Security Risk Assessment and Risk-oriented Defense Resource Allocation for Cyber-physical Distribution Networks Against Coordinated Cyber Attacks

Shuheng Wei, Zaijun Wu, Junjun Xu, Yanzhe Cheng, and Qinran Hu

***Abstract*—With the proliferation of advanced communication technologies and the deepening interdependence between cyber and physical components, power distribution networks are subject to miscellaneous security risks induced by malicious attackers. To address the issue, this paper proposes a security risk assessment method and a risk-oriented defense resource allocation strategy for cyber-physical distribution networks (CPDNs) against coordinated cyber attacks. First, an attack graph-based CPDN architecture is constructed, and representative cyber-attack paths are drawn considering the CPDN topology and the risk propagation process. The probability of a successful coordinated cyber attack and incurred security risks are quantitatively assessed based on the absorbing Markov chain model and National Institute of Standards and Technology (NIST) standard. Next, a risk-oriented defense resource allocation strategy is proposed for CPDNs in different attack scenarios. The trade-off between security risk and limited resource budget is formulated as a multi-objective optimization (MOO) problem, which is solved by an efficient optimal Pareto solution generation approach. By employing a generational distance metric, the optimal solution is prioritized from the optimal Pareto set of the MOO and leveraged for subsequent atomic allocation of defense resources. Several case studies on a modified IEEE 123-node test feeder substantiate the efficacy of the proposed security risk assessment method and risk-oriented defense resource allocation strategy.**

***Index Terms*—Coordinated cyber attack, defense resource allocation, multi-objective optimization, power distribution network, security risk assessment.**

I. Introduction

In order to effectuate a reliable and efficient power supply, power distribution networks have gradually evolved into cyber-physical distribution networks (CPDNs) with the accelerating development of smart grids [1], [2]. As a result, the observability and controllability of CPDNs are greatly enhanced by the bidirectional interaction between cyber and physical constituents. However, the relatively inadequate defense means of CPDNs can hardly isolate cyberspace risks from the physical system, thereby allowing potential cyber attackers to exploit exposed vulnerabilities to damage critical system facilities [3], [4]. Therefore, it is indispensable to accurately assess the operational security risk and reasonably distribute restricted defense resources for CPDNs.

In the context of CPDN that is subject to potential cyber-attack threats, security risk can be generally seen as a comprehensive measure of the occurrence probability and severity of attacks. Existing security risk assessment methods can be broadly categorized into two groups, i.e., risk modeling [5]-[9] and quantification [10]-[14]. In the former group, the security risk assessment for state estimation was devised as a mixed-integer linear programming problem [5]. A Bayesian-regime-based risk assessment model was proposed for gauging security implications by using the epidemic model and optimal load shedding ratio [6]. Denial-of-service (DoS) attacks, known as their capability of jamming cyber communication networks, have drawn much attention in the realm of cyber-physical systems, e.g., sampled-data control [7] and stability analysis [8]. From a game-theoretic point of view, a risk assessment framework was established for power systems with external DoS attacks [9]. However, previous studies mainly focus on exploring risk modeling methods under single-domain attacks, indicating a lack of consideration for complex coordinated attacks in an ever-evolving environment.

For risk quantification methods, the semi-Markov process model was utilized to delineate the process of cyber attacks against the supervisory control and data acquisition (SCADA) system [10], [11]. Involving the feeder automation systems, an entropy-like risk quantification approach was developed for CPDNs [12]. In [13], the cyber intrusion process

Manuscript received: March 16, 2024; revised: May 23, 2024; accepted: June 3, 2024. Date of CrossCheck: June 3, 2024. Date of online publication: July 5, 2024.

This work was supported by the National Natural Science Foundation of China (No. 52377086) and the Postgraduate Research & Practice Innovation Program of Jiangsu Province (No. SJCX23_0063).

S. Wei, Z. Wu (corresponding author), and Q. Hu are with the School of Electrical Engineering, Southeast University, Nanjing 210096, China (e-mail: aussen@seu.edu.cn; zjwu@seu.edu.cn; qhu@seu.edu.cn).

J. Xu is with the College of Automation and College of Artificial Intelligence, Nanjing University of Posts and Telecommunications, Nanjing 210023, China (e-mail: andy-xu199@hotmail.com).

Y. Cheng is with the Shenzhen Power Supply Bureau Co., Ltd., Shenzhen 518001, China (e-mail: 18217699297@163.com).

DOI: 10.35833/MPCE.2024.000288

against substations was emulated by generalized stochastic Petri nets, whereby the security risk was quantified by the product of successful intrusion probability and load loss [13], [14]. In general, the risk provoked by cyber attacks can be well evaluated by the studies above. Nonetheless, the impact of defense resources (also called hardening measures) on the risk propagation process has yet to be further investigated.

