ingegneria sismica
International Journal of Earthquake Engineering
Anno XLIII - Num. 1 - 2026

Research on Security Situational Awareness of Power Grid Communication Network Based on Multi-source Alarm Data Fusion

Yanyan Qin[1,*], *Guoshi Wang*[1], *Yan Wang*[1], *Junfei Zhang*[1] *and Liang Zhang*[1]

[1] The Information and Communication Branch of Hainan Power Grid, Haikou, Hainan, 570000, China

SUMMARY: *In the era of information, cybersecurity of communication networks of power grids has received increasing attention. In this paper, the important attributes are extracted from the alarm data of the multiple sources of the communication network of power grids. Based on these attributes, after time series construction, using multi-step deep learning and data dimensionality reduction techniques, spatiotemporal feature maps of the data are created. The security posture attributes of the communication network components of power grids are discretized using the 3σ criterion, and the Bayesian network is constructed to infer and generate the probability of security postures of network components. The results show that when attacks occur, the correlation of alerts varies between [0.56, 0.89], which shows considerable accuracy. The maximum security posture score of nodes exceeds 200 in all attack phases, showing a decreasing trend.*

KEYWORDS: *Multi-source alarm data; Spatio-temporal features; 3σ rule; Bayesian network; Security posture awareness; Power grid communications*

1 Introduction

With the rise of smart grids, various security threats have appeared in power grid communication networks. Smart grids rely more on the communication of digital information in real time, cover wider geographical areas, and contain more devices than traditional grids. At any node of the grid network, information security risks could occur. Once a security problem occurs, causing failure in the grid system, huge social and economic losses would occur, which can't be measured quantitatively [1-4]. From one side, due to the rapid development of information technology, new security issues should be solved. In recent years, frequent security problems in power grids have attracted wide public attention. From another side, the interaction among power control network and information communication network is still not clear. Combined malicious attacks against these two types of networks may lead to power outages in vast areas with disastrous impacts [5-9]. Hence, it is crucial to take security measures in power grid communication networks, the core of which is the network condition detection.

In order to strengthen the robustness and security of power grids, a mechanism for protection has been formulated by the network companies based on vertical authentication and horizontal isolation, as well as with the inclusion of other systems such as vulnerability assessment and firewalls [10, 11]. Considering the intricacies associated with power networks, security logs are not only enormous but also do not show any connectivity among themselves.

*a20240322@yeah.net
https://doi.org/10.65102/is2026133 Published: 30 April, 2026

In case of any attack, the staff may be required to gather information from various devices and deduce measures against them through analysis. In this way, efficiency and comprehensiveness are compromised [12-15]. Therefore, the need of the hour is to establish a system that allows the staff to monitor the network situation at all times. The Information Age has boosted the development of networks. It has resulted in a rise in both the size of the network as well as its complexity. The number of attacks and their tools has increased, making traditional security techniques obsolete [16, 17].

The concept of cybersecurity situational awareness involves studying the security elements that may affect cybersecurity; in addition, situational awareness involves the synthesis of cybersecurity incidents in order to arrive at meaningful conclusions [18, 19]. In the case of the power grid, cybersecurity situation is associated with the trends in terms of behavior of networks, users, and equipment. It thus requires a comprehensive evaluation of all security elements for efficient perception [20-22]. A power grid information security situational awareness system has been created by Xie and Chen [23] based on virus pre-detection and multidimensional security encryption/decryption computation. It improves the abilities of the system in the management of risk in power data as well as in situational awareness of security situations in the power grid information network. As a result, the transformation of cybersecurity situation awareness from passiveness to proactiveness has been achieved. The multi-scale online model of cybersecurity situational awareness in intelligent substation communication networks has been created by Hao et al. [24].

Liu et al. [25] developed a security situation awareness model for distribution network automation. Using data from multi-source perception factors obtained through sensors, they formulated a DS evidence fusion approach using the ant colony algorithm to integrate data. The model helped develop security situation awareness results. Qian and Xu [26] presented a model for situational awareness of cyber security of power grids under the OODA (Observation, Orientation, Decision, and Action) logic framework. In the model, fusion processing techniques, K-means algorithm to reduce noise in data, and visualization models for asset, vulnerability, and security risk perceptions have been integrated. With the incorporation of a gradient-boosted decision tree algorithm, the model creates an intelligent cyber security protection decision and reaction system. A cybersecurity situational awareness model was proposed by Cui et al. [27] through game theory, machine learning, and threat perception technology. With intelligent analysis assistance from security awareness platforms and intelligent evaluation systems, the cybersecurity situational awareness of data communication devices can be improved in terms of effectiveness and credibility. Hao et al. [28] presented a multi-source fusion data processing unit-assisted cybersecurity situational awareness model for novel power systems. It utilizes a collaborative hardware/software architecture that increases the processing speed and throughput of the system to improve network attack behavior recognition.

The cybersecurity situational awareness technology was created by Hao et al. [29] for 5G networks operated by power grid companies by employing fuzzy theory and gated recurrent units. Through the conversion of attacks and network information into quantitative indicators, real-time response can be achieved. Zhang et al. [30] constructed a machine learning-based power grid information security assessment model to analyze its cybersecurity situational awareness, adding a power grid security awareness system framework to assist grid supervision and promptly detect and respond to potential security issues. Within smart grids and power communication networks, Yu et al. [31] employed tensor computation to fuse heterogeneous and multidimensional big data. They established a situational awareness strategy based on tensor computation and deep reinforcement learning, incorporating multi-agent policy-value algorithms to optimize awareness strategies and enhance power grid communication system performance.

Addressing the need for multi-source alert data processing during power grid communication network security attacks, this paper proposes deep learning-based data fusion and probabilistic cybersecurity posture computation. Key fields from multi-source alerts are extracted to construct time-series data. Following dimensionality reduction preprocessing, deep learning networks perform spatio-temporal feature extraction, holistically correlating multi-source alert data related to power grid communication network security. Situation factors for power grid components undergo discretization, and distribution probabilities are calculated across three dimensions: fundamental operability, vulnerability, and threat level. After determining network parameters, a Bayesian network is constructed. Through Bayesian network inference, the security status of each power grid communication network component is assessed to determine the likelihood and specific location of potential power grid failures.

