Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 1, No.1, January : 2025

WSN- DROVE ELUCIDATIONS FOR SUPERIORITY OF OVERHAUL AND SANCTUARY IN COMMUNIQUÉ LINKAGES

Mrs. T.S. Revathy, Research Scholar (PT), Department of Computer Science, Defence Institute of Advanced Technology, Pune - 411 025. **&** Assistant Professor, Dep. of Computer Application, G.T.N Arts College, Dindigul-624 005
Dr. Dinesh Senduraja Ph.D. Research Associate (RA), MED& COS, Defence Research & Development Organisation (DRDO) Pune- 411 021. **&** Lecturer, Government Art and Science College, Veerapandi, Theni -625 534.

ABSTRACT :
This paper introduces enhanced models for bandwidth prediction and security protection in power communication networks. Initially, a queuing model incorporating quality of service (QoS) technology is developed for bandwidth forecasting. Additionally, a security model that integrates grey relational analysis is proposed to address network attacks. Experimental comparisons validate the performance of the proposed models. The results reveal that the bandwidth prediction model achieves a forecasting rate of 2.21 Mbit/s and 78.89% utilization, surpassing existing methods.
The security model also demonstrates a 26% and 20% improvement in recovery time following siμlated network attacks compared to traditional approaches. The research offers valuable strategies for network optimization and enhanced security. However, the study is limited by a small dataset and lack of model validation. Future research should test these models on larger datasets from power networks.
words: artificial intelligence; communication networks; power systems; security protection; quality of service (QoS) technology.

INTRODUCTION:

Computer communication transmission network security involves safeguarding information in computer networks from unauthorized access, tampering, disruption, or concealed threats. With the widespread adoption and expansion of computer networks, security issues have become more pronounced. This is particularly true in the power industry, where challenges such as unstable power communication networks, interference in power systems, and virus intrusions persist. Consequently, improving the security and efficiency of power communication networks is of utmost importance.
As digitalization and interconnectivity continue to advance, power systems increasingly rely on stable and reliable data communication. Effective bandwidth management and robust network security measures are critical to ensuring the uninterrupted operation of power systems and protecting against potential cyber attacks.
Mch of the existing research focuses on specific areas of network security, such as data encryption and protocol security. However, there is often a lack of comprehensive strategies aimed at enhancing both network performance and security siμltaneously. Additionally, traditional studies tend to overlook the performance assurance of power communication transmission networks under high load and in complex scenarios. This research seeks to bridge this gap by developing advanced defense techniques, optimizing data transmission methods, and leveraging artificial intelligence to improve network management and resilience. By integrating Quality of Service (QoS) technologies, it is possible to enhance both the performance and security of power communication networks in complex environments.
The novelty of this study lies in the introduction and refinement of QoS techniques, along with the development of innovative bandwidth prediction and security protection models. These models not only

optimize data transmission efficiency but also improve the network's resilience to security threats. Through experimental validation, the proposed models demonstrate superior performance over existing models in terms of bandwidth prediction accuracy, utilization rates, and the ability to recover from network attacks.

The significance of enhancing the security of electric power communication networks extends beyond technical considerations. It is crucial for ensuring the stability of national energy infrastructure, supporting ongoing economic development, and safeguarding public safety. Electricity is essential to modern society, and the security of communication networks directly impacts everyday life and various facets of social operation. Therefore, this study aims to address several critical challenges, including strengthening defenses against network attacks, improving the reliability and efficiency of data transmission, managing large-scale data processing, boosting system resilience and adaptability, and developing intelligent security monitoring and management systems.

By implementing these strategies, the research aims to significantly enhance the security and performance of power networks, contributing to national energy security and stable economic and social development. Building on the recognition of the importance of communication network security in the power sector, the innovation of this research is the development of a bandwidth prediction model and a security protection model that integrate QoS technology. This innovation not only improves the data transmission efficiency and bandwidth utilization of power communication networks but also significantly strengthens the network's ability to defend against various security threats through advanced protection strategies. The dual approach, combining bandwidth management with security protection, provides a comprehensive solution for optimizing both security and performance in power communication networks.

This represents a major technological advancement in the realm of communication network security within the power industry. The primary contribution of this research is the proposal of a novel bandwidth prediction model and security protection model, which incorporate QoS techniques. By optimizing queuing models for power communication transmission networks, these models substantially improve bandwidth prediction accuracy and network security. Experimental results demonstrate that the new bandwidth prediction model outperforms existing models in terms of prediction accuracy and utilization, while the security protection model also delivers significant improvements.

Effectively reducing the recovery time of data transmission during network attacks, thereby significantly enhancing both the performance and security of the power computer communication transmission network. The field of computer communication transmission network security is vast and crucial. This study primarily focuses on protecting data, information, and communication devices within computer networks and transmission systems from a variety of threats and attacks.

In recent years, numerous researchers from both domestic and international backgrounds have conducted extensive studies in this area. Grid communication security can be broadly divided into four technological domains: network data transmission and storage security, industrial computer communication network security, wireless local area network security, and anomaly detection in data.

In the field of network data transmission and storage security, Zhao M. et al. proposed a bipolar fuzzy interaction multi-criteria decision model utilizing cumulative prospect theory. Their study demonstrated the effectiveness of multi-criteria decision models in addressing network security issues. However, such models may encounter challenges related to data processing complexity and high computational costs when applied in practical scenarios.

In the realm of industrial computer communication network security, Shim K. S. et al. identified various vulnerabilities in existing industrial computer communication networks during task transmission. To

address these, they proposed a field extraction prediction method for industrial communication network protocol structures. Their experimental results showed that this method could derive the command and protocol structures used in industrial environments, improving the prediction efficiency for various network security issues. However, the method might fall short when dealing with more advanced cyber threats, such as advanced persistent threats (APTs).