To ensure robust cyber-physical interaction and mitigate security risks, researchers have begun probing how to allocate defense resources [15]-[20], which can be seen as an inclusive abstraction of invested physical facilities and defense-related software. With the goal of improving observability and state estimation accuracy, optimal phasor measurement unit (PMU) placement methods have been developed under cyber attacks, e.g., [15], [16], but the demerit is that deploying PMUs cannot fundamentally protect CPDNs from cyber attacks (considering the spoofing of global positioning system) and introduces additional investment. For fortifying operation reliability, robust optimization techniques were adopted to allocate line defense resources and distributed generators against multi-period attacks [17]. When it comes to the transmission level, an actuarial insurance principle was designed to incentivize the optimal defense resource allocation as a Stackelberg security game [18]. Likewise, a two-layer defense resource allocation framework was established considering bounded rationalities in the attack-defense game [19]. In [20], the risk incurred by cyber attacks was quantified via the success rate, and optimal allocation methods with a fixed risk value and limited budget were presented respectively. However, the aforementioned studies either focus on small-scale microgrids [17] or devise game-theoretic models for generator-dominated transmission power grids [18], [19], which yield restricted applicability in CPDNs with unbalanced features and deeply intertwined cyber-physical components. Complex cyber topology and analyses of the cyber-attack process were not considered in [20], which led to an over-idealized risk assessment result and the defense resource was simply allocated according to the risk value proportionally. Moreover, the majority of previous studies presume that system measurements can be fully protected in the presence of cyberspace threats, but such an assumption is not feasible for practical CPDNs. It is more reasonable to assume that the ability of a measurement to withstand cyber attacks depends on the amount of deployed defense resources. In this regard, how to optimize the allocation settings (e.g., the resource budget and allocation precision) and prioritize the optimal solution from the suboptimal strategy set are the key issues that need to be resolved in further research.

Driven by the limitations and challenges above, this paper proposes a security risk assessment method and a risk-oriented defense resource allocation strategy for CPDNs. Evolving from existing studies that mainly consider single-domain attacks, the proposed method takes into account the risk propagation process and vulnerabilities of system measurements according to the attack graph-based CPDN architecture. Based on an absorbing Markov chain model, the CPDN security risk is quantified under coordinated cyber attacks that aim to corrupt pseudo and real-time measurements. The devised resource allocation strategy is risk-oriented following the previous security risk assessment results. By solving a multi-objective optimization (MOO) problem, the optimal defense resource allocation setting is prioritized via a generational distance metric and leveraged for the atomic allocation approach. Overall, the contributions of this paper are mainly threefold:

1) A security risk assessment method for CPDN is proposed under coordinated cyber attacks, in which the probability of a successful attack and provoked security risk are quantitively evaluated based on the constructed attack graph-based CPDN architecture and representative cyber-attack paths.

2) A risk-oriented defense resource allocation strategy is designed to mitigate the quantified security risk. Specifically, the formulated MOO problem addresses the trade-off between security risk and limited resource budget, which is solved by an efficient optimal Pareto solution generation approach.

3) An atomic allocation approach for defense resources is developed to further alleviate the overall system risk, in which the limited budget is divided into atomic units and iteratively deployed to the measurement with the highest risk reduction.

The remainder of this paper is structured as follows. Section II presents the preliminaries and problem formulation. Section III details the proposed security risk assessment method. The risk-oriented defense resource allocation strategy is given in Section IV. Case studies are shown and analyzed in Section V. Finally, Section VI concludes the paper.

II. Preliminaries and Problem Formulation

A. CPDN Structure

Fueled by the proliferating information and communication technologies (ICTs) and advanced metering infrastructures (AMIs), distribution networks are transforming into CPDNs with deep cyber-physical coupling. The schematic diagram of CPDN is displayed in Fig. 1, which can be generally divided into two parts: physical and cyber layers. The physical layer includes transformers, distribution lines, feeder switches, circuit breakers, plug-in electric vehicles, and virtual plants (i.e., the aggregation of wind turbines, photovoltaics, and controllable energy storage devices), etc. The cyber layer is comprised of communication software, protocols, cyber network topology, and other ICT equipment.

As shown in Fig. 1, the typical CPDN can be described as a three-layer hierarchical nested structure. The bottom physical layer contains the user-side feeder and other primary equipment components, as well as intelligent electronic devices (IEDs), feeder terminal units (FTUs), and intelligent terminals. The intermediate access layer adopts mixed communication technologies, e.g., Ethernet passive optical network (EPON), Ethernet with transmission control protocol/Internet protocol (TCP/IP), and wireless public/private network, to exchange command and response between distribution substations and terminal units in the physical layer. In general, the reliability of access and physical layers is relatively lower than that of the backbone layer. The topmost

backbone layer (i.e., backbone network) located in the master station is comprised of the SCADA, management information system (MIS), energy management system (EMS), and man-machine interface, thereby realizing advanced functionalities such as energy management, feeder automation, mobile connectivity, and human-computer interaction. Based on synchronous digital hierarchy (SDH) or multi-service transport platform (MSTP), the backbone network is equipped with the highest level of security protection and is remotely connected to downstream substations via switches and routers.

