IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 1 November 2023, accepted 20 November 2023, date of publication 24 November 2023,
date of current version 6 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3336698

RESEARCH ARTICLE

A Security Situation Prediction Model for Industrial Control Network Based on EP-CMA-ES

YUHE WANG[1], YU YANG[1], RENCAI GAO[2], SHIMING LI[1], AND YAN ZHAO[3]
[1]College of Computer Science and Information Engineering, Harbin Normal University, Harbin 150025, China
[2]College of Computer Science, Baicheng Normal University, Baicheng 137000, China
[3]School of Information Technology, Luoyang Normal University, Luoyang, Henan 471934, China

Corresponding authors: Rencai Gao (rencai_gao@163.com), Shiming Li (hsdlsm@163.com), and Yan Zhao (zhaoyan@lynu.edu.cn)

This work was supported in part by the Provincial Universities Basic Business Expense Scientific Research Projects of Heilongjiang Province under Grant 2021-KYYWF-0179, in part by the Key Scientific Research Project of Henan Province under Grant 21A413001, in part by the Postgraduate Innovation Project of Harbin Normal University under Grant HSDSSCX2023-10, in part by the Social Science Foundation of Heilongjiang Province of China under Grant 21GLC189, and in part by the National Cultivation Fund of Luoyang Normal University under Grant KJQN202001212.

ABSTRACT To solve the problem of industrial control network (ICN) security situation prediction, this paper proposes a security situation prediction model for ICN based on evidential reasoning (ER) and belief rule base (BRB). First, this paper analyzes multiple factors influencing the security situation of the ICN, establishes a framework for security situation assessment, employs the ER algorithm for attribute fusion, and derives the security situation value of the ICN. Second, using historical data combined with expert knowledge, a security situation prediction model for ICN based on the BRB is constructed. Additionally, an extended projection covariance matrix adaptive evolution strategy (EP-CMA-ES) optimization algorithm is proposed, which is employed to optimize the parameters of the prediction model. The model not only comprehensively uses qualitative knowledge and quantitative data, but also integrates more uncertain information, and the reasoning process is interpretable. It also solves the subjectivity problem of expert knowledge, overcomes the problem of small amount of data caused by the difficulty of collecting industrial control safety data, and improves the accuracy of model prediction. Finally, prediction experiments were conducted on industrial datasets, confirming the feasibility and effectiveness of the security situation prediction model for ICN and the EP-CMA-ES optimization algorithm proposed in this paper.

INDEX TERMS Industrial control network, evidential reasoning, belief rule base, security situation, projection covariance matrix adaptive evolution strategy.

I. INTRODUCTION

Industrial control systems (ICSs) are commonly utilized in industrial sectors and critical infrastructure, such as nuclear power plants, thermal power plants, water treatment facilities, power generation, heavy industries, and distribution systems. The functions of ICS, such as automatic control, remote monitoring and optimal adjustment, have greatly improved the efficiency of industrial production [1]. Due to the requirements of large-scale industrial production informatization and intelligence, ICS has progressively integrated technologies such as networking and cloud computing. The emergence of ICN has exposed ICS to most attack vectors using network attacks [2]. However, the capability of ICS to withstand such sophisticated attacks is significantly lower. Low security will severely affect production, equipment, quality, data, and personnel safety and even result in substantial economic losses, reputational damage, and personal injuries [3].

In recent years, there has been a surge in network attacks targeting ICN. For instance, on September 22, 2022, a large-scale network attack hit the Ukraine region, resulting in significant damage to multiple electricity systems and power outages in 40 substations [4]. Similarly, on May 7, 2021, a hacker attack targeted the Colonial Pipeline, the largest refined oil pipeline operator in the United States. It caused

The associate editor coordinating the review of this manuscript and approving it for publication was Chun-Hao Chen.

destructive impacts on the energy supply along the U.S. East Coast. This incident represents the most severe cyberattack ever experienced by the U.S. energy industry. Moreover, in 2020, the Kazan power plant in Russia fell victim to a hacker attack. The attackers used phishing emails to obtain login credentials of the power plant employees and used these credentials to infiltrate the control systems, resulting in equipment damage and a subsequent power outage accident. In 2018, one of the world's largest beer manufacturers, Anheuser-Busch InBev, had one of its factories targeted by ransomware attacks. It caused production interruptions and data losses, significantly impacting the company's supply chain. Furthermore, the increasing breadth of research on the reliability and forecasting of industrial and energy systems [5], [6] underscores the necessity of industrial safety state prediction and warning.

Traditional IT networks are composed of computers, routers, various servers, and other network devices. In contrast, ICNs consist of different industrial control systems, including sensors, controllers, actuators and so on, making their architecture more complex [7]. The enormous scale, distributed structure, and diverse devices and protocols of industrial control networks make them highly heterogeneous and complex. If predicting the security of complex ICNs based on observable network attack data and corresponding methodologies [8], a greater multitude of factors need to be considered. Moreover, these factors often exhibit varying degrees of uncertainty [9], [10], [11]. The distinctiveness of industrial control systems and their high-security demands complicate the collection of security-related data, resulting in limited availability of data [12], [13]. Hence, the establishment of a prediction model for industrial control network security situation not only necessitates the incorporation of diverse factors influencing network security but also demands adept handling of various forms of uncertain information. Furthermore, it is imperative to ensure effective and accurate prediction of the security situation of ICN while operating with limited data volumes.

The focus of security situation prediction for ICN lies in using historical information to establish a model for forecasting the security trends of future network systems. Methods for industrial control network security situation prediction can be primarily categorized into four types: those based on statistical analysis models, those based on qualitative knowledge, those based on quantitative data, and those based on semiquantitative information.

(1) Methods based on statistical analysis models: This category of methods requires the construction of accurate mathematical formulas and extensive computations, but they may face challenges in achieving precise security situation prediction for complex network systems. For instance, methods such as Kalman filters [14], strong tracking filters [15], and particle filters [16] fall into this category. These methods can only offer approximate security situation prediction when they are unable to establish intricate mathematical models for complex network systems, resulting in less precise forecasts.

(2) Methods based on qualitative knowledge: This category of methods utilizes expert knowledge and qualitative information to construct models. However, expert knowledge is subjective leading to the drawback of uncertainty. Additionally, these models cannot effectively leverage quantitative information. For example, methods based on Petri nets [17] and expert systems [18] fall into this category. Due to the complexity of network systems, an accurate prediction model requires not only qualitative knowledge but also quantitative data.

(3) Methods based on quantitative data: This category of methods utilizes existing quantitative data for analysis and modelling, employing techniques such as data mining and machine learning to predict network security situations. It requires the use of a substantial amount of data to discover potential patterns and trends. For example, methods based on BPNN [19], RBF [20], and support vector machines [21] all fall into this category. However, due to the specificity of industrial control networks, collecting data for such complex systems is challenging, which can lead to less accurate results in model training, thus affecting the precision of the predictions.

(4) Methods based on semi-quantitative information: This category of methods combines qualitative and quantitative information, utilizing technologies such as fuzzy logic and belief rule bases to predict security situations. It can handle uncertain and fuzzy information, providing more flexible and comprehensive prediction results. For example, methods based on hidden Markov models [22], [23], fuzzy neural networks [24], and LSTM with Bayesian optimization algorithms [25] fall into this category. These methods are capable of addressing uncertain information by integrating qualitative and quantitative information for security situation prediction. With the involvement of expert knowledge during the initial stages, methods based on semi-quantitative information can accurately predict network security situations even with small sample datasets. However, within the intricate structure of ICNs, there exist various forms of uncertain information, but the existing methods based on semi-quantitative information are limited to handling individual information of uncertainty.