2 Multi-source Alarm Data and Power Grid Communication Network Security Situation Awareness

2.1 Deep Learning-Based Multi-Source Alarm Information Correlation Analysis

2.1.1 Multi-Source Alarm Information Correlation Analysis Process

This study aims to identify and detect attack behaviors from multi-source heterogeneous cybersecurity data, including firewall logs, network traffic, security alerts, and threat intelligence, thereby safeguarding the security of power grid communication networks. Given that the underlying data sources from these various information streams are dispersed, semantically diverse, and format-heterogeneous, we extract key fields from multi-source information, construct time-series data, and then employ deep learning to build feature maps, enabling the correlation of multi-source heterogeneous data.

Key fields extracted from firewall logs encompass communication information exchanged between external and internal interfaces, including: time, device IP, network protocol, source IP address, source MAC address, destination IP address, source port, destination port, etc.

The randomness and burstiness of network traffic introduce interference to cybersecurity detection. Key fields include: start time, duration, end time, source IP address, destination IP address, source port, destination port, packet count, packet size, bits per packet, and average packet size.

Security alert data contains explicit alert key fields, including: alert time, source IP address, destination IP address, source port, destination port, packet information, URL information, and security alert type.

Threat intelligence is evidence-based knowledge about existing or emerging threats to IT and information assets. Here, threat indicators, attack patterns, threat detection tools, and vulnerability information are extracted as key fields for threat intelligence.

Figure 1 illustrates the multi-source alert correlation analysis process. Based on acquired historical multi-source alert data, a multi-source alert time series dataset is constructed to perform preprocessing. Subsequently, feature extraction is applied to the multi-source alert time series data to build a spatio-temporal feature map. This feature map is utilized for attack behavior assessment, where an error function is calculated based on the assessment results to achieve adaptive network parameter updates.

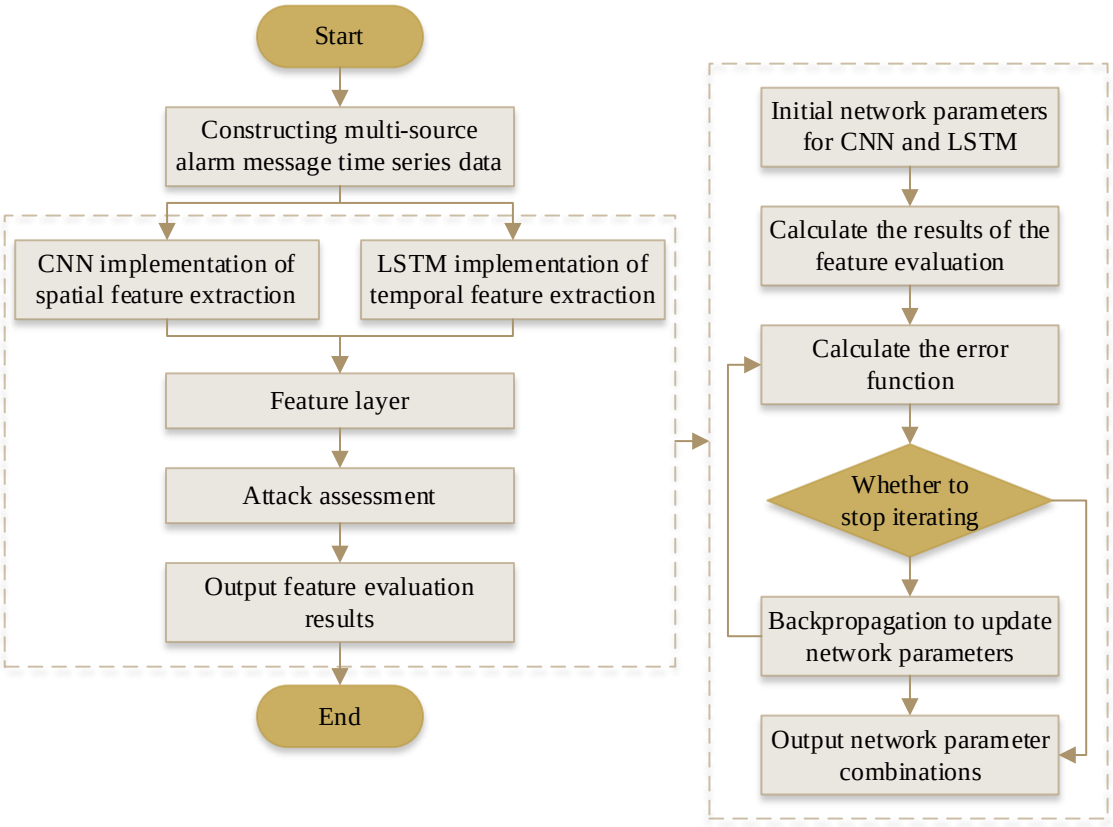

Figure 1: Multi-source alarm information correlation analysis process

2.1.2 Spatiotemporal Feature Extraction Process for Multi-source Alarm Information Data

The process of extracting spatio-temporal features from multi-source alarm information data includes the following: Firstly, a sliding window is applied to extract time series data from multi-source alarms to create samples of certain lengths that become the basic data source to extract spatio-temporal features from. Secondly, a Convolutional Neural Network (CNN) operates convolution and pooling operations on the sample to create spatial feature layers and output local spatial feature maps. Thirdly, the reconstruction of the matrix on the local spatial feature layer takes place. The use of the Long Short Term Memory (LSTM) neural network helps further extract the temporal features from alert information data and output the spatio-temporal feature layer. Lastly, using a Softmax classifier, classification and detection are done on the spatio-temporal features extracted.

2.2 Deep Learning-Based Dimension Reduction for Multi-Source Alarm Data

The multi-source alarm dataset can have lots of spatial and temporal features that interact with each other. As such, it will be necessary to implement feature selection and dimensionality reduction to increase analysis efficiency and effectiveness. Reduction of multiple security posture elements in multi-source alarms involves the process of extracting and integrating security postures using parallel processing.

The first approach to use is ELK stack architecture to collect big multi-source alert data. Figure 2 details the ELK stack architecture.

