

Trustworthiness in Industrial IoT Systems Based on Artificial Intelligence

Zhihan Lv, *Senior Member, IEEE*, Yang HAN, Amit Kumar Singh, *Senior Member, IEEE*, Gunasekaran Manogaran and Haibin Lv

Abstract—The intelligent industrial environment developed with the support of the new generation network physics system (CPS) can realize the high concentration of information resources. In order to carry out the analysis and quantification for the reliability of CPS, an automatic online assessment method for the reliability of CPS is proposed. It builds an evaluation framework based on knowledge of machine learning, designs an online rank algorithm, and realizes the online analysis and assessment in real time. The preventive measures can be taken timely. And system can operate normally and continuously. Its reliability has been greatly improved. Based on the credibility of the Internet and Internet of things, a typical CPS control model based on spatiotemporal correlation detection model is analyzed to determine the comprehensive reliability model analysis strategy. based on this, we propose a cps trusted robust intelligent control strategy and a trusted intelligent prediction model. Through simulation analysis, the influential factors of attack defense resources and the dynamic process of distributed cooperative control are obtained. CPS defenders in distributed cooperative control mode can be guided and select appropriate defense resource input according to the cps attack and defense environment.

Index Terms— CPS and AI; Internet of Things; Trustworthiness model; Against and Attack; Industrial Environments

I. INTRODUCTION

This work was supported by National Natural Science Foundation of China (No. 61902203) and Key Research and Development Plan - Major Scientific and Technological Innovation Projects of ShanDong Province (2019JZZY020101).

Zhihan Lv (*Corresponding Author) is with the School of Data Science and Software Engineering, Qingdao University, Qingdao, China(e-mail: lvzhihan@gmail.com).

Yang Han is with College of Metallurgy and Energy, North China University of Science and Technology, Tangshan, Hebei, China(e-mail: hanyang@ncst.edu.cn).

Amit Kumar Singh is with the Computer Science and Engineering Department, National Institute of Technology Patna, Bihar, India(e-mail: amit_245singh@yahoo.com).

Gunasekaran Manogaran Is with University of California, Davis, USA and College of Information and Electrical Engineering, Asia University, Taiwan(e-mail:gmanogaran@asia.edu.tw).

Haibin Lv is with the North China Sea Offshore Engineering Survey Institute, Ministry Of Natural Resources North Sea Bureau, China(e-mail: lvhaibin@ncs.mnr.gov.cn).

he proposal and development of Cyber-Physical Systems provides a new idea and approach for the deep integration of computer system, information system and communication system. CPS is an intelligent system in which computing units and physical objects are highly integrated and interacted in a network environment[1-3]. CPS includes the Internet of Things, information physical integration energy system or energy Internet, smart grid, intelligent transportation system, intelligent manufacturing system Intelligent logistics systems, etc., have become the core technology to support and lead a new round of industrial transformation[4-5]. In artificial intelligence and machine learning, data and application scenarios are very important. If we can abstract the application scenario into a model, use Data, combined with the correct algorithm, then information trusted applications will be great for network information credibility has become one of the key issues of Internet development and application whether artificial intelligence can be successfully applied to the trusted field, involving Several measurable factors: adaptability, interpretability and enforceability of algorithmic training [6-10]. Traditional physical systems (such as industrial control systems, drive systems, medical devices, etc.) are relatively difficult to access, penetrate, and enforce attacks by attackers because of their relatively isolated operating environment and the use of dedicated channels for communication. Due to the need of informatization and intelligence, traditional physical systems have gradually evolved into cps, and the operating environment of the system has been opened and interconnected through closure and isolation[11-13]. While improving operational efficiency, it also provides new attack channels for attackers, making CPS more vulnerable to internal or external attacks. For example, Stuxnet attacks invade nuclear facility control systems through U disk ferries, while WindShark directly accesses through physics. Manned Wind Farm Control System Once an attacker breaks through the CPS network boundary and enters the internal network, the attack success rate may be higher than the Internet attack, and the threat may be greater [14-17]. Most physical systems design fault diagnosis and safety emergency measures from an engineering safety perspective. For example, the stuxnet attack tampers with the reported system measurement data, making the control center unable to detect system anomalies, black energy destroys the system communication module and uses denial of service Attacks interfere with grid calls [18-20]. The service system makes the system's default emergency response and defense strategies not implemented effectively. The common features of these attacks are: formulating corresponding attack strategies for specific business processes and trusted plans of physical

systems, using network attack technology to implement coordinated attacks on multiple targets, and bypassing physical trusted systems to disrupt the normal operation of the system. Even destroying physical equipment[21-24]. In the future, based on artificial intelligence-based autonomous learning and powerful database analysis capabilities, people can anticipate dangers in advance and truly kill threats in the cradle, thereby greatly improving the agility of network physical credibility. The credible control of CPS is shifting from physical credibility to physical and social factors integrated disaster prevention[25-28]. However, due to the characteristics of CPS, such as large-scale data processing, continuous on-line operation of the system, operators can only conduct closed feedback and so on, it is urgent to realize the real-time reliability evaluation of CPS. To promote the in-depth integration of informatization and industrialization is to profoundly grasp the characteristics of the era of global informationization and the process of accelerating the convergence of industrialization.

II. RESEARCH STATUS OF TRUSTWORTHINESS MODEL

The security status of industrial IoT system is a comprehensive appearance under time accumulation. It is necessary to comprehensively consider the time series evolution law of key parameters of system operation. Therefore, space-time analysis method is needed, and differential equation model is an effective model to describe the spatio-temporal distribution of parameters. In order to eliminate the limitations of the differential equation model for only a few key parameters, this study considers the other redundant parameters of the system state to correct and compensate for the deficiency of the differential equation model[29-30]. The accuracy of system security status detection and forecasting is measured by the length of equipment life extension and system operation stability. These two indicators are also the most critical indicators for the practical application of industrial Internet of Things.