In this paper, the evidential reasoning (ER) algorithm [26] is employed to integrate various factors affecting the security situation of ICNs and evaluate them. A security situation prediction model for ICN is established based on belief rule base (BRB) [27]. Moreover, an extended projection covariance matrix adaptive evolution strategy (P-CMA-ES) [28] is proposed, and this algorithm is utilized to optimize the parameters of the prediction model. The employment of the ER iterative fusion algorithm enables effective utilization of semi-quantitative information, amalgamating a greater array of uncertain factors. The modelling process of the BRB is based on the ER rule representation method, rendering it interpretable and the model's output results traceable. This

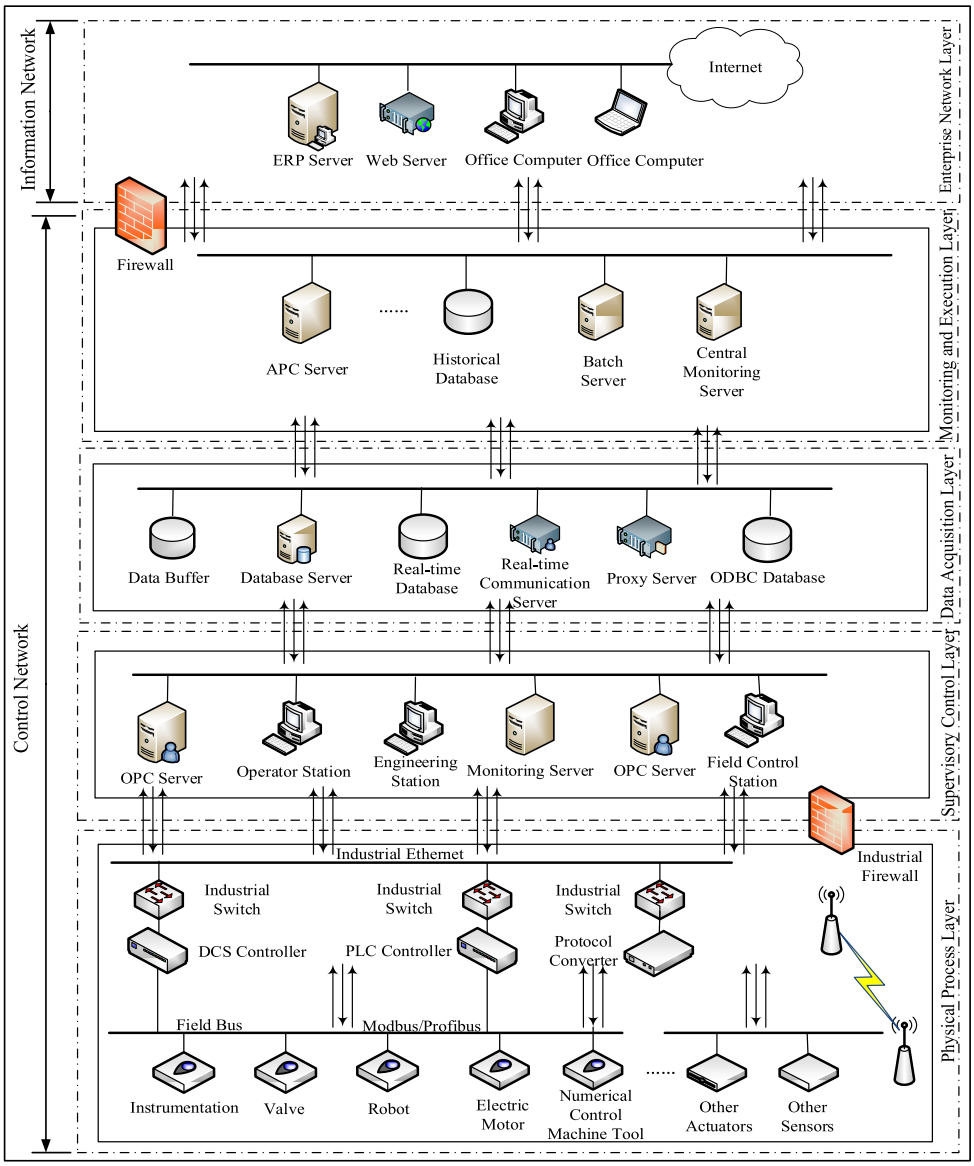


FIGURE 1. Topology diagram of the ICN.

overcomes the issue of lower modelling accuracy stemming from challenges in collecting data from complex industrial control networks with limited datasets. The application of the extended projection covariance matrix adaptive evolution strategy (EP-CMA-ES) addresses subjective aspects of expert knowledge, thus enhancing the accuracy of the prediction model.

In section I, the current situations of ICS security situation prediction are introduced, and the construction of a security situation prediction model for ICN based on EP-CMA-ES is proposed. In section II, the problem of security situation prediction is described. In section III, a detailed introduction is given to the process of building the model. In section IV, experiments are conducted on industrial datasets to demonstrate the effectiveness of the model proposed in this paper. In section V, a summary of the entire work is provided.

II. PROBLEM DESCRIPTION

The prediction of ICN security situations is divided into the following tripartite segments:

(1) Prior to conducting security situation prediction, it is essential to perform a security situation assessment. This involves analyzing the factors influencing the ICN security situation to determine assessment indicators and establish the evaluation framework. Due to the complexity of ICNs, the assessment indicators are numerous, diverse in type, and subject to significant uncertainty. By employing the ER iterative algorithm, the fusion of multiple uncertain indicators can be addressed.

(2) The prediction of the security status at time t+1 is conducted based on the security situation values of the ICN at times t-1 and t. A BRB prediction model is established by harnessing expert knowledge and system data.

(3) As the uncertainty of expert knowledge may result in reduced model accuracy, the EP-CMA-ES algorithm is used to optimize the model parameters and enhance the accuracy of the prediction model.

A. INDUSTRIL CONTROL NETWORK

The types of components included in different industrial control networks may vary depending on the process and production environment. However, they can generally be categorized into three groups: computer-type intelligent components, embedded-type intelligent components, and non-intelligent components [2]. By integrating the structural model standard of industrial control networks published by ANSI/ISA-99 [3] and the cloud manufacturing system framework [29], an Industrial Control Network topology diagram was constructed, as shown in Figure 1.

The ICN is divided into 5 layers: Enterprise Network Layer, Supervisory and Execution Layer, Data Acquisition Layer, Monitoring Layer, and Physical Process Layer. The Enterprise Network Layer serves as the office network, primarily involved in activities such as business planning, human resources, and logistics management. The Supervisory and Execution Layer functions as the production execution network, which is responsible for centralized production process monitoring and production planning at the management center level. The Data Acquisition Layer operates as the data collection network, mainly performing single or multi-point process data collection or transformation on control devices. The Monitoring Layer acts as the control network, primarily responsible for station-level monitoring of production processes, logic modifications, and dissemination. Finally, the Physical Process Layer serves as the field process network, executing various physical processes.

The ICN is further divided into two parts: the information network that handles industrial control system management and decision-making information and the control network that processes real-time measurement and control information in the control field. The information network includes the Enterprise Network Layer, situated in the upper layers of the enterprise, dealing with vast, variable, and diverse information, characterized by high speed and comprehensiveness. On the other hand, the control network comprises the Supervisory and Execution Layer, Data Acquisition Layer, Monitoring Layer, and Physical Process Layer, situated in the lower layers of the enterprise, handling real-time, on-site information with features of strong real-time capability and robust security.

Due to the connection between the Enterprise Network Layer and the enterprise-level IT network, it is highly likely to face security threats from the internet, posing risks to sensitive information and business systems within the enterprise. In contrast, the control network is typically purpose-designed for industrial control systems, with relatively fixed and specialized architectures and protocols. Given its involvement in actual physical processes and device control, the security of the control network is of paramount importance. However, control networks often use outdated control protocols and devices, leading to lower security levels. This vulnerability may render them susceptible to network attacks.

TABLE 1. Parameter definitions.

Parameter	Definition
r	the attack frequency of a certain type of attack
d	the severity of a certain type of attack
a	the fusion result of the attack frequency and severity of a certain type of attack
$\varpi(\bullet)$	the nonlinear function used for data fusion in the ER algorithm
I	the information network assessment result of the ICN
C	the control network assessment result of the ICN
O	the network security situation assessment result of the ICN

B. INTEGRATION OF EVALUATION INDICATORS

By progressively integrating the four-level evaluation indicators of the ICN, a model is established to assess the security state of the ICN. The model construction is represented as Equation (1). The specific meanings of the parameters in Equation (1) are presented in Table 1.

$$\begin{cases} a_i = \overline{\omega}(r_i, d_i)\ (i = 1, 2, \cdots, n) \\ a_j = \overline{\omega}(r_i, d_i)\ (\mathrm{j} = n+1, n+2, \cdots, n+m) \\ I = \overline{\omega}(a_1, a_2, \cdots, a_n) \\ C = \overline{\omega}(a_{n+1}, a_{n+2}, \cdots, a_{n+m}) \\ O = \overline{\omega}(I, C) \end{cases} \tag{1}$$

where r and d are fourth-level assessment indicators, a is a third-level assessment indicator, I and C are second-level evaluation indicators, and O is a first-level assessment indicator.

