Received June 4, 2021, accepted July 21, 2021, date of publication August 2, 2021, date of current version November 11, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3101896

Cross-Space Risk Assessment of Cyber-Physical Distribution System Under Integrated Attack

JIE YANG[1], YIHAO GUO[1], CHUANGXIN GUO[1], (Senior Member, IEEE), ZHE CHEN[2], AND SHENGHAN WANG[1]

[1]College of Electrical Engineering, Zhejiang University, Hangzhou, Zhejiang 310027, China
[2]Electric Power Research Institute, State Grid Zhejiang Electric Power Company, Hangzhou, Zhejiang 310014, China

Corresponding author: Chuangxin Guo (guochuangxin@zju.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant U1866209.

ABSTRACT Assessing cross-space risk of cyber-physical distribution system under integrated attack is investigated in this paper. Firstly, a hierarchical structure of cyber-physical distribution network according to IEC 61850 is established and a deliberate attack scenario with limited adversarial knowledge and stealth requirement is developed based on a general linear model for state estimation. Then, we formulate two optimization problems to describe the attack implementation and propagation process and obtain the likelihood of attacks including a robust solution and a risk solution in a fuzzy Bayesian network (BN). On this basis, a physical impact metric is defined as the integrated deviation of system states and measurements. Thus, the cross-space risk assessment can be performed. Finally, the simulation results of case studies demonstrate that the proposed method is effective and provides a broad and clear view of cyber-physical distribution system security situation.

INDEX TERMS Cross-space risk, cyber-physical distribution network, integrated attack, limited adversarial knowledge, fuzzy Bayesian network, state estimation.

I. INTRODUCTION

Distribution network is a critical part of smart grid which meets the increasing requirement of supply reliability, operation cost-effectiveness and renewable energy consumption by employing advanced information and communication technology (ICT). In addition, it is also the core object of the Electric Internet of Things construction. With the broad-scale sensing and communication networks, distribution network has become one of the largest cyber-physical systems. Since the distribution network directly faces users, its importance is self-evident. Unfortunately, with the introduction of intelligent electronic devices (IEDs) and open communication systems, there are conspicuous security risks in cyber system and they can be further transmitted across spaces to disrupt physical system and cause far reaching impacts [1]. Many real-world events have confirmed this, including the deliberate cyber-attacks on Ukrainian power grid in 2015 [2], Israel Outage in 2016 [3] as well as Venezuela Blackout in 2019. As mentioned above, a clear understanding of the security situation of distribution network is extremely important.

Considering the demand of extensive interconnection and intelligent interaction for the future smart grid, IEC61850 based distribution automation system (DAS) is believed to be one of the most promising development directions. However, IEC 61850 standards do not cover corresponding security functions and hence IEC 62351 is used as complement responsible for related data and communication security in power system. But there is still a long way for this standard to be mature enough to guide large-scale engineering application of the 61850-based smart grid due to the following key problems, i.e., 1) real-time requirements for security protection; 2) security key distribution and management mechanism; 3) compatibility with substation configuration language (SCL). Thus, the security risks and threats of mentioned system mainly come from two aspects. First, unlike substation operating in an enclosed space which is physically isolated, distribution network covers a wide area and a large number of remote-control devices. Once terminal equipment lacks effective protection, it can easily become a starting point for adversaries to initiate attacks. On the other hand, IEC 61850 standards stipulate that SV/GOOSE/MMS data packets are transmitted in plaintext, which lacks effective encryption methods and

The associate editor coordinating the review of this manuscript and approving it for publication was Bin Zhou.

therefore causes security risks [4]–[6], i.e., i) the messages in IEC 61850 standards contain many security vulnerabilities since they focus on solving interoperability between different IEDs and realizing data sharing while not too much attention was given to security; ii) the MMS protocol lacks identity authentication and access control mechanisms and uses plaintext for transmission. Related vulnerabilities, e.g., overflow vulnerability, can cause equipment shutdown or to go offline; iii) SV and GOOSE messages are encoded by ASN.1 without encryption to meet the high requirements for real-time performance, thus the data may be tampered, copied and tapped. With the rapid development of smart grid, the cybersecurity issues of IEC 61850 based distribution network will become more prominent and urgent for both academy and industry [7]. Considering the high dependence with cyber system, attack paths and targets of adversaries, the cyber-attack on distribution network is a cross-space behavior. Consequently, the corresponding risk assessment must naturally cross the cyber-physical space. This paper makes it clear that the cross-space risk assessment is a process of possible cybersecurity threats identification and potential physical loss evaluation, which plays a vital role in guiding cyber vulnerability reducing and system resilience enhancing. This paper exactly focuses on establishing an effective and objective cross-space risk assessment method.

Generally, quantitative risk assessment is preferred because it can provide accurate reflections of system security situation while qualitative methods cannot. The total risk of cyberattacks is defined as the likelihood of attack multiplied by the potential attack impact [8]. Consequently, the research is also carried out from the above two aspects, i.e., the propagation of cybersecurity risk and impact evaluation. For the former one, numerous models have been introduced in recent years, including Bayesian network (BN) [9], Petri net [10], attack tree [11], attack graph [12] and fault tree [13], etc. However, the shortcomings are also obvious, i.e., i) it is difficult to obtain a large amount of cyberattack prior knowledge due to limited corresponding data; ii) it is hard to capture the time-varying characteristics of components and systems since the models are intrinsically static; iii) the attack scenario setting is relatively simple. Undoubtedly, much effort has been performed to address these issues, e.g., reference [14] proposed a fuzzy probability BN for modeling risk propagation to overcome the limitation of historical data. Unfortunately, there is accuracy loss to some degree when mapping from linguistic probability to conditional probability. In [15], a hierarchical Bayesian reliability model was developed to integrate historical data and real-time data for dynamic risk assessment while it may not be suitable for cyber-physical systems. The insufficient cyberattack data is not enough to support the establishment of the mentioned model. Reference [16] defines the cyber-to-physical risk as the physical impact of cyberattacks and presents a cyber to physical dynamic risk assessment method with BN and stochastic hybrid system (SHS) model. However, the complex attack scenarios are not considered in this model and it is assumed that the adversary possesses the full knowledge of the system.

As for the impact evaluation, the researchers can be essentially divided into two categories. One only focuses on cyber system risk assessment. For example, reference [17] uses complex network statistical features to assess the risk of smart grid related to cyber network malfunction and latency. Reference [18] develops a cyber-physical security assessment metric for microgrid by integrating all the resiliency-related factors with Fuzzy Choquet Integral. The other one usually constructs many physical impact metrics. Taking reference [19] as an example, it proposes an impact metric by combining the production loss, incidence loss and economic loss from a perspective of asset. However, the cyber-physical interaction is ignored and the same problem also exists in [20] and [21].

To fill the gaps of the above-mentioned methods, this paper presents a novel method with fuzzy BN and system state estimation to quantify the cross-space risk for IEC 61850 based cyber-physical distribution system. Here, we consider the core links of cyber-physical interaction, i.e., actuators and sensors, to establish a general linear state estimation model for the system. Meanwhile, deliberate attack scenarios are set up, i.e., i) coordinated attacks between actuators and sensors; ii) combined attacks for data integrity and availability. The main contribution is three-fold:

1) This paper proposes a probabilistic indicator to characterize the availability of vulnerabilities and input it to the fuzzy BN as the prior probability. We establish a NP-Hard problem from the perspective of adversary which take two factors into consideration, i.e., i) the limited system knowledge that adversary possesses; ii) the necessity of attacks to keep stealth.

2) To quantify the likelihood of attacks, this paper conducts a risk probability interval with the robust and risk solutions by formulating a linear optimal problem with the fuzzy conditional probability table given by experts and scholars. It is meaningful to formulate security strategies more flexibly according to risk preferences.

3) To objectively assess the cross-space risk which is defined as the physical impact of cyberattacks [16], this paper proposes a physical impact metric which calculates and integrates the deviation of system states and measurements with a general linear state estimation model. The marginal effect of the attack is fully revealed which provides a broader and clearer insight of the system security situation.