In the area of wireless local area network (WLAN) security, Yan Z. et al. developed a mutual authentication method that integrates cryptography to ensure secure data sharing in WLANs. This approach ensures double-ended data confidentiality by providing ease of use, anonymity, and fine-grained access control. Experimental results demonstrated that this method had a high security utility, fulfilling the existing needs for data sharing protection in WLANs. However, challenges related to large-scale deployment, management, and performance may arise with this approach.

In anomaly data detection technology, Gajewski M. et al. proposed a strategy to detect anomalous data to prevent issues like traffic fluctuations, packet corruption, and increased message traffic during network data transmission in building automation systems. Their experimental results indicated that the detection strategy could effectively manage data fluctuations between the service client and the network provider and provide timely feedback. However, the strategy may have limitations in detecting more sophisticated network attack patterns.

Service quality technology (QoS) encompasses a set of methods and mechanisms designed to manage and optimize data transmission within computer networks. The primary objective of QoS technology is to ensure that data transmission meets specific performance and service requirements, including bandwidth, latency, and overall service reliability.

Latency, jitter, reliability, and other factors to meet the requirements of different applications and services. From the perspective of QoS technology application, optimizing data transmission management can significantly enhance network performance and service quality. For instance, the power allocation strategy proposed by Shili M. et al. and the feedback mechanism for mobile edge computing introduced by Aghdam B. M. J. et al. demonstrate how QoS can boost network efficiency. Shili M. et al. introduced a power allocation strategy between users that reduces the detection complexity of non-orthogonal multiple access schemes while ensuring quality of service for users. Their experimental results indicated that this new strategy is more robust than traditional methods, minimizing performance loss even when the channel is uncertain.

Aghdam B. M. J. et al. suggested an effective feedback mechanism that combines QoS technology with a server resource manager to reduce the complexity of mobile edge computing and achieve a local optimal solution. Their results showed that this mechanism effectively meets user service quality requirements and significantly improves system throughput. Fernandez S. A. et al. proposed an intervention strategy that assigns service quality thresholds to potential hubs, exploring the impact of network latency on video signals. Their experimental results demonstrated that this strategy outperforms traditional methods in execution and allocation, substantially reducing losses caused by network latency.

Li L. et al. proposed a framework for evaluating cloud service quality, using service performance and scalability as indicators, with a focus on evaluating node service quality in cloud service systems. The experimental results indicated that this framework can quickly and reliably assess the service capabilities of resource nodes, providing a strong foundation for resource allocation.Despite the progress made in grid communication security and QoS strategies, there remain some limitations. Traditional network security solutions often focus on a single security threat while neglecting network performance optimization, potentially improving security at the cost of data transmission efficiency.

Furthermore, many existing approaches lack flexibility in adapting to complex and dynamic network environments, failing to respond effectively to changing network conditions and attack patterns. In bandwidth management, traditional methods are often inadequate in predicting and adjusting to real-time network traffic changes, leading to suboptimal resource allocation.

To address these limitations, the bandwidth prediction and security models proposed in this study offer a more comprehensive and dynamic solution. By integrating QoS techniques, the bandwidth prediction model can adjust and optimize network resource allocation in real time, enhancing the efficiency and stability of data transmission. This dynamic prediction mechanism adapts to changes in network conditions, ensuring optimal bandwidth utilization. Meanwhile, the security protection model utilizes advanced algorithms to detect and defend against various network threats, such as distributed denial-of-service attacks. This holistic security approach not only strengthens defense capabilities but also ensures that network performance remains uncompromised while enhancing security.

RESEARCH METHOD:

To enhance the effectiveness of the power transmission communication network security protection model, this section first discusses the existing network data transmission queuing model. Subsequently, improvements are introduced, leading to the proposal of a new bandwidth prediction model. The second section focuses on applying this new model to strengthen the security protection of power data transmission networks.

BANDWIDTH PREDICTION MODEL:

As the digitalization and networking of power systems continue to advance, power computer transmission communication networks are facing increasing security threats【14】. These networks vary in their transmission methods depending on the scenario, particularly within the context of smart parks. To address these challenges, this study explores the transmission security of power computer communication networks in smart parks, which operate under the influence of artificial intelligence technologies. With the growing number of terminals, power computer communication transmission networks face ongoing security threats. The current security protection system for these networks in smart parks is illustrated in Fig. 1.

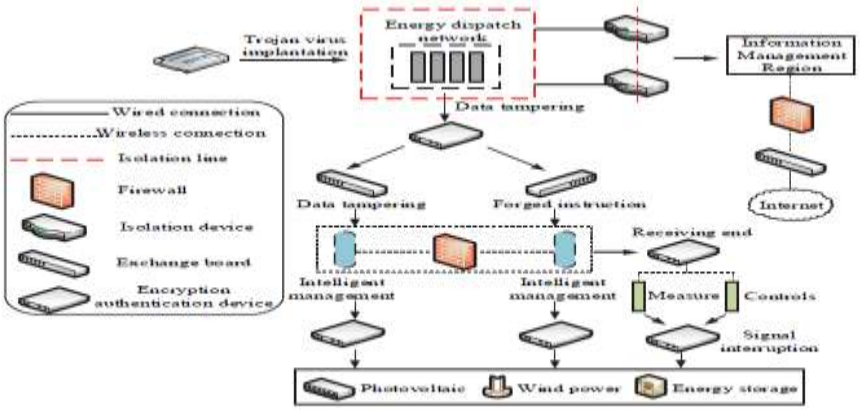

Figure 1 Smart park power computer communication transmission network security protection system