C. SECURITY SITUATION PREDICTION

Based on the results of ICN security situation assessment and expert knowledge, a security situation prediction model of ICN is established. This model utilizes the values of the network security situation at times t-1 and t to forecast future network security status. The prediction outcomes are denoted by y, and the model's construction is depicted as shown in Equation (2).

$$y = \mathrm{BRB}(\mathrm{O}(t-1), \mathrm{O}(t), \eta) \tag{2}$$

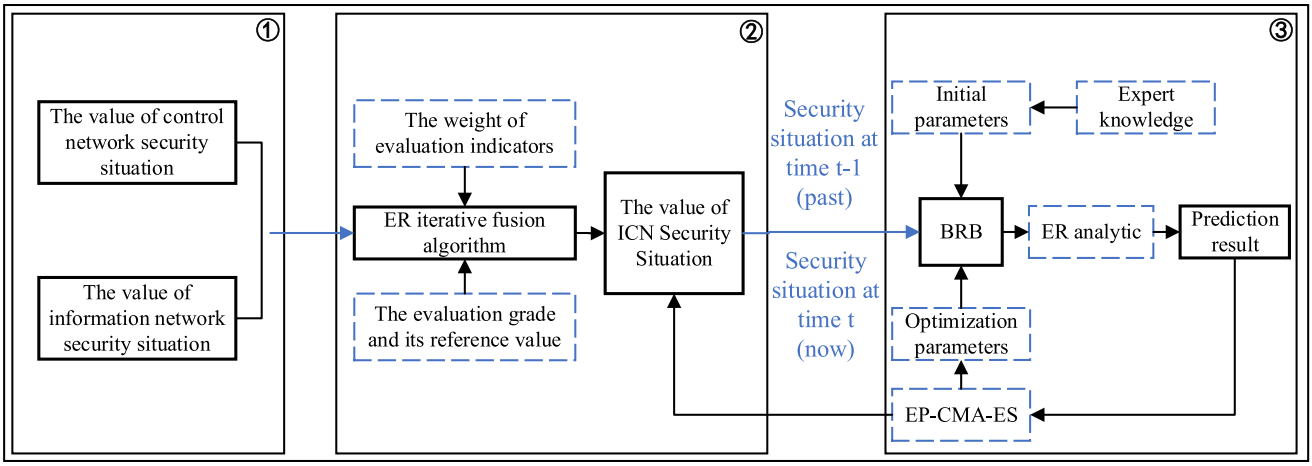


FIGURE 2. Process of ICN security situation prediction.

Among them, BRB (·) represents the non-linear transformation process from the fusion results of assessment indicators based on BRB to prediction outcomes, while η denotes the parameter set of BRB.

D. OPTIMIZATION OF THE PREDICTION MODEL

Due to the complexity of real network systems and the influence of environmental disturbances, the information provided by experts is uncertain. Therefore, optimization of the prediction model's parameters is imperative. Building upon the foundation of the P-CMA-ES, we propose an EP-CMA-ES. By utilizing this algorithm, the prediction model is optimized to improve the accuracy of the ICN security situation prediction model.

III. A SECURITY SITUATION PREDICTION MODEL FOR ICN BASED ON EP-CMA-ES

A. IMPLEMENTATION PROCESS OF ICN SECURITY SITUATION PREDICTION

Step 1: Analyze the influencing factors of the ICN security situation, determine evaluation indicators, and construct a four-level evaluation framework for the ICN.

Step 2: Following the four-level assessment framework for Industrial Control Networks, the ER algorithm is employed to progressively aggregate upwards, yielding the values of the ICN security situation. The security situation of the ICN at times t-1 and t are taken as antecedent attributes for the prediction model based on BRB.

Step 3: Initiate the parameters of the BRB prediction model based on expert knowledge. Then, the EP-CMA-ES optimization algorithm is employed to improve the accuracy of the prediction model, resulting in the ultimate prediction values for the ICN security situation.

The process of ICN security situation prediction is illustrated in Figure 2.

B. IMPLEMENTATION PROCESS ESTABLISHMENT STABLISHMENT OF THE EVALUATION FRAMEWORK

Based on the characteristics of ICN and considering real-world security threats, a four-level evaluation framework for ICN is established. This paper divides the ICN into two parts: the information network, which handles management and decision information for industrial control systems, and the control network, which manages real-time measurement and control information at the control site. Representative security indicators are selected as evaluation attributes to establish the security evaluation framework for the ICN, taking into account the impact of the security situation and practical considerations. The four-level evaluation framework table for ICN is established, as depicted in Table 2.

Based on Table 2, the first-level evaluation indicators encompass the information network and the control network. Given that different network types may be susceptible to distinct threats, information networks may be more vulnerable to the influence of general network threats such as malicious software, data leakage, and unauthorized access. Consequently, the subsequent assessment level for information networks pertains to the various types of attacks experienced by the information network. However, control networks typically encompass control and monitoring devices for industrial processes, such as sensors, actuators, and programmable logic controllers (PLCs). These devices are crucial for the proper functioning of industrial operations. Therefore, it is essential to establish the next-level assessment indicator for control networks, focusing on the devices within the control network that may be vulnerable to attacks. The third-level assessment indicator for control networks pertains to the primary attacks experienced by each type of device. Finally, the final level assessment indicators for both information networks and control networks are the severity and frequency of each attack type. Attack frequency involves quantitative data and is derived from calculating the number of attacks in the collected dataset through statistical means. Attack severity is

TABLE 2. The four-level evaluation framework for ICN.

Indicators	The 1st level	The 2nd level	The 3rd level	The 4th level
ICN (R)	Information Network(r1)	Injection Attack (r11)	Attack frequency (r111)	None
			Attack severity (r112)	None
		DDoS Attack (r12)	Attack frequency (r121)	None
			Attack severity (r122)	None
		Backdoor Attack (r13)	Attack frequency (r131)	None
			Attack severity (r132)	None
		Password Attack (r14)	Attack frequency (r141)	None
			Attack severity (r142)	None
	Control Network (r2)	Historical/Real-time Database (r21)	Scanning vulnerability (r211)	Attack frequency (r2111)
				Attack severity (r2112)
			General scanning (r212)	Attack frequency (r2121)
				Attack severity(r2122)
			Error data injection (r213)	Attack frequency (r2131)
				Attack severity (r2132)
			Ransomware (r221)	Attack frequency (r2211)
				Attack severity (r2212)
		Asset Management System (r22)	Ransom Denial of Service(r222)	Attack frequency (r2221)
				Attack severity (r2222)
			Resource Discovery (r223)	Attack frequency (r2231)
				Attack severity (r2232)
		Industrial Gateway (r23)	Modbus Register Read (r231)	Attack frequency (r2311)
				Attack severity (r2312)
			Brute Force Attack (r232)	Attack frequency (r2321)
				Attack severity (r2322)
			Reverse Shell Attack (r233)	Attack frequency (r2331)
				Attack severity (r2332)
			Man-in-the-Middle Attack (r234)	Attack frequency (r2341)
				Attack severity (r2342)

qualitative knowledge determined by experts based on their own experience and actual investigations.

C. ER-BASED ICN SECURITY SITUATION ASSESSMENT

Industrial control networks are characterized by their large scale and complex architecture, encompassing various types of information, including qualitative knowledge and quantitative data. The ER algorithm can simultaneously integrate these diverse types of information, particularly when handling uncertain and vague qualitative knowledge. The calculation process of the ICN security situation assessment value is illustrated as follows:

Step 1: First, the attribute values and their corresponding weights in the ICN security situation assessment framework are determined, where $\{r_1, r_2, \ldots r_a, \ldots, r_x\}$ represents the x attributes in the four-level assessment framework, $\{w_1, w_2, \ldots w_a, \ldots, w_x\}$ corresponds to the weights of these underlying attributes, and $w_x \in [0, 1]$. The output evaluation level consists of N levels.

Step 2: Calculate the confidence levels corresponding to q evaluation levels for each assessment attribute, with the calculation process as follows:

$$\rho_{a,q} = \begin{cases} \dfrac{R_{a,q+1} - U(r_a)}{R_{a,q+1} - R_{a,q}} & (R_{a,q} \le U(r_a) \le R_{a,q+1}) \\ \dfrac{U(r_a) - R_{a,q}}{R_{a,q+1} - R_{a,q}} & \\ 0 & (k = 1, \cdots, N, m \ne q, q+1) \end{cases} \tag{3}$$

where $U(r_a)$ represents the value of attribute r_a, and $R_{a,q}$ represents the reference value of attribute r_a in the *qth* evaluation level.