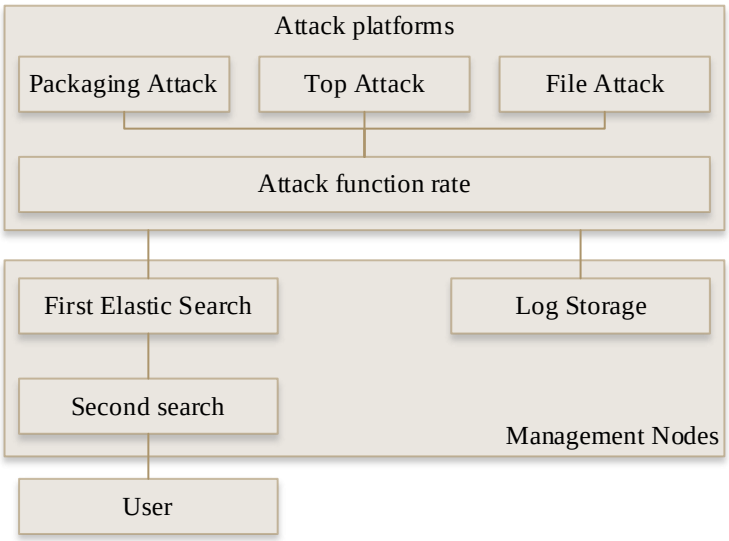

Figure 2: Structure of the ELK component

Splitting the multi-source alert data gathered by ELK parts is essential. One main idea in splitting the data is to divide the original data set into several subsets that can be processed separately, allowing for efficient utilization of computer processing power. The data is to be split by time period based on the timestamp. Assuming the received time data is T and the time interval is Δt, T can be divided into m sub-datasets, expressed as:

$$m = \frac{t_a - t_0}{\Delta t} \tag{1}$$

In the formula, t_a, t_0 denote the end time and initial time, respectively. Each sub-dataset contains data within the time interval $\left[t_0 + i\Delta t, t_0 + (i+1)\Delta t\right]$, where i represents the number of T in the dataset.

After completing data partitioning, dimensionality reduction must be applied to each sub-dataset. For each sub-dataset, let n denote the feature dimension of samples, r denote a set of feature parameters, and c denote the reduced dimension. The reduced-dimension dataset can then be expressed as:

$$x = mn \cdot rc \tag{2}$$

Each sub-dataset is mapped from its original high-dimensional space to a low-dimensional space, thereby reducing data complexity and dimensionality while enhancing processing efficiency. Simultaneously, the dimension-reduced data retains crucial features and information, improving data processing and analysis efficiency. This accelerates the identification and decision-making process for network cybersecurity posture elements, enabling subsequent posture element recognition and security posture assessment.

2.3 Process for Generating Cybersecurity Posture of Power Grid Communication Networks Under Data Fusion

2.3.1 Fundamentals of Security Situation Awareness

The posture factor of the grid communication component can be taken as discrete and continuous, in order to facilitate the application in the Bayesian network model, the continuous type is discretized, and the actual significance of the posture factor is decided according to the values of "high, medium, low" or "normal, general, abnormal" or "0.0, 1.0, 2.0" and so on. If the value is discrete, it can be unchanged.

Lemma 1: Let a continuous random variable $X \sim N\left(\mu, \sigma^2\right)$, then $Z = \dfrac{X-\mu}{\sigma} \sim N(0,1)$. Where: μ denotes the mathematical expectation of the random variable X; σ^2 denotes the variance. The probability of X falling in 3 different regions varies widely. In general, a continuous random variable can be discretized into 3 values in this way.

Definition 1: Let a vector $\mathbf{X} = \left(x_1, x_2, \cdots, x_m\right)^T$ be composed of random variables corresponding to m situation factor. An observation matrix $\mathbf{X}_{ij}$ consists of n observation values, where $i = 1, 2, \cdots, m, j = 1, 2, \cdots, n$. Then the j th column $x_{.j} = \left(x_{1j}, x_{2j}, \cdots, x_{mj}\right)^T$ represents the observation values of this m situation factor, and the i th row $x_{i.} = \left(x_{i1}, x_{i2}, \cdots, x_{in}\right)$ represents all n observation values of the i th situation factor x_i.

Definition 2: Let the L features form a vector $y_2, \cdots, y_L\big)^{\mathrm{T}}$, and an expert recommendation matrix $\mathbf{Y}_{ij}$ be formed from the n expert recommendation values, where $i = 1, 2, \cdots, L, j = 1, 2, \cdots, n$, then the j th column $y_{.j} = \left(y_{1j}, y_{2j}, \cdots, y_{Lj}\right)^{\mathrm{T}}$ is the one-time expert recommendation value for this L feature, and the i th row $y_{i.} = \left(y_{i1}, y_{i2}, \cdots, y_{in}\right)$ is all the n expert-recommended values for the i feature y_i.

When constructing a Bayesian network, leaf node variables (also known as random variables or state factors x_i) must first undergo preprocessing. For continuous variables x_i, they are discretized into three values: 0.0, 1.0, and 2.0. The specific procedure is as follows:

1) Collect n sample values of x_i and compute its mean $\overline{x}_i$, where the mathematical expectation of x_i is $E\left(x_i\right) = \mu = \overline{x}_i$;

2) Similarly, compute the variance of x_i: $D\left(x_i\right) = \sigma^2 = S^2$;

3) Divide x_i into three intervals using the method described above;

4) When obtaining a specific value x_{ij} for x_i, assign the corresponding discrete value based on which interval it falls into.

Definition 3: From a physical perspective, a state factor can be represented by a leaf node, while its observed value can be described by a random variable x_i. Anomalies in the random variable x_i typically fall outside the 3σ region, accounting for a small proportion of probabilities; occurrences within the buffer zone represent a moderate probability; and normal conditions generally fall within the 3σ region, accounting for the largest proportion of probabilities. This is known as the "3σ rule."