A. Typical CPS control model

The ability to defend against information network attacks is an important measure of CPS performance. trustworthiness events in recent years have shown that the means of attack faced by CPS are constantly being updated, and its diversity and concealment greatly increase the cost and cost of defense. Successful systems Defense is usually based on a thorough understanding of system architecture and attacks. Therefore, it is necessary to fully understand the characteristics of CPS attacks and existing anomaly detection mechanisms, and develop targeted defense strategies to enhance system trustworthiness^[29-30].

The coupling of information system and physical system is the difficulty in establishing CPS integrated trustworthiness model. It not only analyzes the topology structure and trustworthiness monitoring mechanism of different systems, but also considers the information exchange mode and trustworthiness vulnerability between the two types of systems. Firstly, the existing CPS system model and trustworthiness monitoring mechanism are summarized. Combined with the existing threat model, focusing on the concealment of control

signals and measurement signals tampering attacks, a CPS integrated trustworthiness model is proposed.

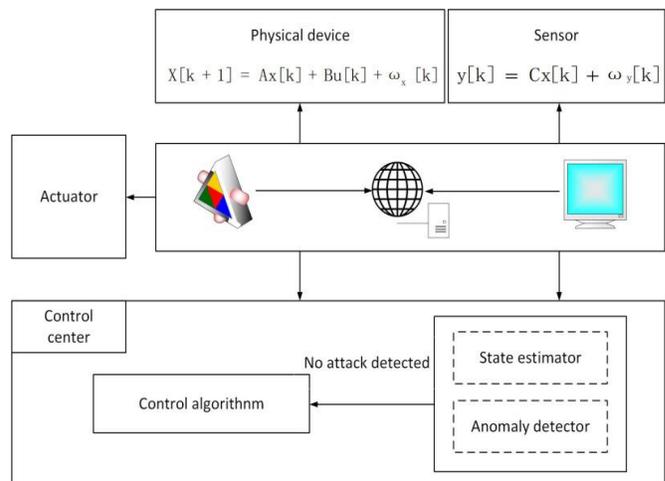


Fig. 1. CPS control model

A typical CPS consists of a control center, physical equipment, actuators, and sensors, as shown in **Fig. 1**. When the system state changes within a certain range, CPS can be approximated as a linear system. Since linear system theory and methods are mature, the linear time invariant (LTI) system of discrete time is taken as an example to illustrate the modeling ideas and methods. Specifically, the LTI model can be described as follows:

$$x[k+1] = Ax[k] + Bu[k] + \omega_x[k] \quad (1)$$

$$y[k] = Cx[k] + \omega_y[k] \quad (2)$$

$x[k]$ and $y[k]$ represent the state of the system and the measured value of the sensor, $u[k]$ represents the control signal, A, B, C represents the system matrix, the control matrix and the measurement matrix respectively. $\omega_x[k]$ and $\omega_y[k]$ both obey the zero mean multivariate Gaussian distribution, and the covariance matrix is Q and R . Both the control signal $u[k]$ and the sensor measurement $y[k]$ are transmitted by the communication network.

The formula presented in Fig 1 is a schematic diagram of the time domain equation of physical parameters as a function of time. In practical applications, these formulas use Laplace transform to transform differential equations into algebraic equations, and the solution process and analysis process can be realized.

The measurement data of the industrial control system needs to be preprocessed, mainly including state estimator and anomaly detector. The detection principle can be divided into two categories: one is to use the state of the system past time to predict the future state, and according to the prediction Results and measurement results were used to detect abnormal data. In this paper, it was named as time-dependent detection. The other type was cross-validation through the correlation between different sensors of the system to achieve the purpose of detection. This article named it space-dependent detection.

B. Time-dependent and spatially correlated detection models

The main members of the steel product traceability system include: steel companies, distribution, product users, quality regulators, etc. The information of the steel enterprise includes the registration information of the enterprise, the raw material composition of the product, the production process data of the product, the product quality data, etc. The information of the distribution includes the batch, packaging, and the logistics date, etc. The information of the product user includes the required product category, use, quality traceability, etc. As a result, part of the data relationship between the product manufacturing chain and the supply chain is shown in Fig. 2, and when a problem occurs at a node, the impact can be traced back or up along the data relationship network to improve the product supply and related dispute resolution efficiency.

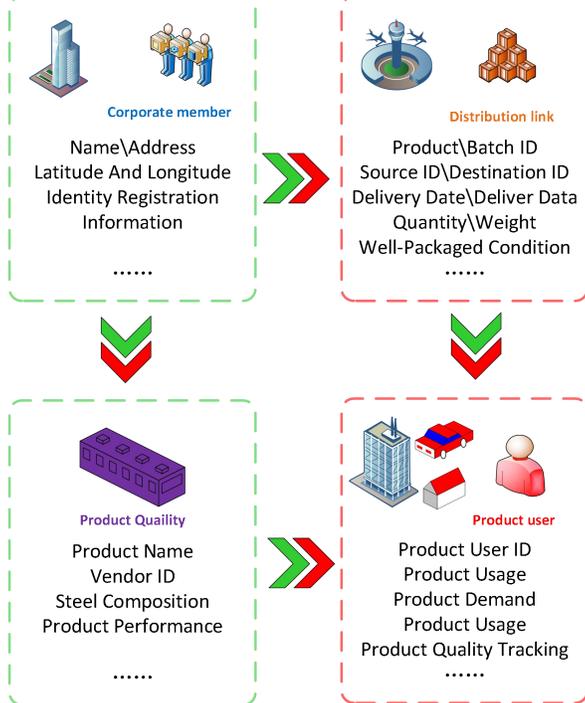


Fig. 2. Partial data structure relationship of Iron and Steel Product traceability system

Update (vertex) begin

$x \leftarrow$ read values of in- and out-edges of vertex.

vertex. Value $\leftarrow f(x)$.

for each edge of vertex do

edge. Value $\leftarrow g(\text{vertex. value})$.

end

end

Fig. 3. The typical node update function update() follows a logical algorithm

At present, the graph computing system generally adopts the node centered programming model or interface. The user can customize a node update function update (), and the graph calculation system will complete the calculation task by calling

the update function for each node. This function describes the operations that a node needs to perform in a round of iterations. A typical node update function, update(), follows the pseudo code shown in Fig. 3.