Step 3: Convert the confidence to the basic probability mass. The calculation process is shown as follows:

$$Q_{a,q} = \omega_a \rho_{a,q} \tag{4}$$

$$Q_{a,\Theta} = 1 - \omega_a \sum_{q=1}^{N} \rho_{a,q} \tag{5}$$

$$\overline{Q}_{a,\Theta} = 1 - \omega_a \tag{6}$$

$$\widetilde{Q}_{a,\Theta} = \omega_a(1 - \sum_{q=1}^{N} \rho_{a,q}) \tag{7}$$

where $Q_{a,q}$ represents the basic probability mass for the *qth* evaluation level of the *ath* assessment attribute and $Q_{a,\Theta}$ represents the basic probability mass for the *ath* assessment attribute that is not allocated. $\overline{Q}_{a,\Theta}$ represents the insignificance of the *ath* assessment attribute, while $\tilde{Q}_{a,\Theta}$ represents the incompleteness of the *pth* assessment attribute. Based on formulas (5) to (7), $Q_{a,\Theta} = \overline{Q}_{a,\Theta} + \tilde{Q}_{a,\Theta}$ can be obtained.

Step 4: The evaluation indicators are progressively fused using the ER iterative algorithm.

First, the fusion of attack frequency and severity for the fourth-level indicators is conducted, resulting in assessment outcomes for various attack types in the third-level indicators. Subsequently, the assessment outcomes of different attack types are further combined to obtain assessment results for information security and control security in the second-level indicators. The final value of the ICN security situation is obtained by merging the two indicators from the second level using the ER algorithm. The ER algorithm's iterative fusion process is as follows:

1) Calculate the combined probability mass

$$\begin{aligned} Q_{S(a+1),q} &= K_{S(a+1)}[Q_{S(a),q}Q_{a+1,q} \\ &\quad + Q_{S(a),q}Q_{a+1,\Theta} + Q_{S(a),\Theta}Q_{a+1,q}] \end{aligned} \tag{8}$$

$$Q_{S(a),\Theta} = \overline{Q}_{S(a),\Theta} + \widetilde{Q}_{S(a),\Theta} \tag{9}$$

$$\begin{aligned} \widetilde{Q}_{S(a+1),\theta} &= K_{S(a+1)}[\widetilde{Q}_{S(a),\theta}\widetilde{Q}_{a+1,\theta} + \widetilde{Q}_{S(a),\theta}\overline{Q}_{a+1,\theta} \\ &\quad + \overline{Q}_{S(a),\theta}\widetilde{Q}_{a+1,\theta}] \end{aligned} \tag{10}$$

$$\overline{Q}_{S(a+1),\theta} = K_{S(a+1)}[\overline{Q}_{S(a),\theta} + \overline{Q}_{a+1,\theta}] \tag{11}$$

In equations (8) to (11), $Q_{S(a),q}$ represents the combined probability mass quality relative to the *pth* evaluation level after the fusion of the first p evaluation attributes. It can be computed using Equation (12):

$$K_{S(a+1)} = \left[1 - \sum_{m=1}^{N} \sum_{q=1,q\neq m}^{N} M_{S(a),m}M_{a+1,m}\right]^{-1} \tag{12}$$

2) Calculate the combined belief mass using equations (13) and (14), as shown below:

$$\rho_q = \frac{P_{S(L),q}}{1 - \bar{P}_{S(L),\theta}} (q = 1, 2, \ldots, N) \tag{13}$$

$$\hat{\rho}_\Theta = \frac{\tilde{P}_{S(L),\Theta}}{1 - \overline{P}_{S(L),\Theta}} \tag{14}$$

where $\hat{\rho}_q$ represents the confidence level relative to the evaluation result Θ_q, and $\hat{\rho}_\Theta$ represents the confidence level not assigned to any evaluation result Θ_q.

3) Combine all confidence rules using the ER parsing algorithm to obtain the final confidence distribution result S(L).

$$S(L) = \{(\Theta_q, \rho_q), q = 1, 2, \cdots, N \tag{15}$$

Step 5: Calculate the fusion result

Assuming that the utility set of evaluation indicators is $P(\theta_q)$, the fusion result can be calculated using the utility formula.

$$O(t) = \sum_{p=1}^{N} P(\theta_q)\rho_{q,\mathcal{S}(L)} \tag{16}$$

The final evaluation result is quantified to the range [1, 0], where a lower evaluation result indicates a safer ICN.

D. BRB-BASED ICN SECURITY SITUATION PREDICTION

Use the ICN security state at times t-1 and t to predict the values of the security situation at time t+1.

The prediction model of the ICN security situation based on BRB can be described as follows:

R_k: If $O(t-1)$ is $A_1^m \wedge O(t)$ is A_2^m,
Then $O(t+1)$is $+1)$ is $\{(I, \rho_{1,m}), (II, \rho_{2,m}), (III, \rho_{3,m}), (IV, \rho_{4,m}), (V, \rho_{5,m})\}$
With rule weight θ_m and attribute weight δ_1, δ_2

where O(t-1) and O(t) represent the ICN security situation values at times t-1 and t, respectively. O(t+1) represents the predicted ICN security situation at time t+1. A_1^m and A_2^m represent the reference values of the two input attributes for the *kth* rule in the model, $\rho_{n,m}$ represents the confidence level of the n-th evaluation grade for the *mth* rule, θ_m represents the weight of the *kth* rule, and δ_1, δ_2 represents the weights of the two input attributes.

The BRB method uses the ER parsing algorithm to infer the ICN security situation prediction model. The detailed calculation process is as follows:

Step 1: Initialization

Based on expert knowledge, set the initial parameters of the BRB prediction model, including attribute weights δ_i, rule weights θ_m representing the relative importance of each rule, and the confidence of the model's output $\rho_{n.m}$.

Step 2: Calculate the attribute matching degree

The degree of matching between the premise attributes and the rules is determined by formula (3) when the data of the premise attributes are available.

Step 3: Calculate the overall matching degree

The overall matching degree of multiple attributes is calculated using Equation (17).

$$\alpha_m = \prod_{i=1}^{M} (\alpha_m^i)^{\delta_i} \tag{17}$$

Step 4: Calculate the activation weights.

Once the input attribute data is available, it activates the belief rules within the evaluation model and calculates the activation weights using Equation (18).

$$w_m = \frac{\theta_m \alpha_m}{\sum_{l=1}^{K} \theta_l \alpha_m} 0 \leq w_m \leq 1, \sum_{m=1}^{K} w_m = 1 \tag{18}$$

Step 5: Combinate Rules

After the activation of the belief rules, the combination of rules is performed using the ER parsing algorithm, and the calculation formulas are shown in (19) and (20), at the bottom of the page.

Step 6: Calculate utility

After obtaining the confidence degree of each evaluation level, the utility formula is used to calculate the final prediction of the ICN, which is the predicted security status of the ICN.

$$O(t+1) = \sum_{n=1}^{N} P(\theta_n)\rho_n \tag{21}$$

E. THE EP-CMA-ES ALGORITHM IS EMPLOYED TO OPTIMIZE THE PREDICTIVE MODEL

Due to the uncertainty of the expert knowledge used in the ICN security situation prediction model, it is necessary to optimize the prediction model using optimization algorithms. Traditional optimization algorithms strictly adhere to the threshold range of candidate solutions. However, exceptions may occur when the following two situations arise: (1) The global optimal solution is located at or near the boundary of the feasible domain; (2) The feasible domain occupies a very small proportion of the search space. In both cases, an infeasible solution that is close to the optimal solution may be more critical than a feasible solution that is far from the optimal solution. Therefore, this paper makes an improvement based on the P-CMA-ES algorithm. According to the degree of constraint violation of infeasible solutions, the search range is expanded. Feasible solutions and infeasible solutions containing important information are allowed to enter the next generation population simultaneously. Then, the projection operator in P-CMA-ES is used to correct solutions that do not satisfy the constraints. The EP-CMA-ES algorithm is used to optimize the parameters of the predictive model to enhance its accuracy.