The rest of this paper is organized as follows. Section II presents the IEC61850-based cyber-physical distribution system model and the integrated attack model with limited adversarial knowledge. Section III proposes the computational methods to describe the implementation and propagation process of attacks in a fuzzy BN. Section IV quantifies the cross-space risk by proposing a physical impact metric which integrates the system states and measurements biases. In Section V, a series of numerical experiments are conducted and further illustrations are presented. Finally, the concluding remarks are given in Section VI.

II. MODELS OF CYBER-PHYSICAL DISTRIBUTION SYSTEM AND INTEGRATED ATTACK

In this section, a hierarchical structure of cyber-physical distribution network according to IEC 61850 is established and its cybersecurity characteristics are analyzed here. Then, a complex attack scenario is considered and modeled.

A. MODEL OF CYBER-PHYSICAL DISTRIBUTION SYSTEM ACCORDING TO IEC 61850

According to the difference in devices and functions, the cyber-physical distribution network can be divided into three layers, i.e., the backbone layer, the access layer and the terminal layer. As shown in Fig. 1, the backbone layer is a pure cyber system, including the master distribution station system, supervisory control and data acquisition (SCADA) system and management information system (MIS), etc. The terminal layer is dominated by the distribution primary system, including circuit breaker (CB), section switch, voltage and current transformers, etc. Note that, the terminal layer contains the entire distribution primary system which includes power source, loads, primary devices, etc. However, we only point out the nodes for cyber and physical interaction, namely actuators and sensors, for the sake of simplicity. The access layer is the information hub of the entire system, as well as the core part of the interaction between information flow and energy flow. It can realize the fault diagnosis, isolation and recovery of the distribution network within the corresponding jurisdiction. Meanwhile, it is also the focus of this paper.

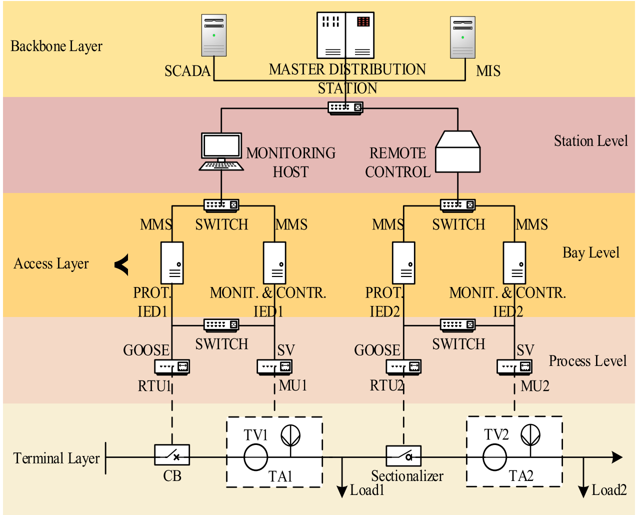


FIGURE 1. **Model of cyber-physical distribution system.**

In order to analyze the system structure of the access layer, i.e., slave distribution station in more detail, this paper constructs the corresponding automation system model according to the IEC61850 standards modeling method, and further divides the access layer into process level, bay level and station level. The data exchanged between the process level and the bay level includes two types. One is the real-time sampling data of voltage and current transformers, which are transmitted from bottom to top through the merging unit (MU); the other is the control data transmitted from top to bottom, e.g., tripping signal and switch position. The above-mentioned data are transmitted through the SV protocol and the GOOSE protocol, respectively. Data exchanged between bays, e.g., blocking control, is transmitted by GOOSE protocol or private protocol. The data exchanged between the bay level and the station level, e.g., protection settings, telemetry, etc., is transmitted through the MMS protocol. So far, the security concerns of the IEC 61850 standards mentioned above are all reflected in this model.

According to the model proposed in this paper, the attack can be launched from two perspectives. For an attack initiated from the top of the model, it generally constructs fake instructions by modifying the key parameters of the CBs or segment switches configuration files, and causes the mistake action and rejecting action of above-mentioned devices. Thereby, the distribution network would be disrupted and fall into trouble. This type of attack can usually be divided into three steps, i.e., 1) using security vulnerabilities of the monitoring host and remote interface to obtain corresponding control authority; 2) using protocol or message vulnerabilities to continuously penetrate and reach related IEDs; 3) interfering or destroying the normal function of IEDs to make the controlled physical devices run in an undesirable state, and disrupt the normal operation of the distribution network. On the other hand, if the attack begins with the power transformers which locate at the bottom of the model, it usually makes the real distribution network states invisible to the control center by tampering and interrupting the sensor data. Consequently, the issued control command will inevitably deviate from the actual demand which leads to the destruction of the distribution network.

B. DESCRIPTION OF SYSTEM STATE AND INTEGRATED ATTACK MODEL

Although the attack can be performed from different perspectives, the ultimate goals are either actuators or sensors. In addition, they are the crucial nodes of the interaction between cyber and physical system. Therefore, to reveal the essential features of cyber-physical interaction and cyber-attacks, it is reasonable to establish the attack model and describe the state of the system after being attacked from these two types of devices. First, for the purpose of simplicity, given the preliminary hypothesis that both the state-transition function and measurement function are linear, the distribution network state can be described as follows [22], [23]:

$$\boldsymbol{x}_{t+1} = \boldsymbol{A}\boldsymbol{x}_t + \boldsymbol{f}_t + \boldsymbol{\omega}_t \tag{1}$$

$$z_t = \boldsymbol{H}\boldsymbol{x}_t + \boldsymbol{v}_t \tag{2}$$

$$\boldsymbol{f}_t = \boldsymbol{B}\boldsymbol{u}_t + \boldsymbol{\delta}_t \tag{3}$$

where $\boldsymbol{x}_t \in \mathbb{R}^n$ represents the system state vector, e.g., voltage magnitudes and phase angles; $\boldsymbol{f}_t \in \mathbb{R}^n$ represents the control vector; $z_t \in \mathbb{R}^m$ represents the measurement vector, including pseudo-measurements, current phasors, etc.; $\boldsymbol{u}_t \in \mathbb{R}^n$ represents system inputs; $\boldsymbol{\delta}_t \in \mathbb{R}^n$ represents the additional inputs by using Holt's linear smoothing method; $\boldsymbol{A} \in \mathbb{R}^{n\times n}$ represents the transition matrix; $\boldsymbol{B} \in \mathbb{R}^{n\times n}$ represents a nonzero diagonal matrix; $\boldsymbol{H} \in \mathbb{R}^{m\times n}$ represents the system model matrix; $\boldsymbol{\omega}_t$ and $\boldsymbol{v}_t$ are usually zero mean Gaussian noise with covariance matrices $\boldsymbol{W}_t$ and $\boldsymbol{V}_t$, respectively.

In addition, common attack methods also include data integrity attacks and availability attacks. Taking the integrity attack on sensors as an example first. The adversary would try to modify the measurement vector z into z_{attack_int} by injecting false data $\boldsymbol{\zeta}_z$ (subscript is omitted for easier reading) [24]:

$$z_{attack\_int} = z + \boldsymbol{\zeta}_z \tag{4}$$

Considering that a successful attack requires the corrupted measurements to keep stealth to the bad data detection scheme which is built in energy management system (EMS), the attack vector $\boldsymbol{\zeta}_z$ should follow $\boldsymbol{\zeta}_z = \boldsymbol{Ha}$. Thus, the measurement vector with integrity attack z_{attack_int} can be written as:

$$z_{attack\_int} = \boldsymbol{H}\left(\boldsymbol{x} + \boldsymbol{a}\right) + \boldsymbol{v} \tag{5}$$

In practice, the data availability attacks, e.g., DoS attacks and jamming attacks are favored by attackers since the required resources are relatively few. Here, we introduce the availability attacks to sensors:

$$z_{attack\_avai} = diag(\boldsymbol{\xi}_z) \cdot (\boldsymbol{Hx} + \boldsymbol{v}) \tag{6}$$

where $\boldsymbol{\xi}_z \in \{0, 1\}^m$ and $\boldsymbol{\xi}_z(i) = 1$ represents that measurement i is unavailable. Note that, it is reasonable to assume that the availability attack would not trigger alerts in bad data detection because data loss is common for SCADA system.