In Fig. 1, the power computer communication transmission network in the smart park experiences frequent business interactions. During these exchanges, security violations, vulnerabilities in operating systems and databases, and the injection of Trojan programs can disrupt signals, potentially leading to

significant economic losses【15】. To mitigate these risks, a common approach is to group and queue various data services within the transmission of power computer communication systems, ensuring that the data remains independent of each other. parameters involved in this process include packet arrival rate, forwarding rate, and the number of windows. The average arrival time at the arrival rate is expressed by Eq. (1):

$$\lambda=\int\int_0^\infty a(t)dt=A(t)$$

In Eq. (1), (λ) denotes the rate at which data packets arrive, (t) represents the time at which the packet arrived, a(t)refers to the probability density of the arrival rate, and A(t) is the distribution function of the arrival rate. The term $\frac{1}{\lambda}$ represents the average arrival time.The forwarding rate is represented by Eq. (2) In Eq. (2), B(t) is the distribution function of the forwarding rate, and b(t) is the density function of the forwarding rate. The term $(\frac{1}{\mu})$refers to the average forwarding time.There are three main processes in which the state of a queuing system changes over time.

$$\mu=\int_0^\infty b(t)dt=B(t)$$

$$P_k(t+\Delta t)=P_k(t)(1-\lambda_k\Delta t-\mu_k\Delta t)$$

The method for calculating the probability that no data packets arrive or are transferred at a given time is shown in Eq. (3):In Eq. (3), (Δ t) represents an infinitesimal time interval. (P_k(t)) denotes the probability distribution of state (k) at time (t), while (λ_k) and (μ_k) are fixed constants.When a packet is not forwarded within a specified time, the calculation method is given in Eq. (4):

$$P\_k(t+\Delta t)=P\_\{k-1\}(t)(\mu\_\{k-1\}\Delta t)$$

In Eq. (4), (P_{k-1}(t)) refers to the state of the queuing system at time (t) as (k-1). If a packet is forwarded but no new packet arrives within the specified time, the calculation is shown in Eq. (5):

$$P\_k(t+\Delta t)=P\_\{k+1\}(t)(\mu\_\{k+1\}\Delta t)$$

In Eq. (5), (P_{k+1}(t)) refers to the queuing system state at time (t) as (k+1). By combining these three states of the queuing system along with the newly emerging businesses, the load on the queuing system will increase. To handle this, the Poisson model is introduced. The queuing system for data services in the power computer communication transmission network of the smart park, under this model, is shown in Fig. 2. From Fig. 2, two representative business data flows are transmitted via a loose mooring process and an interrupted loose mooring process, respectively. After reaching the queuing cache stage, the operation proceeds with bandwidth prediction and allocation.

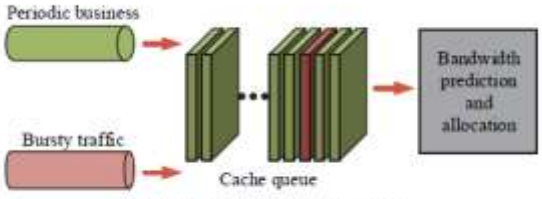

Figure 2 Data service queuing framework

To improve the prediction of business bandwidth and ensure the adaptability of business data resources in the power computer communication transmission network of the smart park, QoS technology is integrated. The system's forwarding rate during service is set to a fixed value, and the data flow is analyzed. The state transitions of the queuing system in the business data transmission network, incorporating QoS technology, are shown in Eq. (6):

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 1, No.1, January : 2025

$$P_{cp} - \sum_{c} \left(\rho_{cp}^{-} - \rho_{cp}^{-}\right)$$

In Eq. (6), (c) represents the number of edge network associations in the system. (λ) is the rate at which business data packets arrive, (μ) is the forwarding rate of a single edge network for business data, (n) is the maximum number of configuration nodes, and (k) represents the system state. (ρ) is the ratio of the data arrival rate to the forwarding rate. The probability of state transition overflow, or the packet loss rate, is given in Eq. (7):

$$P_{loss} = \gamma = \sum_{n} P_k$$

In Eq. (7), (gamma) represents the group cache threshold, (P_e) is the data transfer status of business (e), and (P_k) is the data transfer status of business (k). After the data packet arrives, the average queuing time is represented by Eq. (8):

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

In Eq. (8), (L_s) is the time when business data arrives, and (λ_e) is the rate at which business packets arrive. The bandwidth prediction, or system utilization rate, is shown in Eq. (9):

$$\eta = \frac{\lambda_e}{\mu_c}$$

In Eq. (9), (μ) is the forwarding rate. In summary, the study introduces an enhanced queuing model for accurately predicting the bandwidth needs of power computer communication networks. This model incorporates parameters such as packet arrival rate, forwarding rate, and the number of windows. Notably, the model leverages deep learning techniques to analyze historical data and predict future bandwidth demand, thus facilitating more efficient network traffic management. The model flow is shown in Fig. 3.

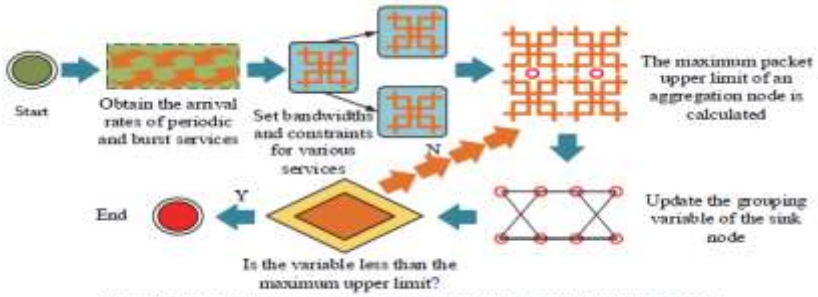

Figure 3 Power computer communication transmission network bandwidth prediction process

In Fig. 3, the arrival rate for each type of power service is first calculated. The transfer probability for each state is then determined, followed by the calculation of the packet loss and delay rates for each service. Next, the sampling interval and constraints for bandwidth prediction are set, including the maximum upper limit for packet cache.