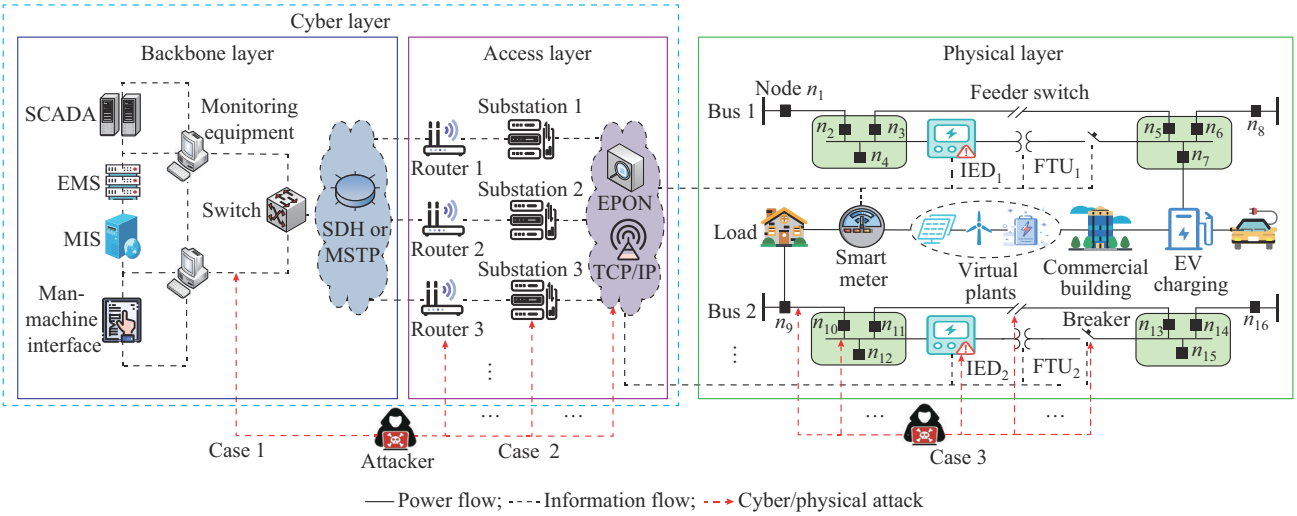

Fig. 1. Schematic diagram of CPDN.

B. Coordinated Cyber Attacks Against CPDN

While the observability and controllability of the network are significantly upgraded by advanced ICTs and widely deployed AMIs, CPDN is also becoming more susceptible to external security risks caused by malicious attacks, which can be categorized according to their targets (e.g., substations, communication links, and physical terminals) into two types: cyber attacks and physical attacks [3], [21].

From the perspective of system operators, to mitigate the mounting cybersecurity threats, intrusion detection systems (IDSs) and firewalls are massively deployed for the backbone layer, which operates in a relatively isolated manner with a very limited number of channels that adversaries can exploit (see Case 1 in Fig. 1). Owing to the relatively low security of the access layer, attackers can take advantage of the security loopholes to invade the cyber network (see Case 2 in Fig. 1), thereby launching data replay, jamming, DoS, man-in-the-middle, and other cyber attacks to interfere the cyber-physical interaction and jeopardize operation reliability. Meanwhile, the broadly distributed IEDs, lines, feeder switches, and breakers can be leveraged by adversaries to initiate data manipulation, line overload, topology, and other physical attacks (see Case 3 in Fig. 1), so as to falsify the system topology and parameters to vandalize the decision-making strategies in the master station. Considering the compulsory $N-1$ and $N-2$ security checks of CPDN, attackers tend to randomly combine multiple cyber and physical attacks in Cases 2 and 3 under different spatial and temporal conditions to boost the severity and success probability [22], thus exposing CPDN to superimposed and intensified security risks. In this study, such a combined attack is defined as a coordinated cyber attack.

III. Proposed Security Risk Assessment Method

Referring to previous records of major outage events [22], antagonistic attacks aiming at damaging power grids typically exhibit a coordinated nature. However, prevailing security risk assessment methods have difficulty in evaluating the coordinated risk and the corresponding propagation path. To bridge the gaps, this section proposes a security risk assessment method for CPDN in the presence of coordinated cyber attacks.

A. Probabilistic Analysis of Successful Attacks

Note that the access and physical layers in CPDN are more susceptible to external security threats, thereby different kinds of cyber and physical attacks under Cases 2 and 3 in Fig. 1 can be arbitrarily combined to form a coordinated cyber attack, which is taken as the focus of this study. Besides, this study aims to develop defense countermeasures against cyber attacks that compromise load profiles and real-time measurements, which are critical for situation awareness and reliable system operation. Since distribution lines, feeder switches, and circuit breakers are spread over a large geographical area in the physical layer, it is rather challenging to coordinate multiple physical attacks simultaneously under different spatial conditions [23]. Therefore, IEDs connected to the access layer are more easily exploited by antagonists to achieve data manipulation attacks. In accordance with Fig. 1, we presume routers, substations, access network, and IEDs (nodes/devices with relatively weak hardening measures) as potential coordinated cyber-attack portals.

