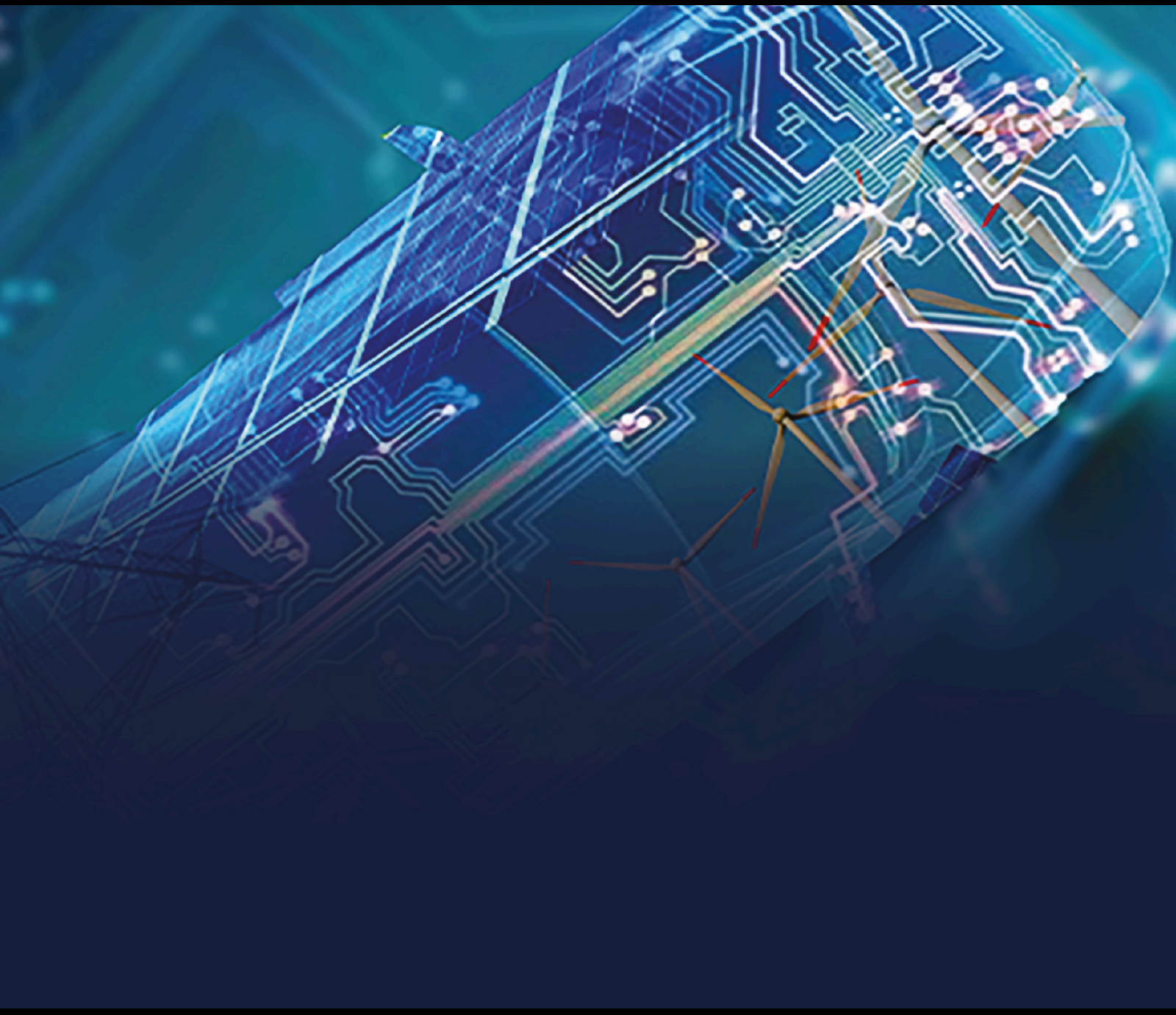
International Transactions on Electrical Energy Systems

Electrical Vehicles Technologies and the Power Quality Challenges

Lead Guest Editor: Ziad M. Ali
Guest Editors: Shady Abdel Aleem and Martin Calasan



Electrical Vehicles Technologies and the Power Quality Challenges

International Transactions on Electrical Energy Systems

Electrical Vehicles Technologies and the Power Quality Challenges

Lead Guest Editor: Ziad M. Ali
Guest Editors: Shady Abdel Aleem and Martin Calasan

Contents

Hindawi
International Transactions on Electrical Energy Systems
Volume 2023, Article ID 8480342, 16 pages
https://doi.org/10.1155/2023/8480342

Research Article

An Effective Method for Sensing Power Safety Distance Based on Monocular Vision Depth Estimation

Leixiong Wang,[1] Bo Wang,[1] Shulong Wang,[1] Fuqi Ma,[1] Xuzhu Dong,[1] Liangzhong Yao,[1] Hengrui Ma,[1] and Mohamed A. Mohamed[2]

[1]*School of Electrical and Automation, Wuhan University, Wuhan, Hubei 430072, China*
[2]*Electrical Engineering Department, Faculty of Engineering, Minia University, Minia 61519, Egypt*

Correspondence should be addressed to Bo Wang; whwdwb@whu.edu.cn

Received 13 November 2022; Revised 5 January 2023; Accepted 19 April 2023; Published 18 May 2023

Academic Editor: Martin Calasan

As an important index of risk protection, the safety distance is crucial to ensure the safe and stable operation of the power system and the safety of personnel's life. Traditional monitoring methods are difficult to balance recognition accuracy and convenience. Therefore, this paper presents a power safety distance sensing method based on monocular visual images to achieve the recognition of the safety distance of external damage in complex scenes of transmission corridors, and proposed a power density depth distance model. In this model, a codec network with skip-connection to extract features and aggregate shallow and deep features for input power system images. Then, the regularization method, migration learning strategy, cosine annealing learning strategy, and data enhancement strategy are used to further optimize the model, so as to obtain a model with good accuracy and generalization in complex conditions. The effectiveness and superiority of the proposed method are verified in comparison to other external damage monitoring methods. The experimental results showed that the proposed method has high accuracy for the distance of external damage in the actual scenario. Moreover, the method has good generalizability, which can be easily deployed in video monitoring systems on different transmission corridors.

1. Introduction

Because the power system has the characteristics of high voltage, strong current, and outward discharge, the power system has strict safety distance standards, operational management measures, and other means to prevent various short-circuit, fire, explosion, and personal injury accidents caused by human body and construction appliance touching or being too close to the charged object [1]. According to the causes of different safety accidents, it can be learned that the control effect of means such as restricting personnel and apparatus from entering the charged areas by means of five preventions and other safety regulations is limited [2]. When power enterprises are under severe pressure of overhaul and maintenance, there are problems such as the poor implementation of safety production responsibilities and lax control of operating sites. For example, during the equipment reconstruction of 500 kV shipping substation of Chongqing Electric Power Company in 2021, due to the insufficient distance between crane lifting equipment and electrified equipment, a bus trip accident was caused. It shows the power system lacked an effective safe distance sensing method [3]. It can be seen that the research on the method of measuring the power safety distance is of great importance to ensure the safe operation of power equipment and the safety of personnel [4].

Currently, safety distance sensing methods for power systems primarily include manual measurement, LiDAR [5], and video monitoring methods [6]. Electric power workers often rely on experience or use theodolite to determine whether there is insufficient safety distance in the inspection section. However, because of the subjective factors of electric power workers, interference from trees and buildings, and visual bias, it is difficult for workers to effectively and accurately determine whether the safety distance is below the standard. The LiDAR method mainly obtains the spatial

geometric structure of the inspected object through inspection by drones equipped with LiDAR, which has the advantages of high-ranging accuracy, strong directionality, and no ground clutter interference [7]. However, the cost is high and requires drones, which cannot be inspected in real-time and is not conducive to the real-time identification of safety hazards. In addition, the processing of laser point cloud data has a high degree of difficulty [8]. The intelligent video surveillance method mainly uses binocular images for depth estimation and safety distance discrimination through the similar triangle principle [9]. Due to the limitation of the early depth estimation principle, this method has a high false alarm and missed alarm rate [10]. Therefore, in order to prevent the occurrence of major accidents affecting the national production life, the power industry needs a power safety distance awareness method that can balance detection accuracy and ease of deployment [11].

Over the past few years, with the rapid development of deep learning, deep neural networks with strong adaptive functionality have been widely accepted by academics [12]. Depth estimation based on deep learning can construct models that correlate image information and depth information to obtain the depth information of the scene [13, 14]. The depth estimation technique based on deep learning gives better results [15]. Currently, they can be categorized as supervised, unsupervised, and semisupervised according to the degree of use of true depth distance [16]. As a supervised approach, the literature [17] achieved good depth estimation performance based on adaptive interval segmentation through deep residual networks for depth-valued classification. The literature [18] uses an unsupervised approach to train the network to obtain depth information of images using the geometric constraint information of neighboring frames of a monocular video stream with multiple frames, reducing the data usage limitation and obtaining promising results. As a semisupervised approach, the literature [19] introduces real depth maps as supervised information in an unsupervised framework, and achieves a blend of supervised and unsupervised by using a more powerful supervised signal for training. Depth estimation techniques based on deep learning have shown great progress in performance [20], and their application in the field of power safety distance perception has become possible.

Summarizing the previous literature on transmission corridor monitoring methods, it can be seen that these methods are difficult to combine both detection accuracy and ease of deployment and are difficult to apply on large-scale transmission corridors. However, in practical applications, transmission line monitoring usually faces problems such as large monitoring area scope, the coexistence of near and distant objects, random operation area, and complex image background [21]. Under the cost limitation, the current method has many problems such as low detection accuracy and low monitoring efficiency. In order to improve the recognition accuracy and efficiency of transmission line safety distance and enhance the generalization capability of transmission line safety distance monitoring, this paper constructs a monocular image-based power safety distance sensing method and proposes a power density depth model based on supervised depth estimation for existing transmission corridor video monitoring systems. The main contributions of this paper are summarized as follows:

(1) A power safety distance sensing method of external damage based on deep learning is constructed to achieve the real-time recognition of the safety distance of external damage, which adapts to most transmission corridor scenarios and improves the monitoring efficiency of the safety distance of external damage

(2) A power density depth model is proposed, which is based on a supervised depth estimation approach using a coder-decoder network architecture with jump connections for image feature extraction aggregation, direct output of spatial distance information in complex scenes of transmission corridors through the network, and multiple optimization strategies to achieve high generalization and recognition accuracy

(3) The effectiveness and superiority of the proposed power safety distance sensing method for safety distance of external damage identification are verified in comparison to traditional manual measurement, LiDAR, and video monitoring methods

The rest of the paper is organized as follows: Section 2 introduces the power safety distance sensing method network structure. Section 3 presents the structure parameter optimization and data enhancement of the power density depth model. In Section 4, experiment results are presented to verify the proposed method, followed by conclusions. Section 5 is the conclusion.

2. Power Safety Distance Sensing Method Based on Power Density Depth Distance Model

This paper proposes a power security distance sensing method based on the power density depth distance sensing model according to the dense depth model [22]. The specific process of this method is shown in Figure 1. This paper adopts the method of "offline training + online application" to build the power safety distance sensing method, the model is constructed and trained offline, and then the trained model is deployed in the transmission corridor video monitoring system for online application. Under the optimization of the regularization method, migration learning strategy, cosine annealing learning strategy, and data enhancement strategy, the offline training phase is mainly to learn the mapping relationship between image pixel information and the corresponding depth distance information by power density depth distance model.

The online application is mainly to input the current moment's images into the trained power density depth distance model to quickly obtain spatial distance information in complex scenes of transmission corridors.

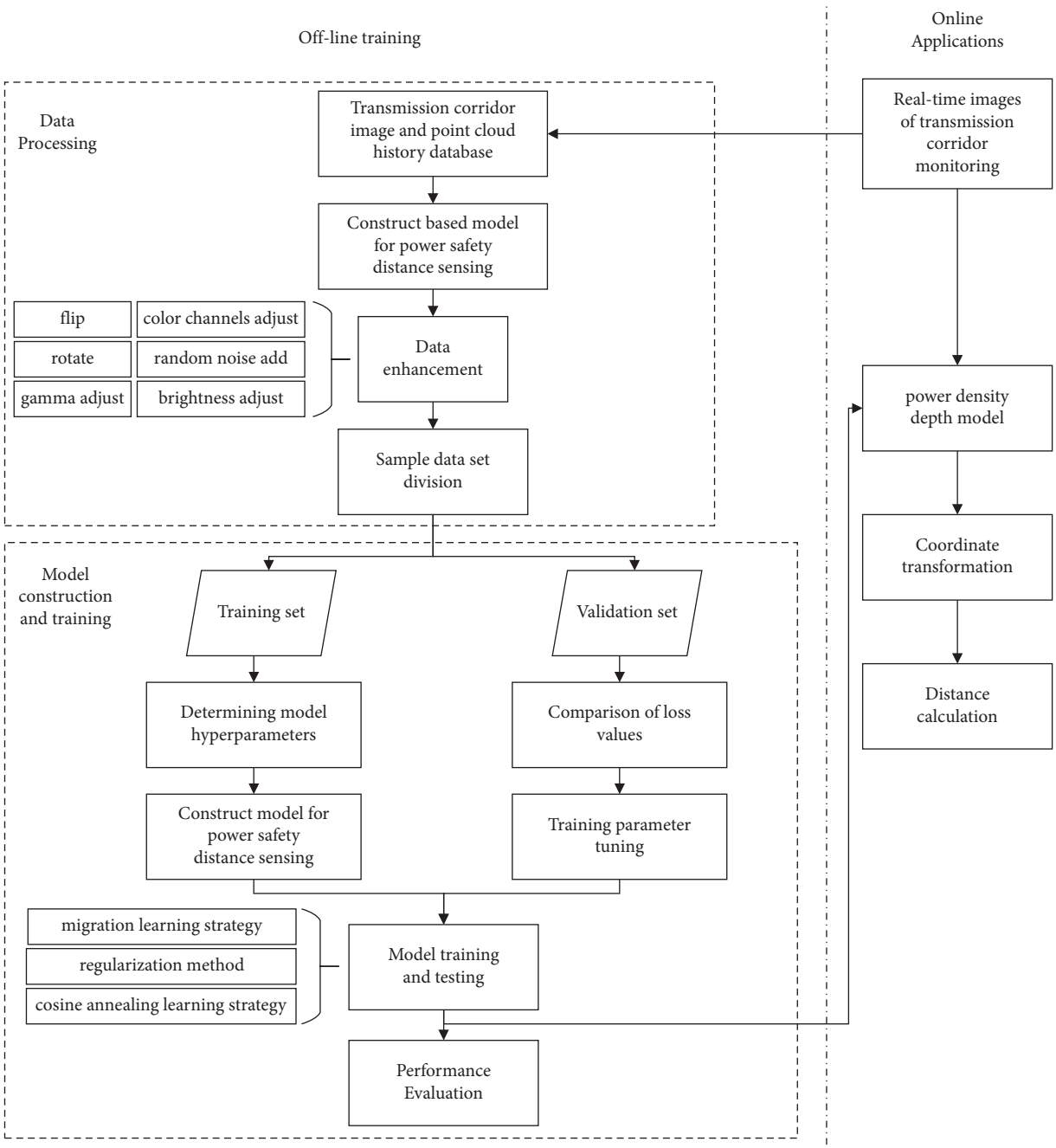


Figure 1: Flowchart of power safety distance sensing method.

Then, the spatial distance information based on the pixel coordinate system is transformed into the depth estimation structure based on the real coordinate system. At last, the coordinate points are manually selected to calculate the distance and judge whether the distance is lower than the safety distance standard.

2.1. Depth Feature Extraction Codec Network Based on DenseNet. The network model is shown in Figure 2; the network extracts the features of the input power system image, aggregates the shallow features and deep features, and extracts the fine structure features to ensure that the network can effectively use the context information provided by the deep features to help the depth estimation of a single point. The shallow features including object contour and position information are effectively used to improve the overall accuracy of the depth estimation algorithm.

The core network of the method is a skip-connected coder-decoder network which is based on the convolutional neural network. In this paper, DenseNet-169 [23] is used for feature extraction of power monocular images as an encoder. The last layer of each convolutional block of the encoder is two bilinear sampling blocks and ReLU activation function with parameters for downsampling, which can obtain more spatial features while reducing the difficulty of calculation.

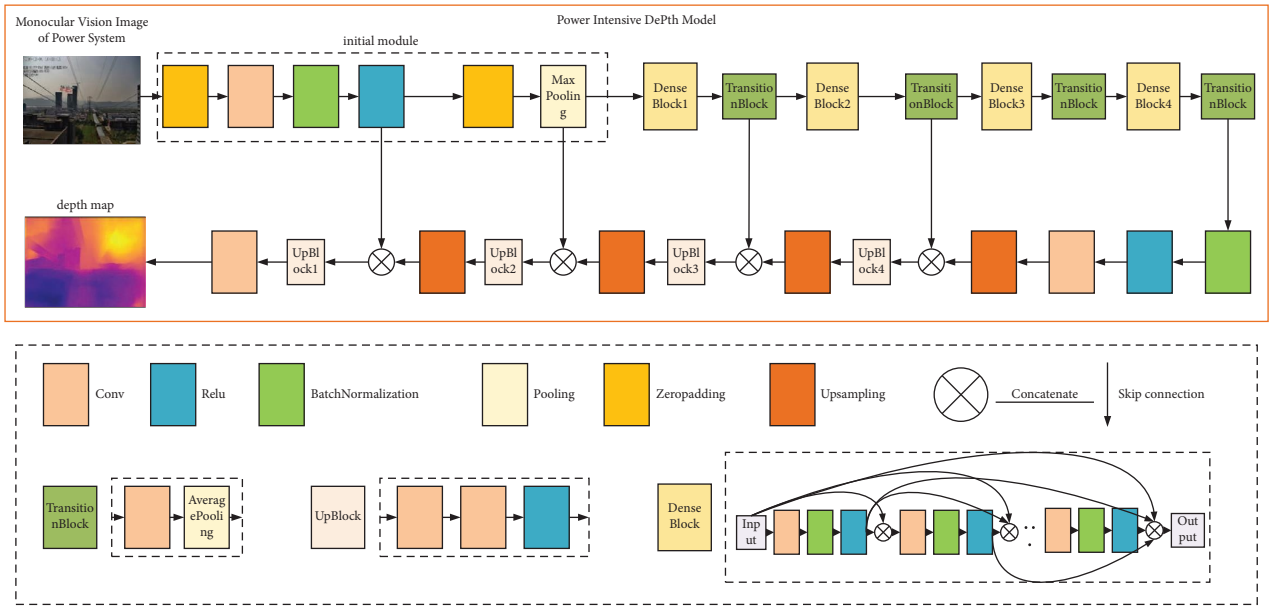


Figure 2: Power density depth distance sensing model.

Input a color monocular image. If the number of convolutional layers is the output eigenvector of the current layer, which is expressed as follows:

$$x_j^l = f\left(\sum_{i \in M_j} x_i^{l-1} * k_{ij}^l + b_j^l\right), \tag{1}$$

where the ReLU function is $(\cdot)$, the output of the current layer is x_j^l, and the convolutional operation is $*$, when the single convolutional kernel of the current convolutional layer is k_{ij}^l and the table convolutional layer offset is b_j^l.

If the number of convolutional layers is m, Formula (2) is the output eigenvector of the pool layer.

$$x_j^m = f\left(\beta_j^m \operatorname{down}\left(x_j^{m-1}\right) + b_j^m\right), \tag{2}$$

where the softmax activation function is $f(\cdot)$, the connection weight is β_j^m, the input of the current pool layer is x_j^{m-1}, the input matrix summation operation is expressed as $\operatorname{down}(\cdot)$, and the current offset is b_j^m.

In this paper, the decoder is composed of convolutional operation and bilinear upsampling operation. The convolutional block of the corresponding encoder is jump connected to the upsampling block of the corresponding decoder. While expanding the feature map, the fine edge structure feature map is obtained to reduce the feature loss. The feature map is the depth map directly output after the convolutional operation. The resolution of the output depth map of the algorithm is 1/2 of the input image.

2.2. Model Loss Function. The main meaning of the loss function of the algorithm is to minimize the depth difference between the predicted depth image $\widehat{D}$ and the original depth image D, and the image detail distortion of the reconstructed depth image $\widehat{D}$.

The composition of the loss function of this algorithm is shown in Formula (3).

$$L_s = \frac{\lambda}{n}\left(\sum_p \left|D_p - \widehat{D}_p\right| + \sum_p \left(\left|g_x\left(D_p, \widehat{D}_p\right)\right| + \left|g_y\left(D_p, \widehat{D}_p\right)\right|\right) + \sum_p \frac{1}{2}\left(1 - \operatorname{SSIM}\left(D_p, \widehat{D}_p\right)\right)\right). \tag{3}$$

In this loss function algorithm, D is the original depth image, $\widehat{D}$ is the reconstructed depth image, p is the pixel point, n is the total number of pixels, and $\lambda = 0.1$ is the weight parameter of depth loss.

The first line on the right side of the equation is depth loss, which means that the pixel difference of the pixel corresponding to the same position p of the reconstructed depth image $\widehat{D}$ and the original depth image D is calculated.

The second line on the right of the equation is the loss of depth smoothness, which represents the minimum second gradient $L1$ criterion defined on the depth image gradient g, where g_x and g_y calculate the difference between the x and y components of the depth image gradient, respectively.

The third line on the right side of the equation is the appearance matching loss structure similarity item, SSIM [24]. SSIM is a commonly used measure in image reconstruction task and expressed as shown in formula (4).

$$\operatorname{SSIM}(D, \widehat{D}) = \frac{\left(2\mu_D\mu_{\widehat{D}} + c_1\right)\left(2\sigma_{D\widehat{D}} + c_2\right)}{\left(\mu_D^2 + \mu_{\widehat{D}}^2 + c_1\right)\left(\sigma_D^2 + \sigma_{\widehat{D}}^2 + c_2\right)}. \tag{4}$$

In SSIM algorithm, μ_D is the average value of the original depth image D, $\mu_{\widehat{D}}$ is the average value of the reconstructed depth image $\widehat{D}$, σ_D^2 is the variance of D, $\sigma_{\widehat{D}}^2$ is the variance of $\widehat{D}$, $\sigma_{D\widehat{D}}$ is the covariance of D and $\widehat{D}$, and $c_1 = (k_1 K)^2$ and

$c_2 = (k_2K)^2$ are the constants used to maintain stability. K is the dynamic range of the pixel values, $K = 255$, $k_1 = 0.01$, and $k_2 = 0.03$.

The reciprocal of depth is used in the actual training prediction of this algorithm. D_{origin} is the original depth map and $D = M/D_{\text{origin}}$ is the target depth map; M is the maximum depth in the scene.

2.3. Coordinate System Transformation. Camera imaging is to change the object to the photosensitive element of the camera through multiple coordinate systems, in which the coordinate systems involved are as follows: world coordinate system ($O_w - X_wY_wZ_w$), which describes the real position of the camera, in M; camera coordinate system ($O_c - X_cY_cZ_c$), the origin is the optical center and the unit is m; image coordinate system($o - xy$), the origin is the midpoint of the imaging plane and the unit is mm; pixel coordinate system (uv), the origin is the upper left corner of the image and the unit is pixel. As shown in Figure 3, p is a point in the world coordinate system; point p with coordinate (x, y) is the imaging point of point p in the image. (u, v) is the coordinate of the pixel coordinate system corresponding to the point. f is the focal length of the camera, representing the distance from o to O_c.