The variable values are adjusted, after which the bandwidth utilization rate and bandwidth prediction values for each service combination are calculated separately. The packet variable for the aggregation node is updated. If this value is less than the maximum allowed packet cache size, the calculation is repeated to determine the bandwidth utilization and predicted bandwidth values again. If the variable exceeds the maximum cache packet limit, the result is output directly. Additionally, parameters of this

new 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's training process consists of collecting historical network traffic data, performing data preprocessing and feature selection, and building a time series prediction model using neural networks. Cross-validation is applied during training and validation, with parameter adjustments made based on the validation outcomes. Finally, the model's performance is tested on a separate independent test set. For the bandwidth prediction model, parameters like data arrival rate, forwarding rate, and cache window size need to be adjusted according to a deep understanding of historical data and current network traffic trends. Specifically, the data arrival rate should be set to accurately reflect actual network traffic, while the forwarding rate μst account for the network's capacity and past performance. The cache window size adjustment aims to balance the delay and data packet loss rate, optimizing the efficiency and stability of the overall network transmission.

DEVELOPMENT OF THE POWER GRID SECURITY MODEL

Building upon the optimization design of the power computer communication transmission network's queuing model, resource adaptation has been enhanced to some extent. This improvement has led to increased bandwidth prediction efficiency for power operations, ensuring the secure functioning of the power computer network within the smart park. However, to implement more precise network security protection, it becomes challenging to conduct correlation analysis of abnormal network attack events using just a single QoS technology. Therefore, in addition to bandwidth prediction, the Grey Relational Analysis (GRA) algorithm is incorporated for supplementary analysis.
The GRA algorithm is primarily used to identify and analyze the relationships between abnormal network events. It is also effective for evaluating the strength of relationships among various factors in complex datasets. In network security, this method helps detect abnormal behaviors or potential attack patterns. The GRA algorithm starts by preprocessing the collected anomaly data, which includes normalization to eliminate scale discrepancies and ensure consistent comparisons across data. It then measures the correlation between data sequences by establishing a Gray correlation. A high Gray correlation indicates a strong similarity between two sequences.
In the context of the security protection model for the electric power computer communication transmission network, the GRA algorithm works by first collecting and normalizing data on network attack events.
Next, it applies the GRA method to develop a correlation analysis model, which helps in identifying abnormal events by calculating the relationship between the data. When potential security threats are identified, appropriate countermeasures are implemented, such as strengthening firewalls, updating security protocols, or isolating parts of the network. The correlation analysis framework for abnormal events in a typical smart park's power computer transmission network is illustrated in Fig. 4.

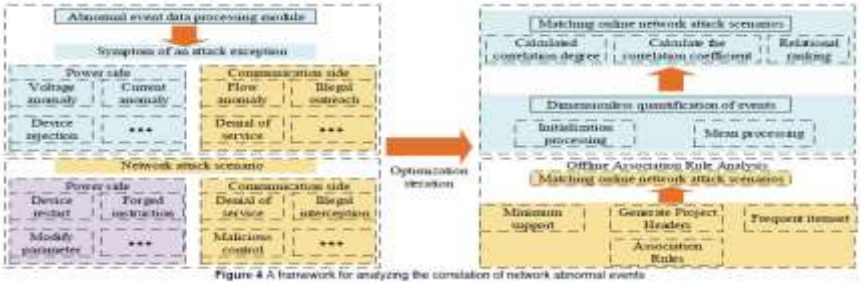

Figure 4 A framework for analyzing the correlation of network abnormal events

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 1, No.1, January : 2025

In Fig. 4, the framework divides the entire power computer transmission network within the smart park into three main components: the online network attack scenario matching, offline association rule analysis, and abnormal event data processing modules. The attribute matching is specifically demonstrated by gathering data related to network attacks, such as attack type, time, frequency, etc. These data are then standardized to form reference sequences, including common attack patterns, comparison sequences, and other collected data. Additionally, rules are generated by calculating the correlation between reference sequences and comparison sequences to evaluate their similarity. Based on these results, it is determined whether they match any known attack patterns.

The preprocessing module for abnormal event data is the most complex and critical part of the framework. It guides the data association process by extracting event feature data. The set of event characteristic factors is represented in Eq. (10).

$$X = \{Si, Ai, Oi\}$$

In Eq. (10), (Oi) represents the data source object, (Ai) represents the abnormal manifestation of network attacks, and (Si) represents the attack scenario. There are typically 9 types of abnormal manifestations, such as voltage anomalies, current anomalies, and device mis-operation. Similarly, there are 9 types of attack scenarios, including session hijacking, device modification, and device locking. These factors are organized into attack correlation matching modules. The correlation analysis between these characteristic factors is shown in Eq. (11).

$$(X_i) = (1, 2, \ldots, 9) \quad (Y_k) = (1, 2, \ldots, n)$$

In Eq. (11), (Xi) represents the abnormal event attribute set, (Yi) represents the reference attribute set for each factor, (t) represents time, and (i) represents different attributes in the attribute set. Each factor belongs to a different category, so correlation analysis requires dimensionless transformation of these factors. This process is shown in Eq. (12).

$$x_i(k) = \frac{x_i(k) - min(x_i)}{max(x_i) - min(x_i)}, \quad i = 1, 2, \ldots, 9$$

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

$$\zeta_i(k) = \frac{|y_i(k) - x_i(k)|}{|y_i(k) - x_i(k)| + |y_i(k) - x_i(k)|}$$

In Eq. (13), (zeta_i(k)) represents the correlation coefficient. The interpretation of other algebraic variables is consistent with the previous equations. After processing, the 9 abnormal manifestations are numbered 1 to 9, and the 9 attack scenarios are labeled A to I. After a random combination, correlation screening is performed. The correlation scanning process for abnormal event data is shown in Fig. 5.