Similarly, the attacks on the actuator can be described as:

$$\boldsymbol{x}_{attack\_int} = \boldsymbol{Ax} + \boldsymbol{B}\left(\boldsymbol{u} + \boldsymbol{b}\right) + \boldsymbol{\delta} + \boldsymbol{\omega} \tag{7}$$

$$\boldsymbol{x}_{attack\_avai} = \boldsymbol{Ax} + diag(\boldsymbol{\xi}_x) \cdot (\boldsymbol{Bu} + \boldsymbol{\delta} + \boldsymbol{\omega}) \tag{8}$$

Note that, the attack vector $\boldsymbol{\zeta}_x$ follows $\boldsymbol{\zeta}_x = \boldsymbol{Bb}$. In addition, the attack expression methods of actuator attacks and sensor attacks, i.e., the attack models are similar, but the attack paths are different. The actuator attacks are initiated from top to bottom and will directly affect the state of the distribution system with the actuator malfunctions or refusal to move. But the sensor attacks will first affect the system measurement data, and then make the actuator malfunctions or refuses to move due to the inability to obtain the real state of the system.

The current advanced cyber-attacks have evolved from a single target and attack method to a diversified development. In order to get closer to engineering reality, this paper sets up an attack scenario which integrates the attack targets, i.e., actuator and sensor with the attack methods, i.e., integrity attack and availability attack all together. The integrated attack model is shown as follows:

$$\boldsymbol{x}_{attack} = \boldsymbol{Ax} + diag(\boldsymbol{\xi}_x) \cdot [\boldsymbol{B}\left(\boldsymbol{u} + \boldsymbol{b}\right) + \boldsymbol{\delta} + \boldsymbol{\omega}] \tag{9}$$

$$z_{attack} = diag(\boldsymbol{\xi}_z) \cdot [\boldsymbol{H}\left(\boldsymbol{x} + \boldsymbol{a}\right) + \boldsymbol{v}] \tag{10}$$

Eq. (9) and (10) are built under a nature assumption that the adversary possesses full system knowledge, i.e., the topology of distribution network, the branch parameters, etc. In other words, details of the control matrix $\boldsymbol{B}$ and system matrix $\boldsymbol{H}$ have been known to the adversary. However, it is impossible for most cases due to well protection of system data in control center. Consequently, we can introduce the limited adversarial knowledge attack models by coupling parts of system model uncertainty $\Delta\boldsymbol{B}$ and $\Delta\boldsymbol{H}$. The integrated attack model is modified and shown as follows:

$$\boldsymbol{x}_{attack} = \boldsymbol{Ax} + diag(\boldsymbol{\xi}_x) \cdot \left[\widehat{\boldsymbol{B}}\left(\boldsymbol{u} + \boldsymbol{b}\right) + \boldsymbol{\delta} + \boldsymbol{\omega}\right] \tag{11}$$

$$z_{attack} = diag(\boldsymbol{\xi}_z) \cdot \left[\widehat{\boldsymbol{H}}\left(\boldsymbol{x} + \boldsymbol{a}\right) + \boldsymbol{v}\right] \tag{12}$$

$$\widehat{\boldsymbol{B}} \triangleq \boldsymbol{B} + \Delta\boldsymbol{B} \tag{13}$$

$$\widehat{\boldsymbol{H}} \triangleq \boldsymbol{H} + \Delta\boldsymbol{H} \tag{14}$$

where $\widehat{\boldsymbol{B}}$ and $\widehat{\boldsymbol{H}}$ represent the control matrix and system matrix, respectively, both are possessed by the adversary with limited knowledge.

III. CYBERSECURITY RISK PROPAGATION

This section develops the details of the cyberattack implementation and propagation process in cyber-physical distribution network which contains the availability of vulnerabilities and cybersecurity risk propagation.

A. THE AVAILABILITY OF VULNERABILITIES

Here, we define a successful attack or vulnerability exploitation is to compromise the measurement or control vector without triggering alerts in bad data detection. Therefore, the contradiction between attack stealth and resources saving always exists for adversary. From the perspective of the adversary, the security of the target system can be described as the ratio of the minimum consumption to the maximum consumption of launching a successful attack. The higher this value, the lower the security of the target system and the higher the availability of the corresponding vulnerabilities. To this end, this paper proposes a metric to quantify the availability of vulnerabilities and input it to the fuzzy BN as the prior probability:

$$P\left(Vul\right) = \gamma \big/ \chi \tag{15}$$

$$\chi = \left|\boldsymbol{\xi}_x\right| + \left|\boldsymbol{\xi}_z\right| + \left|\boldsymbol{\zeta}_x\right| + \left|\boldsymbol{\zeta}_z\right| \tag{16}$$

$$\gamma = \left\|\boldsymbol{\xi}_x\right\|_0 + \left\|\boldsymbol{\xi}_z\right\|_0 + \left\|\boldsymbol{\zeta}_x\right\|_0 + \left\|\boldsymbol{\zeta}_z\right\|_0 \tag{17}$$

where $|\cdot|$ represents the number of elements in attack vectors which equals to either the number of elements in the system state vector or the measurement vector; $\|\cdot\|_0$ represents the number of non-zero elements in attack vectors; χ represents the maximum consumption for a successful attack which is a constant in given system scenario; γ represents the minimum consumption for a successful attack which means the number of elements in measurement and control vectors that should be corrupted to keep stealth. $P\left(Vul\right)$ represents the availability of vulnerabilities. With the limited attack resources and stealth requirement, γ can be given by:

$$\min_{\boldsymbol{\xi}_x,\boldsymbol{\xi}_z,\boldsymbol{a},\boldsymbol{b}} \gamma = \left\|\boldsymbol{\xi}_x\right\|_0 + \left\|\boldsymbol{\xi}_z\right\|_0 + \left\|\boldsymbol{\zeta}_x\right\|_0 + \left\|\boldsymbol{\zeta}_z\right\|_0 \tag{18}$$

$$s.t.\ \boldsymbol{\zeta}_x = diag\left(\boldsymbol{\xi}_x\right) \cdot \widehat{\boldsymbol{B}}\boldsymbol{b} \tag{19}$$

$$\boldsymbol{\zeta}_z = diag\left(\boldsymbol{\xi}_z\right) \cdot \widehat{\boldsymbol{H}}\boldsymbol{a} \tag{20}$$

$$0 \le \boldsymbol{\zeta}_x\left(i\right) \le \alpha_{\max}, \quad \forall i \in \boldsymbol{\Gamma} \tag{21}$$

$$0 \le \boldsymbol{\zeta}_z\left(j\right) \le \beta_{\max}, \quad \forall j \in \boldsymbol{\Gamma} \tag{22}$$

$$\boldsymbol{\zeta}_z\left(l\right) = 0, \quad \forall l \in \boldsymbol{\Lambda} \tag{23}$$

$$\boldsymbol{\xi}_x\left(g\right) = \left\{0, 1\right\}, \quad \forall g \in \left\{1, 2, \cdots, n\right\} \tag{24}$$

$$\boldsymbol{\xi}_z\left(k\right) = \left\{0, 1\right\}, \quad \forall k \in \left\{1, 2, \cdots, m\right\} \tag{25}$$

$$\left\|\boldsymbol{\alpha}\right\|_1 + \left\|\boldsymbol{\beta}\right\|_1 = \Omega \tag{26}$$

where $\alpha_{\max}$ and $\beta_{\max}$ represent the maximum attack magnitude for measurements; $\boldsymbol{\Gamma}$ represents the set of attacked measurements; $\boldsymbol{\Lambda}$ represents the set of pseudo-measurements which cannot be attacked; Ω represents the total attack magnitude, i.e., the total attack resources. The mentioned problem is known as NP-hard to which is usually difficult to find accurate solutions. Thus, many heuristic algorithms are used to find approximate solutions, such as simulated annealing algorithm, while optimal greedy algorithm is also often used. In addition, it can be simplified by adding constraints to specific problems. In this paper, the big M method is performed to transform it as follows:

$$\min_{\boldsymbol{a},\boldsymbol{b},\boldsymbol{q},\boldsymbol{r},\boldsymbol{\xi}_x,\boldsymbol{\xi}_z} \gamma = \sum_{i=1}^{n} \boldsymbol{q}\left(i\right) + \sum_{j=1}^{m} \boldsymbol{r}\left(j\right) + \sum_{g=1}^{n} \boldsymbol{\xi}_x\left(g\right) + \sum_{k=1}^{m} \boldsymbol{\xi}_z\left(k\right) \tag{27}$$