Through the abovementioned coordinate system conversion, a conversion Formula (4) from the pixel to the world coordinate system can be obtained:

$$Z_c\begin{bmatrix} u \\ v \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{dx} & 0 & u_0 \\ 0 & \frac{1}{dy} & v_0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} f & 0 & 0 & 0 \\ 0 & f & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}\begin{bmatrix} R & T \\ \vec{0} & 1 \end{bmatrix}\begin{bmatrix} X_w \\ Y_w \\ Z_w \\ 1 \end{bmatrix} = \begin{bmatrix} f_x & 0 & u_0 & 0 \\ 0 & f_y & v_0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}\begin{bmatrix} R & T \\ \vec{0} & 1 \end{bmatrix}\begin{bmatrix} X_w \\ Y_w \\ Z_w \\ 1 \end{bmatrix}, \tag{5}$$

where the coordinate value of the coordinate point in the camera coordinate system is Z_c, which is obtained by the power density depth distance sensing model. The internal parameters of the camera are the length and width of a single pixel, represented by f_x and f_y. The central coordinate of the imaging surface is (u_0 and v_0). The external parameters of the camera are the rotation matrix R and offset matrix T. In this paper, the internal and external parameters of the camera are obtained through Zhang Zhengyou calibration.

2.4. Safe Distance Calculation. After the conversion of the pixel coordinate system and the real coordinate system, and the manual selection of the coordinate points, it can be determined whether the three-dimensional coordinates enter the charged area. The distance between coordinate points is calculated as follows:

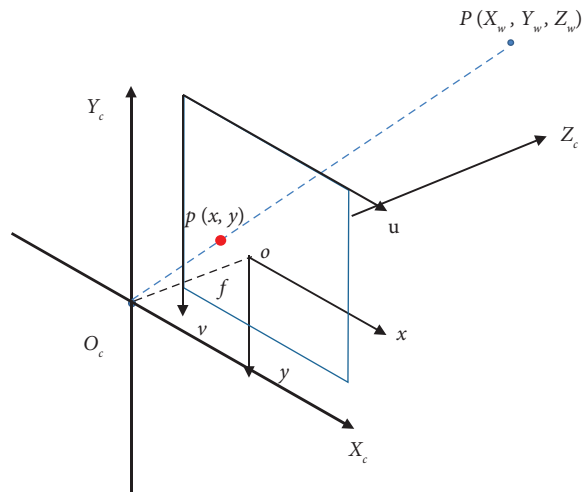


Figure 3: The coordinate system involved in camera imaging.

The Euclidean distance between two points is directly obtained from the three-dimensional coordinates $(X_k, Y_k, \textit{and } Z_k)$ and $(X, Y, \text{and } Z)$ of the two points in the electrically selected monocular image of the power system:

$$d = \sqrt{(X_k - X)^2 + (Y_k - Y)^2 + (Z_k - Z)^2}. \tag{6}$$

After the coordinate system conversion of two points of a manually selected power system monocular image, the distance between two points can be quickly calculated.

3. Structure Parameter Optimization and Data Enhancement of Power Density Depth Model

To meet the need for high accuracy perception of power safety distance, a regularization strategy is used to optimize the power density depth model structure. The model parameters are optimized by the migration learning strategy and cosine annealing learning strategy in order to improve generalization and detection speed. Finally, the sample data are enhanced to improve the stability and accuracy of the network. Figure 4 shows an example of actual sample data.

The monocular image of the power system usually has far and near scenes, and the texture and optical flow characteristics in the image are not obvious. Secondly, the background of the image is more complex, and the image background changes with the change of the four seasons.

3.1. Model Structure Optimization Based on Regularization. In order to reduce the influence of model overfitting, this paper uses a regularization strategy to optimize the model structure, reduce the influence of some parameters on the model, and ensure that the model has a good training effect on the actual data set.

The specific optimization step is to add regularization terms to the loss functions of the convolutional and pooling layers to reduce the sum of values of the parameters, and to improve the accuracy and generalization of the model.

Figure 4: Example of actual sample data.

3.1.1. Convolutional Layer Optimization. The loss function L_{conv} can reduce the difference between output and input and simplify the feature expression. The following is the convolutional loss function Formula (6) after $L2$ regularization:

$$L_{\text{conv}}\left(W, x^{(l)}\right) = \frac{1}{2m}\left[\sum_{i=1}^{m}\left(y_l - W * x_{\text{il}}\right)^2 + \lambda R_{L2}(w)\right], \tag{7}$$

where the convolutional kernel parameter with quantity n is $W = [w_1, w_2, \cdots, w_n]^T$. The first item is the expression ability of the model. The convolutional operation is represented by $*$, and the input of sample l with dimension m is $x^l = [x_{1l}, x_{2l}, \cdots, x_{\text{ml}}]^T$. The actual depth label of the sample l is y_l.

The second item is the regularization term representing the complexity of the parameters. This paper uses $L2$ regularization $\lambda R_{L2}(w)$ to reduce the sum of parameter squares and prevent overfitting; λ is the regularization factor and $R_{L2}(w) = \sum_{j=1}^{n} w_j^2$.

3.1.2. Pooling Layer Optimization. The following is the loss function Formula (7) of the pooling layer after $L2$ regularization:

$$L_{\text{fc}}\left(U, x^{(k)}\right) = \frac{1}{2m}\left[\sum_{i=1}^{m}\left(y_k - U x_{\text{ik}}\right)^2 + \lambda R_{L2}(u)\right], \tag{8}$$

where the first item is the expression ability of the model, and the pooling factor with the number of t is $U = [u_1, u_2, \cdots, u_t]^T$. The second item is the regularization term representing the complexity of the parameters, λ is the regularization factor, and $R_{L2}(u) = \sum_{j=1}^{t} u_j^2$.

When the regularization factor is too small, the reduction of model parameters is small, the model is still easy to overfit, and the model generalization is limited; when the regularization factor is too large, the number of model parameters is sharply reduced, and the whole network becomes a simple approximately linear network, the model features fitting ability is seriously reduced, and the model accuracy is decreased in detail. In order to balance the relationship between the feature-fitting ability of the model and the parametric size of the model, this paper repeatedly verifies the setting of the regularization factor size based on the sample data set to improve the accuracy and generalization of the model.

3.2. Migration Learning Shared Parameter Strategy. Migration learning, which is widely used in image recognition of power systems, will be used to train the target data using network parameters learned from source datasets [25, 26]. Migration learning can be divided into four basic methods: based on sample migration, based on feature migration, based on model migration and based on relationship migration [27]. This paper uses a model-based migration learning method by sharing the parameter information of the pretraining mode to realize the migration

from large source domain datasets to specific learning tasks in the target domain.

For real images of power systems with complex backgrounds, the convolutional neural network is difficult to extract image features effectively and accurately, and it is difficult to obtain enough samples to train the model in practice. These factors will reduce the accuracy and generalization of model distance sensing. Therefore, this paper uses the training strategies of transfer learning, deleting the top-level DenseNet-169 network pretrained on ImageNet [28] related to the original network classification task to extract features from the actual sample data as an encoder, effectively improving the accuracy and generalization of the model.

3.3. Cosine Annealing Learning Strategy. The learning rate of a model is an important factor that affects its accuracy. The loss value of the network decreases too slowly at a lower learning rate. Networks may be trapped in local optimum or divergent when learning rates are high. During algorithm training, network parameters are set by random initialization, so in order to reduce the loss quickly, the network needs to set a larger learning rate. After several iterations, the learning rate should be reduced to avoid local optimum or divergence caused by too fast updating of network parameters. In this paper, we use the learning strategy of cosine annealing, and the formula is as follows:

$$\eta_t = \eta_{\min}^i + \frac{1}{2}\left(\eta_{\max}^i - \eta_{\min}^i\right)\left(1 + \cos\left(\frac{T_{\text{cur}}}{T_i}\pi\right)\right). \tag{9}$$

In (9), i is the current index value, $n_{\max}^i$ and $n_{\min}^i$ represent the maximum and minimum learning rates, respectively, they define the range of learning rates. T_{cur} denotes the number of epochs currently being trained, and T_i represents the total number of epochs in the i-th training. The initial learning rate was set to 0.0001, the minimum learning rate to 0.00001, the maximum learning rate set to 0.001, and the training epoch to 200.

3.4. Data Enhancement. Referring to the methods of Eigen [29], this paper expands the sample data to make the model have better generalization ability. Specific data enhancement operations include the following:

(1) Sample data are flipped horizontally, rotated 90 degrees and 180 degrees; the probability is 50%

(2) Sample data gamma values are randomly chosen from the (0.5, 1.5) range; the probability is 50%

(3) Sample data color channels are randomly multiplied by random numbers in the (0.5, 1.5) range for color adjustment; the probability is 50%

(4) Randomly add 30% noise to the sample with a 50% probability

(5) The sample data are randomly multiplied by random numbers in the (0.5, 1.5) range for brightness adjustment with a probability of 50%

As shown in Figure 5, the sample data are flipped, rotated, gamma adjusted, color channels adjusted, random noise added, and brightness adjusted.

4. Performance Test of Power Safety Distance Sensing Method Based on Power Density Depth Distance Sensing Model

In order to test the effectiveness of the power safety distance sensing method based on the power density depth model, this paper tests and compares the binocular camera [30], SFMlearner unsupervised depth estimation [31], Mono-Depth semisupervised depth estimation [32], DenseDepth supervised depth estimation, and the power security distance sensing methods based on power density depth-sensing model to verify the validity of the methods presented in this paper.

4.1. Experimentation Environment and Dataset Description. This algorithm is based on Keras deep learning framework. The computer is configured as Windows 10 operating system, 8-core Core i7 processor, GTX2060 graphics card, 16 G memory.

As shown in Figure 6, the datasets for the experiment are obtained from the transmission corridor monitoring data from a province in China in recent years. The dataset is mainly based on the transmission channel scene with flat ground and three-dimensional buildings. There are 2025 pairs of RGB image pairs taken by binocular cameras and corresponding depth maps, ranging from 5 to 250 m, which are almost based on the point cloud data of the transmission corridor and filled in the corresponding pixel depth deficit under the guidance of the literature [33]. Based on the average depth of each pair of data, the dataset can be divided into 4 distance scenarios, respectively. The average depth and image quantity of each scenario are shown in Table 1.

4.2. Evaluating Indicator. To evaluate and compare the performance of various depth estimation techniques, this paper adopts a common method of performance evaluation for depth estimation techniques. The method has five evaluation indices: AbsRel (absolute relative error), RMSE (root mean square error), RMSE-log (logarithmic root mean square error), SqRel (relative square error), and % correct (threshold accuracy). This accuracy measure is used as the accuracy [34] by calculating the ratio of pixels whose maximum value is less than the threshold T to the total pixels. The formulas for these indicators are as follows:

(a) (b) (c) (d) (e) (f) (g) (h)

Figure 5: Continued.

(i) (j)

Figure 5: Example of actual sample data enhancement: (a) sample image, (b) rotation, (c) sample image, (d) gamma value adjustment, (e) sample image, (f) color adjustment, (g) sample image, (h) random noise, (i) sample image, and (j) brightness adjustment.

Figure 6: Examples of the dataset.

Table 1: The detail of depth images datasets.

Resolution	Average depth	Training	Testing	Total
1920 ∗ 1080	50	213	46	259
	100	275	87	362
	150	410	157	567
	200	621	216	837
Total	150	1519	506	2025

$$\begin{aligned}
\text{AbsRel} &= \frac{1}{n}\sum_{p}\frac{\left|D_p - \widehat{D}_p\right|}{D_p},\\
\text{RMSE} &= \sqrt{\frac{1}{n}\sum_{p}\left|D_p - \widehat{D}_p\right|^2},\\
\text{RMSE} - \log &= \sqrt{\frac{1}{n}\sum_{p}\left|\log D_p - \log\widehat{D}_p\right|^2},\\
\text{SqRel} &= \frac{1}{n}\sum_{p}\frac{\left|D_p - \widehat{D}_p\right|^2}{D_p},\\
\%\text{correct} &= \max\left(\frac{\widehat{D}_p}{D_p}, \frac{D_p}{\widehat{D}_p}\right) = \delta < T.
\end{aligned} \tag{10}$$

In the equation, D_p is the true depth value of the pixel point p in the initial depth image, $\widehat{D}_p$ stands for the estimated depth value of the pixel point p in the prediction depth image, n is the total number of pixels, and T represents the threshold value. In this paper, $T = 1.25$.

4.3. Depth Map Display. Scene depth is the distance from the scene to the camera imaging center, which is usually visualized by depth maps. The color depth map uses color values to represent the depth of image pixels [35], as shown in Figure 7. In particular, in order to avoid the problem of too large loss function value caused by too large original depth value of transmission line scene, which affects network training, the DenseDepth depth estimation method uses the reciprocal of depth in actual training prediction, so its depth map performance result is opposite to other methods except for the binocular camera [36, 37].

4.4. Setting of Regularization Factor. For selecting the appropriate regularization factor, this paper repeats the test verification based on the power density depth model, and the results are shown in Table 2. Table 2 shows that when $\lambda = 100$, % correct is the highest and the detection speed is relatively fast. Therefore, $\lambda = 100$ is selected for the regularization factor.

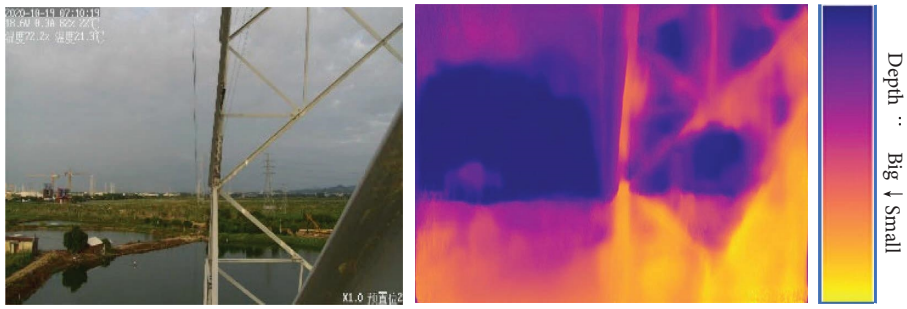


Figure 7: Color depth map representation.

Table 2: Influence of λ value on the detection precision.

λ value	Number of iterations	% correct (%)	Speed (ms per sheet)
0	5000	83.12 84.46	102 79
50	5000	84.45 84.98	77 63
100	5000	84.93 85.81	71 59
200	5000	84.77 84.23	71 66
1000	5000	83.23 83.41	61 55

4.5. Performance Evaluation of Depth and Distance Sensing Method. In order to test the performance of the power-intensive depth model proposed in this paper, this section makes a qualitative and quantitative comparative analysis of five methods: binocular camera, unsupervised depth estimation, semisupervised depth estimation, supervised depth estimation, and the power-intensive depth model proposed in this paper. The test results are shown in Tables 2 and 3.

4.5.1. Qualitative Analysis. Table 2 shows the comparison results between the depth estimation method and other methods on the data set in this paper. Absolute relative error, root mean square error, logarithm root mean square error, relative square error, detection speed, and accurate threshold are used in Table 3. The model proposed in this paper has significantly improved in error, detection speed, and threshold accuracy. According to Table 4, the comprehensive analysis is as follows:

(1) Due to the characteristics of transmission corridor scene image texture, inconspicuous optical flow features, and large scene range, the traditional binocular camera technology and the unsupervised depth estimation SFMlearner algorithm have a threshold accuracy $\delta < 1.5$ of no more than 70%, and the processing speed is greater than 1 sec/each, making it difficult to achieve the transmission corridor scene ranging performance requirements.

(2) Semisupervised depth estimation MonoDepth achieves more accurate depth estimation by introducing the binocular right view into the model as an additional supervised signal on the basis of reducing the difficulty of data set acquisition. However, matching corresponding pixels between binocular images of transmission corridors is difficult, and the reconstruction process of this method is vulnerable in interference. Its root mean square error RMSE is 5.9764, and the percentage of pixels with large errors in the prediction results is large. Therefore, the method is less stable in the transmission corridor scenario.

(3) The supervised depth estimation DenseDepth and the model proposed in this paper directly predict the corresponding pixel depth values for the input monocular images based on real point cloud data, and their threshold accuracy reaches about 80%. By optimizing the structure of the original DenseDepth model through regularization and reasonably reducing the model parameters, the detection speed of the proposed model is improved by 31% compared with that of DenseDepth, and thanks to the optimized model training process by data augmentation strategy, migration learning strategy, and cosine annealing learning strategy; the network features are extracted and fitted well. The RMSE of the proposed model is 5.4645 and the threshold accuracy is 85.36%. In summary, the generalization and accuracy of the power density depth model are improved compared with the initial DenseDepth, which meets the requirements of the transmission corridor scenario for ranging performance.

4.5.2. Quantitative Analysis. The qualitative comparison is shown in Table 4. The power density depth model proposed in this paper has a good depth estimation effect, more local details can be obtained, and ensure that the boundary of the object is obvious. Meanwhile, it has good scene generalization and adaptability. According to Table 3, the comprehensive analysis is as follows:

(1) The model proposed in this paper can obtain more local details. As shown in the detection results of the tower crane in the third row of the image, the power line in the fourth row of the image, and power line and distant trees in the fifth row of the detection

Table 3: Comparison between six kinds of computer vision methods on accuracy and speed.

Method	Lower is better					Higher is better
	AbsRel	RMSE	RMSE-log	SqRel	Speed (per picture)	Correct (%)
Binocular camera	0.3398	7.9764	0.4283	1.8364	2.0 s	64.46
SFMlearner	0.3081	7.6983	0.4887	2.8249	1.0 s	68.42
MonoDepth	0.1898	5.9764	0.2283	0.8364	89 ms	77.88
DenseDepth	0.1550	5.8630	0.2150	0.9051	1.0 s	79.98
Power density depth model	0.1378	5.4645	0.1932	0.8363	69 ms	85.36

image in Table 4, by optimizing the model parameters through transfer learning and cosine annealing learning strategies, the feature extraction network of the proposed method can extract more deep feature information, so as to restore more scene details. It can not only estimate the depth information of smaller tower cranes, power lines, excavators, and other objects, but also better restore the scene level. However, as shown in the upper right area of the image in row 6 of Table 4, the method proposed in this paper may also cause the problem of depth estimation error.

(2) The model proposed in this paper has good depth estimation continuity. As shown in Table 4, the boundaries of the buildings in the upper left area of the detection image in row 3 and the power lines in the image in row 4 are clear and well correspond to the RGB image. This method can effectively use the shallow and deep features, reduce the loss of spatial context features and scale context features, and obtain good depth estimation performance at the object boundary.

(3) The model proposed in this paper has good scene generalization and adaptability. As shown in the image detection results in rows 1 and 2 in Table 4, the scene test image with uneven ground and no three-dimensional building is quite different from the data set in this paper. However, it is obvious that by optimizing the model structure through the regularization method, the proposed method has a good depth estimation effect. It is suitable for the depth information estimation of distant details and can better estimate the boundary depth information of objects in the scene.

In summary, the power density depth model proposed in this paper optimizes the model structure by regularization method and optimizes the model training process by migration learning and cosine annealing learning strategies, and finally the model has a more reasonable parameter training effect and quantity and has a better depth estimation effect. Meanwhile, the method can effectively utilize shallow and deep features through a skip-connected coder-decoder network, reduce the loss of spatial context features and scale context features, and estimate the depth information of distant details appropriately, which can better estimate the boundary depth information of objects in the scene, with higher accuracy and better scene generalization and adaptability to the transmission corridor scenes.

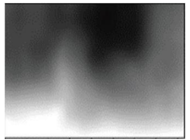
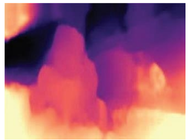
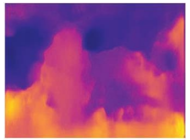
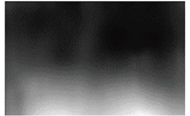
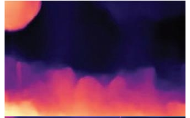
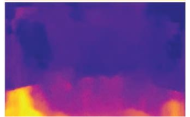
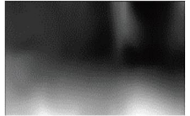
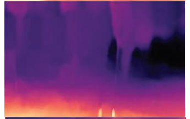
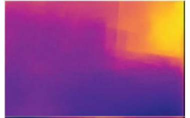
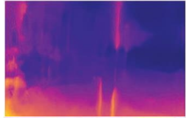
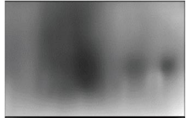
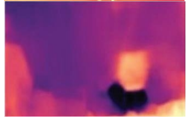
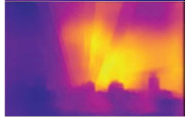
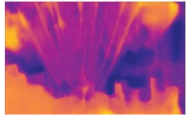
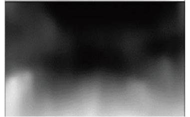
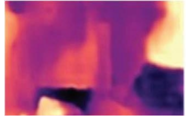
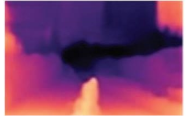
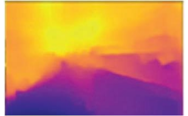
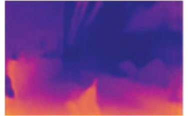
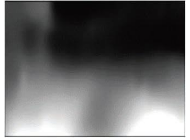
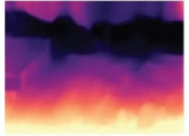
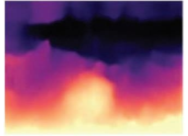
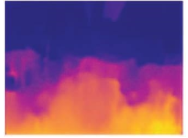
4.6. Result Analysis of Power Security Distance Sensing Method Based on Power Density Depth Model. In this paper, the point cloud data are used to calculate the two-point distance as the real distance data to realize the comparative quantitative analysis of the detection results of the power security distance sensing method based on the power density depth model. The experimental comparison results are shown in Figures 8 and 9 and Table 5.

Comprehensive analysis shows that as shown in Figure 8, when the method proposed in this paper detects the transmission channel image of flat ground and three-dimensional buildings similar to the model training data set, the relative error between the calculated safety distance and the point cloud data is the smallest, which is 11.067%. As shown in Figure 8, when the proposed method detects the transmission channel image with a large difference from the model training data set, the error is the largest, which is 24.295%. Overall, the total average relative error of the proposed method is 18.329%. While reducing the cost, the relative error difference between the proposed method and point cloud data is less than 20%. This method adopts monocular depth estimation technology based on deep learning. On the basis of reducing the cost of safe distance perception, it can perceive the distance between far and near, and improve the accuracy of monocular depth estimation through image, so as to combine detection accuracy and ease of deployment.

At the same time, there are many sources of error in the comparison of results, including the error of training data acquisition, the error caused by the calibration of internal and external parameters of the camera, the error caused by obtaining the coordinates of different objects and wire pixels in the image, and so on.