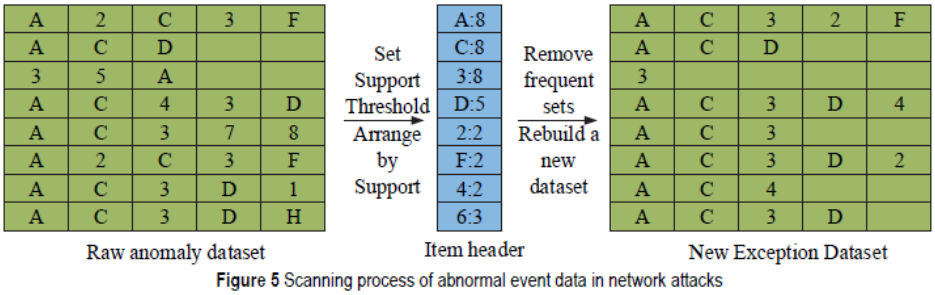

Figure 5 Scanning process of abnormal event data in network attacks

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 1, No.1, January : 2025

In Fig. 5, the original abnormal event data is scanned and filtered to extract the item header event. After applying Grey correlation, frequent occurrences of abnormal data are removed. This results in the creation of a new dataset with the remaining header data. In summary, the Grey correlation degree calculation process follows several steps. First, the difference between the reference and comparison sequences is computed, forming the difference sequence. Next, the difference sequence is normalized to eliminate the impact of varying data sizes. Then, the correlation coefficient between the reference and comparison series is calculated using the GRA forμla, which indicates the degree of similarity between the two. Lastly, the correlation degree is assessed by analyzing the correlation coefficient. A higher correlation coefficient signifies a stronger correlation. The attribute correlation degree for each event throughout the process is expressed in Eq. (14).

$$\zeta_i - \frac{1}{n}\sum_{k=1}^{n} r_i(k), \quad i - 1, 2, \ldots, n$$

In Eq. (14), (r_i) represents the correlation degree of different events. Based on the analysis of the abnormal event detection method and network attack correlation discussed earlier, a security protection strategy model for the power computer communication and transmission network of the smart park is proposed. The model's response strategies to various network attacks for different scenarios are shown in Fig. 6. From Fig. 6, the network attack defense mechanisms on the master side include IP address management, identity authentication, data transmission encryption, and network isolation. On the communication side, defense techniques include bandwidth restriction, data filtering, bandwidth resource allocation, and certificate verification. On the terminal side, defense measures include address encryption, access authorization, and device isolation. Each module operates independently but is interconnected, forming a comprehensive security barrier for the entire power computer communication data transmission network.This security protection model combines machine learning algorithms with GRA. parameters include an anomaly detection threshold of over 30 login attempts per minute, a 10-minute time window, and a Gray correlation threshold of 0.8. The model's training process involves collecting historical security event data, performing feature engineering, modeling with machine learning classifiers, training with historical data, and using GRA to identify security threats. The model is then validated on selected data and deployed to a real network for real-time monitoring and defense.

For the network security protection model, critical parameters involve the correlation threshold, the sensitivity of anomaly detection, and the specific response strategy. The correlation threshold μst be carefully balanced to minimize both the false alarm rate and the detection leakage rate, based on a detailed analysis of historical attack patterns and the current network state. Furthermore, the sensitivity of anomaly detection should be adjusted according to the specific security threats and attack frequencies the network faces, improving detection accuracy. Finally, response strategies μst be designed to meet the specific needs and security requirements of the network, including actions such as traffic restriction and source address blocking to effectively address various security challenges.

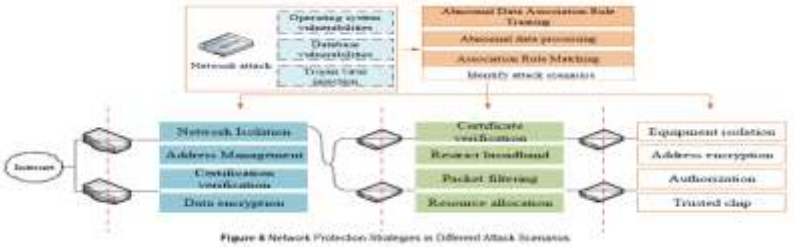

Figure 6 Network Protection Strategies in Different Attack Scenarios

RESULTS AND DISCUSSION:

This study successfully developed innovative models for bandwidth prediction and security protection, significantly improving the performance and security of power communication networks. By leveraging advanced AI techniques, the bandwidth prediction model performs efficiently in high-traffic environments, while the security protection model effectively detects and mitigates various cyber-attacks, particularly in reducing false alarms. These outcomes highlight the immense potential of AI techniques in enhancing power communication networks and set the stage for future advancements in network technology.

Performance Evaluation of the Bandwidth Prediction Model for Power Communication Networks:

The performance of the bandwidth prediction model was evaluated using a real dataset from the power system communication network. The study utilized the UCI machine learning library's network traffic dataset, which includes over 50,000 records detailing network traffic, bandwidth usage, network delays, and packet transmissions. The dataset was split into a training set and a testing set at an 80:20 ratio. Initially, the model was trained on historical network traffic data to learn the patterns and trends in network behavior. To assess the model's prediction accuracy and robustness, a separate test dataset, distinct from the training set, was used for validation. The performance was evaluated using several metrics, including accuracy, latency, and packet loss.

This testing strategy aims to assess the model's ability to predict new data while considering μltiple performance aspects like accuracy, latency, and packet loss. Such an approach ensures that the model is reliable and adaptable for real-world applications in power communication networks. The testing was conducted across four different intelligent distribution rooms, each containing various types of services. These included distributed services, collection services, control services, and monitoring services.

- Distribution Room 1: 5 distributed services, 6 collection services, 2 control services, 2 monitoring services
- Distribution Room 2: 8 distributed services, 3 collection services, 4 control services, 2 monitoring services
- Distribution Room 3: 5 distributed services, 7 collection services, 3 control services, 4 monitoring services
- Distribution Room 4: 5 distributed services, 7 collection services, 5 control services, 5 monitoring servicesperformance indicators such as packet loss rate, latency, and bandwidth utilization were used to evaluate QoS. Matlab2018b was used for the simulation, and the test results are displayed in Fig. 7.