$$s.t.\ \widehat{\boldsymbol{B}}\boldsymbol{b} \le M\left(\boldsymbol{q} + \boldsymbol{\xi}_x\right) \tag{28}$$

$$-\widehat{\boldsymbol{B}}\boldsymbol{b} \le M\left(\boldsymbol{q} + \boldsymbol{\xi}_x\right) \tag{29}$$

$$\widehat{\boldsymbol{H}}\boldsymbol{a} \le M\left(\boldsymbol{r} + \boldsymbol{\xi}_z\right) \tag{30}$$

$$-\widehat{\boldsymbol{H}}\boldsymbol{a} \le M\left(\boldsymbol{r} + \boldsymbol{\xi}_z\right) \tag{31}$$

$$0 \le \widehat{\boldsymbol{B}}\left(i, :\right)\boldsymbol{b} \le \alpha_{\max}, \quad \forall i \in \boldsymbol{\Gamma} \tag{32}$$

$$0 \le \widehat{\boldsymbol{H}}\left(j, :\right)\boldsymbol{a} \le \beta_{\max}, \quad \forall j \in \boldsymbol{\Gamma} \tag{33}$$

$$\widehat{\boldsymbol{H}}\left(l, :\right)\boldsymbol{a} = 0, \quad \forall l \in \boldsymbol{\Lambda} \tag{34}$$

$$\boldsymbol{q}\left(i\right) \in \left\{0, 1\right\}, \quad \forall i \in \left\{1, 2, \cdots, n\right\} \tag{35}$$

$$\boldsymbol{r}\left(j\right) \in \left\{0, 1\right\}, \quad \forall j \in \left\{1, 2, \cdots, m\right\} \tag{36}$$

$$\boldsymbol{\xi}_x\left(g\right) = \left\{0, 1\right\}, \quad \forall g \in \left\{1, 2, \cdots, n\right\} \tag{37}$$

$$\boldsymbol{\xi}_z\left(k\right) = \left\{0, 1\right\}, \quad \forall k \in \left\{1, 2, \cdots, m\right\} \tag{38}$$

$$\left\|\boldsymbol{\alpha}\right\|_1 + \left\|\boldsymbol{\beta}\right\|_1 = \Omega \tag{39}$$

where $\boldsymbol{q}\left(i\right) = 1$ and $\boldsymbol{r}\left(j\right) = 1$ represent the integrity attack on control and measurement vectors, respectively.

B. CYBERSECURITY RISK PROPAGATION

The BN which describes variables and their conditional dependencies with a directed acyclic graph is widely used as propagation model for cybersecurity risk. Given a set of variables $\boldsymbol{Y} = \left\{Y_1, Y_2, \cdots, Y_N\right\}$ which are the Logical Nodes (LNs) [25] in this paper, the joint probability distribution of $\boldsymbol{Y}$ is shown as follows:

$$P\left(\boldsymbol{Y}\right) = P\left(Y_1, Y_2, \cdots, Y_N\right) = \prod_{i \in N} p\left(Y_i \left|\boldsymbol{\pi}_i\right.\right) \tag{40}$$

where $\boldsymbol{\pi}_i$ represents the parent set of Y_i; Y_i has two states, i.e., T for attack success and F for attack failure. Note that, each LN represents the smallest part of a function that exchanges data and may reside logically in one or more physical devices. An example of LNs data exchanging for a typical function is shown in Fig. 2 and more details can be found in [25].

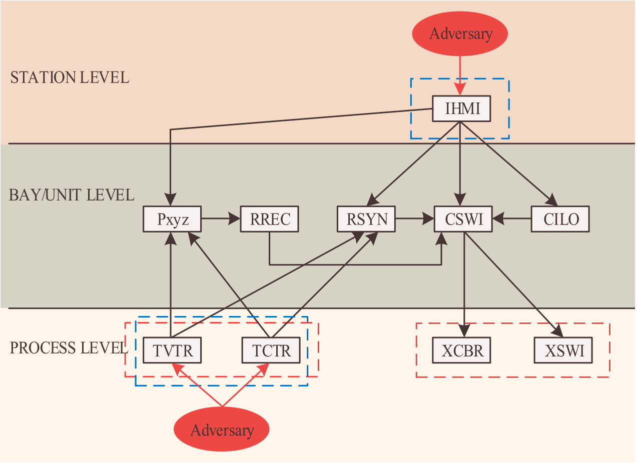


FIGURE 2. Attack graph for IEC 61850 based.

As it can be seen from Fig.2, BN is not suitable for cybersecurity risk propagation modeling directly in IEC 61850 based cyber-physical distribution system since the following issues have not been solved, i.e., i) the complexity of exact inference in BN increases exponentially with the topology of network; ii) the insufficient accurate prior knowledge about risk propagation cannot support for estimation of conditional probability table.

Therefore, this paper presents a fuzzy BN to conduct a fuzzy conditional probability. Specifically, it contains the following steps.

1) DETERMINING A GROUP OF LINGUISTIC PROBABILITIES

The set of linguistic probabilities contains words, e.g., high, neutral, low, etc. which imply fuzzy probabilities and can be represented as $S = \left\{s_1, s_2, \cdots, s_M\right\}, \forall s_m \in \left[\underline{s}_m, \bar{s}_m\right]$. Particularly, the certainty decreases as the subscript increases.

2) DETERMINING THE DEGREE OF MEMBERSHIP

The degree of membership for Y_i locating at the m_th linguistic probability can be represented as $\phi_{im}(Y_i)$. To obtain the degree of membership, we need to build an expert team with more than 10 people [14] to define the linguistic probabilities for each LN. Thus, the degree of membership for Y_i can be calculated by:

$$\phi_{im} = Num_{s_m} \big/ Num_{total} \tag{41}$$

where Num_{s_m} represents the number of experts who select linguistic probability s_m; Num_{total} represents the total number of experts.

3) OBTAINING THE FUZZY CONDITIONAL PROBABILITY

To avoid the information loss during the procedure of mapping the fuzzy conditional probability to the crisp conditional probability, this paper proposes the following linear optimization model to obtain the upper and lower bounds of the fuzzy conditional probabilities:

$$\bar{p}(Y_i|\boldsymbol{\pi}_i) = \max_{\tilde{s}_m} \sum_{m=1}^{M} \phi_{im}\tilde{s}_m \tag{42}$$

$$\underline{p}(Y_i|\boldsymbol{\pi}_i) = \min_{\tilde{s}_m} \sum_{m=1}^{M} \phi_{im}\tilde{s}_m \tag{43}$$

$$s.t.\ \underline{s}_m \le \tilde{s}_m \le \bar{s}_m, \quad \forall m \in \boldsymbol{M} \tag{44}$$

$$\sum_{m=1}^{M} \phi_{im} = 1 \tag{45}$$

Consequently, we can obtain the upper and lower bounds of the joint probability with:

$$\bar{P}(\boldsymbol{Y}) = \bar{P}(Y_1, Y_2, \cdots, Y_N) = \prod_{i \in N} \bar{p}(Y_i|\boldsymbol{\pi}_i) \tag{46}$$

$$\underline{P}(\boldsymbol{Y}) = \underline{P}(Y_1, Y_2, \cdots, Y_N) = \prod_{i \in N} \underline{p}(Y_i|\boldsymbol{\pi}_i) \tag{47}$$

Here, we define $\bar{P}(\boldsymbol{Y})$ as the robust solution which refers to the most severe result of risk assessment once the physical impact is fixed and the highest level of security protection measures should be taken. In addition, $P(\boldsymbol{Y})$ is defined as the risk solution that refers to the lightest assessment result and corresponding protection measures. With the interval of attack likelihood, the system risk can be reflected more comprehensively, and security protection strategies can be formulated more flexibly according to risk preferences.

IV. CROSS-SPACE RISK ASSESSMENT

The quantitative risk is generally assessed as the likelihood of attack multiplied by the potential attack impact [26]. This paper further clarifies that the cross-space risk assessment is the potential impact in physical space under cyberattacks which are initiated from cyber space, which can be shown as follows:

$$R = P(\boldsymbol{Y}) \times L(\boldsymbol{Y}) \tag{48}$$

where $P(\boldsymbol{Y})$ represents the likelihood of cyberattacks; $L(\boldsymbol{Y})$ represents the potential impact in physical space under cyberattacks.