Meanwhile, this paper compares the proposed method with several commonly used transmission corridor monitoring methods, including traditional manual measurement methods, video monitoring methods, and laser point cloud diagnosis methods. The performance indicators include whether to support ranging, the relative error of ranging, false alarm rate, processing time of each image, and whether to support multiple scenes, and the comparison results are shown in Table 6.

Table 4: Comparison of detection results of six depth estimation methods.

Test picture	Binocular camera	SFMlearner	MonoDepth	DenseDepth	Power density depth model
					
					
					
					
					
					

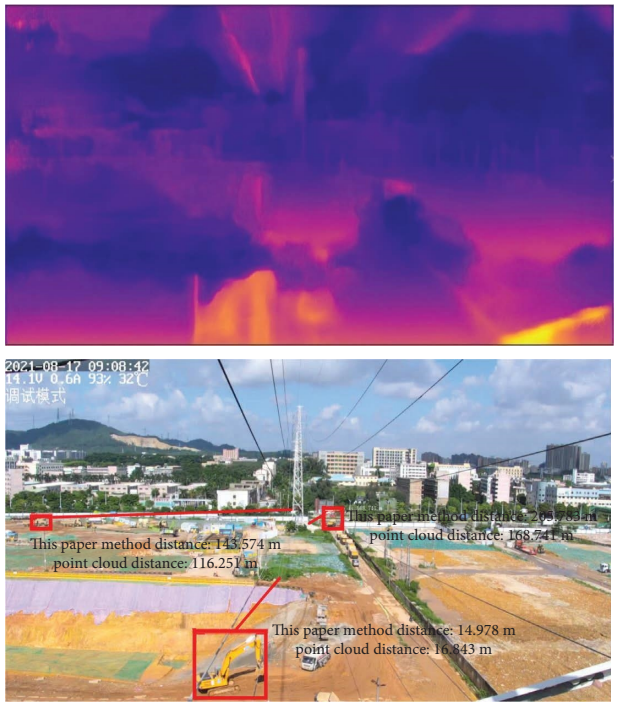


Figure 8: Image 1 of the safety distance sensing result of this method.

Figure 9: Image 2 of the safety distance sensing result of this method.

Results show that in the transmission corridor scenario, the monitoring performance of the traditional manual measurement method is fair, but the method cannot achieve real-time monitoring of the transmission corridor and cannot meet the growing demand for external breakage risk control in the transmission corridor. Although the common monitoring methods based on video monitoring have now been used on a large scale in the transmission corridor due to their low cost, real-time monitoring, and good adaptability to multiple scenes, the method is only through image recognition technology to detect the external broken object, missing distance information; resulting in an alarm once the monitoring perspective inside the external broken object, the false alarm rate is extremely high, monitoring efficiency is low. Although the laser point cloud diagnosis method [7] has the lowest relative error in distance measurement as well as false alarm rate, the method requires a 3D point cloud model for a single transmission corridor and is based on this model for subsequent safety distance measurement of external damage. Due to the large coverage of power system transmission corridors, the method does not support multiple scenarios and real-time detection, and the application cost is extremely high, making it difficult to promote its application. In contrast, by supervised depth estimation, the proposed method can be based on the existing transmission corridor video monitoring system to achieve real-time measurement of the safety distance of external damage at a low cost. By learning the existing transmission corridor images and point cloud data, the applicability of this method can cover most transmission corridors and support multiple scenarios, while the false alarm rate of the distance measurement error of this method is relatively low, which can meet the demand of transmission corridor monitoring.

Overall, the power security distance sensing method based on the power density depth model in this paper is a general method for power security distance sensing; simply use the data corresponding to the scenarios of power security distance perception for training. In this paper, based on the

Table 5: Safety distance measurement result of this method.

Number	The distance measured by the method in this paper (m)	The distance measured by the point cloud data (m)	Absolute error (m)	Relative error (%)
1	10.491	12.447	1.956	15.714
2	11.732	10.333	1.399	13.539
3	143.574	116.251	11.860	23.503
4	19.952	25.607	5.655	22.084
5	30.662	40.502	9.840	24.295
6	86.859	75.721	11.138	14.709
7	14.978	16.842	1.864	11.067
8	26.714	32.027	5.313	16.589
9	29.901	24.950	4.951	19.843
10	205.783	168.741	27.042	21.951

Table 6: Performance comparison of different power safety distance detection methods.

Methods	Technology	Whether to measure the distance	Average relative error (%)	False alarm rate (%)	Processing speed	Whether to support multiple scenes
Traditional monitoring methods	Manual measurement	Yes	10.325	42.44	Non-real-time	Yes
Common monitoring methods	Video monitoring	No	No	67.89	Real-time	Yes
Literature [7]	LiDAR	Yes	3.8971	8.345	Non-real-time	No
The method proposed in this paper	Supervised depth estimation	Yes	11.067	15.35	Real-time	Yes

examination of power system single objective images to reduce the cost of the perception of the safe distance, the method can effectively discover the safe distance between manually selected monitoring points. At the same time, it can have high accuracy and speed of the measurement of the safe distance.

5. Conclusion

To tackle the problem of the recognition of the safety distance of external damage, a power safety distance sensing method based on monocular visual images is proposed to achieve the recognition of safety distance of external damage in a complex scene of transmission corridors. The specific conclusions are as follows:

(1) A power safety distance sensing method based on supervised depth estimation is constructed, which can be used to obtain spatial distance information at low cost by inputting monocular images and realize the safety distance of detecting external damage based on the existing monitoring system, which can effectively improve the monitoring efficiency

(2) A power density depth distance model based on the convolutional neural network is proposed and optimized by the regularization method, migration learning strategy, cosine annealing learning strategy, and data enhancement strategy, which can obtain spatial distance information in complex scenes of transmission corridors while maintaining good accuracy and generalizability.

However, when the proposed method is used for feature extraction, it is easy to ignore the features of the prospective part, resulting in feature loss. This problem will be improved in the follow-up work.

Data Availability

The data used to support the findings of this study are included within the paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the major science and technology special project of Yunnan Provincial Science and Technology Department (202202AD080004).

References

[1] F. Q. Ma, B. Wang, X. Z. Dong, H. G. W., P. Luo, and Y. Y. Zhou, "Safety image interpretation of power industry: basic concepts and technical framework," *Proceedings of the CSEE*, vol. 21, pp. 1–17, 2021.

[2] F. Q. Ma, B. Wang, X. Z. Dong, H. G. W., P. Luo, and Y. Y. Zhou, "Power vision edge intelligence: power depth vision acceleration technology driven by edge computing," *Power System Technology*, vol. 44, no. 6, pp. 2020–2029, 2020.

[3] P. E. N. G. Xiangyang, C. H. E. N. Chi, and X. U. Xiaogang, "Transmission corridor safety distance diagnosis based on point cloud and unmanned aerial vehicle loaded airborne

laser scanning," *Power System Technology*, vol. 18, no. 11, pp. 3262–3267, 2014.

[4] H. Zhao, Y. Zhao, and Y. Jiang, "Supervision and management integrated safety management system based on electric power internet of things[J]," *Electric Safety Technology*, vol. 22, no. 9, pp. 22–25, 2020.

[5] Y. I. N. Jinhua and S. U. N. Chaoyang, *Z H E N G Yanchun*, vol. 28, no. 7, Beijing, China, Beihang University, 2007

[6] H. U. A. N. G. Junjie, L. I. U. Xiaobo, and A. O. Yu, "Research of binocular vision monitoring schemes based on transmission line passage ways," *Electrical Automation*, vol. 41, no. 1, pp. 38–40, 2019.

[7] C. Chen, X. Y. Peng, S. Song, K. Wang, J. J. Qian, and B. S. Yang, "Safety distance diagnosis of large scale transmission line corridor inspection based on LiDAR point cloud collected with UAV," *Power System Technology*, vol. 39, no. 8, pp. 39–42, 2012.

[8] Z. Xu, M. Liu, G. Yang, and N. Li, "Application of interval analysis and evidence theory to fault location," *IET Electric Power Applications*, vol. 3, no. 1, pp. 77–80, 2009.

[9] J. Jiang and X. Zhang, "Depth estimation methods based on computer vision," *Electro-Optic Technology Application*, vol. 26, no. 1, pp. 51–55, 2011.

[10] L. Gao, *Algorithm Research and Design of Transmission Line Video Anti-break System*, LanZhou University of Technology, Lanzhou, China, 2018.

[11] X. Han, *Research on Measurement Method of Distance for Crisscross Span of Overhead Transmission Line Based on Machine Vision*, North China Electric Power University, Beijing, China, 2016.

[12] P. Luo, B. Wang, and H. Ma, "Defect recognition method with low false negative rate based on combined target detection framework," *High Voltage Engineering*, vol. 47, no. 2, pp. 454–464, 2021.

[13] A. Saxena, S. H. Chung, and A. Y. Ng, "Learning depth from single monocular images," in *Proceedings of the 18th International Conference on Neural Information Processing Systems Conference (NIPS)*, pp. 1161–1168, Cambridge, UK, June 2005.

[14] F. Dellaert, S. M. Seitz, C. E. Thorpe, and S. Thrun, "Structure from motion without correspondence," in *Proceedings of the 2000 IEEE conference on computer vision and pattern recognition (CVPR)*, vol. 15, pp. 557–564, Hilton Head, SC, USA, June 2000.

[15] L. I. Yang, X. Chen, Y. Wang, and M. Liu, "Progress in deep learning based monocular image depth estimation," *Laser and Optoelectronics Progress*, vol. 56, no. 19, pp. 9–25, 2019.

[16] T. Bi, Y. Liu, D. Weng, and Y. Wang, "Survey on supervised learning based depth estimation from a single image," *Journal of Computer-Aided Design and Computer Graphics*, vol. 30, no. 8, pp. 1383–1393, 2018.

[17] S. F. Bhat, I. Alhashim, and P. Wonka, "AdaBins: depth estimation using adaptive bins," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pp. 4009–4018, Virtual, July 2021.

[18] J. Watson, O. Mac Aodha, V. Prisacariu, B. Gabriel, and M. Firman, "The temporal opportunist: self-supervised multi-frame monocular depth," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pp. 1164–1174, Virtual, May 2021.

[19] V. Guizilini, J. Li, R. Ambrus, S. Pillai, and A. Gaidon, "Robust semi-supervised monocular depth estimation with reprojected distances," in *Proceedings of the Conference on Robot Learning*, pp. 503–512, Osaka, Japan, September 2020.

[20] C. Shi, *Depth Estimation of Monocular Image Based on Deep Learning*, Beijing University of Chemical Technology, Beijing, China, 2020.

[21] Z. Liu, X. Miao, J. Chen, and H. Jiang, "Review of visible image intelligent processing for transmission line inspection," *Power System Technology*, vol. 44, no. 3, pp. 1057–1069, 2020.

[22] I. Alhashim, P. Wonka, I. Alhashim, and P. Wonka, "High quality monocular depth estimation via transfer learning," 2018, https://arxiv.org/abs/1812.11941.

[23] G. Huang, Z. Liu, L. Van Der Maaten, and Q. Kilian, "Weinberger. Densely connected convolutional networks," in *Proceedings of the 2017 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 2261–2269, Honolulu, HI, USA, July 2016.

[24] W. Zhou, A. C. Bovik, H. R. Sheikh, and P. E. Simoncelli, "Image quality assessment: from error visibility to structural similarit," *IEEE Transactions on Image Processing*, vol. 13, pp. 600–612, 2004.

[25] M. A. Peng and Y. Fan, "Small sample smart substation power equipment component detection based on deep transfer learning," *Power System Technology*, vol. 44, no. 3, pp. 1148–1159, 2020.

[26] H. Yan and J. Chen, "Insulator string positioning and state recognition method based on improved YOLOV3 algorithm," *High Voltage Engineering*, vol. 46, no. 2, pp. 423–431, 2020.

[27] S. J. Pan and Q. Yang, "A survey on transfer learning," *IEEE Transactions on Knowledge and Data Engineering*, vol. 22, no. 10, pp. 1345–1359, 2010.

[28] J. Deng, W. Dong, R. Socher, L. Li, K. Li, and L. Fei-Fei, "Imagenet: a large-scale hierarchical image database," in *Proceedings of the 2009 ieee conference on computer vision and pattern recognition (cvpr)*, pp. 248–255, Miami, FL, USA, June 2009.

[29] D. Eigen, C. Puhrsch, and R. Fergus, "Depth map prediction from a single image using a multi-scale deep network," in *Proceedings of the 27th International Conference on Neural Information Processing Systems (NIPS)*, pp. 2366–2374, Cambridge, MA, USA, December 2014.

[30] X. Li and D. Zhang, "Binocular image ranging algorithm baseol on downsampling clustering," *Journal of Liaoning University Natural Sciences Edition*, vol. 47, no. 3, pp. 277–283, 2020.

[31] T. Zhou, M. Brown, N. Snavely, G. David, and Lowe, "Unsupervised learning of depth and ego-motion from video," in *Proceedings of the The 30th IEEE Conference on Computer Vision and Pattern Recognition*, vol. 7, Honolulu, HA, USA, July 2017.

[32] P. Chen, A. H. Liu, Y.-C. Liu, and Y. C. F. Wang, "Towards scene understanding: unsupervised monocular depth estimation with semantic-aware representation," in *Proceedings of the 2019 IEEE/CVF conference on computer vision and pattern recognition (CVPR)*, pp. 2619–2627, Long Beach, CA, USA, June 2019.

[33] Y. Zhang and F. Thomas, "Deep depth completion of a single RGB-D image," in *Proceedings of the 2018 IEEE/CVF*

conference on computer vision and pattern recognition (CVPR), pp. 175–185, Salt Lake City, UT, USA, June 2018.

[34] H. Xu, *Research on Depth Estimation Algorithms for Monocular Image*, Shandong University, Jinan, China, 2018.

[35] L. I. U. Yi-ying, *Depth Estimation from Monocular Image Based on Deep Convolutional Neural Networks*, Xidian University, Xi'an, China, 2019.

[36] F. Ma, B. Wang, J. Zhou et al., "An effective risk identification method for power fence operation based on neighborhood correlation network and vector calculation," *Energy Reports*, vol. 7, no. 2021, pp. 6995–7003, 2021.

[37] J. Liu, R. Jia, W. Li et al., "High precision detection algorithm based on improved RetinaNet for defect recognition of transmission lines," *Energy Reports*, vol. 6, pp. 2430–2440, 2020.

Hindawi
International Transactions on Electrical Energy Systems
Volume 2023, Article ID 6166738, 13 pages
https://doi.org/10.1155/2023/6166738

Research Article

A Novel Model-Based Reinforcement Learning for Online Anomaly Detection in Smart Power Grid

Ling Wang,[1,2] **Yuanzhe Zhu**,[1,2] **Wanlin Du**,[1,2] **Bo Fu**,[3] **Chuanxu Wang**,[4] **and Xin Wang**[5]

[1]*Electric Power Research Institute of Guangdong Power Grid Co., Ltd., Guangzhou, Guangdong 510080, China*
[2]*Key Laboratory of Power Quality of Guangdong Power Grid Co., Ltd., Electric Power Research Institute of Guangdong Power Grid Co., Ltd., Guangzhou, Guangdong 510080, China*
[3]*Guangdong Power Grid Corporation Zhuhai Power Supply Bureau, Zhuhai, Guangdong 519099, China*
[4]*Guangdong Power Grid Corporation Dongguan Power Supply Bureau, Dongguan, Guangdong 523120, China*
[5]*CET Shenzhen Electric Technology Inc, Shenzhen, Guangdong 518040, China*

Correspondence should be addressed to Ling Wang; wangleng136@gmail.com

Received 7 July 2022; Revised 8 August 2022; Accepted 12 August 2022; Published 28 April 2023

Academic Editor: Martin Calasan

Smart grids must detect cyber-attacks early to ensure their safety and reliability. There have been many outlier detection methods presented in the studies, varying from those requiring instance-by-instance decisions *t* the online diagnosing methods that require the use of accurate models of an attack. This study proposes a novel intelligent online anomaly or attack detection method based on the partially observable Markov decision procedure (POMDP). The proposed model may be categorized as a general detection method according to the reinforcement learning (RL) architecture for POMDP which can help the learning process based on the award concept. The performance of the proposed model is verified using the IEEE test system. Based on numerical results, the suggested RL-based algorithm shows to be very effective in detecting cyber-attacks against the smart grid quickly and accurately.

1. Introduction

The energy grids of the future, the so-called smart grid (SG), rely on enhanced communication and control technology to enhance the quality of the power generation and delivery to the end users. In this way, SGs are vulnerable to cyber-attacks because of these critical cyber infrastructures [1]. Attackers typically aim at damaging or misleading the SG's state estimation (SE) mechanism for generating large-scale energy outages or for manipulating power costs [2]. The most commonly popular kinds of cyber-attacks are denial of service (DoS), jamming, and false data injection (FDI) attacks. In FDI attack (FDIA) meter measurements are tampered with by adding malicious fake data [3, 4], in jamming attacks meter measurements are corrupted by adding additive noise [5], and DoS attacks prevent access of the system to meter measurements [6].

SGs are complex networks and failures or anomalies within them can result in severe damages to the entire system. A quick and efficient response to cyber-attacks depends on detecting them as soon as possible. As a result, detecting a change as quickly as possible [7, 8] can be extremely beneficial. When quickest change detection is being used, changes in the sensing environment happen at unexpected times, and it aims at detecting the changes as quickly as possible with a minimum of false alarms (FAs) using measurements collected gradually over time. Once the decision-makers have obtained measurements for a particular time interval, they either make a change or wait until the next period to acquire additional measurements. The detection speed will decrease when the optimum detection accuracy improves. Therefore, the stopping time, when a change is declared, should be set such that the detection speed and the accuracy are optimally balanced. As the pre-change state and the post-change state are hidden due to the uncertain change-point, a partially observable Markov decision process (POMDP) problem can be used to model the quickest change detection problem. In the case of online

attacks and anomalies in the SGs, in the pre-change condition, the system has been run within usual situations, and the pre-change metering pdf is defined very precisely utilizing the system model.

The control of unknown environments is effectively possible with reinforcement learning (RL) algorithms. In this case, RL is used to efficiently solve the POMDP problem. One solution implies either learning the model underlying POMDPs and then implementing the model-based RL method for POMDPs [9] or applying a model-free RL (MF-RL) algorithm [10–12] with no learning the model. Due to the computational burden of the model-based method and just an approximate model being able to be learned, using the MF-RL method is preferred.

Outlier detection methods like the Euclidean detector [13] or detector according to the cosine-similarity [14] were general since they need no attacking pattern. Basically, they are computing the dissimilation metric among genuine expected and meter measurements by using the Kalman filter (KF) and if the dissimilarity goes above a particular level, an attack/anomaly is declared. This type of detector, though, does not take into account the temporal relationship among attacked or anomalous measurements and makes decisions on a sample-by-sample basis. As a result, they cannot differentiate immediate great-stage random noise from persistent anomalies, such as those resulting from unfriendly interventions. Accordingly, robust universal attack detection methods are more required than outlier detection methods.

RL methods (single-agent RL) are used to develop a useful detection method in the present study, which is based on the perspective of the defender. It should be noted that the problem could also be viewed from the attacker's side, in which case the goal would be to find the best attack strategy to cause as much damage to the system as possible. An analysis of this kind of problem can be extremely useful in identifying the most severe damage an attacker could inflict on the system and then taking precautions accordingly. Many investigations employ RL to analyze vulnerability, such as for FDI attacks in ref [15] and for sequential topology attacks in ref [16]. It should be noted that the problem could be viewed simultaneously from the perspective of the defender and the perspective of the attacker as well, which can correspond to a game-theoretic setting.

It is the multifactorial RL architecture, which extends standalone RL to multiplex-factors, which includes game theory as agents' optimal policies are driven by their environment as well as the policies of their peers. The stochastic game also extends the Markov decision process to the multiplex-factor status in which the game can be consecutive and includes more than one state, and both the transition from one state to the next as well as the payoffs (reward/cost) are determined by the common functions of whole factors. The solution methods based on RL for stochastic games are studied in ref [17], ref [18]. The partially observable stochastic game is one in which the environment, the functions, and Payments from other factors are observed partially, making identifying solutions increasingly problematic generally.

The goal of this paper is to develop online cyber-attack detection (CAD) method based on MF-RL for POMDP. As the suggested algorithm does not rely on attack models, it is universal and shows a general but robust performance. Consequently, the suggested layout can be broadly used, and it is proactive in that it can detect novel attack types. By following an MF-RL method, the defenders learn by trial-and-error how observations translate into actions (*stop* or *continue*). Although the model can be used to produce observation data under normal operating conditions for the pre-change state, obtaining real attack data can be usually challenging in the training phase. Due to this, a robust detection strategy is adopted that trains the defender with a low-magnitude attack corresponding to the worst cases from the perspective of the defender as detecting these types of attacks are challenging. Once trained, the defenders can identify minor changes from normal meter measurements. The robust detection method also considerably reduces the action space in which an attacker can operate. In other words, in order to avoid detection, attackers could just use small magnitudes of the attack, which are not problematic because of the minimum impact on the grid. To the best of the authors;' knowledge, this is the first online CAD work in the SG that uses RL methods.

The model of the system and the SE method are described in Part 2. Part 3 describes the problem formulation and Part 4 proposes a solution. Part 5 demonstrates the effectiveness of the suggested RL-based detection method through a series of simulations. Part 6 concludes the study.

2. Model of the System and SE

2.1. Model of the System. If K meters exist in the system with $N+1$ buses, then there should be $K > N$ in order to ensure the required measurement redundancy versus noise [19]. Assume that one of the buses has been taken as the reference bus, and $\mathbf{x_t} = [x_{1,t}, \ldots, x_{N,t}]^T$ shows the system state at time t in which $x_{n,t}$ represents the phase angle at the time t at bus. $y_{k,t}$ shows the measurement taken at time t at meter k and $y_t = [y_{1,t}, \ldots, y_{K,t}]^T$ represents the measurement vector. The below state-space equations are used for modeling the SG according to the broadly applied linear DC model [19]:

$$\mathbf{x_t} = \mathbf{A}\mathbf{x_t} + \mathbf{v_t}, \tag{1}$$

$$y_t = \mathbf{H}\mathbf{x_t} + \mathbf{w_t}, \tag{2}$$

where the system (state transition) matrix is shown by $\mathbf{A} \in R^{N\times N}$, $\mathbf{H} \in R^{K\times N}$ represents the measurement matrix defined according to the topology of the network, the process noise vector is shown by $\mathbf{v_t} = [v_{1,t}, \ldots, v_{N,t}]^{\mathbf{T}}$, and the measurement noise vector is represented by $\mathbf{w_t} = [w_{1,t}, \ldots, w_{K,t}]^{\mathbf{T}}$. Considering $\mathbf{v_t}$ and $\mathbf{w_t}$ as independent additive white Gaussian random processes in which $\mathbf{v_t} \sim N(0, \sigma_v^2\mathbf{I_N})$,$\mathbf{w_t} \sim N(0, \sigma_w^2\mathbf{I_K})$,, and $\mathbf{I_K} \in R^{K\times K}$ shows an identity matrix. A further assumption is that the network is observable, in other words, the observability matrix has rank N.

$$0 \triangleq \begin{bmatrix} \mathbf{H} \\ \mathbf{HA} \\ \vdots \\ \mathbf{HA}^{\mathbf{N}-1} \end{bmatrix}. \tag{3}$$

Equations (1) and (2) give the system model of normal operation. When a cyber-attack occurs, though, the measurement model from equation (2) does not apply. As an example, in the case of a(n):

(a) The measurement model for an FDI attack launched at time τ is:

$$y_t = \mathbf{Hx_t} + \mathbf{w_t} + \mathbf{b_t}\|\{t \geq \tau\}. \tag{4}$$

Here, an indicator function is shown by $\|$ and the injected malicious data at time $t \geq \tau$ is represented by $\mathbf{b_t} \triangleq [b_{1,t}, \ldots, b_{K,t}]^T$ and the injected false data to the kth meter at time t is shown by. $b_{K,t}$,

(b) The measurement model for a jamming attack with additive noise is as follows:

$$y_t = \mathbf{Hx_t} + \mathbf{w_t} + \mathbf{u_t}\|\{t \geq \tau\}. \tag{5}$$

Here, the random noise realization at time $t \geq \tau$ is shown by $\mathbf{u_t} \triangleq [u_{1,t}, \ldots, u_{K,t}]^T$ and the jamming noise corrupting the kth meter at time t is represented by $u_{K,t}$.