In Fig. 7, it is shown that as the predicted bandwidth increases, the bandwidth utilization rate decreases, indicating the model's effectiveness in handling high bandwidth demands. The optimal performance is observed in Distribution Room 4, suggesting that improving the network structure can significantly enhance performance in scenarios with high demands and elevated QoS metrics. Additionally, the low packet loss rate is a critical indicator of network reliability, highlighting the model's reliability in data transmission. The reduction in latency across all distribution rooms demonstrates the model's ability to manage network congestion effectively and improve data transmission efficiency. The results of the performance analysis for the bandwidth prediction model in Distribution Room 4 are presented in Fig. 8.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 1, No.1, January : 2025

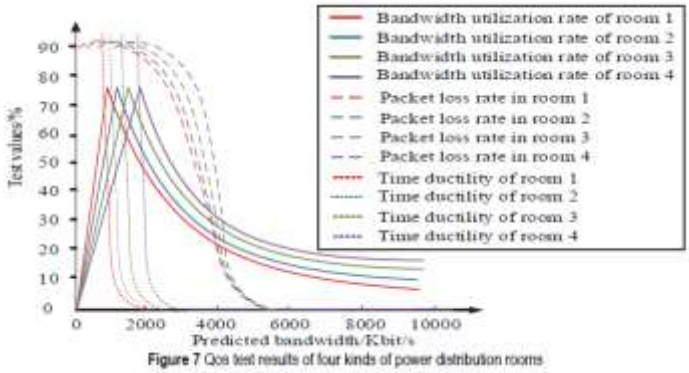

Figure 7 Qos test results of four kinds of power distribution rooms

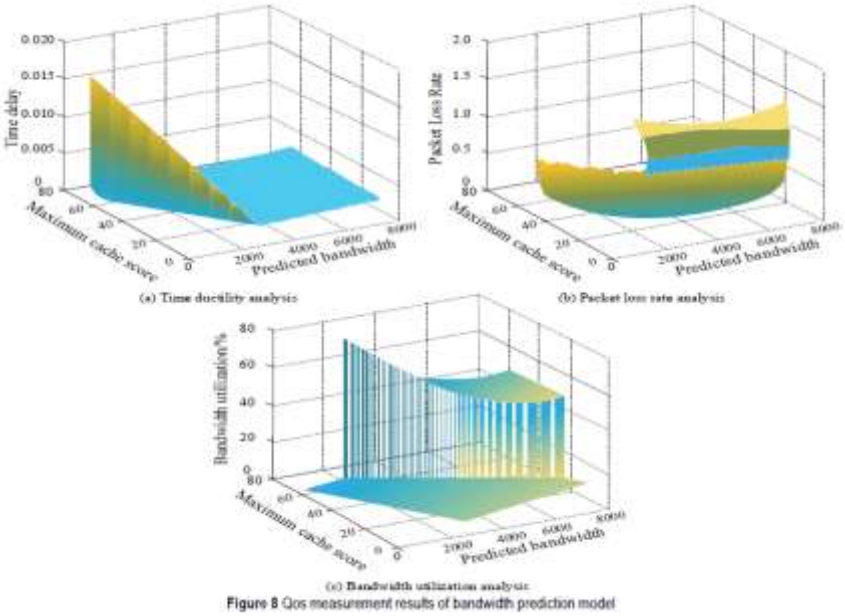

Figure 8 Qos measurement results of bandwidth prediction model

Fig. 8a displays the latency test results for the new bandwidth prediction model, while Fig. 8b shows the packet loss rate test results, and Fig. 8c presents the bandwidth utilization test results. As illustrated in Fig. 8a, latency increases in proportion to the number of cached groups, indicating the model's effectiveness in maintaining low latency when handling large volumes of data. In Fig. 8b, the packet loss rate decreases as the node configuration improves, highlighting the significance of enhancing node capacity in network design. Fig. 8c demonstrates that as bandwidth configuration increases, bandwidth utilization decreases. This suggests that the system becomes more efficient in resource allocation, minimizing resource wastage when higher bandwidth configurations are implemented.

In conclusion, to ensure the security of the electric power computer data transmission network, it is crucial to optimize the transmission network through innovative approaches. First, it is important to ensure that all types of business data meet the QoS indicators and are transmitted and allocated effectively.

Second, enhancing node communication bandwidth can significantly improve QoS metrics such as latency and packet loss rate, thereby boosting the overall service quality of the electric power computer communication network.

To further evaluate the performance of the proposed bandwidth prediction model, indicators such as bandwidth prediction accuracy, bandwidth utilization, latency, and packet loss rate are used. The model's performance is compared with that of the elasticity coefficient algorithm, GCC algorithm, and NADA. The test results are provided 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 proposed model achieves a bandwidth prediction rate of 2.21 Mbit/s, surpassing the highest rates of the other models, demonstrating its superior data processing capabilities. Additionally, the model maintains a bandwidth utilization rate of 78.89%, which is higher than the other models, highlighting its effectiveness in handling high traffic loads. Furthermore, the novel model exhibits exceptional stability in terms of latency and packet loss rate, with a packet loss rate as low as 0.25%, indicating that it ensures data integrity and accuracy while maintaining efficient data transmission. This is made possible by more sophisticated data analysis and prediction mechanisms.

The improved model enhances bandwidth prediction accuracy by thoroughly analyzing historical data and traffic trends, allowing for a more precise evaluation of the network's actual carrying capacity. Compared to traditional bandwidth prediction models based on statistics or basic machine learning, this advanced model, which incorporates cutting-edge artificial intelligence algorithms, shows substantial performance improvements, especially in high-traffic network environments. Notably, the model demonstrates exceptional efficiency in managing complex network behaviors, overcoming the performance limitations of traditional models and exhibiting adaptability to future high bandwidth demands.