The system state information and measurements are further applied to conduct optimal control strategies, that means they would affect the further operations of the system. Once the attacks take place and succeed, the system state and measurements get perturbed. Thus, we design an impact metric which is a function of the deviations on these two indices. First of all, we consider the deviation on measurements.

$$\boldsymbol{\psi}_z = \hat{z}_{attack} - z \tag{49}$$

where $\hat{z}_{attack}$ represents the estimated measurement vector under an integrated attack; z represents the measurement vector without attack. Generally, for Eq. (2), the estimation results $\hat{\boldsymbol{x}}$ and $\hat{z}$ can be obtained with weighted least squares (WLS) criterion which are shown as follows:

$$\hat{\boldsymbol{x}} = \arg\min_{\boldsymbol{x}} (z - \boldsymbol{H}\boldsymbol{x})^T \boldsymbol{V}^{-1} (z - \boldsymbol{H}\boldsymbol{x}) \tag{50}$$

$$\hat{\boldsymbol{x}} = \left(\boldsymbol{H}^T\boldsymbol{V}^{-1}\boldsymbol{H}\right)^{-1} \boldsymbol{H}^T\boldsymbol{V}^{-1}z = \boldsymbol{K}z \tag{51}$$

$$\hat{z} = \boldsymbol{H}\hat{\boldsymbol{x}} = \boldsymbol{H}\boldsymbol{K}z \tag{52}$$

The system state vector under the integrated attack, i.e., $\hat{\boldsymbol{x}}_{attack}$ can be described as follows:

$$\hat{\boldsymbol{x}}_{attack} = \boldsymbol{K}_{z\_avai} z_{attack} = \boldsymbol{x} + \boldsymbol{K}_{z\_avai}\left(\boldsymbol{\upsilon}_{avai} + \boldsymbol{\zeta}_z\right) \tag{53}$$

$$\boldsymbol{K}_{z\_avai} = \left(\boldsymbol{H}_{avai}^T\boldsymbol{V}^{-1}\boldsymbol{H}_{avai}\right)^{-1} \boldsymbol{H}_{avai}^T\boldsymbol{V}^{-1} \tag{54}$$

$$\boldsymbol{\upsilon}_{avai} = diag(\boldsymbol{\xi}_z)\boldsymbol{\upsilon} \tag{55}$$

$$\boldsymbol{H}_{avai} = diag(\boldsymbol{\xi}_z)\boldsymbol{H} \tag{56}$$

Thus, the deviation of measurement vector can be obtained by substituting Eq. (52) – (53) into Eq. (49).

$$\boldsymbol{\psi}_z = \boldsymbol{H}\boldsymbol{K}_{z\_avai}\left(\boldsymbol{\upsilon}_{avai} + \boldsymbol{\zeta}_z\right) \tag{57}$$

Similarly, we can derive the deviation of the system state vector with the above-mentioned method. However, we need to rewrite Eq. (9) first since the focus is on the control vector:

$$\boldsymbol{\lambda}_{attack} = \boldsymbol{x}_{attack} - \boldsymbol{A}\boldsymbol{x} = diag(\boldsymbol{\xi}_x) \cdot [\boldsymbol{B}(\boldsymbol{u}+\boldsymbol{b})+\boldsymbol{\delta}+\boldsymbol{\omega}] \tag{58}$$

Then, the modified deviation of system state vector can be developed as follows:

$$\boldsymbol{\psi}_x = \hat{\boldsymbol{\lambda}}_{attack} - \boldsymbol{\lambda} \tag{59}$$

$$\boldsymbol{\psi}_x = \boldsymbol{B}\boldsymbol{K}_{x\_avai}\left(\boldsymbol{\kappa}_{avai} + \boldsymbol{\zeta}_x\right) \tag{60}$$

$$\boldsymbol{K}_{x\_avai} = \left(\boldsymbol{B}_{avai}^T\boldsymbol{W}^{-1}\boldsymbol{B}_{avai}\right)^{-1} \boldsymbol{B}_{avai}^T\boldsymbol{W}^{-1} \tag{61}$$

$$\boldsymbol{\kappa}_{avai} = diag(\boldsymbol{\xi}_x)(\boldsymbol{\delta} + \boldsymbol{\omega}) \tag{62}$$

$$\boldsymbol{B}_{avai} = diag(\boldsymbol{\xi}_x)\boldsymbol{B} \tag{63}$$

Finally, to take physical impacts from both actuators and sensors into consideration, this paper integrates $\boldsymbol{\psi}_z$ and $\boldsymbol{\psi}_x$ through Eq. (2):

$$\begin{aligned}\boldsymbol{\varepsilon} &= \boldsymbol{\psi}_z + \boldsymbol{H}\boldsymbol{\psi}_x \\ &= \boldsymbol{H}\boldsymbol{K}_{z\_avai}\left(\boldsymbol{\upsilon}_{avai} + \boldsymbol{\zeta}_z\right) + \boldsymbol{H}\boldsymbol{B}\boldsymbol{K}_{x\_avai}\left(\boldsymbol{\kappa}_{avai} + \boldsymbol{\zeta}_x\right)\end{aligned} \tag{64}$$

The expected value of $\boldsymbol{\varepsilon}$ is:

$$E\left(\boldsymbol{\varepsilon}\right) = \boldsymbol{HK}_{z\_avai}\boldsymbol{\zeta}_{\boldsymbol{z}} + \boldsymbol{HBK}_{x\_avai}\boldsymbol{\zeta}_{\boldsymbol{x}} \tag{65}$$

Furthermore, we define the physical impact metric as the 2-norm of $E\left(\boldsymbol{\varepsilon}\right)$ under the integrated attack:

$$L\left(\boldsymbol{Y}\right) = \left\|\boldsymbol{HK}_{z\_avai}\boldsymbol{\zeta}_{\boldsymbol{z}} + \boldsymbol{HBK}_{x\_avai}\boldsymbol{\zeta}_{\boldsymbol{x}}\right\|_2 \tag{66}$$

Specifically, with the given information, model and inference, the cross-space risk assessment procedure under integrated cyber-attacks has been summarized and the pseudo-code is presented below.

Algorithm 1 Cross-Space Risk Assessment

```
1: Input: cyber-physical distribution system topology, LNs, logical connections
2: Initialize: the control matrix $\boldsymbol{B}$, the system matrix $\boldsymbol{H}$, Gaussian noise $\boldsymbol{\omega}$ and $\boldsymbol{\upsilon}$, the attack magnitude $\alpha_{\max}$, $\beta_{\max}$ and $\Omega$, the model uncertainty $\Delta\boldsymbol{B}$ and $\Delta\boldsymbol{H}$.
3: Calculate vectors $\boldsymbol{\xi}_{\boldsymbol{x}}$, $\boldsymbol{\xi}_{\boldsymbol{z}}$, $\boldsymbol{\zeta}_{\boldsymbol{x}}$, $\boldsymbol{\zeta}_{\boldsymbol{z}}$ with the optimization problem Eq. (27) - (39). Note that, the constraints related to $\boldsymbol{\zeta}_{\boldsymbol{x}}$ and $\boldsymbol{\zeta}_{\boldsymbol{z}}$, i.e., Eq. (19) - (23) have been converted to Eq. (27) – (36) with the big M method. Thus, the integrity attack vectors $\boldsymbol{\zeta}_{\boldsymbol{x}}$ and $\boldsymbol{\zeta}_{\boldsymbol{z}}$are converted to $\boldsymbol{q} \in \{0, 1\}^n$ and $\boldsymbol{r} \in \{0, 1\}^m$, respectively.
4: Calculate the availability of vulnerabilities $P\left(Vul\right)$ as the input of the fuzzy BN.
5: Establish the fuzzy conditional probability table with experts and calculate the robust and risk solutions of joint probability with Eq. (41) - (47).
6: Calculate the physical impact metric $L\left(\boldsymbol{Y}\right)$ according to Eq. (66).
7: Calculate the cross-space risk $R$ under the integrated attack with Eq. (48).
8: Output: The cross-space risk $R$.
```

V. CASE STUDY

In this section, we apply the proposed cross-space risk assessment method to IEEE33-node system [27] and validate its effectiveness. The conducted simulations respect to the following preliminaries: i) The CBs and section switches on a feeder line are controlled by the same slave distribution station, and the corresponding control logic of all switch devices is the same; ii) measurements are placed on each bus; iii) buses 4, 9, 14, 19, 23, 26, 31 are treated as zero-injection buses which possess pseudo measurements and cannot be attacked. Specifically, the topology of test system is shown in Fig. 3. The adversary can obtain the exact system topology while the line parameters are under different uncertainty. Here, the slave distribution station 1 is selected as the attack object.