(c) Under an FDIA/jamming hybrid attack [5], the meter measurement appear as follows:

$$y_t = \mathbf{Hx_t} + \mathbf{w_t} + (\mathbf{b_t} + \mathbf{u_t})\|\{t \geq \tau\}. \tag{6}$$

(d) When the system controller is under DOS attack, meter measurements cannot partially be available. Therefore, the measurement model is formulated accordingly:

$$y_t = \mathbf{D_t}(\mathbf{Hx_t} + \mathbf{w_t}). \tag{7}$$

Here, a diagonal matrix including 0s and 1s is shown by $\mathbf{D_t} = \mathrm{diag}(d_{1,t}, \ldots, d_{K,t})$. In particular, when $y_{k,t}$ exists, afterward, $d_{K,t} = 1$, or else $d_{K,t} = 0$. It should be noted that $\mathbf{D_t} = \mathbf{I_t}$ for $t < \tau$,

(e) During a system attack, the matrix of measurement alters. $\mathbf{H_t}$ represents the matrix of measurement subjected to topology attacks at time $t \geq \tau$, therefore:

$$y_t = \begin{cases} \mathbf{Hx_t} + \mathbf{w_t}, & \text{if } t < \tau, \\ \overline{H}\mathbf{x_t} + \mathbf{w_t}, & \text{if } t \geq \tau. \end{cases} \tag{8}$$

(f) In the case of a blended topology and FDIA/jamming hybrid attack, the measurement layout is:

$$y_t = \begin{cases} \mathbf{Hx_t} + \mathbf{w_t}, & \text{if } t < \tau, \\ \overline{H}\mathbf{x_t} + \mathbf{w_t} + \mathbf{b_t} + \mathbf{u_t}, & \text{if } t \geq \tau. \end{cases} \tag{9}$$

2.2. SE. As SG regulation relies on the SE system, SE has traditionally been done utilizing static least squares (LS) estimators [3]. As a result of the time-varying load and energy generation in SGs, they are actually very dynamic systems [20]. Additionally, adversaries can design and perform time-varying cyber-attacks. Therefore, dynamic system modeling like in equations (1) and (2) as well as the use of dynamic state estimators could be really beneficial in the development of real-time SG operations and security [4, 5].when the noise terms are Gaussian in a discrete-time linear dynamic system, the KF can be the best linear forecaster to minimize the average squared SE error [21]. $\hat{x}_{t|t'}$ represents the state estimates at time t in which $t' = t - 1$ is for the prediction step and $t' = t$ is for measurement update stage, the KF equations at time t is:

Prediction:

$$\begin{aligned} \hat{x}_{t|t-1} &= \mathbf{A}\hat{x}_{t-1|t-1}, \\ \mathbf{F}_{t|t-1} &= \mathbf{AF}_{t-1|t-1}\mathbf{A}^T + \boldsymbol{\sigma}_{\mathbf{v}}^2\mathbf{I_N}. \end{aligned} \tag{10}$$

Measurement update:

$$\begin{aligned} \mathbf{G_t} &= \mathbf{F}_{t|t-1}\mathbf{H}^T\left(\mathbf{HF}_{t|t-1}\mathbf{H}^T + \boldsymbol{\sigma}_{\mathbf{w}}^2\mathbf{I_K}\right)^{-1}, \\ \hat{x}_{t|t} &= \hat{x}_{t|t-1} + \mathbf{G_t}\left(y_t - \mathbf{H}\hat{x}_{t|t-1}\right), \\ \mathbf{F}_{t|t} &= \mathbf{F}_{t|t-1} - \mathbf{G_t}\mathbf{HF}_{t|t-1}. \end{aligned} \tag{11}$$

Here, $\mathbf{F}_{t|t-1}$ and $\mathbf{F}_{t|t}$ indicated the approximates of the state covariance matrix according to the measurements up to $t - 1$ and t, respectively. In addition, the Kalman gain matrix at time t is shown by $\mathbf{G_t}$.

Afterward, an illustrative example is used to illustrate the impact of cyber-attack on the SE method. In the IEEE-14 bus power system with $N = 13$, $K = 23$, and system parameters were selected as $A = I_N, \sigma_v^2 = 10^{-4}, and \sigma_w^2 = 2 \times 10^{-4}$ is tested with FDI attacks of various magnitudes/intensities, and the average squared SE error of the KF is analyzed. At time $\tau = 100$, attacks will be launched, which means that the system will be operated under normal conditions until time 100 and then under attack thereafter. There are three levels of attack magnitude:

Level1:
$b_{K,t} \sim u[-0.04, 0.04]$, $\forall k \in \{1, \ldots, K\}$and $\forall t \geq \tau$.
Level2:
$b_{K,t} \sim u[-0.07, 0.07]$, $\forall k \in \{1, \ldots, K\}$and $\forall t \geq \tau$.
Level3: $b_{K,t} \sim u[-0.1, 0.1]$, $\forall k \in \{1, \ldots, K\}$and $\forall t \geq \tau$.

Here, a uniform random variable between $[\zeta_1, \zeta_2]$ is shown by $U[\zeta_1, \zeta_2]$. When cyberattacks occur, the state estimates deviate from the real system states, and the deviation is enhanced by the attack magnitude.

3. Problem Formulation

The following is a description of the POMDP setting prior to introducing the problem formulation. When an agent and an environment are present, the seven-tuple $(S, A, T, R, O, G, \gamma)$

is used to define a discrete-time POMDP in which the group of latent conditions of the environment is shown by S, the group of agent's function is represented by A, the group of contingent transfer probabilities among the conditions is shown by T, R: $S \times A \longrightarrow R$ shows the reward function mapping the condition-function pairs to rewards, the group of agent's observations is shown by O, the set of conditional observation probabilities is indicated by G, and a discount factor is shown by $\gamma \in [0, 1]$ indicating how many current rewards have been preferred than subsequent rewards.

At every time t, the zone is in a certain latent condition $s_t \in S$. An observation $o_t \in O$ is obtained according to the present zone condition with the probability $G(o_t|s_t)$, the agent can take an action $a_t \in A$ and receive a reward $r_t = R(s_t, a_t)$ from the zone according to the function and the present condition of the area. In parallel, the zone can make the transmission to the subsequent condition $st + 1$ with the probability $T(s_{t+1}|s_t, a_t)$. Repetition of the procedure has been required till the final condition has been achieved. In the method, the factor aims at determining the best policy π: $O \longrightarrow A$, which can map observations to functions and maximize the anticipated factor overall discounted rewards, that is, $E[\sum_{t=0}^{\infty} \gamma^t r_t]$. The objective would be to reduce the expected overall discounted cost for an agent that gets costs rather than rewards from the environment. If the latter is taken into account, the POMDP problem is:

$$\min_{\pi:\, O \longrightarrow A} E\left[\sum_{t=0}^{\infty} \gamma^t r_t\right]. \tag{12}$$

Afterward, a POMDP setting is used to define the online CAD issue. The assumption is that at the unspecified time τ, the cyber-attacks have been started against the network, and it aims at detecting the attack soon once it has occurred, without knowing the attacker's capabilities or strategies. Here is the definition of the quickest change detection problem, which aims at minimizing the average detection delay and also the FA rate (FAR). It is possible to express the problem as a POMDP problem (according to Figure 1). There are two hidden states because of the unspecified launch time of the attack τ: *post-attack & pre-attack*. Every time $[t]$, the agent (defender) has two options following receiving the measurement vector $\mathbf{y_t}$: *stop* and express the attack or *go ahead* to make more measurements. When the action *stop* has been selected, the system can move into a *terminal* state and stay there permanently.

In order to reduce both FAs and detection delays, both FA and diagnosing delay occurrences must be accompanied by several costs. $c > 0$ is the relevant cost of the diagnosing delay in comparison with a FA. As a result, when the true basic condition is *pre-attack* and the action *stop* has been selected, there is a FA, and the defender can receive a cost of 1. However, when the underlying state is *post-attack* and the action *continue* has been selected, so the defender can receive a cost of c because of the detection delay. The remaining (hidden) state-action pairs are supposed to have zero costs. Furthermore, if the action *stop* has been selected, the defender does not achieve any more costs as long as staying in the *final* status. The defender aims at minimizing its expected

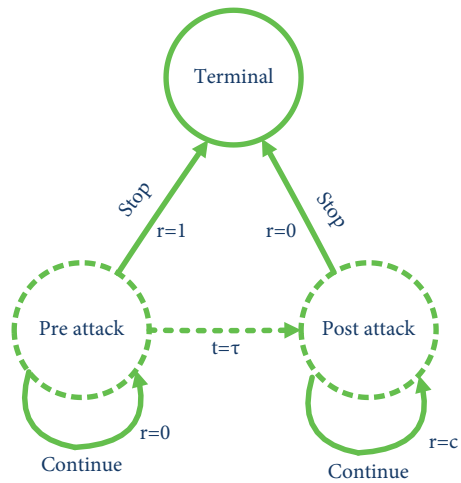


Figure 1: Diagram of state-machine to investigate POMDP adjustment.

overall cost by carefully selecting the functions. In particular, the defender must define the stopping time when an attack has been declared according to its observations.

The stopping time selected via the defender is shown by Γ. In addition, the probability measure is shown by P_k when the attack has been launched at time k, that is $\tau = k$, and the related expectation is shown by E_k. It should be noted that as the attacking strategies are unknown, P_k has been supposed to be unknown. The expected overall discounted cost is calculated for the proposed online CAD issue in the following way:

$$\begin{aligned} E\left[\sum_{t=0}^{\infty} \gamma^t r_t\right] &= E_\tau\left[\|\{t \geq \tau\} + \sum_{t=\tau}^{\Gamma} c\right] \\ &= E_\tau\left[\|\{t \geq \tau\} + c(\Gamma - \tau)^+\right] \\ &= P_\tau(\{\Gamma < \tau\}) + cE_\tau\left[(\Gamma - \tau)^+\right]. \end{aligned} \tag{13}$$

Here, $\gamma = 1$ has been selected as the current and subsequent costs have been weighted equally in the subject, $\{\Gamma < \tau\}$ shows the FA occurrence, which has been penalized with the cost of zero, and $E_\tau[(\Gamma - \tau)^+]$ shows the mean diagnosing lag in which every detection lag has been penalized with the cost of c and $(.)^+ = \max(., 0)$.

According to equations (12) and (13), the online attack detection problem is:

$$\min_{\Gamma} P_\tau(\{\Gamma < \tau\}) + cE_\tau\left[(\Gamma - \tau)^+\right]. \tag{14}$$

As c represents the relevant cost among the FA and the detection lag occurrences, the transaction curve among mean detection lag and FAR is determined via changing c and solving the related problem in equation (14). Furthermore, $c < 1$ is selected for avoiding frequent FAs.

The MF-RL method obtains a solution to equation (14) because the actual POMDP layout is uncertain because of the uncertain attack start time τ and attack strategy, and the RL algorithms have been proved to perform well under uncertain conditions. There is therefore a necessity to learn a direct mapping from observations to functions, that is, the time of stopping $[\Gamma]$.

Moreover, generally, similar observations can be obtained in both *pre-attack* & *post-attack* statuses. It is known as conceptual harmony and avoids well inferences about the underlying status from being made via just watching the observation one time. In addition, it should be noted that in the problem the decision to attack is only according to a single observation, which is equivalent to an outlier detection layout with better detectors that require no learning, refer to [13, 14]. The purpose of this research is to detect sudden and persistent attacks or anomalies caused by a hostile intervention in the system, instead of random disturbances caused by high-level system noise.

The measurements $\{y_t\}$ have been collected via intelligent meters and analysis to gain $o_t = f(\{y_t\})$. The defender observes $f(\{y_t\})$ at every time t and has decided on the CAD statement time $[\Gamma]$.

$f(\cdot)$ shows the function, which can processes a measurement's limit history and produce the observation signal, therefore, $o_t = f(\{y_t\})$ shows the observation signal at time t. Afterward, every time, the defender can observe $f(\{y_t\})$ and decide on the stopping time Γ, according to Figure 2. The defender aims at solving equation (14) via applying an RL algorithm. The following part describes this in more detail.

4. Solution Method

First, the methodology is explained for obtaining the observation signal $o_t = f(\{y_t\})$. The state estimates derived from the KF and the baseline measurement model in equation (2) are used to infer the meter measurements PDF in the pre-attack condition. Particularly, it is possible to estimate the measurements PDF within usual operating statuses according to the following:

$$y_t \sim \mathcal{N}\left(H\hat{x}_{t|t}, \sigma_w^2 I_K\right), \tag{15}$$

$L(y_t)$ is the likelihood of the measurement according to the estimation of base density:

$$\begin{aligned} L(y_t) &= \left(2\pi\sigma_w^2\right)^{(-K/2)} \exp\left(\frac{-1}{2\sigma_w^2}\left(y_t - H\hat{x}_{t|t}\right)^T\left(y_t - H\hat{x}_{t|t}\right)\right) \\ &= \left(2\pi\sigma_w^2\right)^{(-K/2)} \exp\left(\frac{-1}{2\sigma_w^2}\eta_t\right), \end{aligned} \tag{16}$$

where

$$\boldsymbol{\eta}_\mathbf{t} \triangleq \left(\mathbf{y_t} - \mathbf{H}\hat{\mathbf{x}}_{t|t}\right)^T\left(\mathbf{y_t} - \mathbf{H}\hat{\mathbf{x}}_{t|t}\right). \tag{17}$$

Within normal operating situations, it has been anticipated that $L(y_t)$ will be high. If η_t is small (near zero), the system is operating normally. The likelihood $L(y_t)$, however, is anticipated to drop in the cases where the systems deviate from normal operating conditions as a result of an attack or anomaly. When high η_t values persist over time, there may be an attack or anomaly present. As such, η_t might contribute to reducing the uncertainty of the fundamental status in some cases.

Figure 2: An explanation of the online CAD issue in the SG.

Due to the fact that η_t could have any positive amount, the observation area has been continued, making the mapping from every observation to function mathematically impossible. It is possible to decrease the computing burden for these continuous spaces by quantizing the observations. After partitioning the observation area into I disjoint and exclusive reciprocal distances utilizing $\beta_0 = 0 < \beta_1 < \cdots < \beta_I - 1 < \beta_I = \infty$ quantization thresholds, the observation at time t will be described as θ_i if $\beta_{i-1} \le \eta_t < \beta_i$, $i \in 1, \ldots, I$ is met. Next, $\theta_1, \ldots, \theta_I$ indicate possible observations for any particular moment. θ_i's represent the quantization levels; therefore, every θ_i has to have a diverse value.

Moreover, as discussed previously, even though η_t can be used for inferring the underlying state at time T, similar observations can be obtained in the *pre-attack* & *post-attack* statuses. Therefore, a finite history of observations is proposed. M is the sliding observation window (SOW) size, therefore, there are I^M feasible observation windows that exist and the sliding window at time $[t]$ includes the quantized versions of $\{\eta_j\colon t - M + 1 \le j \le t\}$. An observation o is, therefore, a window, meaning that an observation space O includes all possible windows. As an example, when $I = M = 2$, afterward, $O = \{[\theta_1, \theta_1], [\theta_1, \theta_2], [\theta_2, \theta_1], [\theta_2, \theta_2]\}$.

RL algorithm is used for learning a $Q(o, a)$ value, that is, the expected future cost for every observation-action pair (o, a), in which all $Q(o, a)$ values have been saved in the Q-table of size $I^M \times 2$. Following the Q-table's learning, the defender's policy is to choose the function a with the minimal $Q(o, a)$ for every observation o. Generally, as I and M increase the learning efficiency enhances and simultaneously causes in a bigger Q table requiring to enhance in the training episodes number and therefore the calculation burden of the learning step. Therefore, I and M must be selected regarding the anticipated exchange among efficiency and calculation burden.

The learning step and online CAD step are included in the suggested RL-based detection method. SARSA, which is a MF-RL control layout [22], performed better than the model-free POMDP settings [12]. The SARSA algorithm is used in order to train the defender on numerous episodes of experience, and the defender learns a Q-table during the learning phase. According to Figure 3, the simulation environment has been produced for training during which the defender has taken an action according to its observations and received a cost from the simulation in return. On the basis of this experience, a Q-table is updated and learned by the defender. Afterward, according to the observations, in the online CAD stage, the previously learned Q-table is used to choose the action with the minimum anticipated future cost (Q amount) every time. Once the defender selects the action *stop*, the online detection phase ends. An attack has been declared when the *stop* has been selected, and the procedure has been stopped.

In the event of an attack declaration, the online detection phase may be restarted any time the system has recovered and is back to normal operating conditions. After a defender has been trained, additional training is not required.

Every iteration of RL (learning episode) involves repeating the same actions. An RL algorithm's time complexity would then be regarded as a single iteration's time complexity [23]. SARSA updates the Q-table one at the time, and the maximum learning episode time is T, so the time complexity is $O(T)$. Furthermore, $O(TE)$ shows the total complexity of the learning process, since E indicates the number of learning episodes. It should be noted that the space of action and observation does not affect the time complexity. Increasing I or/and M, in contrast, requires learning a more complex Q-table, for which one needs to enhance E. Additionally, the space complexity (memory cost) is $M + 2I^M$ since the SOW is M and the Q-table is $I^M \times 2$. It should be noted that space complexity remains constant through time. With an SG model and several attack models, the measurement data is obtained online throughout the learning process and the defender has been trained using the observed data streams. Due to this, storing enormous amounts of training data for the learning phase is not necessary since the size of SOW (M) has been saved at every stop.

A distributed SG system is implemented using the suggested solution layout, in which learning and CAD tasks have been handled at a single center while meter measurements have been collected on a distributed basis. This setup is shortly described below.

(i) SGs have multiple local control centers as well as a global control center in the large-scale monitoring model. Local centers collect and process measurements from smart meters in their neighborhoods, and they communicate with global centers as well as neighboring local centers.

(ii) A distributed KF, such as the one developed for large-scale SGs in [4] is used to estimate the system state.

(iii) In the measurement matrix, $h_k^T \in R^N$ is the kth row, that is, $H^T = [h_1, \ldots, h_k]$. A negative log-scaled likelihood estimate, η_t, is given by the following (refer to equation (17)):

$$\eta_t = \sum_{k=1}^{K} \left(y_{k,t} - h_k^T \hat{x}_{t|t} \right)^2. \tag{18}$$

The local centers have the capability of estimating the system state via utilizing the distributed KF for every time t. Afterward, the local centers could calculate the term $(y_{k,t} - h_k^T \hat{x}_{t|t})^2$ for their neighborhood meters. R shows the local centers number and S_r denotes the group of meters in the neighbors of the rth local center. Therefore, η_t in equation (18) is:

$$\eta_t = \sum_{r=1}^{R} \sum_{k \in S_r} \left(y_{k,t} - h_k^T \hat{x}_{t|t} \right)^2 = \sum_{r=1}^{R} \eta_{t,r}. \tag{19}$$

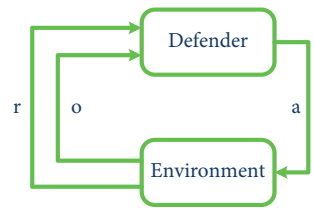


Figure 3: Interaction between the environment and defender within the learning procedure.

(i) A distributed implementation allows every local center to calculate $\eta_{t,r}$ and send it to the global center for summing $\{\eta_{t,r}, r = 1, 2, \ldots, R\}$ and calculating η_t,

(ii) Learning and detection tasks have been carried out at the global center on the same basis as previously described.

5. Simulation Outcomes

5.1. Simulation Setup and Parameters. The IEEE-14 bus electrical network with $[N + 1 = 14]$ buses and $[K = 23]$ intelligent meters is used to perform the simulation. In MATPOWER [24], the DC optimal power flow algorithm is used to determine the initial state variables (phase angles). System matrix A has been selected as the measurement and identification matrixes H based on the IEEE-14 electrical grid. $\sigma_v^2 = 10^{-4}$ and $\sigma_w^2 = 2 \times 10^{-4}$ have been selected as the noise variances for the usual operation of the system. As part of the suggested online CAD layout on the basis of RL, $I = 4$ quantization levels are selected and thresholds $\beta_1 = 0.95 \times 10^{-2}$, $\beta_2 = 1.05 \times 10^{-2}$, and $\beta_3 = 1.15 \times 10^{-2}$ are selected using an offline simulation based on monitoring $\{\eta_t\}$ throughout normal operation. The observation window includes 4 entries, thus $M = 4$. Additionally, $\alpha = 0.1$ and $\epsilon = 0.1$ have been selected as the learning parameters, and $T = 200$ has been selected as the episode length. During the learning stage, the defender has been first trained more than 4×10^5 episodes with the attack start time off $\tau = 100$ and next, more than 4×10^5 episodes with $\tau = 1$ for ensuring that the defender can properly explore the observation space within usual operating situations and also during an attack. As a learning episode ends when the action *stop* has been selected and observations are available to the defender just for $\geq \tau$, $\tau = 1$ has been selected during the half of the learning episodes to ensure that the defender has been adequately trained within the post-attack regime.

The suggested algorithm has been trained for both $c = 0.02$ and $c = 0.2$, for illustrating the trade-off between mean CAD lag and FA probability. It is necessary to train defenders with very low-magnitude attacks associated with small deviations from the baseline in order to achieve a detector, which can be robust and useful versus tiny deviations from the usual exploitation of the system. Several known low-magnitude attack kinds have been applied in this case. One-half of the learning episodes use random FDIAs with attack extents equal to uniform random realization parameter $\pm U[0.02, 0.06]$, i.e., $b_{k,t} \sim U[0.02, 0.06]$ is the injected false data to the kth meter at time time $t \geq \tau$,

$\forall k \in \{1, \ldots, K\}$. The other ones use random hybrid FDI/jamming attacks with $b_{k,t} \sim U[0.02, 0.06]$, $u_{k,t} \sim N(0, \sigma_{k,t})$, and $\sigma_{k,t} \sim U[2 \times 10^{-4}, 4 \times 10^{-4}]$, $\forall k \in \{1, \ldots, K\}$ and $\forall t \geq \tau$. The overall training time costs have been computed about as [5018sec] and [5106sec] for $c = 0.2$ and $c = 0.02$, respectively.