C. Comprehensive Trustworthiness model analysis

This section mainly analyzes the CPS integrated trustworthiness model in the attack scenario. In order to ensure the universality of the analysis, the attack scenario where the control signal and the measured value are simultaneously tampered with is considered. The symbol is used to indicate the normal state. The physical quantity underneath, and define the amount of attack the system suffers as follows (to facilitate the omission of the time index in the definition of this section)

(1) Use x_a and y_a to represent actual system status and sensor measurements, respectively.

(2) Use $\hat{x}_m, \hat{y}_m, \varepsilon_m, u_m$ to represent the state estimation value of the control center, the predicted value of the sensor measurement, the anomaly detector residual and the determined control signal.

(3) Use u_a to indicate the actual control signal received by the actuator. This signal has been tampered with by the attacker. Specifically, $u_a = u_m + a_u$, where u_m is the control command issued by the control center. $a_u \in R^l$ is the malicious injected in um control signal.

(4) Use y_m to indicate the measured value of the sensor received by the control center. This signal has also been tampered with by the attacker. Specifically, $y_m = y_a + a_y$, where $a_y \in R^m$ represents the malicious signal injected into the actual measured value of the sensor y_a .

From the point of view of the controlled physical system, the control commands received by the physical system have been tampered with by the attacker, and the physical system makes an erroneous decision based on the instruction. At the same time, the measured value of the current state is also tampered with by the attacker.

At time k , the control commands, system state equations and measurement results accepted can be expressed as:

$$u_a = u_m + a_u \quad (3)$$

$$x_a[k+1] = Ax_a[k] + Bu_a[k] + w_x[k] \quad (4)$$

$$y_a[k] = Cx_a[k] + w_y[k] \quad (5)$$

From the control center, the measured value y_m received by the attacker has been changed to the data under normal conditions. The control center detects the abnormality of the received measured value. After it is determined to be normal, it will send according to the control policy. Control signal u_m . At time k , the tamper-received sensor measurement will affect the system state estimation process shown in equations (2) and (3), the anomaly detection shown in equation (4), and equation (5). The control algorithm shown in can be expressed as:

$$\hat{x}_m[k+1] = L_1(\hat{X}_m[k], U_m[k], Y_m[k+1]) \quad (6)$$

$$\hat{y}_m[k+1] = L_2(\hat{X}_m[k], U_m[k], Y_m[k]) \quad (7)$$

$$\varepsilon_m[k+1] = y_m[k+1] - \hat{y}_m[k+1] \quad (8)$$

$$u_m[k+1] = L_3(\hat{X}_m[k+1], U_m[k], Y_m[k+1], x_0) \quad (9)$$

The differential equation model with the same structure is adopted, and the model analysis method is consistent with the previous method. The threat model under time-varying attack is taken as an example for analysis. In addition, the threat model under the space-related data integrity attack is similar to the threat model under the time-related attack, which is not described here.

The core idea of the CPS integrated trust model designed in this paper is to abstract the possible situation of CPS attack from the perspective of the system administrator, and abstract it into the system control flow, and adaptively modify the measured values and control commands. The constructed credibility constraint space is a defensive measure that CPS can take during the attack. It provides a feasible theoretical way for researchers and managers to understand the comprehensive reliability of CPS.

III. RESEARCH STATUS OF SAFETY PERFORMANCE ANALYSIS

This paper proposes a new power CPS security risk assessment framework as shown in Fig. 4, which aims to estimate the credibility of industrial IoT systems and provide guidance for the prevention of system security risks. The preferred subject model of attack prediction and defense strategy is the differential equation model. To compensate for the defects of the main model, the data-driven and artificial intelligence algorithms are used to correct the attack prediction model to obtain the optimal defense strategy. The typical case has three parts. Part A introduces the case application framework, Part B introduces the key principles and theoretical analysis, Part C shows the practical application effect, and the three progress in layers to clearly define Trustworthiness in Industrial IoT Systems Based on Artificial Intelligence.

A. CPS Trustworthiness robust control strategy

For the attack defense trustworthiness problem of CPS network, this section proposes a VPP distributed economic scheduling strategy. Based on the designed strategy, even in the network attack threat environment, the micro-increasing rate of the DG group can converge to the optimal solution of the optimization problem according to the convergence rule. In this strategy, a distributed credibility manager is set up to monitor the status of the credibility information of each DG through the designed observing communication network. When the confidence value of a DG falls below the set threshold, it will be isolated by the NCS to avoid the serious harm that the malicious attack may cause to the CPS.

(1) Network to CPS attack detection process

To achieve detection of maliciously following DG n , DG $i \in N_n^+$ uses the N^- information from the observed communication sub-network to assess the feasible range of its rate of increase. In terms of implementation technology, this information can be added to the transmission packet of DG n and sent to all DG $i \in N_n^+$