SIMLATION TESTING OF POWER COMMUNICATION NETWORK PROTECTION MODEL:

To assess the performance of the proposed security protection model, abnormal data from the smart park are used as training samples. The minimum support threshold is set to 0.1, and the minimum confidence threshold is set to 0.5. The testing of the security protection model focuses on evaluating network security. A public dataset, including a variety of network attack records such as those from the KDD Cup 99, is used for training. This dataset contains over 30,000 records of various attack scenarios, including DDoS attacks and intrusion attempts. The data is split into training and test sets in an 80:20 ratio. After training the model, simulated network environments are used to recreate these attack scenarios and evaluate the model's ability to detect and defend against network security threats.

The performance evaluation of the model primarily focuses on metrics such as detection accuracy, response time, and false alarm rate to ensure its effectiveness in real-world power network applications. By simulating real-world attack scenarios in a controlled environment, the model’s detection and response capabilities can be thoroughly tested. The correlation data training time is used as an evaluation

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 1, No.1, January : 2025

metric. The new protection model, which integrates the GRA and Apriori algorithms, is compared to other protection models. The test results are presented in Fig. 9.

In Fig. 9, the model demonstrates superior overall performance in training tests with abnormal data when compared to traditional Apriori and GRA models. Specifically, the improvement is most noticeable in data transmission frequency and power recovery time. For instance, the recovery time is reduced by 26% and 20%, respectively. This result can be attributed to the deep integration of the GRA algorithm with network security protection. By employing more effective detection and correlation analysis of anomalous events, the model is able to identify potential security threats more quickly and accurately, thereby enhancing response speed and processing efficiency

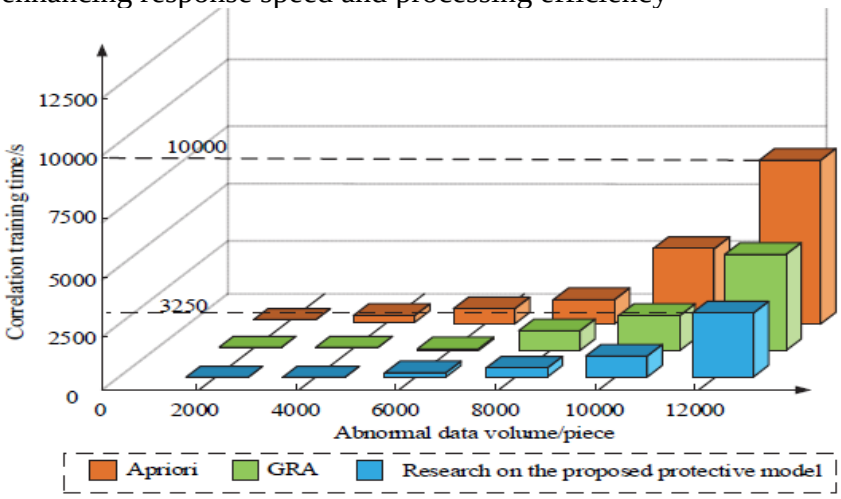

Figure 9 Abnormal data training results for different protection methods

To further assess the performance of the protection model, two different interconnected microgrid regional models are created on the Matlab platform. The configuration parameters for both regional models are nearly identical, with the only difference being the delays, set to 0.28 s and 0.08 s, respectively. Frequency deviation and tie-line power deviation are used as reference indicators. The models are tested under distributed denial of service attacks, and the results of the tests are presented in Fig. 10.

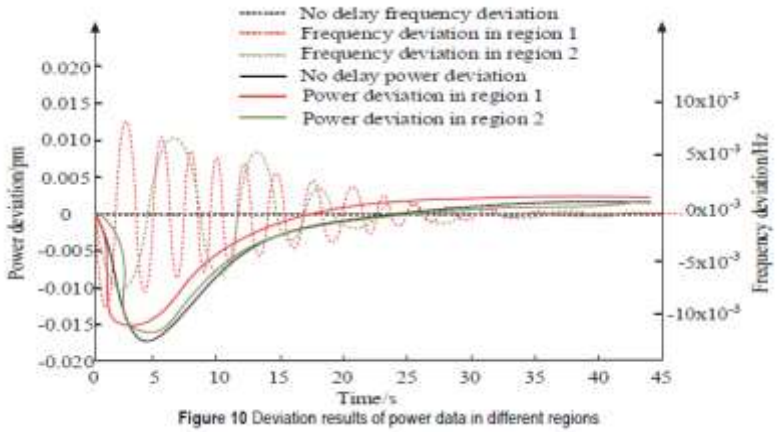

Figure 10 Deviation results of power data in different regions

In Fig. 10, the transmission frequency and power of the two micro grid region models are impacted differently when subjected to distributed denial of service attacks. When there is no attack, both regional models experience relatively small frequency and power deviations, and they can restore to their pre-

attack state. In the case of a smaller delay setting, i.e., Zone 2, the recovery time for both frequency and power increases to 35 seconds and 15 seconds, respectively. However, when the delay setting is larger, i.e., Zone 1, the system's stability is notably reduced, with significant fluctuations.

The recovery time for frequency and power in this case is 35 seconds and 20 seconds. Additionally, as the delay increases, the lowest point of the frequency continues to drop. In summary, regions with lower delays exhibit longer recovery times for frequency and power, emphasizing the significant impact of delay on network stability.

Taking Zone 2 as the experimental context, the frequency deviation and power deviation in the region before and after incorporating the protection model are examined to mitigate the impact of network attacks. The data results are shown in Fig. 11.

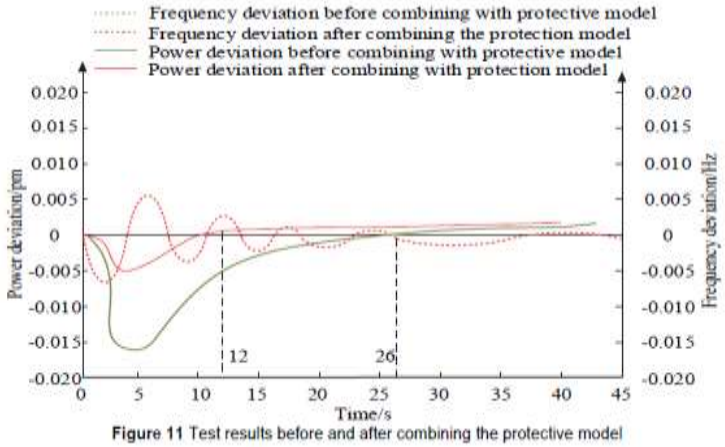

Figure 11 Test results before and after combining the protective model

From Fig. 11, it is evident that after experiencing a distributed denial of service attack, both the data transmission frequency and power are greatly affected in an unprotected power transmission network. After incorporating the proposed protection model, the recovery time for data transmission frequency is 26 seconds, and for power, it is 12 seconds.