A. THE AVAILABILITY OF VULNERABILITIES

To quantify the availability of vulnerabilities of IEC 61850 based distribution network under integrated attack, this paper determines the γ with Eq. (28) – (40) first and the simulation results are shown in Fig. 4.

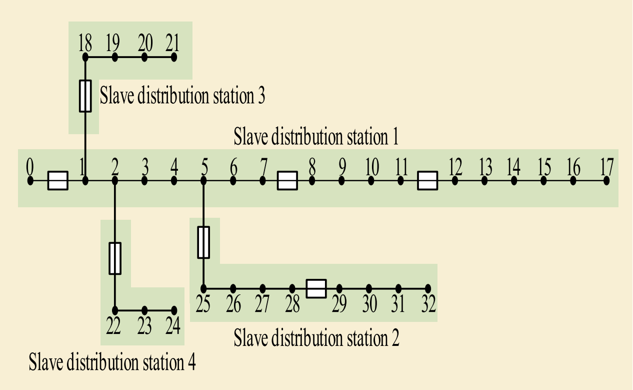

18 19 20 21
Slave distribution station 3
Slave distribution station 1
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
25 26 27 28 29 30 31 32
Slave distribution station 2
22 23 24
Slave distribution station 4

FIGURE 3. IEEE33-node system.

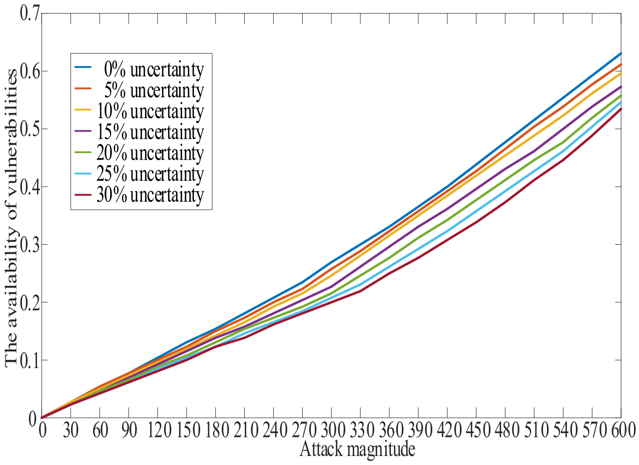


FIGURE 4. The availability of vulnerabilities with limited knowledge.

It can be seen from Fig. 4, given a degree of uncertainty, the availability of vulnerabilities increases with the attack magnitude. For instance, it is enhanced from 0 to 63.08% when the attack magnitude is increased from 0 to 600 under the fixed uncertainty 0%. Note that, the attack magnitude is dimensionless. In addition, no matter how the uncertainty degree changes, the availability of vulnerabilities always possesses the positive relationship with the attack magnitude which is not against intuition and illustrates the proposed method is effective. Besides, this paper also develops case studies under different degrees of uncertainty. The results show that once the attack magnitude is fixed, the availability of vulnerabilities reduces with the heightened uncertainty. In other words, the limited system knowledge will reduce the adversary's ability to attack. Here, we also find another interesting phenomenon, i.e., there is an obvious turning point in the rise of the availability of vulnerabilities. In other words, when the attack magnitude is less than a certain value, the attack effect is relatively poor due to the insufficient attack resources. The availability of vulnerabilities rises slowly.

But once the attack magnitude rises to a certain level, the flexibility of attack resource allocation becomes higher. To this end, the better the attack effect, the higher the availability of vulnerabilities rises. Moreover, as the uncertainty of the system rises, this turning point continues to move toward the direction of increasing attack magnitude. In other words, a higher magnitude attack is needed to compensate for the impact, i.e., the uncertainty of the system weakens the adversary's ability to attack. Thus, the effectiveness of proposed method for quantifying the availability of vulnerabilities is further validated.

B. LIKELIHOOD OF ATTACK IN FUZZY BN

With the attack graph which is given in Section III, this part calculates likelihood of cyber-attack in fuzzy BN. Firstly, the full names and symbols of LNs are shown in TABLE 1. The prior probabilities are conducted in part. A, i.e., the availability of vulnerabilities. In addition, this paper summaries the evaluation results of 12 experts and scholars in the field on the association relationship of LNs in IEC 61850 based slave distribution station. The fuzzy conditional probabilities are shown in TABLE 2. Note that, 0 represents attack failure while 1 represents attack success.

TABLE 1. Function name and number of logical node.

Logical node	Full name	Symbol
IHMI	Human Machine Interface	A
Pxyz	Protection Functions	B
RREC	Automatic Reclosing	C
RSNY	Synchronism-Check	D
CSWI	Switch Controller	E
CILO	Interlocking Bay/Station	F
TVTR	Voltage Transformer	G
TCTR	Current Transformer	H
XCBR	Circuit Breaker	I
XSWI	Switch	J

Specifically, the fuzzy conditional probabilities are calculated by the optimization model of Eq. (43) – (46) with the given evaluation results. Then, the robust and risk solutions of joint probabilities are conducted with Eq. (47) – (48). The risk probability intervals under different attack magnitudes and system uncertainties are shown in Fig. 5. It can be seen that as the attack magnitude increases, both robust solution and risk solution of attack likelihood show a significant upward trend under a given system uncertainty. Secondly, as the system uncertainty rises, the likelihood of attack gradually develops in a direction that is beneficial to the defender and shows a downward trend. In addition, Fig. 5 shows that the increase of attack resources which is reflected in the increase of attack magnitude will significantly enforce attack flexibility to lead to the expansion of the risk probability interval, which is not conducive to the defender to make protection decision. The consistency of the results in multiple simulations shows that the method to calculate the likelihood of attack based on the fuzzy BN proposed in this paper is effective.

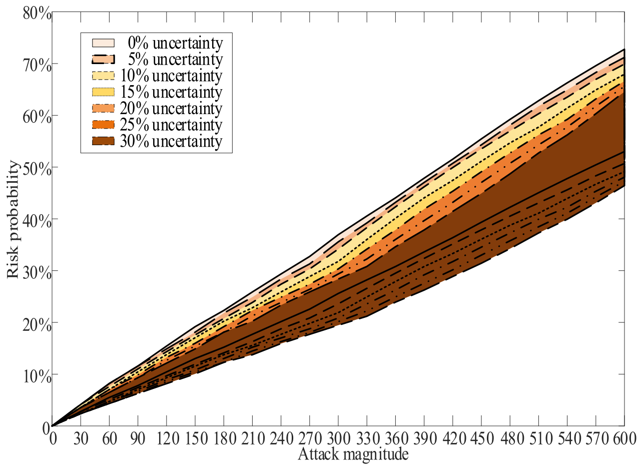


FIGURE 5. The risk probability intervals.

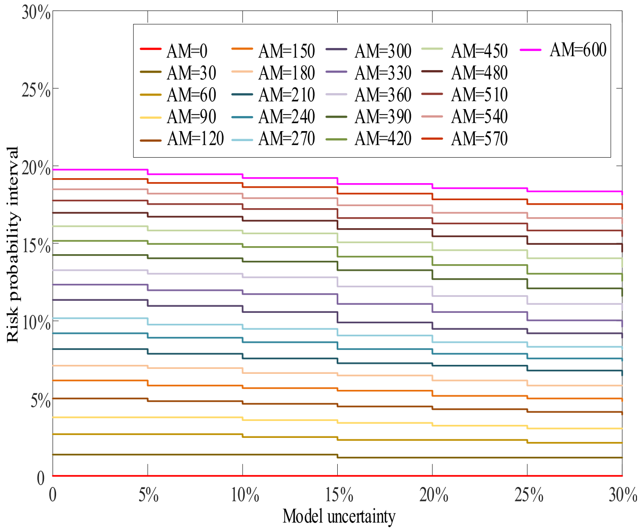


FIGURE 6. The width of the risk probability interval.