2.3.2 Constructing Network-Level Bayesian Networks

When each component i is reasoned about the 3 different dimensions of the security posture from below through a Bayesian net, the 3 values taken for each of the different dimensions generate the probabilities P_{ijk} ($i=1,2,\cdots,N$ denotes the component, $j=1,2,3$ denotes the dimensional component, $k=0,1,2$ denotes the value taken for the (discrete values). For example, the probabilities of component i when its base operability takes the values of "normal, fair, and abnormal" are P_{i10}, P_{i11}, and P_{i12}, respectively; and the corresponding probabilities of vulnerability of component i are P_{i20}, P_{i21}, and P_{i22}, respectively; The corresponding probabilities of the threatening nature of component i are P_{i30}, P_{i31} and P_{i32}.

The work in this section, how to reason upwards from N component probabilities P_{ijk} obtained by inference to the probabilities P_{jk} of the 3 dimensions of the network. The probabilities P_{jk} of the 3 dimensions of the network are then reasoned upwards to form the network security posture SA_n.

In the dimension j of the network security posture j($j=1$ for base operability, $j=2$ for vulnerability, and $j=3$ for threat), the probability of taking the value k is calculated as

$$P_{jk}=\frac{1}{N}\sum_{i=1}^{N}P_{ijk} \tag{3}$$

From this, a network-level Bayesian network can be built, and the corresponding three dimensions of the network can be obtained from the N component 3-dimensional probabilities P_{ijk}, each with a probability of P_{jk}, for a total of 9 probability values.

2.3.3 Parameter learning

The construction of a Bayesian net requires the determination of its network parameters, i.e., the prior probability table (PPT) for each leaf node and the conditional probability table (CPT) for non-leaf nodes, which can be obtained by adopting a Bayesian learning approach to them.

1) Construction of PPT. If the leaf nodes take continuous values, because of the need to discretize them, their prior probabilities are used as the reference of the distribution probabilities in the "3σ rule", and the key is to have objectivity in the selection of the α virtual data samples.

If the leaf nodes would have taken discrete values, it is assumed that the corresponding random variables of the leaf nodes obey the Dirichlet distribution $D[\alpha_1,\alpha_2,\cdots,\alpha_n]$, n denotes the number of nodes, i.e., there are:

$$p(\theta)=\frac{\Gamma(\alpha)}{\prod_{i=1}^{n}\Gamma(\alpha_i)}\prod_{i=1}^{n}\theta_i^{a_i-1} \tag{4}$$

where $\alpha=\sum_{i=1}^{n}\alpha_i$, where assuming $p(\theta)$ for the Dirichlet distribution is equivalent to assuming that prior knowledge about θ is equivalent to α dummy data samples, where the number of samples that satisfy $X=x_i$ is α_i. It can be roughly scaled to satisfy

$\alpha_0 / \alpha = PS_0, \alpha_1 / \alpha = PS_1, \alpha_2 / \alpha = PS_2$.

Given θ, the conditional probability $p(D|\theta)$ of a sample D is called the likelihood function of θ satisfying the binomial distribution:

$$\begin{aligned} L(\theta|D) &= p(D|\theta) = \prod_{i=1}^{n} \theta_i^m i \\ p(\theta|D) &\propto p(\theta)L(\theta|D) = \prod_{i=1}^{n} \theta_i^{m_i+a_i-1} \end{aligned} \tag{5}$$

That is, $p(\theta|D)$ obeys the Dirichlet distribution $D[\alpha_1+m_1, \alpha_2+m_2, \cdots, \alpha_n+m_n]$, after sample learning, the next sample is a Bayesian estimate (probability) of x_i:

$$p(D_{m+1} = x_i | D) = \int \theta_i p(\theta|D) \mathrm{d}\theta = \frac{m_i+\alpha_i}{m+\alpha}, m = m_1+m_2+\cdots+m_n \tag{6}$$

2) CPT construction. Denote by θ_{ijk} the conditional probability that $y_i = k$ at the ith child node y_i with parent state $II_i = j$.

Let r_j denote the number of values of the variable x_j of one parent node of y_i, then $q_i = II_{x_j \in u_i} r_j$ denotes the number of states of all the parent nodes of y_i, i.e., the product of the number of states of all of its parents. If the child node y_i has three parents taking consecutive values, the total number of states of its parents is 3 × 3 × 3.

Under the parameter independence assumption, each variable y_i and its parent state $II_i = j$ obey the Dirichlet distribution:

$$\begin{aligned} p(\theta_{ij1}, \theta_{ij2}, \theta_{ij3}) &= \mathrm{Dir}(\alpha_{ij1}, \alpha_{ij2}, \alpha_{ij3}) \\ L(\theta|D) &= p(D|\theta) = \prod_{i=1}^{n} \prod_{j=1}^{q_i} \prod_{k=1}^{r_i} \theta_{ijk}^{m_{ijk}} \end{aligned} \tag{7}$$

The posterior distribution under the dataset D remains a Dirichlet distribution:

$$\begin{aligned} p(\theta_{ij1}, \theta_{ij2}, \theta_{ij3}|D) &= \mathrm{Dir}(\alpha_{ij1}+n_{ij1}, \alpha_{ij2}+n_{ij2}, \alpha_{ij3}+n_{ij3}) \\ p(\theta|D) &\propto p(\theta)L(\theta|D) = \prod_{i=1}^{n} \prod_{j=1}^{q_i} \prod_{k-1}^{r_i} \theta_{ijk}^{m_{ijk}+\alpha_{ijk}-1} \end{aligned} \tag{8}$$

where y_i has 3 values, α_{ijk} is the a priori information, and n_{ijk} is the observations of the data D.