The parameters of the prediction model are optimized. The optimization model and constraints for the ICN security prediction model are represented as follows in Formula (22).

$$\begin{aligned} &\min MSE(\delta_i, \theta_m, \rho_{n,m}) \\ &s.t. \quad 0 \le \delta_i \le 1, i = 1, \ldots, M \\ &\qquad 0 \le \theta_m \le 1, m = 1, \ldots, L \\ &\qquad 0 \le \rho_{n,m} \le 1, n = 1, \ldots, N, \ k = 1, \ldots L \\ &\qquad \sum_{n=1}^{N} \rho_{n,m} \le 1, \ m = 1, \ldots L \end{aligned} \tag{22}$$

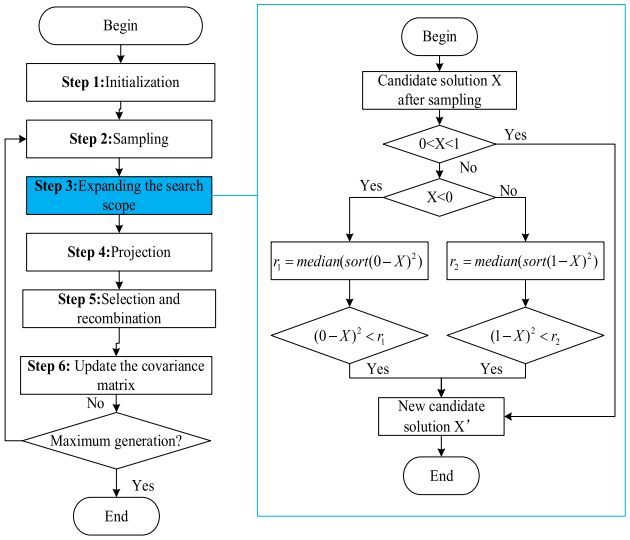


FIGURE 3. The process flow of the EP-CMA-ES algorithm.

In this context, *MSE* (•) represents the mean squared error function, which reflects the accuracy of the BRB-based ICN security prediction model. It is calculated using the following formula:

$$MSE(\theta_m, \rho_{n,m}, \delta_i) = \frac{1}{T}\sum_{t=1}^{T}(output_{estimated} - output_{actual})^2 \tag{23}$$

where $output_{actual}$ signifies the factual security status of the ICN, while $output_{estimated}$ represents the outcome derived from the predictive model's computation utilizing the formula $output_{estimated} = \sum_{n=1}^{N} P(\theta_n)\rho_n$. Here, T stands for the number of training samples. The primary goal in model optimization is the minimization of the mean squared error (MSE), and lower MSE values correspond to higher accuracy of the prediction model. The procedure of the EP-CMA-ES algorithm is visually depicted in Figure 3.

The step-by-step calculation process is outlined as follows:

Step 1 Initialization

$$\rho_n = \frac{\psi\left[\prod_{m=1}^{M}(w_M\rho_{n,m} + 1 - w_m\sum_{j=1}^{N}\rho_{j,m}) - \prod_{m=1}^{M}(1 - w_m\sum_{j=1}^{N}\rho_{j,m})\right]}{1 - \psi\left[\prod_{m=1}^{M}(1 - w_m)\right]} \tag{19}$$

$$\psi = \left[\sum_{n=1}^{N}\prod_{m=1}^{M}(w_m\rho_{n,m} + 1 - w_m\sum_{j=1}^{N}\rho_{j,m}) - (N-1)\prod_{m=1}^{M}(1 - w_m\sum_{j=1}^{N}\rho_{j,m})\right]^{-1} \tag{20}$$

Determination of the initial parameter vector Ω^0, which serves as the initial expectation for the EP-CMA-ES algorithm. The description of Ω^0 is as follows:

$$\Omega^0 = \left\{\theta_1, \ldots, \theta_K, \rho_{1,1}, \ldots, \rho_{N,K}, \delta_1, \ldots, \delta_M\right\} \tag{24}$$

Step 2 Sampling

Perform a selection operation to generate the population using Equation (29).

$$\Omega_k^{t+1} \sim m^t + s^t N(0, CM^t) k = 1 \cdots \lambda \tag{25}$$

where Ω_k^{g+1} is the kth offspring of the g+1 generation, $m^g m^g$ is the mean of the t+1 generation, s^t is the overall dimension that controls the distribution, called the step size, and the sampling population follows a normal distribution with a covariance matrixCM^t.

$$m^t + s^t N(0, CM^t) \sim N(m^t, (s^t)^2 CM^t) \tag{26}$$

Step 3 Expanding the search space

Based on the constraint conditions, the randomly generated population can be divided into feasible and infeasible solutions. The degree of constraint violation of infeasible solutions is sorted, and a new boundary threshold is determined according to formula (29). Infeasible solutions within the threshold range are retained, considering them to contain important information. These infeasible solutions are then treated as candidate solutions to participate in the subsequent optimization process.

The detailed process is shown below:

(1) Calculate the constraint violation degree of the infeasible solutions, denoted by ς_k.

$$\varsigma_{k,1} = (0 - \Omega_k)^2 \tag{27}$$

$$\varsigma_{k,2} = (1 - \Omega_k)^2 \tag{28}$$

(2) Determine the new boundary threshold values.

$$r = mediam(sort(\varsigma_k)) \tag{29}$$

Step 4 Projection

Utilizing Equation (30), the projection operation is executed to remap the candidate solutions to the feasible region, ensuring adherence to the constraint conditions.

$$\begin{aligned}\Omega_k^{t+1}&(1 + on_e \times (xn - 1) : on_e \times xn) \\ &= \Omega_k^{t+1}(1 + on_e \times (xn - 1) : on_e \times xn) \\ &\quad - A_e^T \times (A_e \times A_e^T)^{-1} \times \Omega_k^{t+1}(1 + on_e \\ &\quad \times (xn - 1) : on_e \times xn) \times A_e\end{aligned} \tag{30}$$

where on_e is the number of constraint variables in the solution, xn is the number of equality constraints, and A_e^T is the equation parameter vector.

The representation of the hyperplane can be expressed as follows:

$$A_e \Omega_k^t (1 + on_e \times (xn - 1) : on_e \times xn) = 1 \tag{31}$$

Step 5 Selection and recombination

Update the next generation mean using Equation (32).

$$m^{t+1} = \sum_{k=1}^{\tau} h_k \Omega_{k:\lambda}^{t+1} \tag{32}$$

Step 6 Update the covariance matrix.

Update the covariance matrix based on the fitness of the current population. The overarching procedure for updating the covariance matrix can be delineated as follows:

$$\begin{aligned}CM^{t+1} &= (1 - a_1 - a_\tau) CM^t + a_1 ep^{t+1} (ep^{t+1})^T \\ &\quad + a_\tau \sum_{k=1}^{\tau} h_k \left(\frac{\Omega_{k:\lambda}^{t+1} - m^t}{s^t}\right)\left(\frac{\Omega_{k:\lambda}^{t+1} - m^t}{s^t}\right)^T\end{aligned} \tag{33}$$

where $a \leq 1$ indicates the learning rate. Normally, the value a is 1.

The update of the covariance matrix includes two evolutionary paths. The first path is represented by Equation (34):

$$\begin{aligned}ep^{t+1} &= (1 - a_{ep}) ep^t \\ &\quad + \sqrt{a_{ep}(2 - a_{ep}) \left(\sum_{k=1}^{\tau} h_k^2\right)^{-1}} \frac{m^{t+1} - m^t}{s^t}\end{aligned} \tag{34}$$

Then, the estep size is updated through Equation (35):

$$s^{t+1} = s^t \exp\left(\frac{a_s}{d_s}\left(\frac{\left\|ep_s^{t+1}\right\|}{E\left\|N(0, I)\right\|} - 1\right)\right) \tag{35}$$

where d_s is the damping coefficient and $E\left\|N(0, I)\right\|$ is the mathematical expectation of the normal distribution $\|N(0, I)\|$.

The second method of path update is represented by the following formula:

$$\begin{aligned}ep_s^{t+1} &= (1 - a_s)\, ep_s^t + \sqrt{a_s (2 - a_s) \left(\sum_{k=1}^{\tau} h_k^2\right)^{-1}} \\ &\quad \times CM^{t - \frac{1}{2}} \frac{m^{t+1} - m^t}{s^g}\end{aligned} \tag{36}$$

Finally, the two path are combined.

The above steps are repeated until the population reaches the maximum number of evolutionary generations.