Furthermore, in the case of a given attack magnitude, the width of the risk probability interval is negatively correlated with system uncertainty. That is to say, the less system knowledge the adversary possesses, the better it is for the defender to recognize the security situation of the system. This conclusion is consistent with the aforementioned experimental results, and further proves the effectiveness of the method proposed in this paper.

C. CROSS-SPACE RISK ANALYSIS

To validate the effectiveness of the proposed cross-space risk assessment method and analyze the system security situation, this part calculates the system risk range with Eq. (66) and (48). Firstly, we develop the system cross-space risk assessment under 0% system uncertainty and the result is shown in Fig. 7.

It can be seen from Fig. 7 that the risk of system is increasing with the attack magnitude and the risk range is larger as well. The overall system security situation is developing in a direction that is not conducive to defenders. This validates

TABLE 2. Expert evaluation summary table.

Event	Conditional probability	Fuzzy probability (%)									
		100~90	90~80	80~70	70~60	60~50	50~40	40~30	30~20	20~10	10~0
$P(B=1\|A=0,G=0,H=1)$	15.00~25.00%								6	6	
$P(B=1\|A=0,G=1,H=0)$	17.50~27.50%							1	7	4	
$P(B=1\|A=0,G=1,H=1)$	25.00~35.00%						1	5	5	1	
$P(B=1\|A=1,G=0,H=0)$	80.00~90.00%	3	7	1	1						
$P(B=1\|A=1,G=0,H=1)$	81.67~91.67%	3	8	1							
$P(B=1\|A=1,G=1,H=0)$	83.33~93.33%	4	8								
$P(B=1\|A=1,G=1,H=1)$	89.17~99.17%	11	1								
$P(C=1\|B=1)$	84.17~94.17%	7	3	2							
$P(D=1\|A=0,G=0,H=1)$	5.83~15.83%								2	3	7
$P(D=1\|A=0,G=1,H=0)$	4.17~14.17%								1	3	8
$P(D=1\|A=0,G=1,H=1)$	6.67~16.67%							1	1	3	7
$P(D=1\|A=1,G=0,H=0)$	77.50~87.50%	1	7	4							
$P(D=1\|A=1,G=0,H=1)$	79.17~89.17%	1	9	2							
$P(D=1\|A=1,G=1,H=0)$	80.83~90.83%	2	9	1							
$P(D=1\|A=1,G=1,H=1)$	89.17~99.17%	11	1								
$P(E=1\|A=0,C=0,D=0,F=1)$	37.50~47.50%						9	3			
$P(E=1\|A=0,C=0,D=1,F=0)$	25.00~35.00%							7	4	1	
$P(E=1\|A=0,C=0,D=1,F=1)$	38.33~48.33%					1	8	3			
$P(E=1\|A=0,C=1,D=0,F=0)$	48.33~58.33%					10	2				
$P(E=1\|A=0,C=1,D=0,F=1)$	59.17~69.17%			2	7	3					
$P(E=1\|A=0,C=1,D=1,F=0)$	53.33~63.33%				4	8					
$P(E=1\|A=0,C=1,D=1,F=1)$	65.83~75.83%		2	5	3	2					
$P(E=1\|A=1,C=0,D=0,F=0)$	55.83~65.83%			2	4	5	1				
$P(E=1\|A=1,C=0,D=0,F=1)$	70.83~80.83%		4	6	1	1					
$P(E=1\|A=1,C=0,D=1,F=0)$	70.00~80.00%		4	5	2	1					
$P(E=1\|A=1,C=0,D=1,F=1)$	79.17~89.17%	6	2	2	1	1					
$P(E=1\|A=1,C=1,D=0,F=0)$	71.67~81.67%		4	6	2						
$P(E=1\|A=1,C=1,D=0,F=1)$	83.33~93.33%	7	3	1	1						
$P(E=1\|A=1,C=1,D=1,F=0)$	82.50~92.50%	7	2	2	1						
$P(E=1\|A=1,C=1,D=1,F=1)$	90.00~100.00%	12									
$P(F=1\|A=1)$	84.17~94.17%	6	5	1							
$P(I=1\|E=1)$	89.17~99.17%	11	1								
$P(J=1\|E=1)$	87.50~97.50%	10	1	1							

that the proposed method is effective. Specifically, the risk situation of system can be divided into three stages, i.e., i) When the attack magnitude is between 0 to 240, the system risk rises slowly due to the limited attack resources and robustness of system. The adversary can only cause less damage to the control and measurement vectors; ii) The system risk rises significantly faster while the attack magnitude is between 240 to 450 which illustrates that the adversary can flexibly allocate attack resources when they are relatively abundant and the control and measurement vectors are compromised in a large area; iii) The system risk growth slows down when the attack magnitude is greater than 450 due to the marginal effect of attack because the control and measurement vectors are already perturbed significantly. It is difficult to increase the system risk further linearly even if the attack magnitude is reinforced.

Moreover, this paper also conducts the system cross-space risk assessment under different system uncertainties and the results are shown in Fig. 8. The positive correlation between system risk and attack magnitude is always the same while the system uncertainty changes. At the same time, the risk growth rate is also slow first and then become fast, and the turning point moves in the direction of increasing attack magnitude as the uncertainty of the system rises. In summary, the cross-space risk assessment method for IEC 61850 based cyber-physical distribution system proposed in this paper is

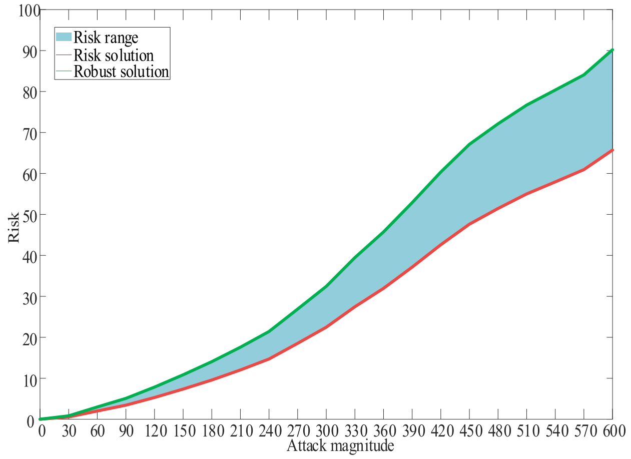
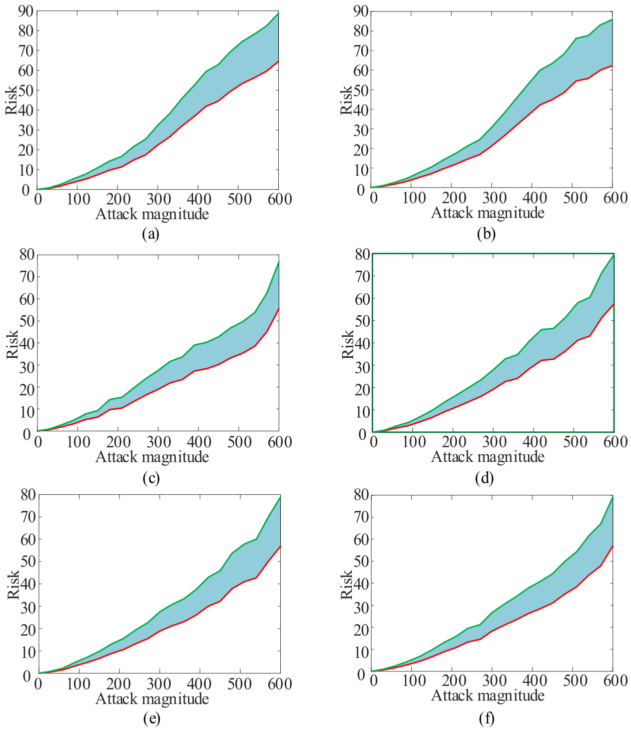


FIGURE 7. The cross-space risk under full knowledge.



(a)

(b)

(c)

(d)

(e)

(f)

FIGURE 8. The cross-space risk under different system uncertainty: (a) 5% uncertainty; (b) 10% uncertainty; (c) 15% uncertainty; (d) 20% uncertainty; (e) 25% uncertainty; (f) 30% uncertainty.

effective and can clearly reveal the relationship between system risk and attack resources and their dynamic development trend.