Similarly, the following formula can be used to calculate the conditional probability:

$$
\begin{aligned}
&E\left(\theta_{ijk} \mid D\right)=\frac{\alpha_{ijk}+n_{ijk}}{\alpha_{ij}+n_{ij}} \\
&\alpha_{ij}=\sum_{k=1}^{3}\alpha_{ijk}, n_{ij}=\sum_{k=1}^{3}n_{ijk} \\
&p\left(D_{m+1}=x_i \mid D\right)=\int \theta_i p(\theta \mid D)\mathrm{d}\theta \\
&\theta_{ijk}=\frac{m_{ijk}+\alpha_{ijk}}{\sum_{k=1}^{r_i}\left(m_{ijk}+\alpha_{ijk}\right)}
\end{aligned}
\tag{9}
$$

2.3.4 Generating a cybersecurity posture

Upon collecting real-time data for all situational factors X_i, after discretization via the "3σ rule", the probability $P_{ijk}(i=1,2,\cdots,N, j=1,2,3, k=0,1,2)$ of component i (which can be regarded as a leaf node in the network) is obtained through Bayesian network inference rules. Starting from the probability P_{ijk} of component i, network-level Bayesian network inference generates the three-dimensional probability values $P_{jk}(j=1,2,3, k=0,1,2)$ of the network. . This enables the generation of the component security posture SA_c vertically and the network security posture SA_n horizontally. The methods for generating SA_c and SA_n are similar; the following explanation uses the generation of the network security posture SA_n as an example.

Based on expert experience, the weights assigned to each dimension are $w_i(i=1,2,3), w_1+w_2+w_3=100.00$; This paper defines the network's security posture as a three-dimensional weighted composite of its foundational operability, vulnerability, and threat exposure. The value for each dimension is calculated by multiplying the assigned weight by the probability of taking value 0 (P_{j0}) minus the probability of taking value 2 (P_{j2}). Since P_{j2} typically exhibits minimal fluctuation even during anomalies, since normal components constitute the majority. To facilitate differentiation, P_{j2} is scaled by a factor of λ, yielding:

$$
SA_{\mathrm{n}}=\sum_{j=1}^{3} w_j\left[P_{j0}-\lambda \cdot P_{j2}\right] \tag{10}
$$

The generation of a component's security posture SA_c follows a similar process. When a component's security posture falls below a set threshold, it proactively sends an anomaly signal to the network management center. Alternatively, when the security postures of a majority of components become abnormal, this is immediately reflected as an anomaly in the network security posture SA_n. Based on the received anomaly signals, the location of the abnormal components can then be pinpointed.

3 Cybersecurity Practices for Power Grid Communication Networks Under Multi-Source Alarm Data Fusion

3.1 Attack Scenario Assessment and Multi-Source Alert Data Preparation

To collect effective multi-source alert data, this section extracted 15 power grid communication network attacks from public datasets, encompassing 5 attack types, as individual behaviors

involving interactions between non-malicious and malicious power grid communication system entities. Simultaneously, to ensure the validity of these network attacks and enhance the accuracy of multi-source alert data collection, attack data statistics and validity checks were performed on these 15 attack scenarios. Table 1 presents statistics on attack nodes, connected edges, and interaction data for the five attack types. Table 2 shows statistical data on attack detection results for these five attack types. Among the 15 selected network attacks across five categories, these attacks pose threats to power grid communication network security through extensive node connections and both benign and malicious interaction behaviors. For example, for "backdoor extension" attack category, a total of 1,057 interaction nodes were found including 553 benign and 504 malicious nodes, almost half with potential vulnerabilities. The main performance metric for attack validation is "the number of samples that actually comprise attacks and that are identified correctly." The TP counts for the five attack types reached 1,020, 261, 54,927, 16, and 15 respectively, each accounting for over 90% of the total node count. This indicates that the selected network attacks are effective and can collect usable multi-source alert data for power grid communication network security situation awareness research.

Table 1: Five types of attack nodes, links, and interaction statistics

Type of attack	Number of nodes	Number of edges			Interaction count	
		Ancestry chart	Bipartite graph	Knowledge Graph	Benign	Maliciousness
Expanding the backdoor	1057	1374	1057	2431	553	504
Firefox backdoor	265	283	265	548	102	163
Pine Back Door	55083	55201	55083	110284	3840	51243
The executable file for fishing	19	18	19	37	6	13
The executable file for Infectious virus	16	13	16	29	2	14

Table 2: Statistics of attack detection results for 5 types of attacks

Type of attack	Test results			
	TP	TN	FP	FN
Expanding the backdoor	1020	21	14	2
Firefox backdoor	261	3	1	0
Pine Back Door	54927	121	30	5
The executable file for fishing	16	2	1	0
The executable file for Infectious virus	15	1	0	0

3.2 Analysis of Alarm Data Correlation and Application Effectiveness

3.2.1 Correlation Analysis of Alarm Data

Preprocess the collected alert data and generate a Bayesian alert correlation graph by adding correlation constraints between various alerts based on their interrelationships. Conditional probabilities between different alert types can be derived from historical attack data across multiple network attacks. The resulting conditional probability matrix (CPM) further enriches the alert data. The conditional probability matrix comprises conditional probabilities between different alert types. Figure 3 presents the CPM for five super-alert categories. Enriching the alert data related to these five types of cyberattacks reveals diverse conditional probabilities

between categories: S1:S2=0.62, S1:S3=0.45, S2:S1=0.85, S3:S1=0.93... Such rich associations between the alert data support the process of logical analysis of the cybersecurity state of communication network of power grids.

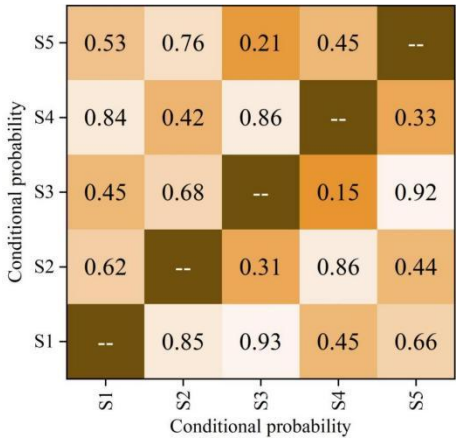

Figure 3: The conditional probability matrices of the 5 major alarm categories

3.2.2 Correlation Results Analysis

After enriching the correlation of alert data, we compare the matching results for different vulnerabilities and attack patterns to ensure the effectiveness of subsequent correlation and inference in the Bayesian alert correlation graph. This section uses two attack patterns—phishing program executables and infectious virus files—as examples to simulate the similarity and correlation of vulnerabilities displayed in alert data when the power grid communication network is subjected to a specific external attack. Figure 4 presents the correlation results for the two attack patterns. When attacked by phishing program executables, the correlation coefficients of 19 nodes in the alert data ranged from 0.22 to 0.56. In contrast, when attacked by infectious virus files, the correlation coefficients of 16 nodes in the alert data ranged from 0.36 to 0.65. The vulnerability similarity and correlation revealed by the alert data association for infectious virus files are higher than those for phishing executable files. This aligns with the comparison results of attack intensity between the two attack patterns.