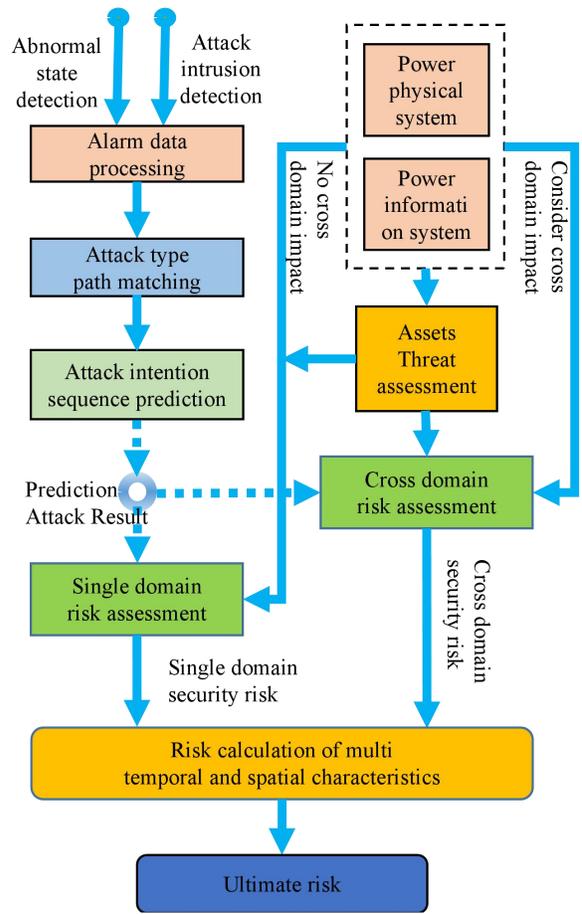


Fig. 4. Overall frame map

When certain conditions are met, by virtue of the information in the observed communication sub-network, any DG $i = \{1, \dots, N\}$ can estimate the upper and lower limits of the micro-increment rate in the next iteration of any of its receiving neighbors DG $j = N_n^-$:

Where η is the lower bound of the adjacency matrix element;

$\lambda_j^{\max}(k)$ and $\lambda_j^{\min}(k)$ are defined as

$$\lambda_j^{\max}(k) = \max \{ \lambda_i(k) \mid \forall i \in N_n^- \}, \lambda_j^{\min}(k) = \min \{ \lambda_i(k) \mid \forall i \in N_n^- \}$$

$D_j^{\max}(k)$, and $D_j^{\min}(k)$ are defined as

$$D_j^{\max}(k) = \{ l \mid \lambda_l(k) = \lambda_j^{\max}(k) \}, D_j^{\min}(k) = \{ l \mid \lambda_l(k) = \lambda_j^{\min}(k) \}$$

The above formula gives the maximum and minimum possible reasonable values of the micro-increment rate of DG j in the next iteration period. If the following inequality is not true

$$\lambda_j^{\text{low}}(k) \leq \lambda_j(k) \leq \lambda_j^{\text{up}}(k) \quad (10)$$

Then DG i suspects that it receives the neighbor DG j state abnormality, determines that it is a suspicious node, and prepares to initiate the edge and isolation process; where $\lambda_j(k)$ is the micro-increment rate information that DG i receives from DG j . This establishes a detection mechanism for following DG.

On the other hand, in the mechanism for detecting the malicious leader DG, one of the neighboring DGs of the leader DG can be set as the agent leader DG, which is responsible for

direct monitoring. Take the DoS attack and replay attack as an example. The detection principle is as follows:

1) If the following relationship is true

$$\lambda_l(k) = \phi \quad (11)$$

It is believed that the leading DG is attacked by DoS.

2) If the following relationship is true

$$|P_{ref} - P_{out}| > e_{conv} \text{ and } \lambda_l(k) \equiv \lambda_l(k+1) \quad (12)$$

The leader DG is considered to be replayed; where e_{conv} is a reasonable convergence error constant.

(2) Marginalization and isolation process

The DCLM located local to each DG information terminal can maintain and update the confidence $c_{ij}(k)$ ($\forall j \in N_i^-$) of its receiving neighbor DG j . The initial value of the credibility is set to $c_{ij}(0)$. The credibility update principle is

$$c_{ij}(k+1) = \begin{cases} \max\{c_{ij}(k)-1, 0\} & \text{If, DG } j \text{ Suspicious} \\ c_{ij}(k) & \text{Other} \end{cases} \quad (13)$$

For the malicious DG j that is attacked, the sending neighbor DG i will gradually reduce its credibility. At this time, DG j will be gradually marginalized according to the following rules:

$$a_{ij}(k) = \frac{[c_{ij}(k)]_{c_{ij}^+}^+}{\sum_{l \in N_i^-} [c_{ij}(k)]_{c_{ij}^+}^+} \quad (14)$$

Where c_{ij}^+ is the threshold of credibility $c_{ij}(k)$, which can be calculated by an advanced intelligent algorithm; $[x]_y^+$ is defined as

$$[x]_y^+ = \begin{cases} x & \text{if } x \geq y \\ 0 & \text{other} \end{cases} \quad (15)$$

Assume that the adjacency matrix $A(k)$ is a row random. According to the above principle, the weight of the control communication line connected to the malicious DG will gradually decrease until it is finally 0, at which time its transmitting neighbor will disconnect all communication lines between them. When all relevant control communication lines are removed, the malicious DG is also completely isolated from the communication network. At the same time, the malicious DG is also physically isolated from the distribution network, completely preventing its possible harmful effects on the entire system.

It should be noted that in the case where the leader DG is attacked, when the original malicious leader DG is isolated, the agent leader DG starts to receive the information $P_{ref}=P_{out}$ delivered by the superior EMS, so that the VPP is again controllable.

The VPP distributed economic scheduling strategy robust to network attacks proposed by this research has strong convergence characteristics, and can resist various types of network attacks including non-collusion and collusion network attacks, and various types of communication failures. When a malicious DG violates the above conditions, it will be gradually marginalized and isolated from the NCS. Robustness' intuitive expression is shown in Fig. 5.