To characterize the cross-domain security risk propagation process triggered by coordinated cyber attacks against load profiles and real-time measurements, two representative

graph-based cyber-attack paths consisting of logical nodes and topology are drawn in Fig. 2. As can be observed, potential cyber attacks commenced from the router, substation, access network, and IED are denoted by the orange nodes. CPDN nodes/devices are represented by the blue nodes, which are denoted as logical nodes in the sequel. Communication networks and the attack target are marked by green nodes and red dashed circles, respectively. Arrows in different colors show the direction of security risk propagation. For each attack portal, a certain number of security loopholes are assumed to be exploitable, thus constructing the subsequent propagation path. However, it should be noted that the number of loopholes that need to be exploited to form an attack path should be as few as possible considering the attacker's limited attack means. Thus, it is reasonable to assume that after infiltrating the loophole at the entry point in Fig. 2, the attacker is likely to manipulate the attack to propagate through the black arrows (i.e., the transition probability between logical nodes) in sequence [24], instead of continuing to exploit intractable security loopholes.

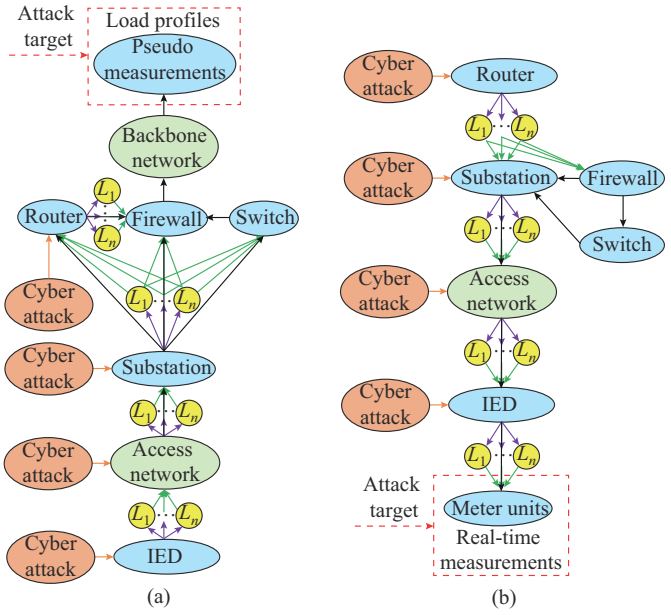

Fig. 2. Graph-based cyber-attack paths in CPDN. (a) Load profile attack. (b) Real-time measurement attack.

1) Selection of Attack Portals

Malicious cyber attackers can randomly pick attack portals and exploit the corresponding security loopholes to capture the control permissions. In CPDN, the logical nodes are assumed to be independent of each other, namely, the infiltration of a specific portal does not affect the attack path formed by other portals. Therefore, it is presumed that: ① the selection of attack portals is independent of each other; and ② an attack path can only be formed from a single attack portal. In this way, the attacker can intercept and spoof data packets to eavesdrop or falsify the load profile/real-time measurement starting from the orange arrows in Fig. 2. The following constraint specifies the probability range of an attack portal being selected:

$$P_{R,i}, P_{Sub,i}, P_{IED,i}, P_{AN,i} \in [0, 1] \tag{1}$$

where $P_{R,i}$, $P_{Sub,i}$, $P_{AN,i}$, and $P_{IED,i}$ are the independent probabilities of router, substation, access network, and IED being designated to form a specific attack path i, respectively.

2) Selection of Security Loopholes

The yellow nodes and purple arrows in Fig. 2 represent the inherent security loopholes of portals and the selected probabilities, respectively. However, the differences in the availability of different security loopholes will also lead to the attacker's varying intrusion choices. That is, the higher the exploitability, the greater the probability of security loopholes being selected by the attacker. Therefore, for a single attack path, we define the likelihood of a loophole being chosen as the ratio of its exploitability to the sum of the exploitability of all adjacent loopholes, which is expressed as:

$$P_{Sel}(L_j) = P_{Exp}(L_j) \Big/ \sum_{j=1}^{n_L} P_{Exp}(L_j) \tag{2}$$

where $P_{Sel}(L_j)$ and $P_{Exp}(L_j)$ are the selected probability and exploitability of the security loophole L_j, respectively; and n_L is the total number of loopholes ($j = 1, 2, \ldots, n_L$) at a specific portal.