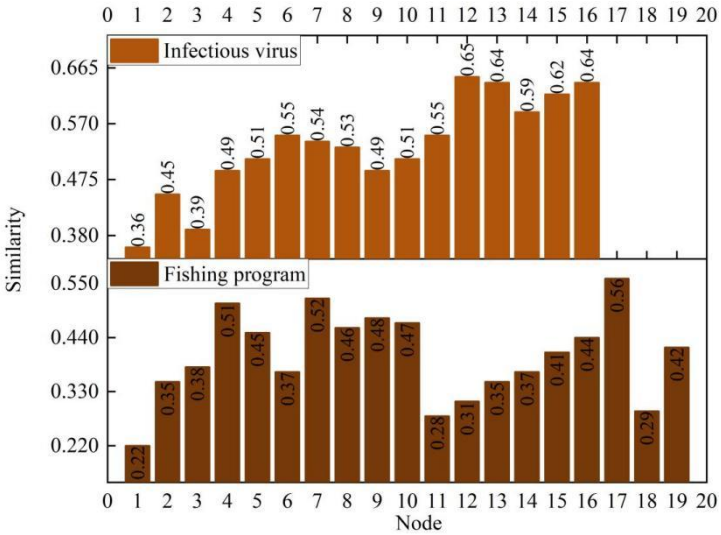

Figure 4: The alarm correlation results of the two attack modes

Combining two types of cyberattacks to exploit vulnerabilities in power grid communication networks. Figure 5 shows the correlation results of the combined attack. When the two attack patterns are combined, the correlation of the alarm data across 19 nodes increases to the range [0.56, 0.89], indicating that the correlation of alarm data changes with the attack pattern. Through the attack-alarm data correlation, it can be determined that the constructed alarm correlation network possesses relatively accurate predictive capabilities.

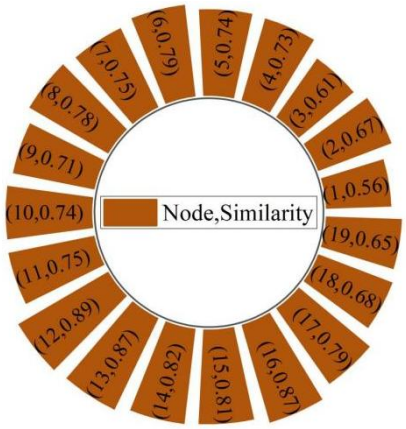

Figure 5: Correlation results of combined attack of 2 types of network attacks

3.3 Assessment of Cybersecurity Posture in Power Grid Communication Networks Based on Alarm Data

3.3.1 Node Security Posture Assessment

A total of 15 network attacks with 5 patterns were made against the power grid communications network, generating 5 alarm correlation data sets. For each attack step, the cybersecurity posture evaluation was performed. Posture computation and data fusion were done through approaches such as parameter learning. As the network comprises a massive number of hosts and the same actions are taken by each attack step, the following results of Phase One will be given focusing on key hosts. Phase One mainly focused on active host discovery using the IPsweep attack method. This is achieved by scanning through five different IP addresses as nodes and sending many ICMP probe packets, which produced many echo requests and replies. Improperly configured ICMP is the main vulnerability exploited. With regards to the mentioned services and vulnerabilities, the following table gives the fusion results of certain vital nodes. From the fusion results, it is evident that the security posture in Phase 1 is high. The P(St) values for the five nodes are 0.945, 0.952, 0.917, 0.958, and 0.962 respectively—all exceeding 0.900. There were multiple warnings generated throughout these nodes along with the existence of vulnerabilities that can enable attacks, leading to an increase in their composite postures. Network administrators should be more cautious about this issue.

Table 3: The integrated results of the situations of some key nodes

Host address	P(St)	P(Valus)	M	A	S
188.76.162.210	0.945	0.95	3	8	10.54
190.78.160.212	0.952	0.95	3	8	10.98
192.84.168.222	0.917	0.91	2	6	9.76
200.80.160.208	0.958	0.96	4	9	11.05
204.78.164.216	0.962	0.96	4	9	11.64

Since this experiment primarily targets these five IP nodes to analyze their security posture, the following outlines the security posture trends of these five nodes across 15 attack phases. The trends of security postures of the five nodes can be seen in Fig. 6. By obtaining the quantified security posture values of the nodes, we can get the trends of changes in overall security postures of the power grid communication network during different attack periods through corresponding calculation formulas. The trend of security posture changes of the power grid communication network is illustrated in Fig. 7. The highest security postures of the five nodes were achieved in the third attack period, which were 200.183, 216.408, 191.795, 226.552, and 239.454 respectively—more than 200. At this point, the power grid communication network faced the most severe security threats. Higher security status values indicate greater risks. As the attack proceeds, the corresponding administrators make responses according to the alert correlation data, ensuring that most of the security statuses' values remain under 150. In general, the security status of nodes first rose during the attack period and then fell because of human intervention.