5.2. Efficiency Assessment. This part evaluates the efficiency of the suggested CAD method on the basis of RL and compares it with several current detector methods [25]. First, E∞ [_] is reported as the mean FA cycle of the suggested CAD method, that is, the 1th time on the mean the suggested detector has given an alarm, however, no anomaly/attack occurs at a whole ($\tau = \infty$). The mean FA period for $c = 0.2$ is about $E_\infty[\Gamma] = 9.4696 \times 10^5$ and it is about $E_\infty[\Gamma] = 7.921 \times 10^6$ for $c = 0.02$. It is anticipated that the FAR of the suggested detector decrease by increasing the relevant cost of the FA occurrence, $1/c$.

According to the optimization problem in equation (14), the efficiency factors include the probability of FA, that is, $P_\tau(\{\Gamma < \tau\})$, and the average detection delay, that is, $E_\tau[(\Gamma - \tau)^+]$. It should be noted that the unknown attack launch time τ affects both efficiency factors. Therefore, generally, the efficiency factors must be computed for every possible τ. To illustrate efficiency, τ as the numeral random parameter is selected with variable ρ so, $P(\tau = k) = \rho(1-\rho)^{k-1}, k = 1, 2, 3, \ldots$ in which $\rho \sim U[10^{-4}, 10^{-3}]$ shows a uniform random variable.

Monte Carlo simulations over 10000 trials are used to calculate the average detection delay and the probability of FA of the suggested detector, the Euclidean detector [13], and the cosine-similarity factor on the basis of the detector [14]. The thresholds of the benchmark tests are changed as well as c for the suggested algorithm is changed in order to determine the efficiency curves. $c = 0.02$ and $c = 0.2$. I are used for evaluating the suggested algorithm [26]. In addition, the F-score, recall, and precision for whole simulation scenarios are reported. The bound as ten-time units is selected. Afterward, the F-score, recall, and precision out of 1×10^4 tests are calculated in the following way:

$$\text{Precision} = \frac{\#\text{trials}(\tau \leq \Gamma \leq \tau + 10)}{\#\text{trials}(\tau \leq \Gamma \leq \tau + 10) + \#\text{trials}(\Gamma < \tau)},$$

$$\text{Recall} = \frac{\#\text{trials}(\tau \leq \Gamma \leq \tau + 10)}{\#\text{trials}(\tau \leq \Gamma \leq \tau + 10) + \#\text{trials}(\Gamma < \tau + 10)}, \quad (20)$$

$$F - \text{score} = 2\frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}.$$

Here, "# trials" shows "the number of tests with." The suggested and the benchmark detectors are evaluated within the below attack case studies:

(1) First, the detectors versus the random FDIA are evaluated in which $b_{k,t} \sim U[-0.07, 0.07]$, $\forall k \in \{1, \ldots, K\}$ and $\forall t \geq \tau$. Figure 4 shows the related tradeoff curves.

(2) Second, the detectors versus a structured FDI attack are evaluated [3], in which the injected data b_t is located on the column space of the measurement matrix H. $b_t = Hg_t$ is selected in which $g_t \triangleq [g_{1,t}, \cdots, g_{N,t}]^T$ and $g_{n,t} \sim U[0.08, 0.12]$, $\forall n \in \{1, \ldots, N\}$ and $\forall t \geq \tau$. Figure 5 shows the related efficiency curves.

(3) Afterward, the detectors are evaluated when the jamming attack occurs with zero-mean AWGN in which $u_{k,t} \sim N(0, \sigma_{k,t})$ and $\sigma_{k,t} \sim u(10^{-3}, 2e-3)$, $\forall k \in \{1, \ldots, K\}$ and $\forall t \geq \tau$. Figure 6 shows the related tradeoff curves. 4) The detectors are evaluated when a jamming attack occurs with jamming noise related over the meters in which $u_t \sim N(0, U_t), U_t = \sum_t \Sigma_t^T$, and Σ_t shows a random Gaussian matrix with its entry at the ith row and the jth column can be $\sum_{t,i,j} \sim N(0, 8 \times 10^{-5}$. Figure 7 shows the related efficiency curves.

(4) In addition, the detectors are evaluated in the case of the hybrid FDIA or jamming attack in which $b_{k,t} \sim U[-5, 5] \times 10^{-2}$, $u_{k,t} \sim N(0, \sigma_{k,t})$, and $\sigma_{k,t} \sim U[5 \times 10^{-4}, 10^{-3}]$,$\forall k \in \{1, \ldots, K\}$ and $\forall t \geq \tau$. Figure 8 shows the related tradeoff curves.

(5) Next, the detectors are evaluated when a random DoS attack occurs in which the measurement of every smart meter is not available for the controller at every time with probability of 0.2. It means that for every meter k, $d_{k,t}$ can be zero with probability $2e-1$ and one with probability $8e-1$ at every time $t \geq \tau$. Figure 9 shows the efficiency curves versus the DoS attack.

(6) In addition, a network topology attack is considered in which the lines among the buses (9, 10) and (12, 13) break down. So, the measurement matrix. H_t for $t \geq \tau$ has been obtained. Figure 10 shows the related tradeoff curves.

(7) Finally, a combined technique and hybrid FDIA or jamming attack are considered, in which the lines among buses 9–10 and 12–13 break down for $t \geq \tau$ and so, $b_{k,t} \sim U[-0.05, 0.05], u_{k,t} \sim N(0, \sigma_{k,t})$, and $\sigma_{k,t} \sim U[5 \times 10^{-4}, 10^{-3}], \forall k \in \{1, \ldots, K\}$ and $\forall t \geq \tau$. Figure 11 shows the related efficiency curves.

The F-score, recall, and precision for the suggested detector on the basis of RL for $c = 2e-1$ and $c = 2e-2$ are summarized in Table 1 and 2, respectively versus whole the proposed simulation case studies earlier. In addition, in the case of the random FDI attack, the precision against recall curves for the suggested and benchmark detectors is illustrated Figure 12. Because meter measurements are not partially available in DoS attacks, therefore, the system significantly strays from the usual operation, whole detectors are capable of detecting DoS attacks with nearly zero mean detection lags (refer to Figure 9).

Eventually, the impact of the window size, M, is evaluated on the efficiency of the detector on the basis of RL (trained for $c = 2e-1$) versus random FDIAs with changing

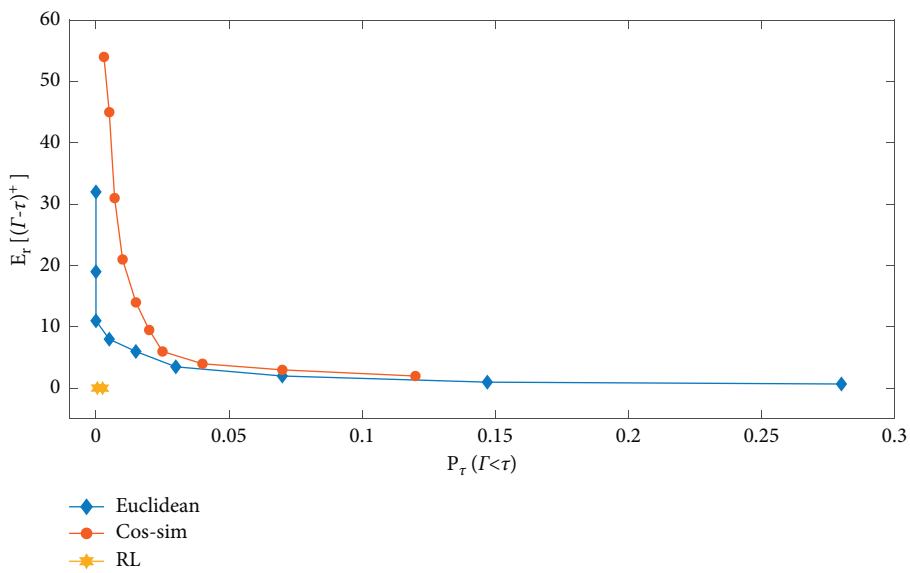


Figure 4: Mean CAD lag versus probability of FA curves for the suggested method and the benchmark trails in case of the random FDIA.

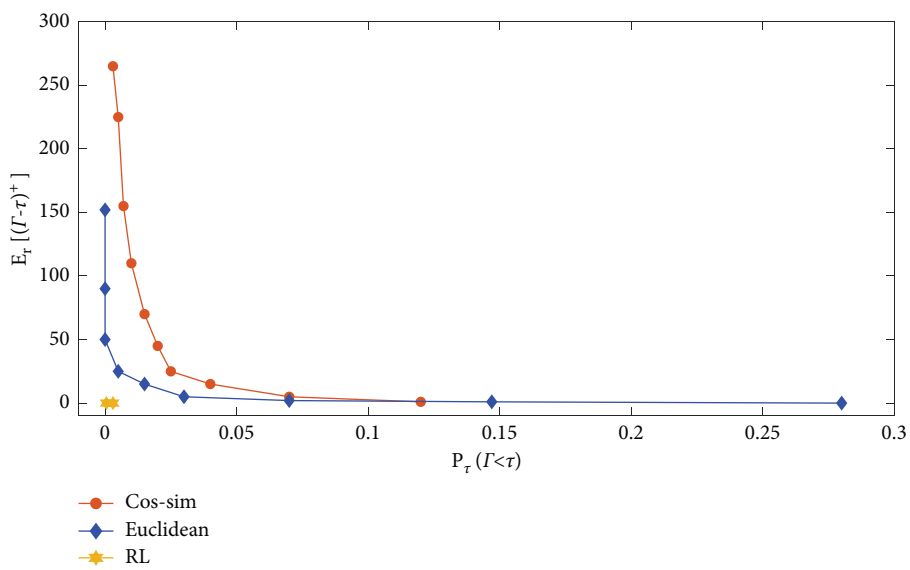


Figure 5: Proficiency curves for the suggested method and the benchmark trails in the case of the structured FDIA.

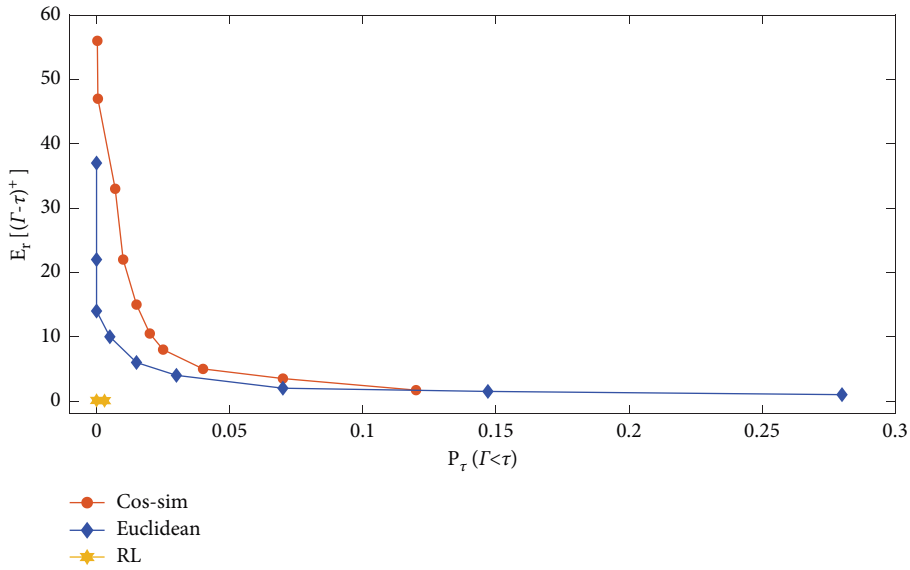


Figure 6: Proficiency curves for the suggested method and the benchmark trails in case of the jamming attack with AWGN.

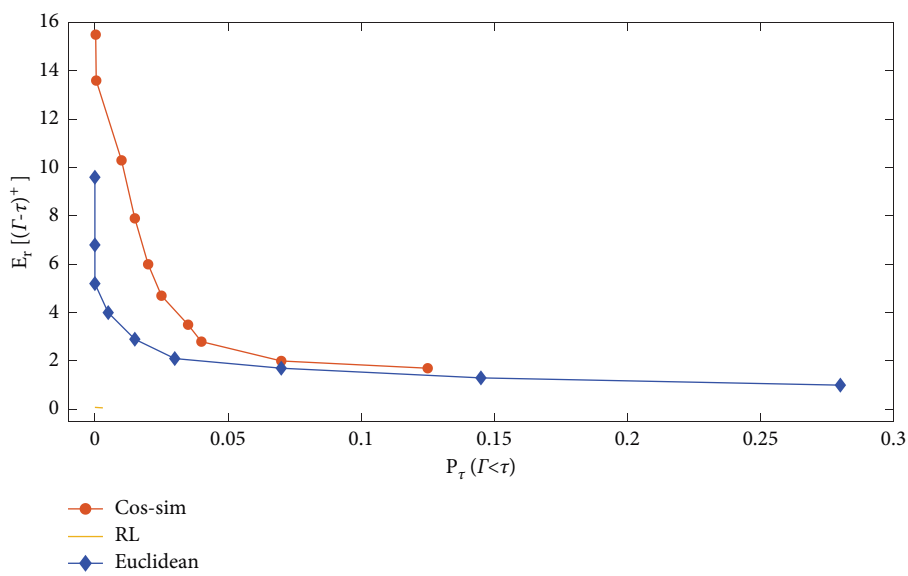


Figure 7: Proficiency curves for the suggested method and the benchmark trails in case of a jamming attack with jamming noise associated with the area.

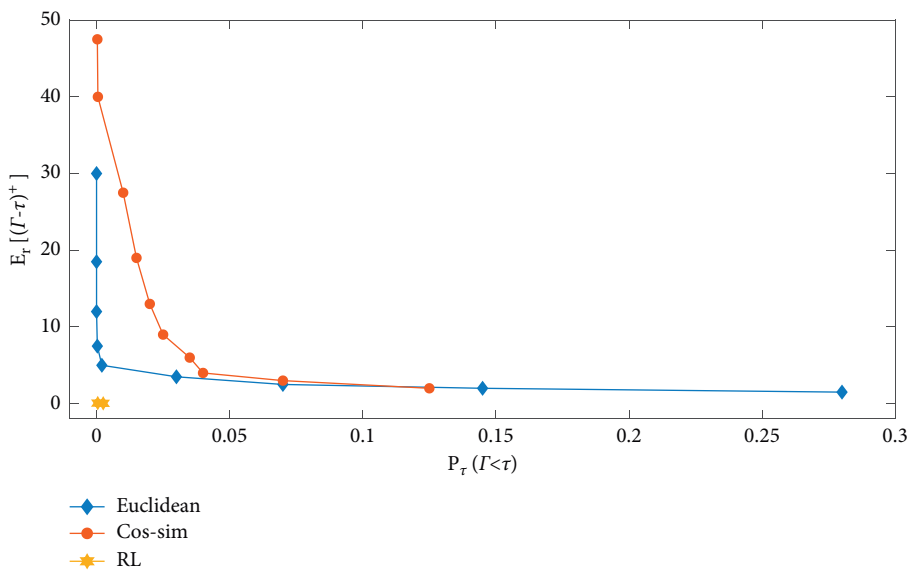


Figure 8: Proficiency curves for the suggested method and the benchmark trails in case of a hybrid FDI/jamming attack.

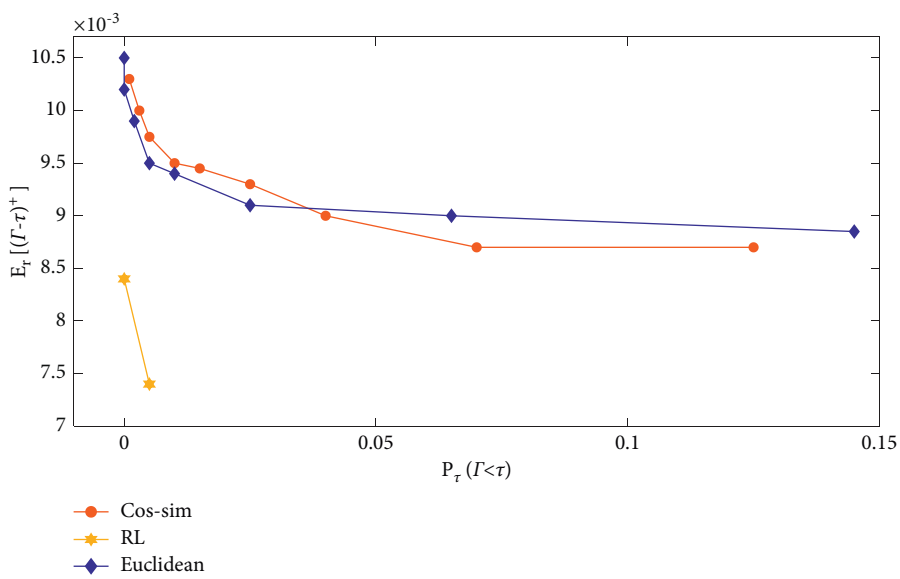


Figure 9: Efficiency curves for the suggested method and the benchmark trails when the DoS attack occurs.

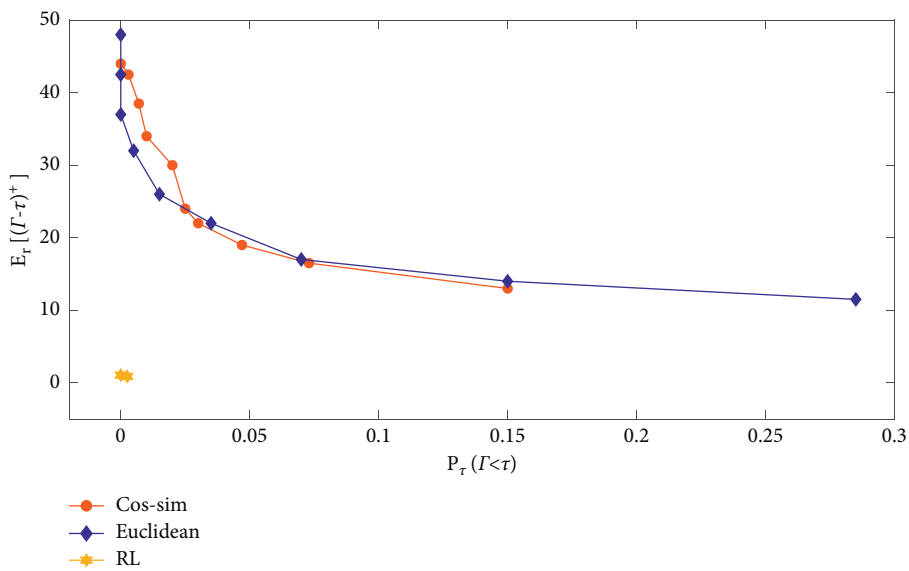


Figure 10: Efficiency curves for the suggested method and the benchmark trails under the network topology CAD.

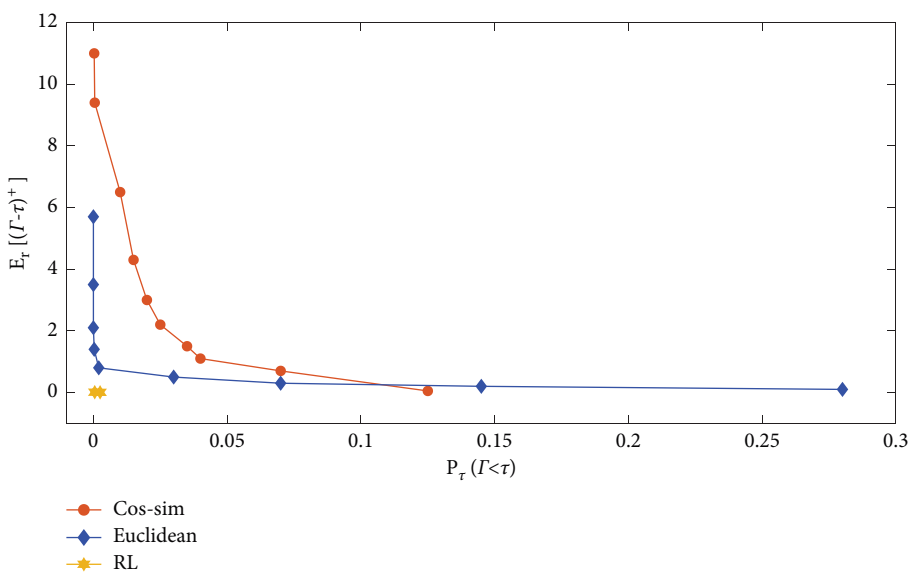


Figure 11: Efficiency curves for the suggested method and the benchmark trails under a mixed system topology and hybrid FDIA or jamming attack.

Table 1: *F*-score, recall, and precision for the suggested detection method ($c = 0.2$) in different kinds of cyber-attacks.

Measure	*F*-score	Recall	Precision
Structured FDI	0.9860	0.9755	0.9967
Corr. Jamm	0.9983	1	0.9967
DOS	0.9987	1	
Jamming	0.9986	1	0.9974
Hybrid	0.9985	1	0.9972
FDI	0.9987	1	0.9976
Topology	0.9889	0.9807	0.9971
Mixes	0.9985	1	0.9972

Table 2: F-score, recall, and precision for the suggested detection method (c = 0.02) in different kinds of cyber-attacks.

Measure	*F*-score	Recall	Precision
Structured FDI	0.9712	0.9448	0.9992
Corr. Jamm	0.9998	1	0.9997
DOS	0.9996	1	0.9994
Jamming	0.9996	1	0.9993
Hybrid	0.9997	1	0.9996
FDI	0.9998	1	0.9997
Topology	0.9890	0.9784	0.9998
Mixes	0.9996	1	0.9994

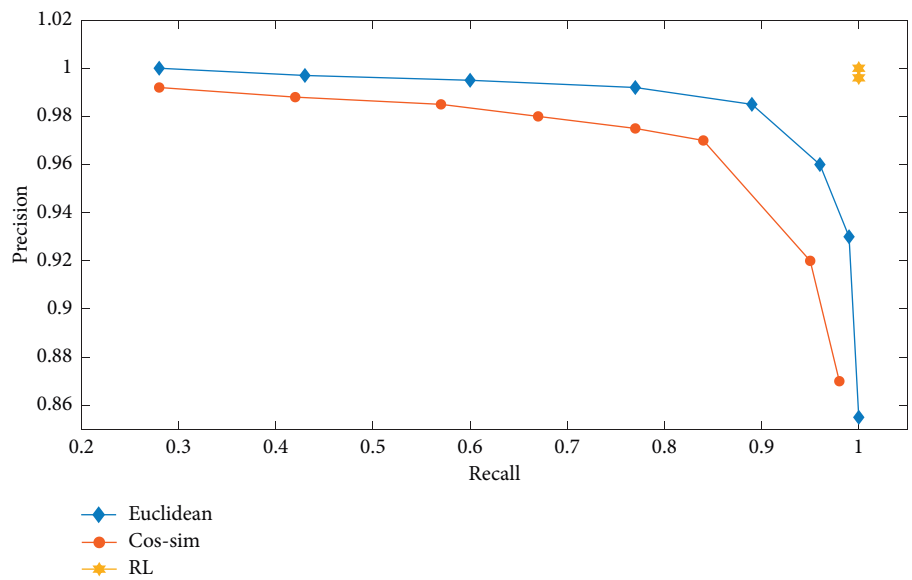


Figure 12: Precision, recall for the suggested and the benchmark CAD methods versus the random FDIA.

