://doi.org/10.47852/bonviewJCCE2202216

[19] Ma, L., Christou, V., & Bocchini, P. (2022). Framework for probabilistic simulation of power transmission network performance under hurricanes. *Reliability Engineering and System Safety, 217*(1), 519-537. https://doi.org/10.1016/j.ress.2021.108072

[20] Muthulakshmi, K., Kalirajan, K., Jean Justus, J., & Sivamalar, P. (2024). QoS Aware Data Congestion Control Routing in Mobile Ad Hoc Networks for Intelligent Transportations Systems. *Tehnički vjesnik, 31*(1), 240-246. https://doi.org/10.17559/TV-20230427000582

[21] Cao, Z., Huang, Q., & Wu, C. Q. (2020). Maximize Concurrent Data Flows in Multi-radio Multi-channel Wireless Mesh Networks. *Computer Science and Information Systems, 17*(3), 759-777. https://doi.org/10.2298/CSIS200216019C

Contact information:

Jingyuan SHENG
Shenyang University of Chemical Technology,
College of Computer Science and Technology,
Shenyang, Liaoning, China, 110142
E-mail: z2019240@stu.syuct.edu.cn