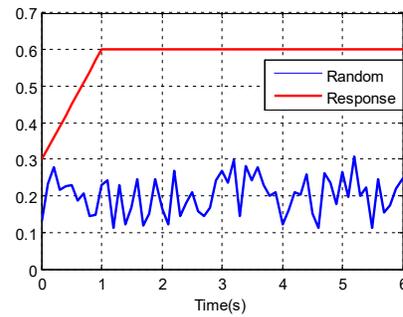


Fig. 5. Robustness

B. CPS Trustworthiness assessment method

Traditional grid risk assessment is generally based on historical data or current data. The results obtained are “static” results in the current state of a single time scale, which are transient short-term scale risks, while multi-time scale risk assessments are required. Consider the risk of the system for a period of time in the future, namely the long-term scale risk. The power CPS trustworthiness assessment proposed in this paper comprehensively considers the single domain trustworthiness and the cross-domain trustworthiness. The former represents the direct loss caused by the attack on a single information and physical system, and only considers the current vulnerability of the system and the risk of being attacked. The static short-time scale risk can guide the defender to protect the relevant equipment in time; the latter considers the fault propagation process caused by the attack, and studies the system risk in the future period after the attack occurs, which belongs to the long-term scale risk, and the power CPS The re-planning of the safety structure has important guiding significance. Therefore, the combination of the two can more fully understand the trustworthiness of CPS.

The safety risk calculation method in this paper adopts the classic risk assessment model - the Rand risk assessment model: $RT=PVC$. RT is the expected value of the ultimate loss of the target, representing the risk; P is the probability of a target being attacked, “threatening”; V is the probability that a target will eventually be destroyed after being attacked, “vulnerability”; C is a target The magnitude of the damage caused by the attack and eventually being destroyed represents the consequences.

The cross-domain trustworthiness assessment method adopted in this paper first establishes an information system network model $N_1=(V_1,\alpha_1)$ and a power system network model $N_P=(V_P,\alpha_P)$ based on complex network theory. Among them, V_1 is a set of middle nodes in N_1 , V_P is a set of middle nodes in N_P , N_1 satisfies the idempotent rate, that is, the proportion of nodes whose degree is k in the network N_1 is $P_1(k)$. Then, using the attack prediction result as input, combined with the power CPS network topological degree distribution characteristics and the information physical interaction system cross-domain connection characteristics, the probability model of the attack fault cross-domain propagation process is established, and the dynamic fault probability is calculated. The times of successes is positive, and the times of failures is negative. Attack experiment warning is shown in Fig. 6.

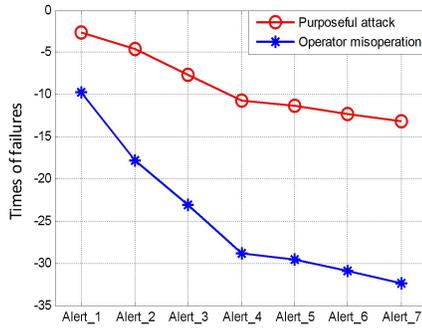


Fig. 6. Attack Experiment Warning

The online queuing algorithm is used to predict the system state in real time. The online queuing algorithm can evaluate CPS transparently and automatically. It can work in parallel with CPS without any influence. It has high feasibility. The whole evaluation process works on-line and circularly, keeping synchronous with the operation of CPS system, which can effectively improve the system reliability. The workflow steps are as follows:

Step1. Obtain system status information and component experience data set information from CPS.

Step2. According to the collection and information, the online queuing algorithm is used to build the prediction queue to evaluate the reliability of the system.

Step3. As the evaluation result, the predicted queue is fed back to the operator's visual interface in the form of alarm.

Step4. The operator shall refer to the alarm information and take corresponding improvement measures for specific components of the components that may trigger the next system fault to ensure that the CPS operates without fault.

In CPS, a physical system node is called a power element, an information system node is called an information element, a power element that provides power support for an information element is called a supporting power element, and an information element that provides control support for a power element is called a supporting information element. Define the meaning of the power element/information element fault to avoid confusion with traditional faults.

Pseudo code of online queuing algorithm, as shown in Fig. 7.

Because the system will not fail only if its own node is not faulty and at least one neighbor node is not faulty, that is, the non-fault probability is $1-\gamma=(1-\theta)(1-\rho)$, so the average failure probability of the node is

$$\gamma = 1 - (1 - \theta)(1 - \rho) = \theta + \rho + \theta\rho \quad (16)$$

After the above attack failure cross-domain propagation algorithm, the final power CPS failure probability is obtained (γ_1, γ_p) . Since the fault loss is the product of the node average failure probability γ and the total node value C , the final cross-domain trustworthiness can be calculated according to the power element and information element value and vulnerability index C_i^p, V_i^p and C_j^i, V_j^i . obtained from the single domain trustworthiness assessment phase.

$$R_c = \gamma_1 \sum C_i^I V_i^I + \gamma_p \sum C_j^P V_j^P \quad (17)$$

OnlineRank($L, \Delta, \gamma, \theta, \tau, \lambda$)

```

1  $L \leftarrow \{\}$ 
2 while {true}
3 do At time  $t$  equals  $t$ 
4   Ranking  $i(t) \leftarrow m_i(\text{Capture}(t))$  for  $m_i \in M$ 
5    $\Lambda \leftarrow$  The top  $\Delta$  models in model queue  $Q$ 
6   Ranking( $t$ ) Weighed_average( $\{\omega_i \times \text{Ranking}(t) \mid m_i \in \Lambda\}$ )
7   if new fault occurs Faults( $n, t$ )
8     then  $z_i = \text{Estimate}_{m_i}(n, t)$  for  $m_i \in M$ 
9      $z_{best} \leftarrow \max(z_1, z_2, \dots, z_{|M|})$ 
10     $z_{worst} \leftarrow \min(z_1, z_2, \dots, z_{|M|})$ 
11    for  $m_i \in M$ 
12      do  $d_i = (z_{best} - z_i) / (z_{best} - z_{worst})$ 
13       $\omega_i = \omega_i \times \gamma^{d_i}$ 
14    if elapsed time interval  $\lambda$ 
15      then add a new model  $m_{|M|+1}$  to  $M$ 
16       $\omega_{new} \leftarrow \omega_{min} + \tau \times (\omega_{max} - \omega_{min})$ 
17       $\omega_{|M|+1} \leftarrow \omega_{new}$ 
18       $M \leftarrow M \cup \{m_{|M|+1}\}$ 
19      if  $|M| > L$ 
20        then delete the worst model according to  $\omega_i \times \theta^{age(m_i)}$ 

```

Fig. 7. Pseudo code of online queuing algorithm

The security protocol research includes two aspects: node security and information security between nodes. The main solutions for current node security include trusted root-based identity authentication, which uses the trusted platform module as a built-in trusted root, and uses this as a starting point, combined with secure boot, data storage protection, integrity metrics, and trusted delivery. And other technologies, adopting step-by-step measurement, verification and delivery methods to complete node credibility evaluation. In this paper, a secure link state routing protocol based on node credibility is applied. By introducing trust and CPK-based security authentication mechanism in the network, the security of information interaction is enhanced on the one hand, and the node is considered comprehensively in routing decision. Credibility and path credibility, the path to choose high security credibility for information transmission.