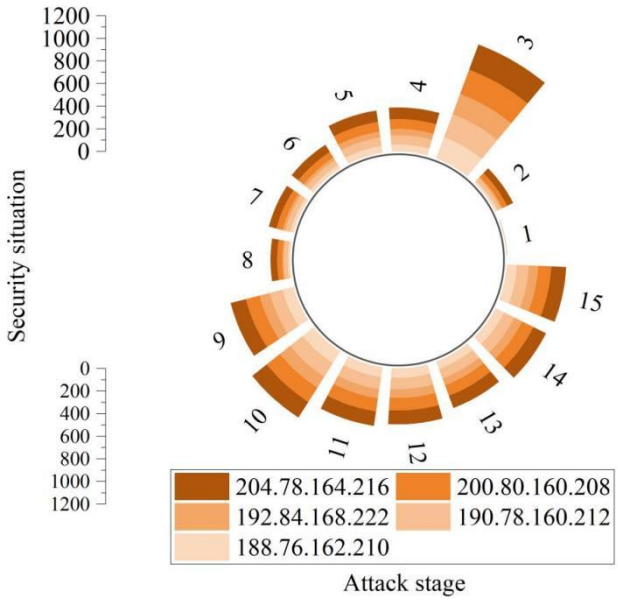

Figure 6: The security situation trends of the 5 nodes

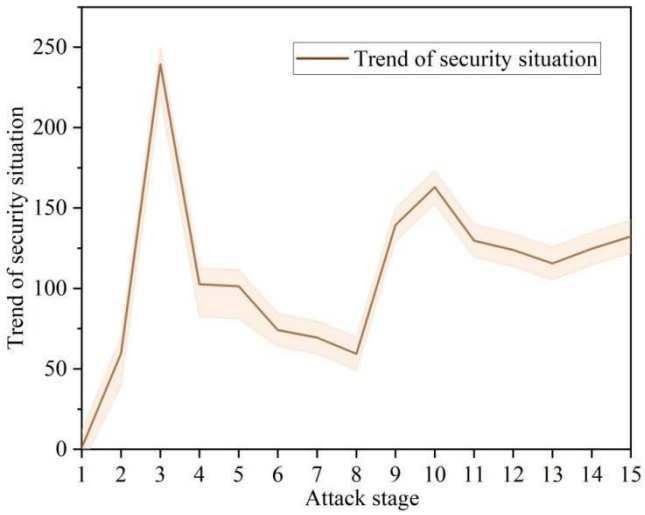

Figure 7: The trend of cybersecurity in power grid communication networks

3.3.2 Comparison of Results from Various Experimental Methods

In order to illustrate the efficiency of the proposed multi-source alarm data fusion approach in this paper, another two comparison approaches have been chosen to make comparisons. Table 4 below is the comparison result of the three approaches. The D-S synthesis approach and Yager synthesis approach show that there exists an inconsistency with common sense that when one error occurs with a probability of 0.000, the following probabilities will be extremely large or extremely small at 0.000 or 1.000. However, the synthesis of the attack probability using this paper's fusion approach shows that the results are consistently at 1.000 and no extremely large or extremely small value occurs in m(Y) or m(N).

Table 4: The comparison results of the three integration methods

	D-S Synthesis Rule			Yager synthesis rule			This paper integrates method		
	m(Y)	m(N)	m(⊖)	m(Y)	m(N)	m(⊖)	m(Y)	m(N)	m(⊖)
1	0.923	0.077	0.000	0.923	0.077	0.000	0.923	0.077	0.000
2	0.000	1.000	0.000	0.000	0.000	1.000	0.789	0.211	0.000
3	0.923	0.077	0.000	0.923	0.077	0.000	0.923	0.077	0.000
4	0.000	1.000	0.000	0.000	0.000	1.000	0.211	0.789	0.000
5	0.000	1.000	0.000	0.000	0.000	0.000	0.789	0.211	0.000
6	0.000	1.000	0.000	0.000	0.000	1.000	0.211	0.789	0.000
7	0.923	0.077	0.000	0.923	0.077	0.000	0.923	0.077	0.000
8	0.000	1.000	0.000	0.000	0.000	1.000	0.789	0.211	0.000
9	0.000	1.000	0.000	0.000	0.000	0.000	0.923	0.077	0.000
10	0.000	1.000	0.000	0.000	0.000	1.000	0.211	0.789	0.000
11	0.923	0.077	0.000	0.923	0.077	0.000	0.789	0.211	0.000
12	0.000	1.000	0.000	0.000	0.000	1.000	0.211	0.789	0.000
13	0.000	1.000	0.000	0.000	0.000	0.000	0.923	0.098	0.000
14	0.000	1.000	0.000	0.000	0.000	1.000	0.211	0.789	0.000
15	0.923	0.077	0.000	0.000	0.000	0.000	0.789	0.211	0.000

4 Conclusion

The paper employs multi-source alarms in the power grid communication networks that are under attack for predicting possible failures in the communication network. In a single-vector attack, the correlation between the alarm data is in the range of 0.22-0.56 or 0.36-0.65. During a hybrid attack, alarm data correlation rises to become in the range of 0.56-0.89. There are real time dynamics observed in alarm correlation. In phase three of the attack, five nodes had their security status reach their peak status of 200.183, 216.408, 191.795, 226.552, and 239.454 before falling as a result of manual control.

About the Authors

Yanyan Qin (1989-12), female, Zhuang Nationality, Haikou, Hainan, bachelor degree, engineer, main research direction network security.

Guoshi Wang (1986-6), male, Han Nationality, Hainan Haikou, master degree, associate senior engineer, research interests network security, safe operation.

Yan Wang (1993-6), female, Han Nationality, Hainan Qionghai, bachelor degree, engineer, research direction: network security of ubiquitous power Internet of Things.

Junfei Zhang (1990-4), male, Han Nationality, Yuanping, Shanxi Province, bachelor degree, engineer, research direction safety operation.

Liang Zhang (1983-1), male, Han Nationality, Haikou, Hainan, bachelor degree, engineer, research direction: power communication network architecture, transmission technology and security.

References

[1] El Mrabet, Z., Kaabouch, N., El Ghazi, H., & El Ghazi, H. (2018). Cyber-security in smart grid: Survey and challenges. Computers & Electrical Engineering, 67, 469-482.

[2] Lamba, V., Šimková, N., & Rossi, B. (2019). Recommendations for smart grid security risk management. Cyber-Physical Systems, 5(2), 92-118.

[3] Islam, S. N., Baig, Z., & Zeadally, S. (2019). Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures. IEEE Transactions on Industrial Informatics, 15(12), 6522-6530.

[4] Peng, C., Sun, H., Yang, M., & Wang, Y. L. (2019). A survey on security communication and control for smart grids under malicious cyber attacks. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(8), 1554-1569.

[5] Pereira, T., Barreto, L., & Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. Procedia manufacturing, 13, 1253-1260.

[6] Wu, Y., Ru, Y., Lin, Z., Liu, C., Xue, T., Zhao, X., & Chen, J. (2022). Research on cyber attacks and defensive measures of power communication network. IEEE internet of things journal, 10(9), 7613-7635.