These recovery times are reduced by 26% and 20%, respectively, compared to the previous network. In conclusion, the frequency and power deviation recovery times are notably shortened after integrating the protection model, demonstrating its effectiveness in mitigating network attacks and swiftly restoring normal operation. Moreover, the security protection model shows superior efficiency in detecting novel and complex network attacks, particularly when compared to earlier models that rely on static rules, by introducing an adaptive learning mechanism. Remarkably, the model excels in reducing false alarms, addressing a common issue in traditional security models and making it more suitable for countering the evolving threats in today's cyber security landscape.

CONCLUSION:

With the rise of big data and artificial intelligence, alongside the growing volume of communication network data, the security of existing power communication networks faces significant challenges. To address these challenges, this study aimed to optimize network data transmission methods and enhance security strategies by integrating Quality of Service (QoS) technology. This paper introduced two improved models: a bandwidth prediction model incorporating QoS technology and a security protection model utilizing Grey Relational Analysis (GRA). Comparative tests showed the superior performance of these new models compared to existing methods.

The proposed bandwidth prediction model achieved a maximum prediction rate of 2.21 Mbit/s and a bandwidth utilization of 78.89%, surpassing other models and demonstrating a 13% improvement over current methods. This contributes to enhanced power network planning.The security protection model reduced recovery times for frequency and power by 26% and 20%, respectively, after simulated network attacks, thus strengthening the network's resilience to attacks.The integration of QoS and security enhancement strategies offers significant network optimization and robustness.

In summary, this research presents innovative, data-driven optimization strategies that improve power network efficiency, planning, and security. The bandwidth prediction model, which uses advanced AI algorithms, outperforms traditional statistical or basic machine learning models, particularly in high-traffic environments. It shows exceptional efficiency in handling complex network behavior, overcoming the limitations of conventional models, and adapting to future high-bandwidth demands.

The security protection model also demonstrates excellent efficiency in detecting and defending against new and complex network attacks. By incorporating an adaptive learning mechanism, it reduces false alarms, addressing a common issue in traditional models and making it more suitable for the evolving cybersecurity landscape.

This study successfully develops an innovative bandwidth prediction and security model that significantly enhances the performance and security of power communication networks. By leveraging AI techniques, the bandwidth prediction model performs well in high-traffic environments, and the security protection model effectively identifies and defends against various cyber-attacks, particularly in reducing false alarms. These findings highlight the potential of applying AI to power communication networks, providing a foundation for future advances in network technology.

Furthermore, by improving the bandwidth prediction model and security protection strategies, this research contributes to more efficient and stable network performance for communication transmission networks in the power industry. The innovative application of QoS technology in network security provides a novel protection strategy for computer communication transmission networks within the power sector. This research offers critical theoretical support and practical strategies for network security in the power industry, especially in the context of network attacks and big data.

The results not only enhance the performance of electric power computer communication networks but also provide insights and solutions for similar challenges faced by other industries. These advancements have significantly improved the operational efficiency and security of the power communication network, offering crucial technical support and a theoretical foundation for addressing the challenges of future network technologies.

While this study has made considerable progress in bandwidth prediction and network security, some limitations remain. Primarily, the validity and accuracy of the models depend on the existing datasets, which could limit their adaptability to more complex or diverse network environments. Additionally, as network attack technology continues to evolve, security protection models may need to be continually updated to stay ahead of new threats. Future research should focus on applying these models to real-world power network environments and validating their performance. Furthermore, exploring the adaptability and scalability of the models in different network environments and broader application scenarios is essential. As data volume increases, optimizing the models to handle large-scale data while maintaining efficient network performance will be crucial.

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 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. IETinformation 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 EnergyResearch, 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 IntelligentSystems, 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 TelecommunicationsTechnologies, 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. Tehničkivjesnik, 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 mmWavebeamspace 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 ofSimulation, 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-assistedSecure Routing Protocol for Cluster-based Mobile-ad HocNetworks. International Journal of ComputersCommunications & Control, 18(2), 1-18.https://doi.org/10.15837/ijccc.2023.2.5144
16. Torre, P. S. & Hidalgo-Gonzalez, P. (2022). DecentralizedOptimal Power Flow for time-varying network topologiesusing 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 WebServices using Context-Aware Dynamic Bayesian NetworkModel. Tehničkivjesnik, 25(Supplement 2), 241-248.https://doi.org/10.17559/TV-20161104072515
18. John, Y. M., Sanusi, A., & Yusuf, I. (2023). ReliabilityAnalysis of Multi-Hardware–Software System with FailureInteraction. Journal of Computational and CognitiveEngineering, 2(1), 38-46.https://doi.org/10.47852/bonviewJCCE2202216
19. Ma, L., Christou, V., &Bocchini, P. (2022). Framework forprobabilistic simulation of power transmission networkperformance under hurricanes. Reliability Engineering andSystem 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 ControlRouting in Mobile Ad Hoc Networks for IntelligentTransportations Systems. Tehničkivjesnik, 31(1), 240-246.https://doi.org/10.17559/TV-20230427000582
21. Cao, Z., Huang, Q., & Wu, C. Q. (2020). MaximizeConcurrent Data Flows in Multi-radio Multi-channelWireless Mesh Networks. Computer Science andInformation Systems, 17(3), 759-777.https://doi.org/10.2298/CSIS200216019C.