3) Exploitability of Security Loopholes

The exploitability of security loophole L_j (i.e., $P_{Exp}(L_j)$) is represented by the green arrows in Fig. 2. Analytically, $P_{Exp}(L_j)$ is related to the access vector (AV), access complexity (AC), and authentication (AU) under the common vulnerability scoring system (CVSS) standard [25], [26]. Besides, the exposure duration of loopholes t_{L_j} also exerts a significant influence on $P_{Exp}(L_j)$. Taking into account the factors above, the Pareto distribution and CVSS standard are leveraged to describe the exploitability of security loopholes [27], which can be expressed as:

$$P_{Exp}(L_j) = [1 - (k_1/t_{L_j})^{k_2}] C_{L_j}^{AV} C_{L_j}^{AC} C_{L_j}^{AU} \tag{3}$$

where k_1 and k_2 are the scale and shape parameters, respectively; and $C_{L_j}^{AV}$, $C_{L_j}^{AC}$, and $C_{L_j}^{AU}$ are the AV, AC, and AU scores of L_j under the CVSS standard, respectively.

4) Transition Probability Between Logical Nodes

The black arrows in Fig. 2 indicate the transition probability between logical nodes, which is pertinent to the vulnerability of communication links and attack resources available to the adversary. In this study, the specific tools or technical levels the attacker possesses are considered as the attack resource and its practical significance will be detailed in Section III-B. Analogous to the equipment failure setting in [10] and [28], this study adopts the exponential function to model the relationship between the vulnerability of communication links and offensive resources. Formally, for the i^{th} attack path, the transition probability within the communication link between logical nodes is:

$$P_i^{Tr}(r_i^A) = 1 - \mathrm{e}^{-\lambda_i r_i^A} \quad 0 < P_i^{Tr}(r_i^A) \le 1 \tag{4}$$

where r_i^A is the disposed attack resource for a single attack; and λ_i is the scaling coefficient, which yields $\lambda_i = -\ln(1 - AF_i)/AC_i$. The fraction AF_i satisfies $0 < AF_i \le 1$, and AC_i indicates the attacker's cost for exploiting the vulnerability of the communication link.

5) Success Probability of Multiple Attack Paths

To derive the probabilistic expression for cyber-attack paths shown in Fig. 2, this study constructs the attack graph based on the absorbing Markov chain model [29] as it encompasses the following properties: ① an attack graph contains at least one absorbing state; and ② in an attack graph, starting from every state, one can eventually reach an absorbing state.

Attack portals and the pseudo/real-time measurements in Fig. 2 are defined as the initial state and attack target (i.e., the absorbing state), respectively, and other logical nodes are defined as transient states. Once a single attack reaches the absorbing state, CPDN is considered to be in a compromised state. As a result, the system remains in this state until security practitioners react to eliminate the anomaly.

Combining (1)-(4), the transition probabilities between different logical nodes can be calculated, thereby constituting the transition matrix of an absorbing Markov chain as:

$$\boldsymbol{C}_{trans}=\begin{bmatrix}\boldsymbol{T} & \boldsymbol{A}\\ \boldsymbol{0} & \boldsymbol{I}\end{bmatrix}\in\mathbb{R}^{(t+a)\times(t+a)} \tag{5}$$

where $\boldsymbol{A}\in\mathbb{R}^{t\times a}$ and $\boldsymbol{T}\in\mathbb{R}^{t\times t}$ are the matrices of a absorbing states and t transient states, respectively; and $\boldsymbol{I}$ is the identity matrix.

Recall the Property ② above, the probability that the chain will be absorbed always equals one. Hence, when the cardinality of states $n\to\infty$, we have $\boldsymbol{T}^n\to 0$. For the canonical form (5) of absorbing Markov chain $\boldsymbol{C}_{trans}$, the matrix $\boldsymbol{I}-\boldsymbol{T}$ has an inverse $\boldsymbol{Inv}=(\boldsymbol{I}-\boldsymbol{T})^{-1}=\boldsymbol{I}+\boldsymbol{T}+\boldsymbol{T}^2+\boldsymbol{T}^3+\ldots$, which is the fundamental matrix of $\boldsymbol{C}_{trans}$. To measure the likelihood of a single attack eventually reaching the absorbing state, $\boldsymbol{Inv}$ and $\boldsymbol{A}$ in the canonical form (5) are used to calculate the success probability of each attack path $Q=\boldsymbol{Inv}\cdot\boldsymbol{A}$. The element q_{ij} signifies the probability of being absorbed by state j given an initial state i. Therefore, Q can be described as $Q=(\boldsymbol{I}-\boldsymbol{T})^{-1}\boldsymbol{A}$, which is derived by successively multiplying the selected probability, loophole exploitability, and logical node transition probabilities (1)-(4).