C. Analysis of safety risk assessment results

In the experiment, appsim simulation platform is used, Matlab / Simulink software is integrated, data classification, redundancy check and trend monitoring are used to build the model, and self tuning is realized by this method. For the acquired system state information, 80% of the data is used for classification model training, and 20% of the data is used for blind test. In order to check the redundancy, firstly, the history and test system state information instances are transformed into vector groups by using vector space model.

As shown in Fig. 8 is Cascade mean failure probability change caused by attack. It is known that θ is the probability of failure caused by the failure of the node itself in the system, ρ is the failure probability caused by all the failures of the neighbor nodes in the system, and γ is the probability that any node in the system will leave the maximum connectivity graph of the network due to the failure, that is, the average failure of the node Probability.

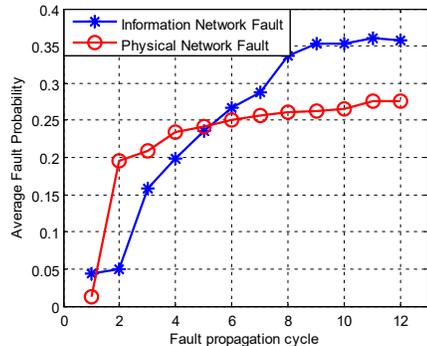


Fig. 8. Cascade mean failure probability change caused by attack

The total number of offensive and defensive resources S^A and S^D are two key factors affecting the level of system vulnerability during the game phase. The sensitivity analysis of them are shown in the Fig. 9.

The simulation results and analysis conclusions of this section can help guide the CPS defenders of the distribution network with distributed collaborative control mode, and choose how to invest the appropriate amount of defense resources according to the CPS attack and defense environment.

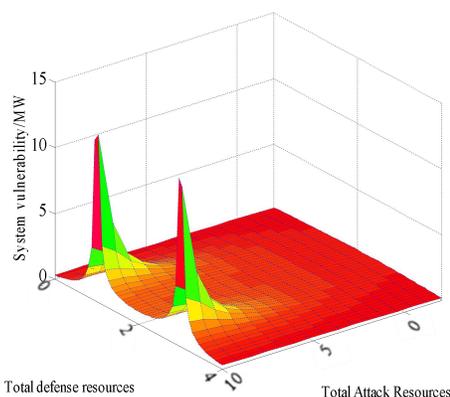


Fig. 9. 3D map of the impact of changes in total offensive and defensive resources on system vulnerability

In the game phase, in addition to the influencing factors of the network attack and defense, the dynamic convergence process of the distributed collaborative control itself will also affect the system vulnerability assessment results. The following is a description of the influence mechanism through the simulation example, and then the sensitivity analysis.

Simulation analysis of the impact of network attack time and control scheduling commands on the vulnerability of distribution network CPS. The simulation results are shown in Fig. 10.

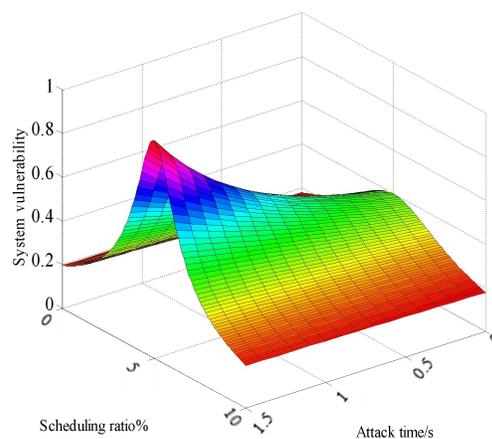


Fig.10. 3D map of the impact of collaborative control dynamic processes on system vulnerability

where the scheduling ratio is defined as the ratio of the reference power P_{ref} to the maximum allowable output of the VPP, which shows that as the VPP dynamically adjusts according to each control scheduling command, the attack and defense game is performed at each moment. Corresponding system vulnerability. It can be seen from the figure that in the process of VPP accepting a certain instruction P_{ref} scheduling, the system vulnerability changes obviously at the beginning stage, and gradually becomes fixed after a period of time; meanwhile, as the P_{ref} increases, the system vulnerability gradually increases. Upgrade. This is because under the new scheduling command, each DG will initially adjust its own output quickly, and P_{ref} is positively correlated with the value of the scheduling command. According to this, the grid defender can pre-arm according to the VPP scheduling situation, and reasonably plan the investment timing of the defense resources according to the vulnerability of the system.

It can be seen that the control system has strong fault tolerance under a certain (structure, size) parameter perturbation, and maintains the system's strong defensiveness. According to the different definitions of performance, it can be divided into stable robustness and performance robustness. The defense robustness obtained in this study not only has its own stable robustness, but also has performance robustness.

IV. CONCLUSION

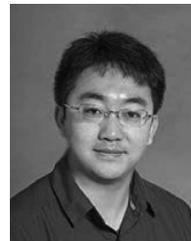
In this paper, the reliability of CPS is studied, and an automatic online evaluation method of CPS reliability based on machine learning is proposed. In one step, the work mainly focuses on CPS model, algorithm and implementation tools.