IV. CASE STUDY

To validate the effectiveness of the proposed model in predicting Industrial Control Network behavior, two different industrial control datasets were selected. For the information network component, the TON-IoT [30], [31], [32] dataset was used, which includes network data collected from an Industrial Internet of Things (IIoT) test platform, consisting of telemetry data, operating system data, and network data. For the control network component, the X-IIoTID Dataset [33] was utilized, which contains labelled network and host data. This dataset records the activities of the network and

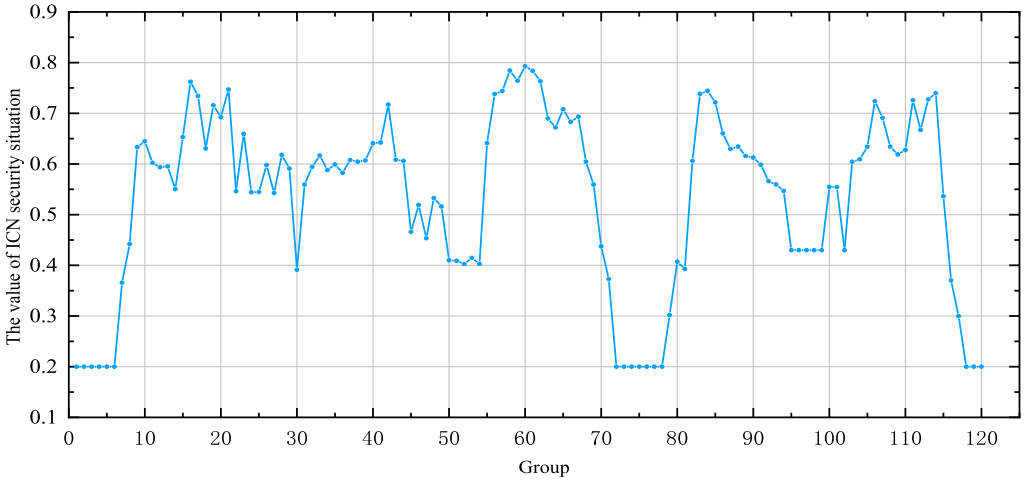


FIGURE 4. The value of industrial control network security situation within 120 h.

system, including network traffic, host resources, logs, security mechanism alerts, connection protocols, attack strategies, attack techniques, and attack processes.

A. PROBLEM DESCRIPTION

The attacks in the X-IIoTID dataset are categorized into attacks targeting historical/real-time databases, asset management systems, and industrial gateways. Each type of device experiences three to four types of attacks. Attacks on historical/real-time databases primarily include scanning vulnerabilities, general scans, and erroneous data injections. Asset management systems are targeted with attacks such as encryption ransomware, ransom denial-of-service, and resource discovery. The main attacks on industrial gateways consist of Modbus register read brute force attacks, reverse shell attacks, and MITM attacks. The TON-IoT dataset includes four types of attacks: injection attacks, DDoS attacks, backdoor attacks, and password attacks.

Filter, preprocess, and integrate these attack data, select 120 continuous hours of attack data, calculate the attack frequency per hour, and determine the severity of attacks based on the attack frequency. A sliding window approach was used to generate 118 sets of data samples from these 120 hours of data.

B. USING THE ER ITERATIVE ALGORITHM FUSE ASSESSMENT INDICATORS

Based on the assessment framework in section III-B, the industrial security situation assessment indicators are gradually fused using the ER fusion method, obtaining the security situation values of the ICN for 120 consecutive hours, as shown in Figure 4. The security situation values at times t-1 and t are taken as inputs to the prediction model to forecast the security status of the ICN at time t+1.

C. CONSTRUCTING A BRB-BASED ICN SECURITY SITUATION PREDICTION MODEL

Using the security situation values at time t-1 and t as inputs to the prediction model, the security status of the ICN at time t+1 is forecasted. According to the network security basic situation security index grading released by CNCERT/CC, the reference points for the two antecedent attributes, namely the security situation values of the ICN at times t-1 and t, as well as the predicted result at time t+1, are set as Excellent (I), Good (II), Moderate (III), Poor (IV), and Critical (V).

TABLE 3. Reference points and reference values for O(t-1), O(t), and O(t+1).

Reference Points	I	II	III	IV	V
Reference Values	0.2	0.4	0.6	0.7	0.8

The security situation prediction model for ICN based on BRB can be described as follows:

R_k: If $O(t-1)$ is $A_1^m \wedge O(t)$ is A_2^m,
Then $O(t+1)$ is $(I,\rho_{1,m})$, $(II,\rho_{2,m})$, $(III,\rho_{3,m})$, $(IV,\rho_{4,m})$,$(V,\rho_{5,m})\}$
With rule weight θ_m and attribute weight δ_1, δ_2

The reference values for the evaluation levels of the two antecedent attributes O(t-1), O(t), and the predictive result O(t+1) in the prediction model are provided by experts, as shown in Table 3.

The initial values of the rule weights and attribute weights are set to 1, and the initial confidences are provided by experts. The constructed initial rule-based confidence model is shown in Table 4.

D. OPTIMIZATION OF THE BRB-BASED ICN SECURITY SITUATION PREDICTION MODEL

The processed data are used for testing and training. Out of the 118 sets of sample data, 108 sets are chosen at random for the training set, while the remaining 10 sets constitute the testing set. During the training process, the EP-CMA-ES algorithm is applied to optimize the model's parameters. The optimized model rule confidences and rule weights are shown in Table 5. The testing sets are utilized to compute the accuracy of the model's predictions.

TABLE 4. Initial confidence rule base model.

No.	θ_m	O(t-1)	O(t)	$\{\rho_{1,m},\rho_{2,m},\rho_{3,m},\rho_{4,m},\rho_{5,m}\}$
1	1	I	I	{1,0,0,0,0}
2	1	I	II	{0.5,0.5,0,0,0}
3	1	I	III	{0.5,0.25,0.25,0,0}
4	1	I	IV	{0,0.5,0.25,0.25,0}
5	1	I	V	{0,0.25,0.5,0.25,0}
6	1	II	I	{0,0.5,0.3,0.2,0}
7	1	II	II	{0.5,0.3,0.2,0,0}
8	1	II	III	{0,0.5,0.2,0.2,0.1}
9	1	II	IV	{0.6,0.2,0.1,0.1,0}
10	1	II	V	{0.2,0.4,0.1,0.1,0.2}
11	1	III	I	{0.4,0.2,0.15,0.15,0.1}
12	1	III	II	{0.1,0.2,0.3,0.3,0.1}
13	1	III	III	{0.2,0.2,0.2,0.2,0.2}
14	1	III	IV	{0.2,0.1,0.3,0.2,0.2}
15	1	III	V	{0.4,0.1,0.15,0.15,0.2}
16	1	IV	I	{0.5,0.3,0.15,0,0.05}
17	1	IV	II	{0,0.1,0.1,0.2,0.6}
18	1	IV	III	{0.1,0.1,0.2,0.2,0.4}
19	1	IV	IV	{0.15,0.25,0.2,0.3,0.1}
20	1	IV	V	{0.1,0.2,0.2,0.4,0.1}
21	1	V	I	{0.2,0.35,0.25,0.15,0.05}
22	1	V	II	{0,0.5,0.25,0.25,0}
23	1	V	III	{0,0.1,0.1,0.3,0.5}
24	1	V	IV	{0,0,0.2,0.2,0.6}
25	1	V	V	{0,0,0,0.3,0.7}

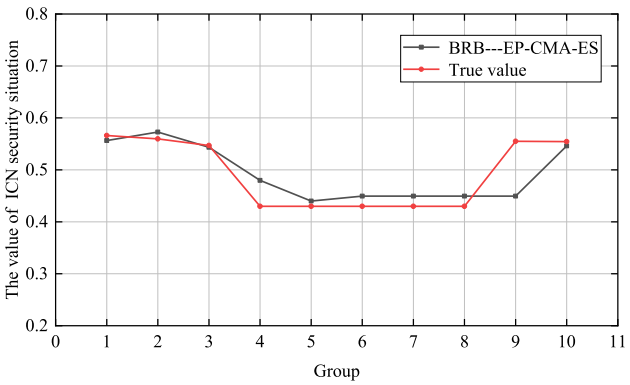


FIGURE 5. Predicted results of the prediction model.

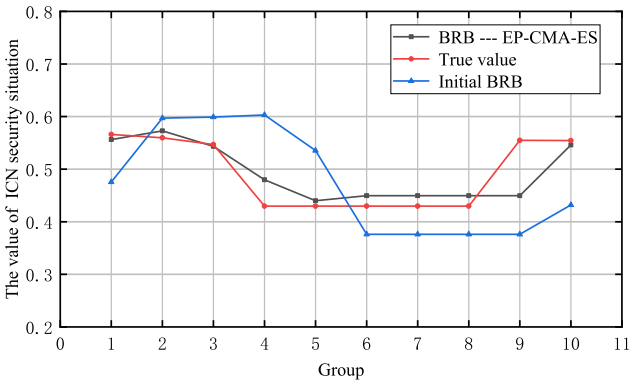


FIGURE 6. Comparison results before and after model optimization.