Table 3: The window size effect (M) on the efficiency of the detector on the basis of RL for $c = 2e - 1$ within random FDIA with diverse amount stages every entrance in the table displays the outcomes according to the following expression: $P_\tau(\{\Gamma < \tau\})/E_\tau[(\Gamma - \tau)^+]/F$-score/recall/precision.

Measure	M			
	1	2	4	6
$\varphi = 0.03$	0.0187/8.4208/0.7119/0.8226	0.0021/15.9532/0.9957/0.4872/0.6543	0.0021/14.8548/0.9959/0.5077/0.6725	0.0021/14.2506/0.996/0.6841
$\varphi = 0.04$	0.0187/1.2219/0.9813/0.9995/0.9903	0.0021/1.9046/0.9979/0.9923/0.9951	0.0021/1.8437/0.9979/0.9943/0.9961	0.0021/1.8207/0.9979/0.9955/0.9967
$\varphi = 0.05$	0.0187/0.2606/0.9813/1/0.9906	0.0021/0.4049/0.9979/1/0.9989	0.0021/0.4016/0.9979/1/0.9989	0.0021/0.4016/0.9979/1/0.9989

extents. Table 3 shows the outcomes for $M = 1, M = 2, M = 4$, and $M = 6$ in which $b_{k,t} \sim U[-\varphi, \varphi]$, $\forall k \in \{1, \ldots, K\}$, $\forall t \geq \tau$ and φ has the amounts of [3, 4, and 5] $\times 10^{-2}$.

6. Conclusion

The present study formulates an online CAD structure as the POMDP subject and proposes a solution on the basis of MF-RL for POMDPs. In the numerical tests, the suggested detection layout proves to be efficient, reliable, and quick in CADs that target the SG. In addition, RL algorithms have been shown to have a strong potential for solving difficult cyber-security problems. It is possible to greatly improve the algorithm suggested in this study by utilizing additional enhanced techniques. This study is concluded by considering a single-agent RL setting to optimize the defender's policy, such that the attacking methods, like the attack kinds, magnitudes, set of attack meters, and so on, do not affect the defender's optimal policy. The optimal policy for the defender after launching an attack is to *stop* and declare an attack.

Data Availability

All data are available in the paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Science and technology project support of the China Southern Power Grid Corporation (No. GDKJXM20210170 (036100KK52210070)).

References

[1] O. Lukačević, A. Almalaq, K. Alqunun et al., "Optimal CONOPT solver-based coordination of bi-directional converters and energy storage systems for regulation of active and reactive power injection in modern power networks," *Ain Shams Engineering Journal*, vol. 13, no. 6, Article ID 101803, 2022.

[2] Y. Li, B. Wang, H. Wang et al., "Importance assessment of communication equipment in cyber-physical coupled distribution network based on dynamic node failure mechanism," *Frontiers in Energy Research*, p. 654, 2022.

[3] M. Dehghani, T. Niknam, M. Ghiasi, P. Siano, H. Haes Alhelou, and A. Al-Hinai, "Fourier singular values-based false data injection attack detection in AC smart-grids," *Applied Sciences*, vol. 11, no. 12, p. 5706, 2021.

[4] J. Chen, M. A. Mohamed, U. Dampage et al., "A multi-layer security scheme for mitigating smart grid vulnerability against faults and cyber-attacks," *Applied Sciences*, vol. 11, no. 21, p. 9972, 2021.

[5] K. Alnowibet, A. Annuk, U. Dampage, and M. A. Mohamed, "Effective energy management via false data detection scheme for the interconnected smart energy hub–microgrid system under stochastic framework," *Sustainability*, vol. 13, no. 21, Article ID 11836, 2021.

[6] W. Xu, J. Li, M. Dehghani, and M. GhasemiGarpachi, "Blockchain-based secure energy policy and management of renewable-based smart microgrids," *Sustainable Cities and Society*, vol. 72, Article ID 103010, 2021.

[7] G. Rovatsos, G. V. Moustakides, and V. V. Veeravalli, "Quickest detection of moving anomalies in sensor networks," *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 2, pp. 762–773, 2021.

[8] U. Bermejo, A. Almeida, A. Bilbao-Jayo, and G. Azkune, "Embedding-based real-time change point detection with application to activity segmentation in smart home time series data," *Expert Systems with Applications*, vol. 185, Article ID 115641, 2021.

[9] B. Wu and Y. Feng, "Policy reuse for learning and planning in partially observable Markov decision processes," in *Proceedings of the 2017 4th International Conference on Information Science and Control Engineering (ICISCE)*, pp. 549–552, IEEE, Bejing China, 2017 July.

[10] T. P. Le, N. A. Vien, and T. Chung, "A deep hierarchical reinforcement learning algorithm in partially observable Markov decision processes," *IEEE Access*, vol. 6, pp. 49089–49102, 2018.

[11] M. Igl, L. Zintgraf, T. A. Le, F. Wood, and S. Whiteson, "Deep variational reinforcement learning for POMDPs," *InInternational Conference on Machine Learning*, vol. 3, pp. 2117–2126, 2018.

[12] J. Zhang, L. Tai, M. Liu, J. Boedecker, and W. Burgard, "Neural slam: learning to explore with external memory," 2017, https://arxiv.org/abs/1706.09520.

[13] M. Khalaf, A. Youssef, and E. El-Saadany, "Detection of false data injection in automatic generation control systems using kalman filter," in *Proceedings of the 2017 IEEE Electrical Power and Energy Conference (EPEC)*, pp. 1–6, IEEE, Saskatoon, Canada, 2017 October.

[14] X. Niu, J. Li, J. Sun, and K. Tomsovic, "Dynamic detection of false data injection attack in smart grid using deep learning," in *Proceedings of the 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pp. 1–6, IEEE, Washington, DC, USA, 2019 February.

[15] A. Almalaq, S. Albadran, and M. A. Mohamed, "Deep machine learning model-based cyber-attacks detection in smart power systems," *Mathematics*, vol. 10, p. 2574, 2022.

[16] H. Jiang, Z. Wang, and H. He, "An evolutionary computation approach for smart grid cascading failure vulnerability analysis," in *Proceedings of the2019 IEEE Symposium Series on Computational Intelligence (SSCI)*, pp. 332–338, IEEE, Xiamen, China, 2019 December.

[17] C. Xu, S. Liu, C. Zhang, Y. Huang, Z. Lu, and L. Yang, "Multi-agent reinforcement learning based distributed transmission in collaborative cloud-edge systems," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1658–1672, 2021.

[18] A. Marinescu, I. Dusparic, and S. Clarke, "Prediction-based multi-agent reinforcement learning in inherently non-stationary environments," *ACM Transactions on Autonomous and Adaptive Systems*, vol. 12, no. 2, pp. 1–23, 2017.

[19] J. Zhao, J. Qi, Z. Huang et al., "Power system dynamic state estimation: motivations, definitions, methodologies, and future work," *IEEE Transactions on Power Systems*, vol. 34, no. 4, pp. 3188–3198, 2019.

[20] M. Dehghani, M. Ghiasi, T. Niknam et al., "Cyber-attack detection based on wavelet singular entropy in AC smart islands: false data injection attack," *IEEE Access*, vol. 9, pp. 16488–16507, 2021.

[21] M. J. Grimble, "Polynomial systems approach to optimal linear filtering and prediction," *International Journal of Control*, vol. 41, no. 6, pp. 1545–1564, 1985.

[22] P. R. Montague, "Reinforcement learning: an introduction, by sutton, RS and barto, AG," *Trends in Cognitive Sciences*, vol. 3, no. 9, p. 360, 1999.

[23] K. Cobbe, O. Klimov, C. Hesse, T. Kim, and J. Schulman, "Quantifying generalization in reinforcement learning," 2019, https://arxiv.org/abs/1812.02341.

[24] S. Chen, Z. Wei, G. Sun, D. Wang, and H. Zang, "Steady state and transient simulation for electricity-gas integrated energy systems by using convex optimisation," *IET Generation, Transmission & Distribution*, vol. 12, no. 9, pp. 2199–2206, 2018.

[25] A. Almalaq, S. Albadran, A. Alghadhban, T. Jin, and M. A. Mohamed, "An effective hybrid-energy framework for grid vulnerability alleviation under cyber-stealthy intrusions," *Mathematics*, vol. 10, p. 2510, 2022.

[26] M. Ćalasan, A. F. Zobaa, H. M. Hasanien, S. H. Abdel Aleem, and Z. M. Ali, "Towards accurate calculation of supercapacitor electrical variables in constant power applications using new analytical closed-form expressions," *Journal of Energy Storage*, vol. 42, Article ID 102998, 2021.

Hindawi
International Transactions on Electrical Energy Systems
Volume 2022, Article ID 5820126, 13 pages
https://doi.org/10.1155/2022/5820126

Research Article

An Effective Node-To-Edge Interdependent Network and Vulnerability Analysis for Digital Coupled Power Grids

Yifan Li,[1] Bo Wang,[1] Hongxia Wang,[1] Fuqi Ma,[1] Hengrui Ma,[2] Jiaxin Zhang,[1] Yingchen Zhang,[1] and Mohamed A. Mohamed[3]

[1]*School of Electrical and Automation, Wuhan University, Wuhan, Hubei 430072, China*
[2]*Tus-Institute for Renewable Energy, Qinghai University, Xining, Qinghai 810016, China*
[3]*Electrical Engineering Department, Faculty of Engineering, Minia University, Minia 61519, Egypt*

Correspondence should be addressed to Bo Wang; whwdw@whu.edu.cn

Received 25 July 2022; Revised 20 August 2022; Accepted 23 August 2022; Published 29 September 2022

Academic Editor: Martin Calasan

With the deep coupling between the cyber side and the physical side of power systems, the failure of any link of both sides may lead to power outages, so it is necessary to analyze their vulnerability and vulnerable links for targeted improvement of systems. By dynamically attacking the coupled network nodes, this paper proposes a multilevel model and node-to-edge cyber-physical power system and the corresponding indexes system to analyze the vulnerability of the coupled power grid and its key components. The results showed that in the order of the indexes proposed in this paper, attacking surviving power nodes and cyber nodes results in a network crash rate of 25.0% and 66.7% faster than that in the order of "betweenness" and that attacking surviving cyber nodes results in a network crash rate of 89.4% faster than that in the order of "degree." In terms of attacking power nodes, the index proposed in this paper has the same rate as "degree." Therefore, the proposed model can better describe the vulnerability of the power grid to withstand attacks.

1. Introduction

With the digital transformation of modern power systems, the number of sensors of power systems, intelligent terminals, and decision-making units of information systems has surged [1]. A growing amount of external information directly or indirectly affects the power system through various business channels, bringing convenience to the power system [2]. However, physical power systems and electrical power communication networks (EPCN) are deeply coupled to form the cyber-physical power systems (CPPS) [3, 4], which makes it more likely to form interactive chain faults and further expand the scale of power accidents [5, 6]. For instance, blackouts in Ukraine in 2015 and Venezuela in 2019, both linked to cyber-attacks, caused huge loses to the national economy [7, 8]. The deep coupling between the cyber side and the physical side of power systems leads to the superposition of structural vulnerability and increases the possibility of expanding the fault range. Therefore, to maintain the security and stability of the power system, it is necessary to identify the vulnerable and critical components or devices and master the system structure vulnerability so as to carry out targeted and differentiated maintenance of complex and diverse devices and improve the system stability.

Related studies about vulnerability evaluation of CPPS are primarily based on two kinds of modeling, cosimulation [9–12] and complex networks [13–18].

The advantages of cosimulation lie in clear physical meaning and accurate calculation results. The authors in Ref. [9] developed a WAMS cyber-physical testbed using a real-time digital simulator with hardware-in-the-loop simulation integrating hardware, software, and wide area measurement systems components and protocols. In Ref. [10], the authors proposed a state-caching-based synchronization mechanism to balance accuracy and efficiency. In Ref. [11], a virtualized cyber-physical testbed was developed using real industrial communication protocols. A joint simulation platform of

cyber physical systems based on RT-LAB, OPENT, and control platform has been developed in Ref. [12]. It follows that cosimulation requires fine interface construction, and it has a limitation of high cost in platform construction, which demands the combination of hardware, software, and communication protocol.

Complex network focus on the most intuitive physical properties of networks. For power systems, the theory of complex networks is a proper tool to identify the robustness of the existing architecture from a long-term planning perspective and has better adaptability. From the perspective of model granularity, this paper introduces the modeling of CPPS by complex networks into two aspects: plant-level networks and device-level networks as follows:

In plant-level networks, a complex network model regards the power plant, substation, control center, and other plant stations as the basic nodes, which can analyze the network topology vulnerability of a large power grid with high computational efficiency. The authors in Ref. [13] came up with a flexible framework to analyze cascading effects in CPPS, with buses represented as nodes and lines represented as edges of a graph. Li et al. [14] took the substation and the dispatching terminal as the communication nodes. In Ref. [15], the authors proposed a heterogeneous interdependent network model in which the substations, control centers, and generators are abstracted as nodes. All those studies take the plant-level (bused and real stations) as the node. It is impossible to formulate targeted operation and maintenance strategies for specific devices because the model is not fine-grained enough.

In device-level networks, a complex network model regards the part of the communication business, communication devices, and power devices as the basic nodes. In Ref. [16], communication devices are mapped as the nodes, and communication links between devices are mapped as the edges, ignoring the impact of the physical grid. Qi et al. [17] and Xu et al. [18] considered the information link and took the business of the information network as the node. The latter one is practical to recognize the significant power and communication services, but they map the influence of the physical system to the edge weight or service importance of the information system. Therefore, they lack the modeling of the dynamic process of topological interaction of coupled networks, and cannot evaluate the structural robustness of the coupled network.

Literature proves that existing studies when analyzing the influence of more fine-grained components, failed to consider the impact of the chain reaction on the whole system resulting from the interdependent interaction between the component and its other side. Nonetheless, the deep coupling between the cyber side and the physical side is one of the most important reasons for the rapid expansion of the fault scope. Therefore, it is important to assess the vulnerability of networks and components, even as small as a device. In view of the mentioned above, this paper proposes a node-to-edge interdependency between EPCN and the physical power grid and a fine-grained CPPS model to analyze the vulnerability of coupled power systems. The contributions of this research are summarized as follows:

(a) Aiming at the limitation that plant-level models are not fine-grained enough, the method of a multilevel CPPS model establishment by combining the device-level model and site-level model according to the logical connection of devices in the power business.

(b) To overcome the limitation of the device-level networks caused by the lack of modeling dynamic process of topological interaction of coupled networks, a node-to-edge interdependent relationship is put forward. It can both conforms to the interaction of EPCN and physical power grids and model a device instead of an entire site.

(c) An index system of vulnerability evaluation including 3 indexes is constructed to distinguish the influence of nodes and analyze the vulnerability of power grids.

The rest of the paper is organized as follows: In Section 2, the "node-to-edge" interdependent network model is proposed. In Section 3, the fine-grained and device-level communication model of the substation is put forward and its corresponding constraint conditions are listed. In Section 4, the vulnerability evaluation of a local power grid cyber-physical system model is investigated by comparing the traditional indexes about complex networks and the indexes in this paper. Section 5 concludes this paper.

2. Node-to-Edge Interdependent Network

Although breakers control the on-off of the power line in the physical power grid, they belong to status information controlled by intelligent terminals of EPCN. Consequently, the breaker and its corresponding power line are a "cyber node-power edge" correspondence, where the device (breaker) on the cyber side is equivalent to a node, and a power line on the power side is equivalent to an edge. Based on that, this paper first introduces a variety of coupling relations of the interdependent network, and analyzes the limitations of the original interdependent network, then proposes a "node-to-edge" interdependent network model.

2.1. Theory of Interdependent Network and Its Limitations. With the development of network theory, many researchers have investigated the interaction between CPPS by extracting the topology of the power network and the cyber network to establish the dependency. Various approaches for coupling two unilateral networks into a dependent network were proposed by different researchers and classified as follows: "one-to-one" [19], "partially" [20], "multidependent" [21], "one-to-many" [22], "many-to-many" [23] interdependent networks. The models are shown in Figure 1. The interdependent network in each subfigure is made up of two-part: a power grid and an EPCN. The edge between them is called the dependent edge. Components of the grid and the EPCN were mapped to nodes. Then, a connecting edge was formed by connecting components on the same side in electrical or communication relations. The

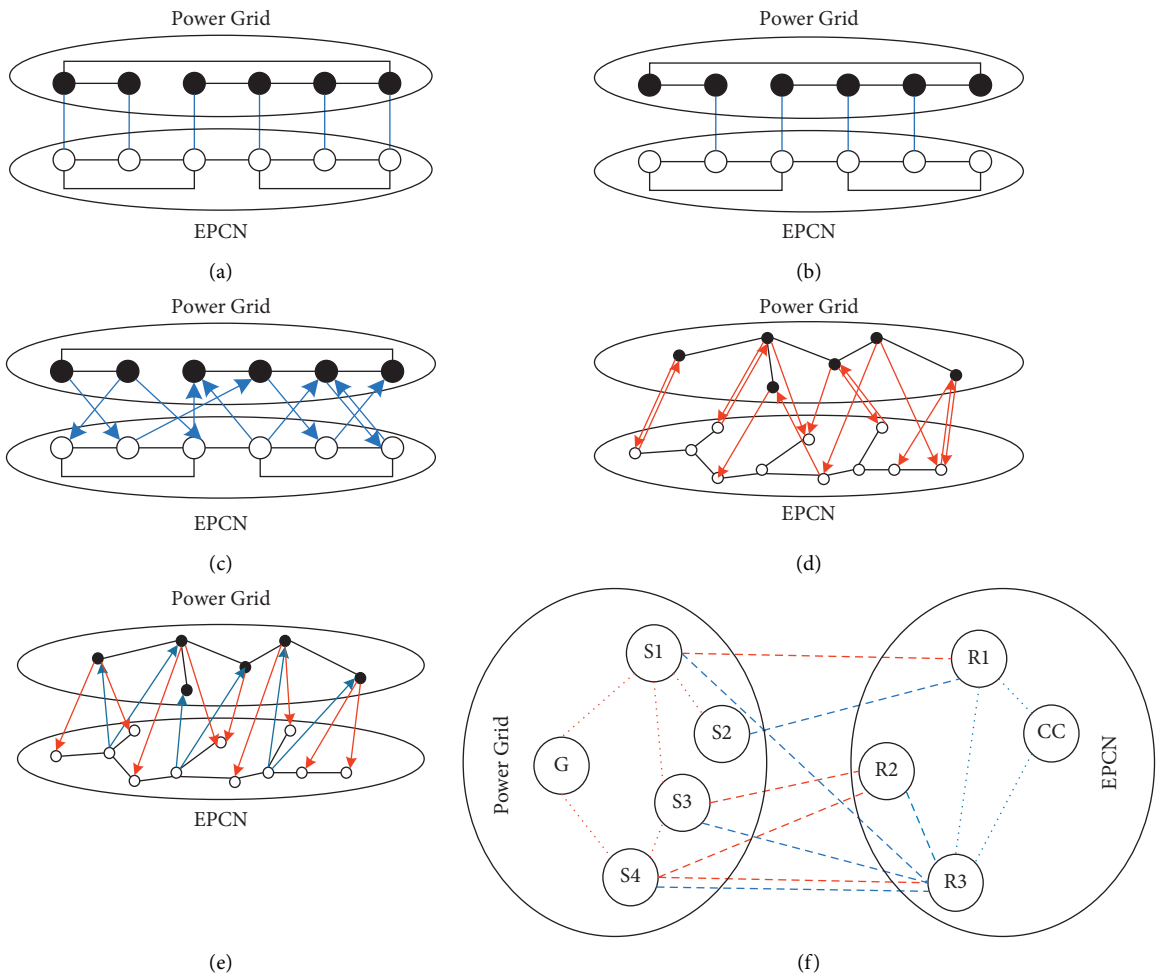


Figure 1: Origin models for interdependent networks. (a) "One-to-one" interdependent network. (b) "Partially interdependent" network. (c) Multidependent interdependent network. (d) "One-to-many" interdependent network. (e) "Many-to-many" interdependent network. (f) Cyber-physical power interdependent network considering node heterogeneity.

abovementioned models completely summarize "node-to-node" dependence relationships between two networks, which means both ends of a dependent edge are two nodes. They are suitable for cases where nodes are equivalent to plants or stations. However, when a more fine-grained model is established and a specific communication device needs to be evaluated, EPCN and power grid are not always coupled to each other through nodes. For example, there is a "device-power line" relationship between a circuit breaker and its corresponding power line as shown in Figure 2. A device is abstracted as a node, while a power line is abstracted as a connecting edge to connect two stations. Obviously, line 12 in Figure 2(a) is a complete power line, only connected and disconnected two states. But in Figure 2(b), when the system is abstracted as a graph, it is cut into three pieces so that three lines correspond to 2^3 states, which is illogical. The traditional theory cannot accurately involve the situation of coupling between "node" and "edge." This paper expands the original interdependent network and proposes a node-to-edge interdependent network model in Section 2.2, which describes the interdependent relationship between node (circuit breaker) and edge (power line).

2.2. Model of Node-to-Edge Interdependent Network

2.2.1. Model Description. Only cascading failures due to topological interactions are considered in this paper. Based on that, there are two hypotheses:

Hypothesis 1. The capacity of the power lines is sufficient.

Hypothesis 2. The capacity of generating units can meet the demand for electricity

For the "node-to-edge" interdependent network proposed here, the following descriptions are concluded based on the working characteristics of the power system:

Description 1: Faults are not transmitted between nodes in a one-sided network.

Description 2: When the node fails, all its connecting edges and dependent edges fail.

Description 3: Outliers belong to invalid nodes.

Description 4: In the initial network, if a node is connected to a dependent edge, the node will fail when the dependent edge disappears.

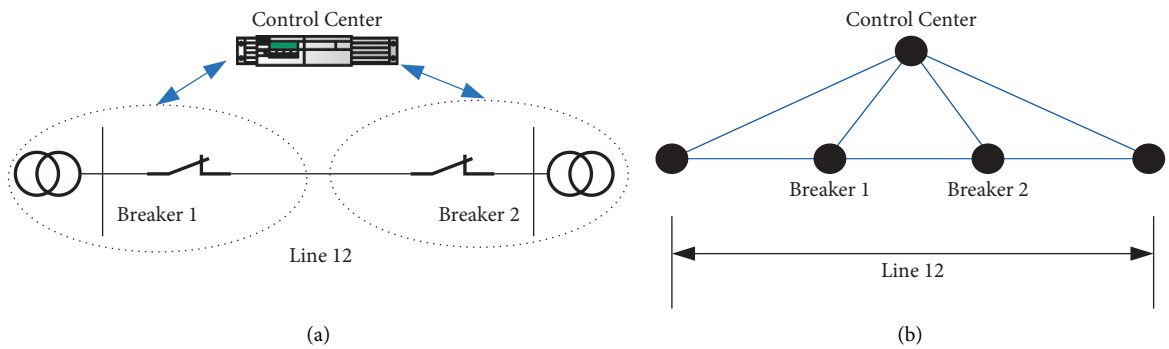


Figure 2: An example of node-to-node CPPS. (a) A micro CPPS. (b) The graph of the CPPS.