[7] Tu, C., He, X., Liu, X., & Li, P. (2018). Cyber-attacks in PMU-based power network and countermeasures. IEEE Access, 6, 65594-65603.

[8] Chen, Z., Wu, J., Xia, Y., & Zhang, X. (2017). Robustness of interdependent power grids and communication networks: A complex network perspective. IEEE Transactions on Circuits and Systems II: Express Briefs, 65(1), 115-119.

[9] Chehri, A., Fofana, I., & Yang, X. (2021). Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence. Sustainability, 13(6), 3196.

[10] Jarmakiewicz, J., Parobczak, K., & Maślanka, K. (2017). Cybersecurity protection for power grid control infrastructures. International Journal of Critical Infrastructure Protection, 18, 20-33.

[11] Huang, X., Qin, Z., & Liu, H. (2018). A survey on power grid cyber security: From component-wise vulnerability assessment to system-wide impact analysis. IEEE Access, 6, 69023-69035.

[12] Ashok, A., Govindarasu, M., & Wang, J. (2017). Cyber-physical attack-resilient wide-

area monitoring, protection, and control for the power grid. Proceedings of the IEEE, 105(7), 1389-1407.

[13] Natarajan, A. K., Galety, M. G., Noekhah, S., Soundararajan, R., Xurshed, S., & Xasan, Z. (2024, November). Enhancing Cybersecurity in Smart Grid Systems Through Advanced Log File Analysis with Machine and Deep Learning Techniques. In 2024 Third International Conference on Sustainable Mobility Applications, Renewables and Technology (SMART) (pp. 1-10). IEEE.

[14] Cheng, K., Tang, W., Tan, L., Yang, J., & Chen, J. (2025). SLNALog: A log Anomaly Detection Scheme Based on Swift Layer Normalization Attention Mechanism for Next-Generation Power Communication Networks. IEEE Transactions on Network and Service Management.

[15] Wang, Q., Tai, W., Tang, Y., & Ni, M. (2019). Review of the false data injection attack against the cyber-physical power system. IET Cyber-Physical Systems: Theory & Applications, 4(2), 101-107.

[16] Soltan, S., Yannakakis, M., & Zussman, G. (2018). REACT to cyber attacks on power grids. IEEE Transactions on Network Science and Engineering, 6(3), 459-473.

[17] Amin, B. R., Taghizadeh, S., Rahman, M. S., Hossain, M. J., Varadharajan, V., & Chen, Z. (2020). Cyber attacks in smart grid–dynamic impacts, analyses and recommendations. IET Cyber-Physical Systems: Theory & Applications, 5(4), 321-329.

[18] Zhang, J., Feng, H., Liu, B., & Zhao, D. (2023). Survey of technology in network security situation awareness. Sensors, 23(5), 2608.

[19] Li, Y., Huang, G. Q., Wang, C. Z., & Li, Y. C. (2019). Analysis framework of network security situational awareness and comparison of implementation methods. EURASIP Journal on Wireless Communications and Networking, 2019(1), 205.

[20] Nafees, M. N., Saxena, N., Cardenas, A., Grijalva, S., & Burnap, P. (2023). Smart grid cyber-physical situational awareness of complex operational technology attacks: A review. ACM computing surveys, 55(10), 1-36.

[21] Lei, W., Wen, H., Wu, J., & Hou, W. (2021). MADDPG-based security situational awareness for smart grid with intelligent edge. Applied Sciences, 11(7), 3101.

[22] Kim, K., Youn, J., Kim, H., Shin, D., & Shin, D. (2024). State-of-the-Art in Cyber Situational Awareness: A Comprehensive Review and Analysis. KSII Transactions on Internet & Information Systems, 18(5).

[23] Xie, M., & Chen, Z. (2020). A Situation Awareness System for the Information Security of Power Grid. Journal of Computers, 31(1), 192-198.

[24] Hao, W., Yang, Q., Li, Z., Hu, S., Liu, B., & Ruan, W. (2022). Multi-scale traffic aware cybersecurity situational awareness online model for intelligent power substation communication network. IEEE Internet of Things Journal, 10(2), 1666-1681.

[25] Liu, J., Yang, H., Qu, Q., Liu, Z., & Cao, Y. (2024). Research on distribution automation

security situational awareness technology based on risk transmission path and multi-source information fusion. Cybersecurity, 7(1), 57.

[26] Qian, J., & Xu, H. (2022, October). Research on network security situational awareness technology for building multi-element, integrated and highly elastic power grid. In The International Conference on Forthcoming Networks and Sustainability (FoNeS 2022) (Vol. 2022, pp. 424-428). IET.

[27] Cui, X., Xia, F., Meng, F., Ning, L., & An, X. (2025, April). Investigation on Security Situation Awareness and Intelligent Evaluation of Data Communication Network Equipment. In Proceedings of the 2nd International Conference on Machine Intelligence and Digital Applications (pp. 243-249).

[28] Hao, J., Li, Y., Bai, H., Dong, X., Wang, H., & Xiao, Y. (2024, September). DPU-Enhanced Network Security Situation Awareness Model for New Power Systems. In Proceedings of the 2024 3rd International Conference on Algorithms, Data Mining, and Information Technology (pp. 294-299).

[29] Hao, Y., Ming, J., Wang, D., Liangjie, C., Wei, W., & Yuxiang, L. (2024, March). Intelligent Awareness Method of Power 5G Network Security Situation Based on Neural Network and Fuzzy Theory. In 2024 IEEE 7th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) (Vol. 7, pp. 1142-1145). IEEE.

[30] Zhang, X., Shen, W., & Cui, L. (2023, November). Power Network Security Situation Analysis Based on Machine Learning. In 2023 3rd International Conference on New Energy and Power Engineering (ICNEPE) (pp. 1023-1026). IEEE.

[31] Yu, Q., Wang, X., Lv, D., Qi, B., Wei, Y., Liu, L., ... & Zhang, W. (2023). Data fusion and situation awareness for smart grid and power communication network based on tensor computing and deep reinforcement learning. Electronics, 12(12), 2606.