Different attack paths can be elaborately combined for a single attack target to reconfigure the load profile or real-time measurements. Thus, it is assumed that multiple attack paths can be exploited concurrently and the success probability of a single attack path is independent of each other. As a result, the success probability of multiple attack paths can be calculated:

$$P_m=\sum_{i=1}^{N_P}Q_{\{i\}}=\sum_{i=1}^{N_P}(\boldsymbol{I}-\boldsymbol{T}_{\{i\}})^{-1}\boldsymbol{A}_{\{i\}} \tag{6}$$

where N_P is the number of all possible attack paths for compromising the m^{th} attack target; $Q_{\{i\}}$ is the success probability; and $\boldsymbol{T}_{\{i\}}$ and $\boldsymbol{A}_{\{i\}}$ are the matrix quantities (which have been defined above) corresponding to the i^{th} attack path.

B. Security Risk Assessment

As illustrated in Section III-A, specific approaches and skill levels of an attacker are considered as the attack resource. Similarly, the defense resource can be represented by the degrees of practical defense means. To evaluate the risk, the attack and defense resources need to be quantified by the same metric considering the practical significance. That is, all attack and defensive means can be evaluated by the monetary value.

Practical security controls, e.g., IDSs, firewalls, anti-virus software/hardware, and data integrity checking software, require significant monetary expense to be effective. Likewise, a great amount of monetary expenditure is indispensable for antagonists to elaborate on valid attack strategies. Therefore, the practical significance of the amount of attack/defense resources is defined by the monetary value, and the base number of a resource unit can be presumed as one thousand or one million in any currency. In this way, the attacker/system operator can quantify the employed intrusion techniques or security controls via dividing their monetary investments by the base number of a resource unit, so as to derive the dimensionless resource value.

Since the attack in this study targets load profiles and real-time measurements, the attack resource is represented by the relative cost of exploiting loopholes and executing attacks for a cyber intrusion, while the expense required (i.e., invested physical facilities and defensive software) for mitigating the vulnerability of a single measurement signifies the defense resource. Real-time measurements originate from meter units in the physical domain, and a successful attack on a single unit means that any measurement channel collected by that unit can be falsified. As for the load profile represented by pseudo measurements, we presume that it interacts with other logical nodes through data packets, of which successful interception can manipulate an arbitrary load data it contains. Similar to (4), the relationship between measurement vulnerability v_m and deployed defense resource r_m^D is written as [10], [24]:

$$v_m(r_m^D)=\mathrm{e}^{-\alpha_m r_m^D}\quad 0<v_m(r_m^D)\le 1 \tag{7}$$

$$\alpha_m=-\ln(DF_m)/DC_m\quad 0<DF_m\le 1 \tag{8}$$

where r_m^D is the disposed defense resource for the m^{th} measurement unit; and α_m is the defender's cost DC_m to reduce $v_m(r_m^D)$ with the predetermined fraction DF_m.

Without losing generality, assuming that an attacker aims to alter $N_{\mathcal{M}}$ measurements. For the single m^{th} measurement unit with N_P attack paths available, the probability of a successful attack can be obtained by firstly accumulating the success probability of each path by (6), and then multiplying them by the measurement vulnerability (7) as: $P_m v_m(r_m^D)$. As a consequence, the success probability of a coordinated cyber attack can be computed by multiplying the success probability of each measurement unit cumulatively:

$$P^{CO}=\prod_{m=1}^{N_{\mathcal{M}}}P_m v_m(r_m^D)=\prod_{m=1}^{N_{\mathcal{M}}}\left[\sum_{i=1}^{N_P}(\boldsymbol{I}-\boldsymbol{T}_{\{i\}})^{-1}\boldsymbol{A}_{\{i\}}\right)\mathrm{e}^{-\alpha_m r_m^D}\right] \tag{9}$$

Remark 1: it can be intuitively inferred from (9) that the success probability is proportional to the number of attack paths N_P for a single target measurement. However, raising the number of target measurement units $N_{\mathcal{M}}$ can degrade the likelihood of successful coordinated cyber attacks.

Referring to the National Institute of Standards and Technology (NIST) SP 800-82r3 standard for risk assessment [30], the accidental risk is denoted by the product of acci-

dent probability and its physical consequence, whereas system risk is the sum of all anticipated accidental risks. Hence, the coordinated cyber attack is considered as a special kind of incident in this study based on the NIST standard, and the resultant security risk is expressed as the product of its success probability (9) and physical consequence. As a result, the overall system risk of CPDN R^{Sys} can be defined as the sum of risks induced by all coordinated cyber attacks as:

$$\begin{cases} R_k^{CO} = P_k^{CO} C_k \\ R^{Sys} = \sum_{k=1}^{N_K} R_k^{CO} \end{cases} \tag{10}$$

where R_k^{CO} and C_k are the security risk and physical consequences provoked by the k^{th} coordinated cyber attack, respectively; P_k^{CO} is the success probability of the k^{th} attack; and N_K is the total number of coordinated cyber attacks.

Remark 2: existing studies mostly employ load shedding as the indicator for C_k. However, such a metric for transmission systems may not be applicable to CPDNs under quasi-steady operation conditions. In contrast, the number of corrupted measurements is adopted for modeling the game in [31], which can be defined as the attacker's and defender's objective simultaneously. Thus, the physical consequence C_k is denoted by the number of falsified measurement units, thereby simplifying the calculation process and facilitating the subsequent risk-oriented defense resource allocation.