A comparison of the rule weights and confidence values in Tables 4 and 5 reveals a significant alteration in the optimized rule weights and confidences. This change can be attributed to the potential influence of expert subjectivity or errors, which can result in the establishment of unreasonable weights and confidences. Utilizing optimization algorithms to refine model parameters serves to mitigate this underlying bias.

The fitting curve between the predicted values of the ICN security situation prediction model constructed in this paper and the actual security situation values is shown in Figure 5.

E. COMPARATIVE EXPERIMENTS

A comparison was conducted between the initial BRB model and the BRB model refined through utilization of

TABLE 5. Optimized confidence rule base model.

No.	θ_m	O(t-1)	O(t)	$\{\rho_{1,m},\rho_{2,m},\rho_{3,m},\rho_{4,m},\rho_{5,m}\}$
1	0.60	I	I	{0.699,0.072,0.161,0.053,0.012}
2	0.47	I	II	{0.250,0.106,0.224,0.195,0.223}
3	0.19	I	III	{0.073,0.216,0.218,0.407,0.084}
4	0.62	I	IV	{0.196,0.048,0.122,0.543,0.088}
5	0.42	I	V	{0.124,0.030,0.117,0.460,0.267}
6	0.51	II	I	{0.593,0.357,0.034,0.001,0.013}
7	1	II	II	{0.366,0.312,0.231,0.068,0.019}
8	0.05	II	III	{0.172,0.474,0.195,0.018,0.139}
}9	0.52	II	IV	{0.552,0.024,0.099,0.165,0.158}
10	0.50	II	V	{0.032,0.114,0.216,0.058,0.578}
11	0.12	III	I	{0.409,0.076,0.198,0.275,0.040}
12	0.51	III	II	{0.433,0.168,0.123,0.045,0.229}
13	0.98	III	III	{0.160,0.292,0.212,0.50,0.284}
14	0.56	III	IV	{0.186,0.036,0.055,0.232,0.489}
15	0.71	III	V	{0.408,0.209,0.057,0.173,0.152}
16	0.42	IV	I	{0.024,0.103,0.151,0.314,0.405}
17	0.62	IV	II	{0.489,0.205,0.239,0.001,0.063}
18	0.71	IV	III	{0.718,0.116,0.032,0.030,0.105}
19	0.29	IV	IV	{0.145,0.040,0.581,0.016,0.216}
20	0.09	IV	V	{0.118,0.109,0.021,0.350,0.399}
21	0.19	V	I	{0.236,0.163,0.325,0.131,0.143}
22	0.06	V	II	{0162,0.291,0.063,0.123,0.358}
23	0.11	V	III	{0.093,0.144,0.329,0.314,0.118}
24	0.77	V	IV	{0.024,0.113,0.358,0.329,0.174}
25	0.42	V	V	{0.009,0,0.008,0.028,0.953}

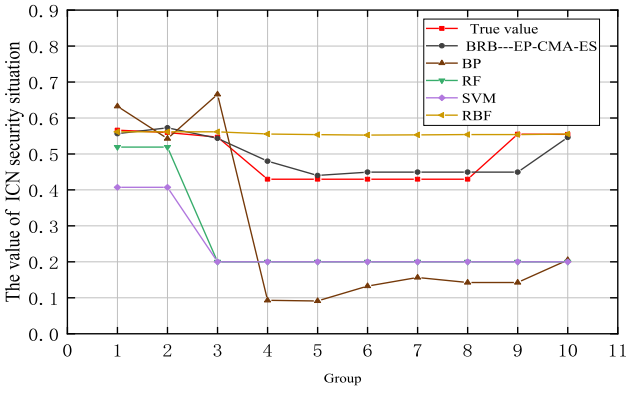


FIGURE 7. Comparison of predictive results by different models.

TABLE 6. MSE values of different models.

Method	MSE	RMSE	MAPE
Initial BRB	0.0111	0.073	9.56%
BRB---EP-CMA-ES	0.0081	0.0321	1.60%
BP	0.0473	0.1877	64.12%
RF	0.0488	0.1206	68.38%
SVM	0.0501	0.1464	70.40%
RBF	0.0232	0.1516	11.27%

the EP-CMA-ES algorithm. The comparative outcomes are presented in Figure 6.

According to Figure 6, we can clearly see that compared to the initial BRB model, the optimized BRB prediction model predicts industrial control network security situation values that are closer to the actual values. By assessing the degree of fit with the curve of actual values, it can be demonstrated that employing the EP-CMA-ES algorithm for parameter optimization of the proposed forecasting model effectively addresses the issue of reduced assessment accuracy resulting from uncertainties in expert knowledge.

To prove the superiority of the proposed BRB model prediction method, the backpropagation neural network (BP) prediction model, random forest prediction model (RF), support vector machine prediction model (SVM) and radial basis function (RBF) were selected for comparison. The fitting curves of the predicted results and the actual prediction results of the four models are shown in Figure 7.

By calculating the Mean Squared Error (MSE), Root Mean Squared Error (RMSE), and Mean Absolute Percentage Error (MAPE) between the predicted values of different models and the actual values, we validate the superiority of the industrial control network security state forecasting model proposed in this study compared to other machine learning models. The average MSE, RMSE, and MAPE values for each model after ten rounds of validation are presented in Table 6.

According to Table 6, it is evident that the BRB prediction model, which combines qualitative knowledge and quantitative data, has a significantly more accurate predictive effect compared to prediction models based solely on quantitative data. Due to the complexity and specificity of ICNs, the available sample data is limited, resulting in lower prediction accuracy for models that rely solely on quantitative data. The prediction model optimized by the EP-CMA-ES algorithm has improved accuracy compared to the initial BRB prediction model. This demonstrates that the optimization algorithm effectively addresses the impact of uncertainty in expert knowledge on the predictive model.

V. CONCLUSION AND FUTURE WORKS

Through the analysis of various factors influencing the ICN security situation, this paper establishes a four-level assessment framework for security situations. The security situation value for the ICN is acquired through the gradual fusion of assessment indicators using the ER fusion algorithm. Subsequently, a BRB-based ICN safety situation prediction model is established, and the EP-CMA-ES optimization algorithm is used to optimize the predictive model. The security situation of the ICN at time t+1 is predicted using the security situation values at times t-1 and t. Experiments show that compared to other machine learning methods, the security situation prediction model based on ER and BRB achieves higher accuracy, making it more suitable for complex systems such as industrial control networks for which it is difficult to collect security data. However, to further enhance the accuracy of the prediction model, it may be necessary to incorporate more historical information as input for the BRB model. Nevertheless, the number of rules in the BRB model equals the Cartesian product of the input attribute count and the number of reference values. When the number of input attributes increases, it leads to exponential growth in the number of combination rules, resulting in a combinatorial explosion and decreased prediction efficiency. Based on the aforementioned description, future research directions could be pursued as follows: improving the BRB model by altering the structure of combined rules to address the issue of rule explosion when input attributes are increased.

REFERENCES

[1] T. Alladi, V. Chamola, and S. Zeadally, "Industrial control systems: Cyberattack trends and countermeasures," *Comput. Commun.*, vol. 155, pp. 1–8, Apr. 2020.

[2] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, "Cybersecurity for industrial control systems: A survey," *Comput. Secur.*, vol. 89, Feb. 2020, Art. no. 101677.

[3] L. Hu, H. Li, Z. Wei, S. Dong, and Z. Zhang, "Summary of research on IT network and industrial control network security assessment," in *Proc. IEEE 3rd Inf. Technol., Netw., Electron. Autom. Control Conf. (ITNEC)*, Mar. 2019, pp. 1203–1210.

[4] M. D. Firoozjaei, N. Mahmoudyar, Y. Baseri, and A. A. Ghorbani, "An evaluation framework for industrial control system cyber incidents," *Int. J. Crit. Infrastruct. Protection*, vol. 36, Mar. 2022, Art. no. 100487.

[5] Y. Keshun, Q. Guangqi, and G. Yingkui, "Remaining useful life prediction of lithium-ion batteries using EM-PF-SSA-SVR with gamma stochastic process," *Meas. Sci. Technol.*, vol. 35, no. 1, Jan. 2024, Art. no. 015015.