VI. CONCLUSION

This paper establishes a cross-space risk assessment method with fuzzy BN and system state estimation for IEC 61850 based cyber-physical distribution system and takes the integrated attack and limited adversary knowledge into consideration. The simulation results show that the system cross-space risk is positively correlated with attack magnitude and negatively correlated with system uncertainty, i.e., the limited adversary knowledge, and the proposed method is effective. Furthermore, with the proposed method, the marginal effect of the attack is fully revealed which provides a broader and clearer perspective to help the defender to understand the system security situation. Third, by developing the risk range which is composed by the robust and risk solutions proposed in this paper, the defender can formulate security strategies more flexibly according to risk preferences. Future work will focus on building a hardware-in-the-loop simulation platform to further verify the effectiveness of the proposed method.

REFERENCES

[1] A. Sundararajan, T. Khan, A. Moghadasi, and A. I. Sarwat, "Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies," *J. Mod. Power Syst. Clean Energy*, vol. 7, no. 3, pp. 449–467, May 2019.

[2] S. Soltan, M. Yannakakis, and G. Zussman, "REACT to cyber attacks on power grids," *IEEE Trans. Netw. Sci. Eng.*, vol. 6, no. 3, pp. 459–473, Jul./Sep. 2019.

[3] Q. Dai, L. Shi, and Y. Ni, "Risk assessment for cyberattack in active distribution systems considering the role of feeder automation," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 3230–3240, Jul. 2019.

[4] *Power Systems Management and Associated Information Exchange-Data and Communications Security—Part 6: Security for IEC 61850*, IEC Standard 62351-6, Jun. 2007.

[5] J. G. Wright and S. D. Wolthusen, "Stealthy injection attacks against IEC61850's GOOSE messaging service," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. Eur. (ISGT-Europe)*, Sarajevo, Bosnia and Herzegovina, Oct. 2018, pp. 1–6.

[6] J. O'Raw, D. M. Laverty, and D. J. Morrow, "IEC 61850 substation configuration language as a basis for automated security and SDN configuration," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Chicago, IL, USA, Jul. 2017, pp. 1–5.

[7] Z. Liu and L. Wang, "Leveraging network topology optimization to strengthen power grid resilience against cyber-physical attacks," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1552–1564, Mar. 2021.

[8] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in distributed power systems," *Proc. IEEE*, vol. 105, no. 7, pp. 1367–1388, Jul. 2017.

[9] B. Cai, X. Kong, Y. Liu, J. Lin, X. Yuan, H. Xu, and R. Ji, "Application of Bayesian networks in reliability evaluation," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2146–2157, Apr. 2019.

[10] P. Mahmoudi-Nasr, "Toward modeling alarm handling in SCADA system: A colored Petri nets approach," *IEEE Trans. Power Syst.*, vol. 34, no. 6, pp. 4525–4532, Nov. 2019.

[11] R. Kateb, M. H. K. Tushar, C. Assi, and M. Debbabi, "Optimal tree construction model for cyber-attacks to wide area measurement systems," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 25–34, Jan. 2018.

[12] A. T. A. Ghazo, M. Ibrahim, H. Ren, and R. Kumar, "A2G2V: Automatic attack graph generation and visualization and its applications to computer and SCADA networks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 10, pp. 3488–3498, Oct. 2020.

[13] H. S. Lallie, K. Debattista, and J. Bal, "An empirical evaluation of the effectiveness of attack graphs and fault trees in cyber-attack perception," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 5, pp. 1110–1122, May 2018.

[14] Q. Zhang, C. Zhou, Y.-C. Tian, N. Xiong, Y. Qin, and B. Hu, "A fuzzy probability Bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2497–2506, Jun. 2018.

[15] Z. Zeng and E. Zio, "Dynamic risk assessment based on statistical failure data and condition-monitoring degradation data," *IEEE Trans. Rel.*, vol. 67, no. 2, pp. 609–622, Jun. 2018.

[16] K. Huang, C. Zhou, Y. Tian, S. Yang, and Y. Qin, "Assessing the physical impact of cyberattacks on industrial cyber-physical systems," *IEEE Trans. Ind. Electron.*, vol. 65, no. 10, pp. 8153–8162, Oct. 2018.

[17] W. Zhu, M. Han, J. V. Milanović, and P. Crossley, "Methodology for reliability assessment of smart grid considering risk of failure of communication architecture," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 4358–4365, Sep. 2020.

[18] V. Venkataramanan, A. Hahn, and A. Srivastava, "CP-SAM: Cyber-physical security assessment metric for monitoring microgrid resiliency," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1055–1065, Mar. 2020.

[19] X. Li, C. Zhou, Y.-C. Tian, N. Xiong, and Y. Qin, "Asset-based dynamic impact assessment of cyberattacks for risk analysis in industrial control systems," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 608–618, Feb. 2018.

[20] L. Che, X. Liu, Z. Shuai, and J. Zhao, "The impact of ramp-induced data attacks on power system operational security," *IEEE Trans. Ind. Informat.*, vol. 15, no. 9, pp. 5064–5075, Sep. 2019.

[21] A. K. Srivastava, T. A. Ernster, R. Liu, and V. G. Krishnan, "Graph-theoretic algorithms for cyber-physical vulnerability analysis of power grid with incomplete information," *J. Mod. Power Syst. Clean Energy*, vol. 6, no. 5, pp. 887–899, Sep. 2018.

[22] J. Zhao, J. Qi, Z. Huang, A. P. S. Meliopoulos, A. Gomez-Exposito, M. Netto, L. Mili, A. Abur, V. Terzija, I. Kamwa, B. Pal, and A. K. Singh, "Power system dynamic state estimation: Motivations, definitions, methodologies, and future work," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 3188–3198, Jul. 2019.

[23] A. L. da Silva, M. B. D. C. Filho, and J. F. de Queiroz, "State forecasting in electric power systems," *IEE Proc. C, Generat., Transmiss. Distrib.*, vol. 130, no. 5, pp. 237–244, 1983.

[24] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, "Cyber risk analysis of combined data attacks against power system state estimation," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3044–3056, May 2019.

[25] *Communication Networks and Systems in Substations—Part 5: Communication Requirements for Functions and Device Models*, IEC Standard 61850-5, 2003.

[26] R. S. Ross, "Guide for conducting risk assessments," NIST, Gaithersburg, MD, USA, Tech. Rep. SP 800-30 Rev. 1, Sep. 2012.

[27] M. E. Baran and F. F. Wu, "Network reconfiguration in distribution systems for loss reduction and load balancing," *IEEE Trans. Power Del.*, vol. 4, no. 2, pp. 1401–1407, Apr. 1989.

JIE YANG received the B.S. and M.S. degrees in electrical engineering from Central South University, Changsha, China, in 2015 and 2018, respectively. He is currently pursuing the Ph.D. degree with the College of Electrical Engineering, Zhejiang University.

His research interests include smart grid cyber security and smart grid reliability.

YIHAO GUO received the B.S. degree in electrical engineering from Wuhan University, Wuhan, China, in 2017. He is currently pursuing the Ph.D. degree with the College of Electrical Engineering, Zhejiang University, Hangzhou, China.

His research interests include cyber physical power systems and power system operation.

CHUANGXIN GUO (Senior Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical engineering from the Huazhong University of Science and Technology, China, in 1992, 1994, and 1997, respectively.

He is currently a Professor with the College of Electrical Engineering, Zhejiang University, Hangzhou, China. Prior to joining Zhejiang University, he was the Director of Beijing Dongfang Electronics Research Institute. His research interests include power system operation and planning, and power systems information and communication technologies.

ZHE CHEN received the B.S. and Ph.D. degrees from the College of Electrical Engineering, Zhejiang University, Hangzhou, China, in 2016 and 2021, respectively.

He is currently an Engineer with the Electric Power Research Institute, State Grid Zhejiang Electric Power Company. His research interests include power system operation and planning, renewable integration, and microgrids.

SHENGHAN WANG received the B.S. degree in electrical engineering from South China University of Technology, Guangzhou, China, in 2018. He is currently pursuing the Ph.D. degree with the College of Electrical Engineering, Zhejiang University, Hangzhou, China.

His research interests include integrated energy system optimization and blockchain technology.