With the continuous development of CPS in recent years, the development of high real-time, automatic and intelligent CPS has gradually become the common demand of various industries. With the application of information network technology such as sensor, embedded processing, digital communication, artificial intelligence and so on, the various vulnerabilities and vulnerabilities in the information network have seriously affected the safe operation of CPS, and have caused great losses while improving the performance and efficiency of existing systems. With the maturity of artificial intelligence technology, the application of artificial intelligence in the field of network physical space credibility (AI CPS)

cannot only improve the response speed and response speed of various threats in cyberspace, but also improve the predictability and accuracy of risk prevention in an all-round way. Therefore, artificial intelligence technology has been fully applied in the field of CPS, and has played a great potential in dealing with all kinds of human integrity problems in the intelligent era.

REFERENCES

- [1] Chu Y , Chen Q , Fan Z , et al. Tunable V-Cavity Lasers Integrated With a Cyclic Echelle Grating for Distributed Routing Networks[J]. *IEEE Photonics Technology Letters*, 2019, PP(99):1-1.
- [2] Muhammad M, Romana, T, Ali H S, et al. "A Multi-sensor Data Fusion Enabled Ensemble Approach for Medical Data from Body Sensor Networks." *Information Fusion*, Elsevier, Vol. 53, No.2020, pp.155-164, 2020.
DOI 10.1016/j.inffus.2019.06.021
- [3] Lu C , Liang W , Min G , et al. Terahertz Transmittance of Cobalt-doped VO₂ Thin Film: Investigated by Terahertz Spectroscopy and Effective Medium Theory[J]. *IEEE Transactions on Terahertz Science and Technology*, 2019, PP(99):1-1.
- [4] Lin, Yu Chuan , et al. "Development of Advanced Manufacturing Cloud of Things (AMCoT) - A Intelligence Manufacturing Platform." *IEEE Robotics and Automation Letters*, vol. 2, no. 1, pp.1809-1816, 2017.
DOI 10.1109/LRA.2017.2706859
- [5] Chen, Chao Chun , et al. "A Novel Automated Construction Scheme for Efficiently Developing Cloud Manufacturing Services." *IEEE Robotics & Automation Letters*, vol. 3, no. 3, pp.1378-1385, 2018.
DOI 10.1109/LRA.2018.2799420
- [6] Shin, Seungwon , H. Wang , and G. Gu . "A First Step Toward Network Security Virtualization: From Concept To Prototype." *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2236-2249, 2015.
DOI 10.1109/TIFS.2015.2453936
- [7] Romana T, Mohammad S O, Muhammad M, et al. "A decentralised approach to privacy preserving trajectory mining." *Future Generation Computer Systems* , Vol.102, pp.382-392, Jan.2020
DOI: 10.1016/j.future.2019.07.068
- [8] Xie, Haomeng , et al. "Data Collection for Security Measurement in Wireless Sensor Networks: A Survey." *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2205-2224, 2019.
DOI 10.1109/JIOT.2018.2883403
- [9] Wang, Hui Ming , et al. "Physical Layer Security in Heterogeneous Cellular Networks." *IEEE TRANSACTIONS ON COMMUNICATIONS*, vol. 64, no. 3, pp. 1204-1219, 2016.
DOI 10.1109/TCOMM.2016.2519402
- [10] Yang, Yixian , et al. "General Theory of Security and a Study Case in Internet of Things." *IEEE Internet of Things Journal*, vol. 4, no. 2, pp. 592-600, 2016.
DOI 10.1109/JIOT.2016.2597150
- [11] Elkhodr M, Hassan Q F, Shahrestani S A, et al. "Chapter#16: Energy-efficiency in Wireless Body Sensor Networks, Book Title: Networks of the Future Architectures, Technologies, and Implementations." *Chapman & Hall/CRC Computer and Information Science Series*, pp.492, CRC Press (Taylor & Francis Group), Oct. 2017.
- [12] Gao, Yansong , et al. "PUF Sensor: Exploiting PUF Unreliability for Secure Wireless Sensing." *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 9, pp. 2532-2543, 2017.
DOI 10.1109/tcsi.2017.2695228
- [13] Kyriacou, Alexis , et al. "Distributed Contaminant Detection and Isolation for Intelligent Buildings." *IEEE Transactions on Control Systems Technology*, vol. 26, no. 6, pp. 1925-1941, 2018.
DOI 10.1109/TCST.2017.2754986
- [14] Wang, Xun , et al. "iLOC: An invisible Localization Attack to Internet Threat Monitoring Systems." *IEEE Transactions on Parallel & Distributed Systems*, vol. 20, no. 11, pp. 1611-1625, 2009.
DOI 10.1109/TPDS.2008.255
- [15] Fairley, Peter, "Blockchain world - Feeding the blockchain beast if bitcoin ever does go mainstream, the electricity needed to sustain it will be enormous," *IEEE Spectrum*, vol. 54, no. 10, pp. 36-59, 2017.
DOI 10.1109/MSPEC.2017.8048837
- [16] Han Y, Zhang C J, Wang L, et al. "Industrial IoT for Intelligent Steelmaking with Converter Mouth Flame Spectrum Information Processed by Deep Learning." *IEEE Transactions on Industrial Informatics*, pp. 1-1, 2020.
DOI 10.1109/THI.2019.2948100
- [17] Lv Z H, Kong W J, Zhang X, et al. "Intelligent Security Planning for Regional Distributed Energy Internet." *IEEE Transactions on Industrial Informatics*, pp. 1-1, 2020.
DOI 10.1109/THI.2019.2914339
- [18] Choi, Woo Young, and J. S. Lai. "Application of Internet of Things Technology and Convolutional Neural Network Model in Bridge Crack Detection." *IEEE ACCESS*. vol. 6, no.(2018): 39442-39451, 2018.
DOI 10.1109/ACCESS.2018.2855144
- [19] Rastegarfar, Houman , et al. "Cyber-Physical Interdependency in Dynamic Software-Defined Optical Transmission Networks." *Journal of Optical Communications and Networking* 7.12(2015):1126.
DOI 10.1364/JOCN.7.001126
- [20] Ribeiro, Luis , and M. Bjorkman . "Transitioning From Standard Automation Solutions to Cyber-Physical Production Systems: An Assessment of Critical Conceptual and Technical Challenges." *IEEE Systems Journal* (2017):1-13.
DOI 10.1109/JSYST.2017.2771139
- [21] Roy, Debayan , et al. "Semantics-Preserving Cosynthesis of Cyber-Physical Systems." *Proceedings of the IEEE* 106.1(2018):171-200.
DOI 10.1109/JPROC.2017.2779456
- [22] Lu, Chenyang , et al. "Real-Time Wireless Sensor-Actuator Networks for Industrial Cyber-Physical Systems." *Proceedings of the IEEE* (2015):1-12.
DOI 10.1109/JPROC.2015.2497161
- [23] Ye, Hua , et al. "Eigen-Analysis of Large Delayed Cyber-Physical Power System by Time Integration-Based Solution Operator Discretization Methods." *IEEE Transactions on Power Systems* (2018):1-1.
DOI 10.1109/TPWRS.2018.2826576
- [24] Xin, Shujun , et al. "Cyber-Physical Modeling and Cyber-Contingency Assessment of Hierarchical Control Systems." *IEEE Transactions on Intelligence Grid* 6.5(2017):2375-2385.
DOI 10.1109/TSG.2014.2387381
- [25] Adhikari, Uttam , T. Morris , and S. Pan . "WAMS Cyber-Physical Test Bed for Power System, Cybersecurity Study, and Data Mining." *IEEE Transactions on Intelligence Grid* 8.6(2017):2744-2753.
DOI 10.1109/TSG.2016.2537210
- [26] Xin, Shujun , et al. "Information-Energy Flow Computation and Cyber-Physical Sensitivity Analysis for Power Systems." *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* (2017):1-13.
DOI 10.1109/JETCAS.2017.2700618
- [27] Khan, Muhammad , et al. "CPS Oriented Control Design for Networked Surveillance Robots with Multiple Physical Constraints." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (2016):1-1.
DOI 10.1109/TCAD.2016.2524653
- [28] Keller, and L. Keith . "Leveraging Biologically Inspired Models for Cyber - Physical Systems Analysis." *IEEE Systems Journal* (2017):1-11.
DOI 10.1109/JSYST.2017.2739426
- [29] Watson, Robert N. M. , et al. "Fast Protection-Domain Crossing in the CHERI Capability-System Architecture." *IEEE Micro* 36.5(2016):38-49.
DOI 10.1109/MM.2016.84
- [30] Liu, Xindong , et al. "Power System Risk Assessment in Cyber Attacks Considering the Role of Protection Systems." *IEEE Transactions on Intelligence Grid* 8.2(2017):572-580.
DOI 10.1109/TSG.2016.2545683