[6] J. Li, Y. Jia, M. Niu, W. Zhu, and F. Meng, "Remaining useful life prediction of turbofan engines using CNN-LSTM-SAM approach," *IEEE Sensors J.*, vol. 23, no. 9, pp. 10241–10251, May 2023.

[7] J. Zhao and D. Wu, "The risk assessment on the security of industrial Internet infrastructure under intelligent convergence with the case of G.E.'s intellectual transformation," *Math. Biosci. Eng.*, vol. 19, no. 3, pp. 2896–2912, 2022.

[8] W. Han, Z. Tian, Z. Huang, L. Zhong, and Y. Jia, "System architecture and key technologies of network security situation awareness system YHSAS," *Comput., Mater. Continua*, vol. 59, no. 1, pp. 167–180, 2019.

[9] D. Codetta-Raiteri and L. Portinale, "Decision networks for security risk assessment of critical infrastructures," *ACM Trans. Internet Technol.*, vol. 18, no. 3, pp. 1–22, Aug. 2018.

[10] H. Song, D. Zhao, and C. Yuan, "Network security situation prediction of improved Lanchester equation based on time action factor," *Mobile Netw. Appl.*, vol. 26, no. 3, pp. 1008–1023, Jun. 2021.

[11] Z. Feng, Z. Zhou, C. Hu, X. Ban, and G. Hu, "A safety assessment model based on belief rule base with new optimization method," *Rel. Eng. Syst. Saf.*, vol. 203, Nov. 2020, Art. no. 107055.

[12] Q. Zhang, C. Zhou, and Y. C. Tian, "A fuzzy probability Bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2497–2506, Nov. 2017.

[13] K. L. Keung, Y. Y. Chan, K. K. H. Ng, S. L. Mak, C. H. Li, Y. Qin, and C. W. Yu, "Edge intelligence and agnostic robotic paradigm in resource synchronisation and sharing in flexible robotic and facility control system," *Adv. Eng. Informat.*, vol. 52, Apr. 2022, Art. no. 101530.

[14] Z. Xue, Y. Zhang, C. Cheng, and G. Ma, "Remaining useful life prediction of lithium-ion batteries with adaptive unscented Kalman filter and optimized support vector regression," *Neurocomputing*, vol. 376, pp. 95–102, Feb. 2020.

[15] L. Wang, L. Wu, Y. Guan, and G. Wang, "Online sensor fault detection based on an improved strong tracking filter," *Sensors*, vol. 15, no. 2, pp. 4578–4591, Feb. 2015.

[16] G. Lu and D. Feng, "Network security situation awareness for industrial control system under integrity attacks," in *Proc. 21st Int. Conf. Inf. Fusion (FUSION)*, Jul. 2018, pp. 1808–1815.

[17] K. Kumar, Sumit, S. Kumar, L. K. Singh, and A. Mishra, "Predicting reliability of software in industrial systems using a Petri net based approach: A case study on a safety system used in nuclear power plant," *Inf. Softw. Technol.*, vol. 146, Jun. 2022, Art. no. 106895.

[18] X. Liu, C. Fang, and D. Xiao, "Intrusion diagnosis and prediction with expert system," *Secur. Commun. Netw.*, vol. 4, no. 12, pp. 1483–1494, Dec. 2011.

[19] R. Zhang, Z. Pan, Y. Yin, and Z. Cai, "A model of network security situation assessment based on BPNN optimized by SAA-SSA," *Int. J. Digit. Crime Forensics*, vol. 14, no. 2, pp. 1–18, Jun. 2022.

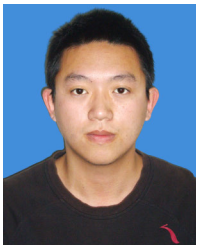
[20] G. Chen, "Multimedia security situation prediction based on optimization of radial basis function neural network algorithm," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–8, Apr. 2022.

[21] H. Lu, G. Zhang, and Y. Shen, "Cyber security situation prediction model based on GWO-SVM," in *Proc. Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*. Cham, Switzerland: Springer, 2020, pp. 162–171.

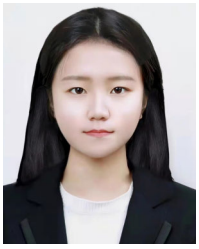
[22] W. Liang, Z. Chen, X. Yan, X. Zheng, and P. Zhuo, "Multiscale entropy-based weighted hidden Markov network security situation prediction model," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, Jun. 2017, pp. 97–104.

[23] Z.-J. Zhou, C.-H. Hu, D.-L. Xu, M.-Y. Chen, and D.-H. Zhou, "A model for real-time failure prognosis based on hidden Markov model and belief rule base," *Eur. J. Oper. Res.*, vol. 207, no. 1, pp. 269–283, Nov. 2010.

[24] S. Chatterjee, S. Nigam, and A. Roy, "Software fault prediction using neuro-fuzzy network and evolutionary learning approach," *Neural Comput. Appl.*, vol. 28, no. S1, pp. 1221–1231, Dec. 2017.
[25] E. S. Pour, H. Jafari, A. Lashgari, E. Rabiee, and A. Ahmadisharaf, "Cryptocurrency price prediction with neural networks of LSTM and Bayesian optimization," *Eur. J. Bus. Manage. Res.*, vol. 7, no. 2, pp. 20–27, Mar. 2022.
[26] J.-B. Yang, J. Liu, J. Wang, H.-S. Sii, and H.-W. Wang, "Belief rule-base inference methodology using the evidential reasoning approach-RIMER," *IEEE Trans. Syst. Man, Cybern. A, Syst. Humans*, vol. 36, no. 2, pp. 266–285, Mar. 2006.
[27] Y.-M. Wang, J.-B. Yang, D.-L. Xu, and K.-S. Chin, "The evidential reasoning approach for multiple attribute decision analysis using interval belief degrees," *Eur. J. Oper. Res.*, vol. 175, no. 1, pp. 35–66, Nov. 2006.
[28] Z.-J. Zhou, G.-Y. Hu, B.-C. Zhang, C.-H. Hu, Z.-G. Zhou, and P.-L. Qiao, "A model for hidden behavior prediction of complex systems based on belief rule base and power set," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 48, no. 9, pp. 1649–1655, Sep. 2018.
[29] S. Li, X. Xu, G. Zhou, Y. Wang, Z. Li, Y. Zhao, and W. Zhao, "Cybersecurity status assessment of cloud manufacturing systems based on semiquantitative information," *IEEE Access*, vol. 11, pp. 43458–43471, 2023.
[30] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems," *IEEE Access*, vol. 8, pp. 165130–165150, 2020.
[31] M. Al-Hawawreh, E. Sitnikova, and N. Aboutorab, "X-IIoTID: A connectivity-agnostic and device-agnostic intrusion data set for industrial Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3962–3977, Mar. 2022.
[32] N. Moustafa, "A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets," *Sustain. Cities Soc.*, vol. 72, Sep. 2021, Art. no. 102994.
[33] T. M. Booij, I. Chiscop, E. Meeuwissen, N. Moustafa, and F. T. H. D. Hartog, "ToN_IoT: The role of heterogeneity and the need for standardization of features and attack types in IoT network intrusion data sets," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 485–496, Jan. 2022.



YUHE WANG received the B.Eng. and Ph.D. degrees from the Harbin University of Science and Technology, Harbin, Heilongjiang, China, in 2012 and 2019, respectively. He was a Lecturer with the Changchun University of Technology. He is currently a Lecturer with Harbin Normal University, Harbin. He has published approximately five articles. His research interests include intelligent computing, industrial network security, and belief rule base.



YU YANG was born in China, in 2001. She is currently pursuing the master's degree with Harbin Normal University. Her research interests include network security and information security.

RENCAI GAO received the M.D. degree from Jilin University. He is currently an Associate Professor with the College of Computer Science, Baicheng Normal University. His main research interest includes network security.

SHIMING LI received the M.D. degree from the Harbin Institute of Technology. He is currently an Associate Professor with the College of Computer Science and Information Engineering, Harbin Normal University (HRBNU), China Computer Society (CCF 37474M). His main research interests include network security, information security, industrial internet, and the Internet of Things.

YAN ZHAO received the Ph.D. degree from the College of Network and Space Security, PLA Information Engineering University, in 2019. She is currently with the School of Information Technology, Luoyang Normal University. Her research interests include information security, the Internet of Things, and embedded systems.