Description 5: In the initial network, if the connecting edge is connected to the dependent edge when the dependent edge disappears, the connecting edge also fails.

On the physical side, when a component disappears, the components around it can keep working after a proper scheduling process even though its working parameters will change. For the cyber side, nodes can work when they are charged. When a node fails, it cannot obtain external power and information support. So, that is why descriptions 1 and 2 are true. After a node becomes an outlier, it loses power and communication contact with the outside world and cannot affect the system. Therefore, it is a failed node, which is, why description 3 is true.

If a node is connected to a dependent edge in the initial network, it needs support from the other side of the interdependent network to keep working; otherwise, it does not need it. That is why description 4 is true. If an edge is connected to a dependent edge in the initial network, it needs support from the other side of the interdependent network to keep working; otherwise, it does not need it. That is why description 5 is true. When node failure occurs, the network structure changes according to the mentioned above.

2.2.2. Topological Change Process of the Model. A broken node is, respectively, set on both sides of the coupled network and analyzes the change process of topology. Meanwhile, this paper compares the model proposed in this paper with the "node-to-node" model with added virtual nodes (which is called the traditional model in this paper, proposed by Buldyrev et al. [19], the first people, who came up with the interdependent networks) by attacking nodes of both sides of the interdependent network. What is needed to explain first is that the attack here refers to the node being deleted from the topology due to some failure.

It is found that the "node-to-edge" model is more adaptable when the breaker is the key coupling node in terms of the topology complexity and the fault propagation mechanism.

(1) Attack on the cyber side. In the "node-to-edge" model, as shown in Figure 3(a), the black edge is the interdependent edge, the blue nodes and edges belong to the device-level EPCN, and the green nodes and edges belong to the physical power grid. Set the dark blue color as the failed node of the device-level EPCN without considering the chain failure of nodes belonging to the same network. Firstly, the dependent edge of the broken node and the connection edge of the device-level EPCN fail, as shown in Figure 3(b). Then, due to the failure of the dependent edge, the connecting edge on the physical power grid side of the dependent edge successively fails. Subsequently, the green node on the far left becomes an outlier. Thus, this isolated node fails finally. Figure 3(c) shows the ultimate maximum connected branch.

Virtual nodes are the ones with no actual meaning. Their existence is to meet the structure of the traditional model. Because present structures of the interdependent network are that both ends of dependent edges are nodes.

In the traditional model, as shown in Figure 4(a)v, virtual nodes are added at the junction of all dependent edges and physical grid connection edges. When a faulty node occurs in the device-level EPCN; both the connecting edge and the dependent edge of the corresponding device-level EPCN fail, as shown in Figure 4(b). Then, due to the failure of the dependent edge, the virtual node connected by the dependent edge in the physical power grid also fails, resulting in the disappearance of the connecting edge of the virtual node. Thus, the green node on the far left becomes an outlier, which successively fails as shown in Figure 4(c). A comparison of the two processes reveals that the results are equivalent in terms of cascading faults between networks, where the "node-to-node" model adds nodes to the physical power grid.

(2) Attack on the physical side. In the "node-to-edge" model, when a node failure occurs in the network where an edge of a dependent edge resides, the topology changes according to the descriptions in this paper, and the final steady-state is shown in Figure 5(c).

Similarly, in the traditional model, a virtual node is added at the junction of the dependent edge and the network side connecting edge, as shown in Figure 6. At this moment, the fault terminates at the established virtual node and cannot continue to propagate according to the hypotheses.

(3) Propagation mechanism of failure. In view of the topological evolution process of the abovementioned model, the following laws in the "node-to-edge" interdependent

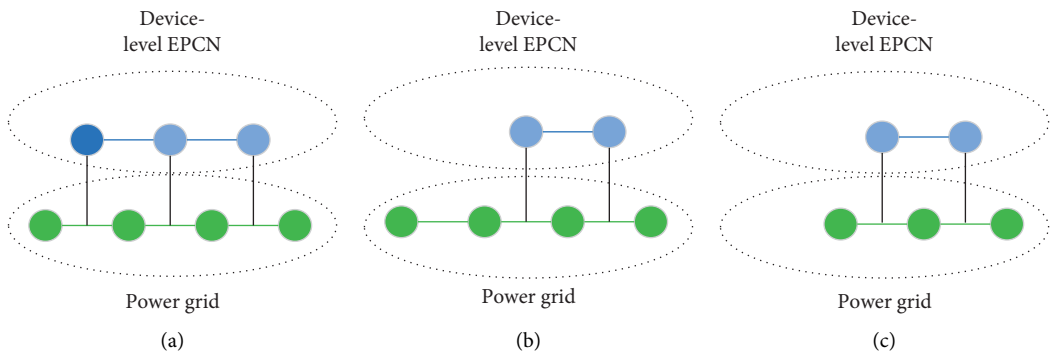


Figure 3: Cascading process of cyber node failure.

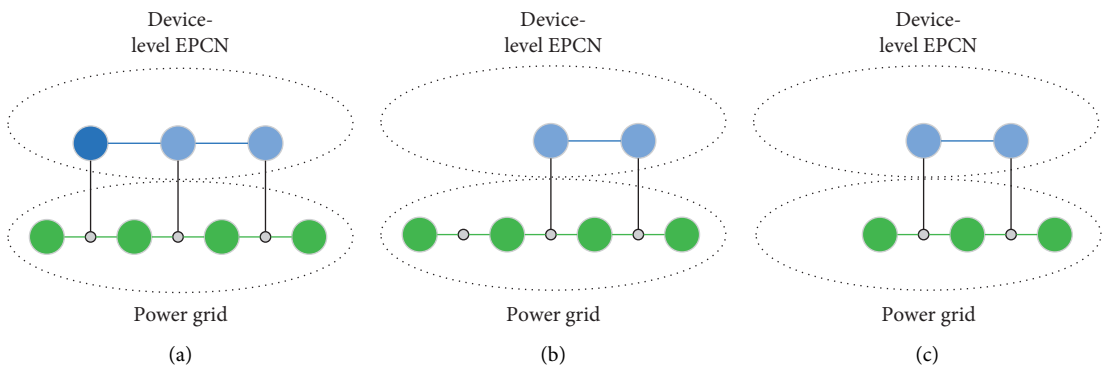


Figure 4: Cascading process with virtual nodes added to cyber node failure.

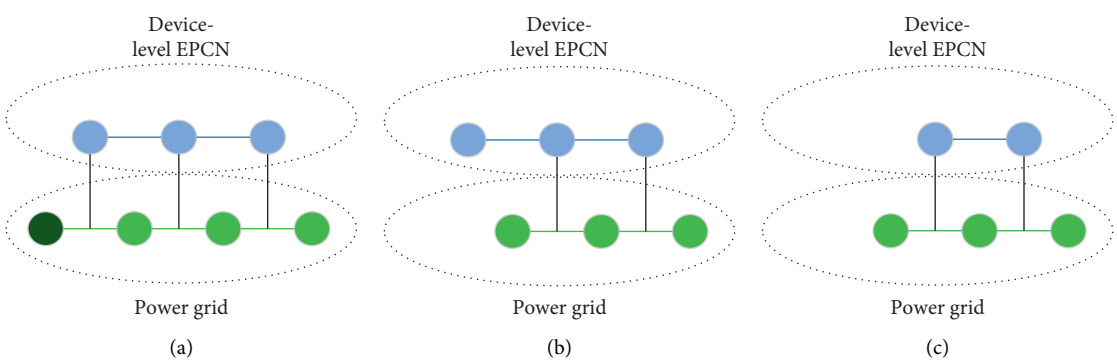


Figure 5: Cascading process of physical node failure.

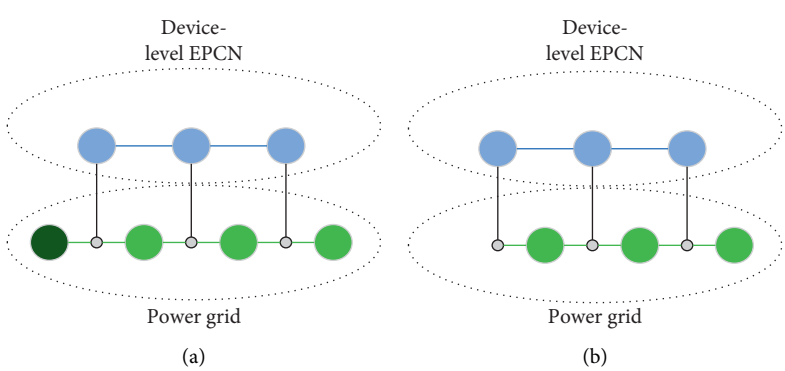


Figure 6: Cascading process with virtual nodes added to physical node failure.

network model can be summarized as follows: when one end of the dependent edge is a node and the other end is a connecting edge.

(i) Attacking a node of the network belonging to the "node" end, the model is equivalent to adding virtual nodes to the "edge" end of the "node-to-node" interdependent network. But the traditional model increases the complexity of the coupled network.

(ii) Attacking a node of the network to which the "edge" belongs, the failure may be terminated at the virtual node, to stop cross-system propagation, while it will not stop when attacking the same node in the "node-to-edge" model.

(4) Difference between the "node-to-node" model and "node-to-edge" model. As mentioned above, the difference between the two models lies in the topology complexity and the fault propagation mechanism.

(a) For the same power system, there are fewer nodes in "node-to-edge" model, because it has no virtual nodes compared with the traditional model.

(b) The node-to-node interdependent network cannot cover all coupling cases. When a node of the network to which the "edge" belongs is attacked, the resulting topologies of the two models are different. The failure may be terminated at the virtual node, to stop cross-system propagation, while it will not stop when attacking the same node in the "node-to-edge" model, that is to say, the equivalent of adding virtual nodes is conditional only in some cases. It is because the newly added nodes divide the power line into two pieces, and when an attack occurs on the side on which a newly added node lies, it will terminate at this intersection just like Figure 3(b). However, in the node-to-edge model, the edges, which are the end of dependent edges are a whole. Based original model, the undirected dependent edge model $E_{\leftrightarrow}$ is improved. Since one end of the dependent edge is a node of EPCN and the other end is an edge of the physical power grid, $E_{\leftrightarrow}$ is shown in (1)as follows:

$$E_{\leftrightarrow} = \begin{cases} \{i \in V_A, j \in E_B | (V_{Ai}, E_{Bj})\}, \\ \{i \in V_B, j \in E_A | (V_{Bi}, E_{Aj})\}, \\ \{i \in V_A, j \in E_B, k \in V_B, l \in E_A | (V_{Ai}, E_{Bj}) \text{or} (V_{Bk}, E_{Al})\}, \end{cases} \quad (1)$$

where V_A and V_B are, respectively, the sets of all nodes from network A and network B. E_A and E_B are, respectively, the sets of all edges from network A and network B.

3. Model of CPPS Based on Node-to-Edge Interdependent Network

In general, the control centers at all levels, power plants, and substations are regarded as undifferentiated nodes in the modeling method of cyber-physical interdependent networks. Then nodes are connected according to the actual connections. However, regarding a site as a node make it impossible to analyze the robustness of EPCN at the device level. Therefore, this paper refines the cyber-physical interdependent network composed of control centers at all levels and substations and establishes a complex network model of CPPS, of which one side is a device-level network and the other side is a plant-level network. First, the establishment of a device-level topology of a station is introduced. And then the topology of a multilevel power system is extended.

Through the establishment of the abovementioned model, this paper analyzes the vulnerability and weak links on this basis.

3.1. Device-Level Topology Modeling Based on Cyber-Physical Power Service. Compared with the abnormal alarm analyzed by a certain communication protocol, it is more intuitive for substation staff to know whether the secondary device services are running normally. Consequently, connections among services in the device business are referred to model the substation monitoring system to accurately evaluate the importance of devices inside the substation. According to the main power business that each secondary device needs to bear, the device of a smart substation can be divided into three layers: station control layer, interval layer, and process layer. The communication network model of the substation monitoring system is established as shown in Figure 7.

To simplify the model, a device-level topology model of a station is established, and the automation systems of control centers at all levels are regarded as control nodes. Each device in EPCN in each substation is regarded as a node, and the physical and cyber connection between devices is regarded as an edge. If there is information transferring between devices, such as control instructions or state information up and down, it indicates that there is a connection between the two devices.

3.2. Multilevel Topology Modeling of Power Grid and Communication Devices. Secondary devices of power systems play a critical role in power systems. It is difficult to reflect the reality of the power system to build a network model from the physical network or the EPCN only. Hence, the interaction between EPCN and the physical power grid should be taken into account. In view of that coupling relationship, the breaker is considered as the interactive node between the two systems. Consequently, this paper controls the connecting edge of the physical network through the state of the breaker node of EPCN. The bidirectional relationship between them is as follows: the circuit breaker controls the power line, and the on-off state of the power line is uploaded to the dispatching center through the circuit breaker and other devices. When a circuit breaker fails, the breaker node loses control of the power line, so the power line cannot be operated by the circuit breaker and disappears from the power topology. That is to say, the probability here is a 0–1 variable, which is 0% or 100%. It follows that one side of the model is a device-level network while the other side is a plant-level network, which is called the multilevel topology model in this paper.

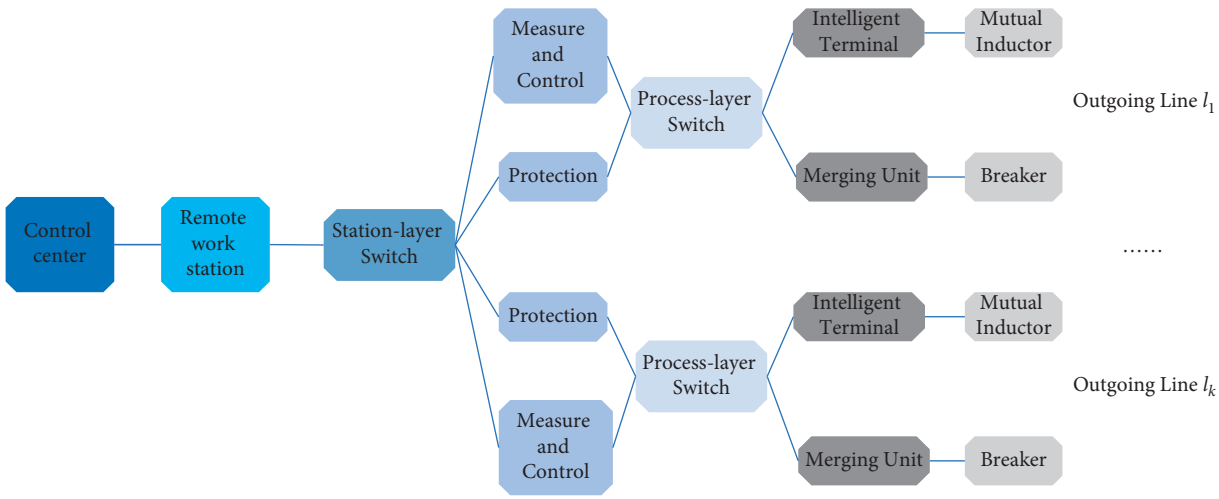


Figure 7: Communication network of substation monitoring system.

According to the topology modeling method presented in Section 2.2, for a general power grid, the steps of establishing the multilevel model are as follows:

Step 1: Model all substations based on the service chain (Section 3.1).

Step 2: Expand all the models in step 1 as the basic unit. And connect the remote workstations of the substations with the control nodes to which the substations, respectively, belong.

Step 3: Connect physical nodes according to the topology of the physical power grid.

Step 4: According to the outgoing lines of each substation, circuit breakers, and sensors, the set of all dependent edges can be obtained.

An undirected node-to-edge interdependent network model is established, accordingly. The model described above can be represented by the graph $G(V, E)$. The description $G(V, E)$ is shown in (2) and (3):

$$V = \left[V_p, V_c\right], \tag{2}$$

$$E = \left\{E_p, E_c, E_{\leftrightarrow}\right\}, \tag{3}$$

where $V_p = [v_{p1}, v_{p2}, \ldots v_{pn_p}]^T$, $V_c = [v_{c1}, v_{c2}, \ldots v_{cn_c}]^T$, respectively, denotes all nodes of the power grid and device-level EPCN. $E_p = \left\{i, j \in V_p | (i, j)\right\}$, which means that there is a connecting edge between node i and node j from the power grid. Same thing with E_c. $E_{\leftrightarrow} = \left\{E_{pi} \in E_p, \quad V_{cj} \in V_c | E_{pi}, V_{cj}\right\}$, namely, "set of the dependent node to edge."

The adjacent matrix $A = \begin{bmatrix} A_p & 0 \\ 0 & A_c \end{bmatrix}$ can be obtained by $G(V, E)$.

$$A_x = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n_x} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n_x 1} & a_{n_x 2} & \cdots & a_{n_x n_x} \end{bmatrix}, \tag{4}$$

where $a_{ij} = 1$ when there is an edge between node i and node j, otherwise $a_{ij} = 0$ when there is no edge between node i and node j or $i = j$. x means p or c. n_x denotes the number of nodes of corresponding networks.

Obviously, an adjacent alone cannot represent the whole interdependent network on account of no equation representing the coupling relationship between two networks. Thus, $E_{\leftrightarrow}$ is needed, as shown in (5)as follows:

$$G(V, E) = G\left(A, E_{\leftrightarrow}\right). \tag{5}$$

3.3. Assessment of the Interdependent Vulnerability Based on Node Failure. For the reason of the influence evaluation of nodes in the coupled network, the attacked nodes are deemed completely invalidated. In the proposed model, the normal operation conditions of physical nodes are different after the failure of cyber nodes and physical nodes. Consequently, node attacks are classified into cyber node attacks and physical node attacks. Then, combined with constraints, a vulnerability index adapted to this paper's CPPS model is proposed in Section 3.3.3.

3.3.1. Constraints of Operations. All the power nodes are classified into 2 types: the first type is power generation nodes (which mean power stations) and the second type is what cannot generate electricity. If a fault occurs, the graph may be divided into several subgraphs. To ensure the operation of the second nodes, there must be a direct or indirect electrical connection between the two types of nodes.

"d_{kj}" ("d" denotes distance) is used to judge whether there is the connection mentioned above between node k and node j. d_{kj} is the length of the shortest path from k to j. If there is no path to get from k to j, then $d_{kj} = \infty$ or $1/d_{kj} = 0$.

Hence, if "d"s from a second node to any power generation nodes are all infinite, which indicates that the station has no power source, the second node will stop functioning. Purely from the perspective of the structure of networks, as long as this node has the abovementioned connection with at least one power generation node, the node still exists in the network. Then, the "d"s are calculated from node k (a second node) to all power generation nodes (node 1 to m).

$\sum_{j=1}^{j=m} 1/d_{kj} = 0$ means there is no connection between k and all power generation nodes.

So, $\sum_{j=1}^{j=m} 1/d_{kj} > \varepsilon$ $(0 < \varepsilon < \infty)$ is one of the prerequisites for the second node to run.

The normal operation of the physical nodes (except power generation nodes) shall meet the constraints: $\exists \varepsilon > 0$, in Equation (6), it is established in the case that the physical nodes of the physical power grid are attacked.

$$\text{S.t.} \quad \sum_{j=1}^{j=m} \frac{1}{d_{kj}} > \varepsilon, \tag{6}$$

where d_{kj} is the distance from physical node k to physical node j $(\forall j \in [1, m], d_{kj} \geq 0)$. Moreover, nodes l to m are power generation nodes.

For cyber nodes, the devices outside the giant component will stop working:

$$\text{S.t.} \quad i \in G_{C\max}, \tag{7}$$

where $G_{C\max}$ is the largest connected subgraph (LCS) of EPCN.

3.3.2. Indexes of Vulnerability. In the face of attacks, researchers study the vulnerability of networks from the perspective of giant components, average shortest path, k core, and entropy. In this paper, the ratio of lost nodes (*RLN*) is used to quantitatively calculate the changes of the network subjected to different faults to reflect the vulnerability of the network [24, 25]. In this paper, *RLN* is calculated by the following Equation (8):

$$\text{RLN} = \frac{N^* - N}{N^*}, \tag{8}$$

where N^* is the number of nodes of the initial network, and N is the number of nodes of the current network.

Different constraints on physical nodes and cyber nodes determine the different ways of calculating the number of nodes in normal operation. For cyber nodes, the nodes of LCS and their edges make up the current network. Yet even physical nodes that do not belong to the LCS may operate normally, resulting in the unsuitability of the LCS in describing the functioning physical power grid. Furthermore, physical nodes, power generation nodes, substation nodes, and connecting edges form together the current operating network [26]. If there is no generation node connected to substation nodes or vice versa, the substation nodes or the generation nodes do not belong to the current functioning network [27].

The influence of node i on network vulnerability can be revealed by the relative change of RLN before and after node i fail, as shown in Equation (9)as follows:

$$\Delta\overline{RLN_{ci}} = \frac{N_c^* - N_{ci}}{N_c^*}, \Delta\overline{RLN_{pi}} = \frac{N_p^* - N_{pi}}{N_p^*}, \tag{9}$$

where $\Delta\overline{RLN_c}$ is the index of the importance of node i for cyber-network, $\Delta\overline{RLN_p}$ is the index of the importance of node i for physical network, N_c^* is the number of initial EPCN's nodes, $N_{\max Gi}$ is the number of nodes of EPCN's LCS after node i fails, N_p^* is the number of the initial power grid, N_{pi} is the number of normal nodes of power grid after node i fails.

The importance of node i is defined as the weighted mean value of the damage of the coupled network which consists of $\Delta\ \overline{RLN}$ of the two single-sided networks:

$$\Delta\overline{RLN_i} = w_c\Delta\overline{RLN_{ci}} + w_p\Delta\overline{RLN_{p\,i}}. \tag{10}$$

The average distance of EPCN D_c and the physical power grid D_p is calculated first to measure pivotal nodes' proportion prone to high risk to the network. And failure is more likely to propagate across systems when there are many critical nodes. So, the weight calculation method is as follows Equation (11):

$$\begin{cases} w_c = \dfrac{D_p}{D_c + D_p}, \\ \\ w_p = \dfrac{D_c}{D_c + D_p}. \end{cases} \tag{11}$$

The calculation of the average distance is shown in (12).

$$D = \frac{2}{N(N-1)} \sum_{1 \leq i < j \leq N} \mathrm{d}_{ij}, \tag{12}$$

where $d_{ij}\,(i, j = 1, 2, \ldots, N)$ denotes the shortest distance from node i to node j.

4. Simulation and Discussion

This paper takes the local power grid shown in Figure 8 to conduct simulation verification on the proposed node-to-edge model and vulnerability assessment indexes. Brown nodes are power generation nodes, and yellow nodes are substation nodes. Table 1 presents the connections between substations and control centers.

The control center of each substation node is divided according to the region, as shown in Figure 9. The blue node is the control center of the backbone layer; it is connected to the main control center and the spare control center of the core layer.

A coupled network with a total of 544 nodes and 65 dependent edges is obtained. There are 512 nodes in the EPCN, and 580 connecting edges. The number of nodes in the physical power grid is 32, and the number of connected edges is 39.