Zhihan Lv (M'16, SM'19) received the Ph.D. degree from Paris Diderot University and the Ocean University of China, in 2012. He was a Research Associate with University College London. He has been an Assistant Professor with the Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, from 2012 to 2016. He was with CNRS, France, as a Research Engineer, with Umea University, Sweden, as a Postdoctoral Research Fellow, and Fundación

FIVAN, Spain, as an Experienced Researcher. He is currently an Associate Professor with Qingdao University.

Dr. Lv is a Program Committee Member of ACM IUI 2015-2020, IEEE BIGDATA4HEALTH Workshop 2016, IEEE/CIC WIN Workshop 2016, IIKI 2016, and WASA 2016. He has been an Associate Editor of the PLOS One (since 2016), the IEEE Access (since 2016), the Neurocomputing (since 2016), and the IET Image Processing (since 2017), and is a Lead Guest Editor of the IEEE Transactions on Industrial Informatics, IEEE Transactions on Intelligent Transportation Systems, IEEE Network, and IEEE Sensors.



Yang Han was born in Jizhou, Hebei, China, in 1987. He received the B.S. and M.S. degrees from North China University of Science and Technology in 2010 and 2018, respectively. He is currently a Ph.D. student at North China University of Science and Technology. His main research interests include numerical computation, iron and steel big data, and intelligent computation, etc.



Amit Kumar Singh is currently an Assistant Professor with the Computer Science and Engineering Department, National Institute of Technology Patna, Bihar, India. He received his PhD from National Institute of Technology Kurukshetra, Haryana, India in 2015. He has authored over 100 peer-reviewed journal, conference publications, and book chapters. He has authored three books and edited four books with internationally recognized publishers such as Springer and Elsevier. He is the associate editor of IEEE Access (Since 2016), IET Image Processing (Since 2020), and former member of the editorial board of Multimedia Tools and Applications, Springer (2015-2019). He has edited various international journal special issues as a lead guest editor. He has obtained the memberships from several international academic organizations such as ACM and IEEE. His research interests include data hiding, image processing, biometrics, & Cryptography.



Gunasekaran Manogaran is currently working as a Big Data Scientist in University of California, Davis, USA. He is also an Adjunct Assistant Professor, Department of Computer Science & Information Engineering, Asia University, Taiwan and Adjunct Faculty in School of Computing, SRM Institute of Science and Technology, Kattankulathur, India. He is a visiting researcher/scientist in University of La Frontera, Colombia and International University of La Rioja, Spain. He received his PhD from the Vellore Institute of Technology University, India. He received his Bachelor of Engineering and Master of Technology from Anna University, India and Vellore Institute of Technology University, India respectively. He is the author/co-author of

more than 100 papers. He is a member of IEEE Society and International Society for Infectious Diseases and Machine Intelligence Research labs. His current research interests include Big Data Analytics, Internet of Things and Soft Computing.



Haibin Lv graduated from the First Institute of Oceanography, State Oceanic Administration, Qingdao, China, in 1990. He is currently a Professor at the North China Sea Offshore Engineering Survey Institute, Ministry Of Natural Resources North Sea Bureau.