The premise of the analysis is that the capacity of the power lines is sufficient and that the capacity of generating units can meet the demand for electricity. Based on the hypotheses, first, the nodes of EPCN are attacked. Then, nodes of the physical power grid follow. Furthermore, attacks are divided into two major types, that is, traversal attacks and continuous attacks. The former type means each attack is based on the origin coupled network, and the latter type means each attack is on the basis of the attacked network.

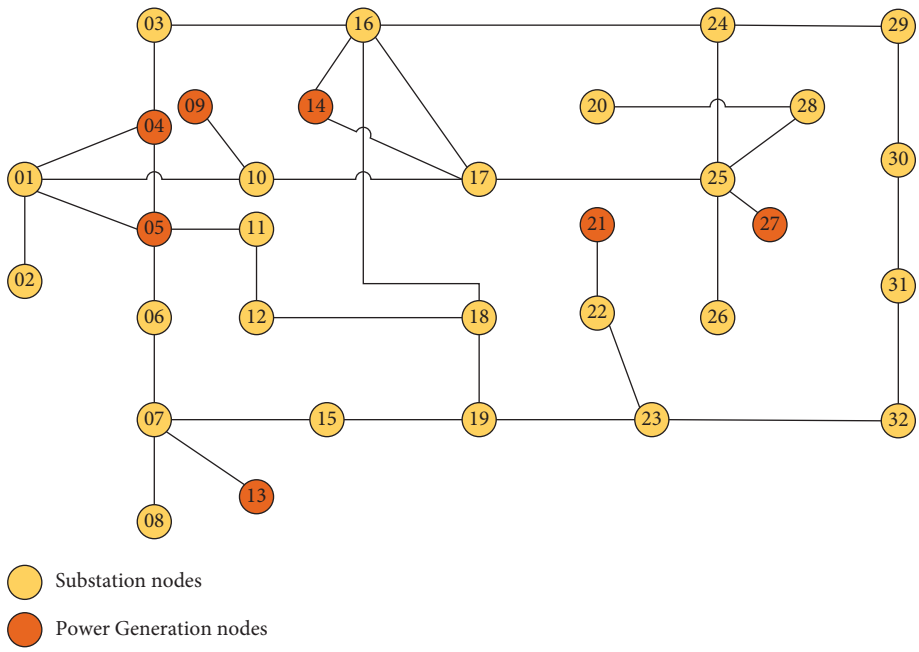


Figure 8: Topology of local power grid.

Table 1: Connection between substations and control centers.

Control centers	Substations
Control center a	1 2 3 10 11
Control center b	6 7 8 15
Control center c	12 16 17 18 19
Control center d	22 23
Control center e	20 24 25 26 28 29 30 31 32

4.1. Results of Vulnerability

4.1.1. Impact Analysis of Communication Attacks

(1) Node Importance of Device-Level EPCN. For the node traversal attack of the communication network, the value of RLN after the topology reaches the steady state is calculated. It should be noted that every cyber node is attacked on the basis of the original coupled network each time, so as to rank the influence of nodes on the network.

By comparing the three curves in Figure 10, the red curve shows a distinct stepped shape, indicating that the index, RLN, of the power grid has multiple nodes with the same value, which is insufficient to distinguish all nodes. The blue curve has the same weakness. The RLN of the coupled network integrates characters of both sides of the network, and the line segment parallel to the X-axis is shorter than the other two curves, which has a better result to distinguish the influence of nodes.

(2) Network Vulnerability Analysis under Multimode Attack Based on Node Importance. Three kinds of descending order of node importance in three kinds of modes were obtained in Section 4.2.1 (1), and calculated the betweenness and degree of the original network nodes. Then 5 vectors of descending order were generated: RLN of communication network,

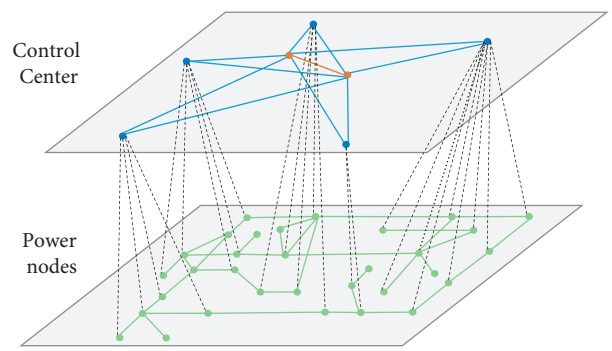


Figure 9: "Node to node" interdependent network of the local grid.

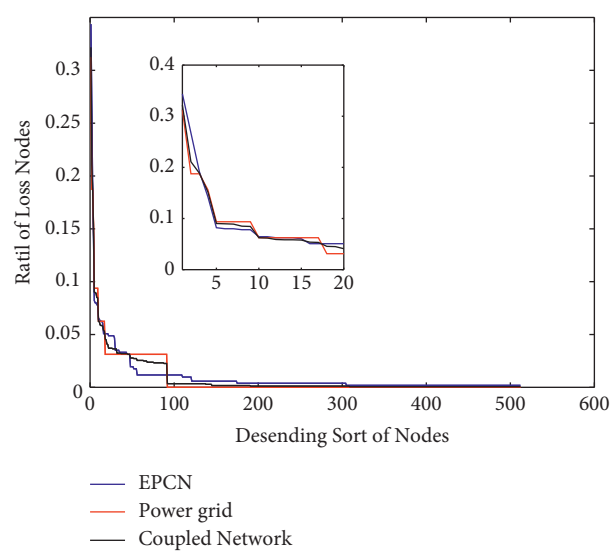


Figure 10: Rln of cyber nodes of three subjects.

RLN of the power grid, RLN of the coupled network, betweenness of communication network, degree of communication network, corresponding to attacking mode 1 to attacking mode 5, respectively.

Based on the five attacking modes, this section carries out multiple continuous attacks on the established coupled network. The nodes under each attack are the remaining normal nodes in the network after the last attack. Attack stops when all nodes in the EPCN fail. Figure 11 shows the results. "Attacking times" is used to measure the evaluation ability of different indexes. The larger the value of attack times is, the more nodes need to be attacked for network collapse. On the one hand, it shows the attack capability of different modes. On the other hand, it can reflect the vulnerability of a network.

Under different attack modes, the curve trend is roughly the same, but the inflection points of the five curves are very different. So are the lengths of the curves. Table 2 summarizes the results of the abovementioned five attack modes.

From Table 2, the coupled network has the fastest crash speed in mode 1, followed by mode 3 and mode 4. So, EPCN has more importance in coupled networks. Under the corresponding mode, coupled network crashes, respectively, 25.0% and 89.4% more easily than in modes 4 and 5.

Beginning RLN refers to damage of the first attack. Modes 1 to 4 are the same beginning value because the first node of the four-node attacking vectors is the same node, no.510. Therefore, the betweenness of no.510 is the highest, and their failures cause the most serious damage to both EPCN and the power grid. The beginning RLN of mode 5 is much lower than the others. Nevertheless, the *degree* is a common index to evaluate the centrality status of whole networks. It is concluded that centrality status cannot always reveal the impact of nodes on networks due to the interdependent edges.

The lowest value of attacking times is 9 of mode 1. The first nine RLNs of each mode are adopted. And the number of overlapped nodes is calculated. Figure 12 indicates that nodes that cause the collapse of the coupled network 9 times in mode 1 are the same components of mode 3, and it is similar to those of mode 4. The important cyber nodes to EPCN coincide highly with those to the coupled network and the high-betweenness cyber nodes. The curves of the three in Figure 11 are similar in length. Even so, the turning points are not consistent, because the nodes have similar compositions but different orders.

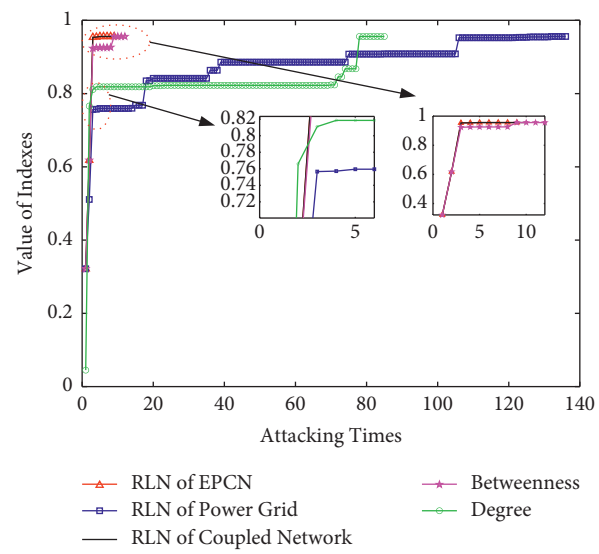


Figure 11: Indexes curve of 5 modes under cyber attacks.

Table 2: Attacking times and beginning RLN of 5 modes.

	Mode 1	Mode 2	Mode 3	Mode 4	Mode 5
Attacking times	9	136	10	12	85
Beginning RLN	0.3217	0.3217	0.3217	0.3217	0.0451

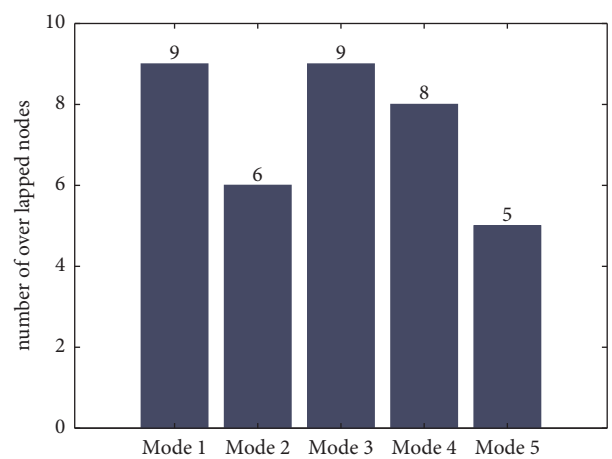


Figure 12: Number of overlapped nodes.

4.1.2. Impact Analysis of Physical Attacks

(1) Node Importance of Physical node. In accordance with the same method as 3.2.1, the node traversal attack on the physical power grid is carried out, and the value of RLN after the topology reaches a steady state is calculated to obtain three curves as shown in Figure 13.

There are quantities of nodes whose RLN are close to each other among the three curves of Figure 13. One of the reasons is that the number of nodes in the power grid is small. However, the black curve still distinguishes the nodes better than the others, while the other two curves only have two or three kinds of value.

(2) Network Vulnerability Analysis under Multimode Attack Based on Node Importance. In the same way, 5 physical node vectors in descending order were obtained: RLN of communication network, RLN of the power grid, RLN of the coupled network, betweenness of power grid, degree of the power grid, corresponding to attacking mode 1 to attacking mode 5, respectively. Figure 14 is the results after the multiple continuous attacks on the established coupled network.

Under different attack modes, the turning nodes are also before and after, and the lengths of the curves are different. Table 3 summarizes the results of the abovementioned five attack modes:

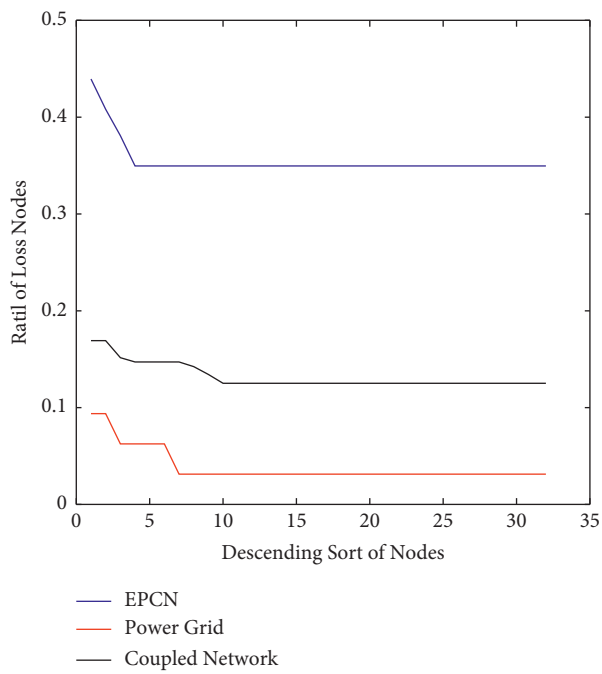


Figure 13: Rln of physical nodes of three subjects.

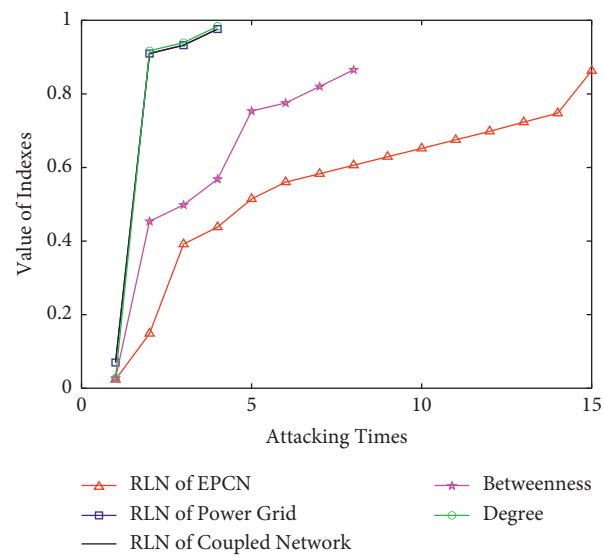


Figure 14: Indexes curve of 5 modes under physical attacks.

Table 3: Attacking times and beginning RLN of 5 modes.

	Mode 1	Mode 2	Mode 3	Mode 4	Mode 5
Attacking times	15	4	4	12	4
Beginning RLN ($\times 10^{-2}$)	2.38	7.01	7.01	2.72	2.72

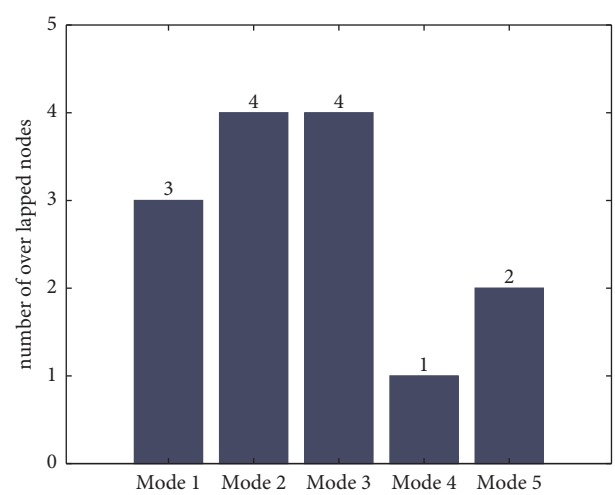


Figure 15: Number of overlapped nodes.

From Table 3, the coupled network has the fastest crash speed in modes 2, 3, and 4, much less than modes 1 and 4. So, the power grid has more importance in coupled networks, the coupled network crashes 66.7% more easily than mode 4. Although mode 5 behaves in the same way, both attacks show that mode 5 behaves in an erratic manner according to cyber-attacks.

The beginning value of modes 2 and 3 are the same, and the highest. It means that the physical node, which is the most significant to EPCN is the most crucial to the coupled network at the same time. Moreover, the curves of modes 2 and 3 coincide exactly; both are similar to the curve of mode 5.

From the results of section 4.2.1, the high-betweenness cyber nodes are quite important, while the high-betweenness physical nodes are not more vital to coupled networks than high-degree nodes. So, it is concluded that the same evaluation index has different effects on different sides of the node-to-edge network. This is because traditional indexes of a complex network evaluate the structural significance of nodes on a single side.

From Table 3, the lowest value of attacking times is 4 of mode 1. The first four RLNs of each mode are adopted. And the number of overlapped nodes is calculated. Figure 15 indicates that nodes that cause the collapse of the coupled network 4 times in mode 2 are the same components of mode 3.

Compared with *betweenness*, the indexes proposed under cyber and physical attack is, respectively, 25.0% and 66.7% easier in-network crash. Compared with a *degree*, the indexes proposed under cyber-attacks is 89.4% easier in-network crash and behave the same under physical attacks. Therefore, the indexes in this paper presented a more robust accuracy than *betweenness* and *degree*. *Betweenness* and *degree* are static process calculation network indexes and difficult to adapt to the general network structure. The dynamic process based on node failure evaluation in this paper solves the abovementioned problems well.

5. Conclusion

Based on the structure of power systems and interdependency between power sites and control centers, a multilevel CPPS model with a node-to-edge interdependent network

and an index system including 3 indexes are proposed in this paper to distinguish vulnerable components and the vulnerability of the coupled system. The following conclusions are drawn:

(1) The node-to-edge interdependent coupling relationship proposed is more suitable than the existing interdependent network about breaker services in transmission network substations with a simpler topology and a wider range of applications.

(2) The trajectory of indexes under continuous attack in this paper can characterize the vulnerability of the power grid to withstand attacks.

(3) The proposed indexes presented a better accuracy than "betweenness" and "degree."

The study presented in this paper is helpful for the long-term planning of each station and dispatching center of power systems and also contributes to the differential maintenance of key equipment and power stations. However, the presented research fails to define "multidependent," "many-to-many," "partially" interdependency like the traditional models. It can be easily extended in several directions, such as the vulnerability analysis with different node-to-edge interdependencies. And further work will be dedicated to research on how to enhance the robustness of CPPS.

Data Availability

Data are available in the paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This paper is supported by National Key Research and Development Program (Grant No. 2021YFB2401302).

References

[1] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (CPPS): a review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151019–151064, 2020.

[2] J. Chen, M. A. Mohamed, U. Dampage et al., "A multi-layer security scheme for mitigating smart grid vulnerability against faults and cyber-attacks," *Applied Sciences*, vol. 11, no. 21, p. 9972, 2021.

[3] L. Shi, Q. Dai, and Y. Ni, "Cyber–physical interactions in power systems: a review of models, methods, and applications," *Electric Power Systems Research*, vol. 163, no. A, pp. 396–412, 2018.

[4] R. Zhou, M. Peng, and X. Gao, "Vulnerability assessment of power cyber-physical system considering nodes load capacity," in *2021 6th International Conference on Intelligent Computing and Signal Processing (ICSP)*, pp. 1438–1441, Xi'an, China, 2021.

[5] L. Liu, B. Wang, F. Ma et al., "A concurrent fault diagnosis method of transformer based on graph convolutional network and knowledge graph," *Frontiers in Energy Research*, vol. 10, 2022.

[6] M. A. Mohamed, S. Mirjalili, U. Dampage, S. H. Salmen, S. A. Obaid, and A. Annuk, "A cost-efficient-based cooperative allocation of mining devices and renewable resources enhancing blockchain architecture," *Sustainability*, vol. 13, no. 18, Article ID 10382, 2021.

[7] F. Li, X. Yan, Y. Xie, Z. Sang, and X. Yuan, "A review of cyber-attack methods in cyber-physical power system," in *2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP)*, pp. 1335–1339, Xi'an, China, 2019.

[8] L. F. Fang, L. Huang, Q. Zhao, and A. Q. Pan, "Discussion on megalopolis power grid safety from the perspective of Venezuelan blackout," *Power and Energy*, vol. 40, no. 6, pp. 674–677, 2019.

[9] U. Adhikari, T. Morris, and S. Pan, "WAMS cyber-physical test bed for power system, cybersecurity study, and data mining," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2744–2753, 2017.

[10] Q. Wang, Z. Liu, and Y. Tang, "SCCO: a state-caching-based coagulation platform for cybor-physical power system evaluation," *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1615–1625, 2021.

[11] D. L. Marino, C. S. Wickramasinghe, V. K. Singh, J. Gentle, C. Rieger, and M. Manic, "The virtualized cyber-physical testbed for machine learning anomaly detection: a wind powered grid case study," *IEEE Access*, vol. 9, pp. 159475–159494, 2021.

[12] Y. Li, B. Wang, H. Wang et al., "Importance assessment of communication equipment in cyber-physical coupled distribution network based on dynamic node failure mechanism," *Frontiers in Energy Research*, p. 654, 2022.

[13] N. Wirtz and A. Monti, "A flexible framework to investigate cascading in interdependent networks of power systems," in *2020 6th IEEE International Energy Conference (ENERGYCon)*, pp. 38–41, Gammarth, Tunisia, 2020.

[14] B. Li, J. Zhang, S. S. Chen, C. Y. Zhu, D. S. Jing, and B. Qi, "Expansion strategy of power communication network survivability based on complex network," *Power System Technology*, vol. 42, no. 06, pp. 1974–1980, 2018.

[15] A. Sturaro, S. Silvestri, M. Conti, and S. K. Das, "A realistic model for failure propagation in interdependent cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 817–831, 1 April-June 2020.

[16] B. Fan, C. Zheng, and L. Tang, "Risk assessment of power communication network based on node importance," in *2019 IEEE 3rd Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, pp. 818–821, Chongqing, China, 2019.

[17] B. Qi, S. F. Liu, B. Li, Y. Sun, D. Jing, and Z. Cheng, "Routing optimization strategy for power communication network with shared risk link group and risk balance," *Automation of Electric Power Systems*, vol. 44, no. 08, pp. 168–175, 2020.

[18] L. Xu, Q. L. Guo, X. Z. Liu, and H. Sun, "Robust optimization method of communication network to improve resilience of cyber-physical power system," *Automation of Electric Power Systems*, vol. 45, no. 03, pp. 68–75, 2021.

[19] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.

[20] D. Zhou, J. Gao, H. E. Stanley, and S. Havlin, "Percolation of partially interdependent scale-free networks," *Physical Review E*, vol. 87, no. 5, Article ID 052812, 2013.

[21] J. Shao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Cascade of failures in coupled network systems with multiple support-dependence relations," *Physical Review E*, vol. 83, no. 3, Article ID 036116, 2011.

[22] H. Zhen, W. Cheng, S. Ruj, M. Stojmenovic, and A. Nayak, "Modeling cascading failures in smart power grid using interdependent complex networks and percolation theory," in *8th IEEE Conference on in Industrial Electronics and Applications*, pp. 1023–1028, IEEE, Melbourne, Australia, 2013.

[23] Z. Huang, C. Wang, M. Stojmenovic, and A. Nayak, "Balancing system survivability and cost of smart grid via modeling cascading failures," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 1, pp. 45–56, 2013.

[24] A. Almalaq, S. Albadran, A. Alghadhban, T. Jin, and M. A. Mohamed, "An effective hybrid-energy framework for grid vulnerability alleviation under cyber-stealthy intrusions," *Mathematics*, vol. 10, no. 14, p. 2510, 2022.

[25] A. Almalaq, S. Albadran, and M. A. Mohamed, "Deep machine learning model-based cyber-attacks detection in smart power systems," *Mathematics*, vol. 10, no. 15, p. 2574, 2022.

[26] M. Ćalasan, A. F. Zobaa, H. M. Hasanien, S. H. Abdel Aleem, and Z. M. Ali, "Towards accurate calculation of supercapacitor electrical variables in constant power applications using new analytical closed-form expressions," *Journal of Energy Storage*, vol. 42, Article ID 102998, 2021.

[27] O. Lukačević, A. Almalaq, K. Alqunun et al., "Optimal CONOPT solver-based coordination of bi-directional converters and energy storage systems for regulation of active and reactive power injection in modern power networks," *Ain Shams Engineering Journal*, vol. 13, no. 6, Article ID 101803, 2022.