IV. Risk-oriented Defense Resource Allocation Strategy

CPDNs generally suffer from the inadequacy of security controls, thereby the protection of critical assets needs to be prioritized. To fully utilize the limited defense resource budget and mitigate cybersecurity risks, a novel risk-oriented defense resource allocation strategy is proposed in this section.

A. Attack-defense Interactions

Because the system risk R^{Sys} is delineated by the product of occurrence probability and physical impact, the attacker can boost the risk level by distributing more resources for a cyber intrusion, and the risk can be mitigated by an increased number of defense resources. Thus, from the perspective of system operators, the defense resource allocation problem can be investigated considering the interaction of attackers and defenders, where each player's action space comprises all the possible attack and defense strategies. For the attacker, the attack strategy is the practical means by which coordinated cyber attacks can be implemented and the amount of attack resources can be deployed for a specific one. Assume the attacker launches N_K coordinated cyber attacks, then the disposed attack resource $\boldsymbol{\gamma}$ can be written as a column vector:

$$\boldsymbol{\gamma} = [r_1^A, r_2^A, \ldots, r_{N_K}^A]^{\mathrm{T}} \tag{11}$$

$$\sum_{k=1}^{N_K} r_k^A = \tau^A \tag{12}$$

where r_k^A is the attack resource positioned for the k^{th} attack and satisfies $0 \le r_k^A \le \tau^A, k = 1, 2, \ldots, N_K$; and τ^A is the limited attack resource budget. On the contrary, the defender distributes a limited defense resource budget τ^D over all the N_M system measurements. Similarly, the column vector of defense resource $\boldsymbol{\xi}$ is given by:

$$\boldsymbol{\xi} = [r_1^D, r_2^D, \ldots, r_{N_M}^D]^{\mathrm{T}} \tag{13}$$

$$\sum_{m=1}^{N_M} r_m^D = \tau^D \tag{14}$$

where r_m^D is the deployed defense resource for the m^{th} measurement and satisfies $0 \le r_m^D \le \tau^D, m = 1, 2, \ldots, N_M$. Note that the practical significance of attack and defense resources have been illustrated in Section III-B.

The payoff within attack-defense interactions is generally assessed by the system loss/gain value (i.e., the variation of system risks) caused by the attack/defense strategy. The attacker's objective is to maximize the risk by increasing the success probability and physical consequence to the greatest possible extent, whose payoff can be formulated as:

$$\{\boldsymbol{\gamma}^*, \boldsymbol{\xi}^\dagger\} \in \arg\max_{\boldsymbol{\gamma}^\dagger} \mathcal{P}^A(\boldsymbol{\gamma}^\dagger, \boldsymbol{\xi}^\dagger) \triangleq \arg\max_{\boldsymbol{\gamma}^\dagger} \Delta R^{Sys}(\boldsymbol{\gamma}^\dagger, \boldsymbol{\xi}^\dagger) \tag{15}$$

where $\boldsymbol{\gamma}^\dagger$ and $\boldsymbol{\xi}^\dagger$ are the arbitrary non-optimal strategies of the attacker and defender, respectively; and $\boldsymbol{\gamma}^*$ is the attacker's optimal strategy that can maximize the payoff $\mathcal{P}^A(\boldsymbol{\gamma}^\dagger, \boldsymbol{\xi}^\dagger)$, denoted by the incremental risk $\Delta R^{Sys}(\boldsymbol{\gamma}^\dagger, \boldsymbol{\xi}^\dagger)$.

For the defender, an opposite objective is endowed, who intends to minimize the incremental risk $\Delta R^{Sys}(\boldsymbol{\gamma}, \boldsymbol{\xi})$ in the presence of an attack strategy $\boldsymbol{\gamma}$ as:

$$\{\boldsymbol{\gamma}^\dagger, \boldsymbol{\xi}^*\} \in \arg\min_{\boldsymbol{\xi}^\dagger} \mathcal{P}^D(\boldsymbol{\gamma}^\dagger, \boldsymbol{\xi}^\dagger) \triangleq \arg\min_{\boldsymbol{\xi}^\dagger} \Delta R^{Sys}(\boldsymbol{\gamma}^\dagger, \boldsymbol{\xi}^\dagger) \tag{16}$$

where $\boldsymbol{\xi}^*$ is the optimal defense resource allocation strategy that can minimize $\Delta R^{Sys}(\boldsymbol{\gamma}^\dagger, \boldsymbol{\xi}^\dagger)$, i.e., the payoff $\mathcal{P}^D(\boldsymbol{\gamma}^\dagger, \boldsymbol{\xi}^\dagger)$. Therefore, the four-tuple strategy $\{\boldsymbol{\gamma}^*, \boldsymbol{\xi}^*, \boldsymbol{\gamma}^\dagger, \boldsymbol{\xi}^\dagger\}$ of attack-defense interactions subjects to the following inequality set:

$$\mathcal{P}^A(\boldsymbol{\gamma}^*, \boldsymbol{\xi}^\dagger) \ge \mathcal{P}^A(\boldsymbol{\gamma}^\dagger, \boldsymbol{\xi}^\dagger) \ge 0 \tag{17}$$

$$\mathcal{P}^D(\boldsymbol{\gamma}^\dagger, \boldsymbol{\xi}^*) \le \mathcal{P}^D(\boldsymbol{\gamma}^\dagger, \boldsymbol{\xi}^\dagger) \le 0 \tag{18}$$

$$R^{Sys}(\boldsymbol{\gamma}^*, \boldsymbol{\xi}^\dagger) \ge R^{Sys}(\boldsymbol{\gamma}^*, \boldsymbol{\xi}^*) \ge R^{Sys}(\boldsymbol{\gamma}^\dagger, \boldsymbol{\xi}^*) \ge 0 \tag{19}$$

B. MOO and Solution Selection

Referring to related studies [32], [33], the cybersecurity concerns are well addressed by MOO-based defensive approaches. To address the decision-making issue, i.e., the comprehensive trade-off between overall system security risk and limited resource budget, the determination of defense resource allocation settings is devised as a MOO problem from the defender's point of view. Based on Section IV-A, the MOO is devised to identify the optimal solution that minimizes the security risk R_k^{CO} and defense resource budget τ_k^D simultaneously in the presence of coordinated cyber attacks. Formally, the MOO can be formulated as:

$$\begin{cases} \min\limits_{\boldsymbol{\gamma}, \boldsymbol{\xi}} \sum\limits_{k=1}^{N_K} R_k^{CO} \\ \min\limits_{\boldsymbol{\gamma}, \boldsymbol{\xi}} \sum\limits_{k=1}^{N_K} \tau_k^D \end{cases} \tag{20}$$

s.t.

$$R_k^{CO} = P_k^{CO} C_k \quad \forall \boldsymbol{\gamma}, \forall \boldsymbol{\xi}, \forall k \tag{21}$$

$$\begin{cases} \tau^A = \sum_{k=1}^{N_K} r_k^A \\ \tau_k^D = \sum_{m=1}^{N_M} r_{m,k}^D \end{cases} \quad \forall \boldsymbol{\gamma}, \forall \boldsymbol{\xi}, \forall k \tag{22}$$

$$\tau_{\min}^D \le \tau_k^D \le \tau_{\max}^D \quad \forall \boldsymbol{\gamma}, \forall \boldsymbol{\xi}, \forall k \tag{23}$$

$$x_{\min}^D \le x_k^D \le x_{\max}^D \quad \forall \boldsymbol{\gamma}, \forall \boldsymbol{\xi}, \forall k \tag{24}$$

$$\tau_k^D : r_{1,k}^D = r_{2,k}^D = \ldots = r_{N_M-1,k}^D = r_{N_M,k}^D \quad \forall \boldsymbol{\gamma}, \forall \boldsymbol{\xi}, \forall k \tag{25}$$

where $r_{m,k}^D$ is the defense resource deployed for the m^{th} measurement against the k^{th} attack; $\tau_{\min}^D$ and $\tau_{\max}^D$ are the lower and upper bounds of resource budget, respectively; and $x_{\min}^D$ and $x_{\max}^D$ are the lower and upper limits of allocation precision, respectively.

The MOO objective (20) aims to minimize R_k^{CO} and τ_k^D simultaneously with the defense strategy (i. e., the decision variable $\boldsymbol{\xi}$) under all the N_K potential coordinated cyber attacks (i.e., the decision variable $\boldsymbol{\gamma}$). Constraints (21) and (22) specify the constitution of R_k^{CO}, τ^A, and τ_k^D from (10), (12), and (14). Constraints (23) and (24) indicate the lower and upper limits for the defense resource budget τ_k^D and the allocation precision x_k^D (which will be detailed in Section IV-C), respectively. Constraint (25) ensures that defense resources are initially allocated to each measurement equally.

By solving the formulated MOO, the optimal solution can only be described by a set of optimal Pareto solutions due to the contradiction of the two objective functions. Note that the number of attacks is relatively small at the beginning of cyber intrusions, and the defense strategy space scale is therefore limited. In this case, traversing methods can be leveraged to approach the optimal Pareto front. However, the strategy space can be exponentially expanded in practice as the attack-defense interactions evolve with time. To address the issue, the nondominated sorting genetic algorithm III (NSGA-III) [34] is employed to solve the MOO with a relatively large strategy space. Based on a reference-point-oriented elitist selection approach, NSGA-III is capable of converging to the optimal Pareto front with superior efficiency and diversity preservation performance, in contrast with traditional traversing methods and the nondominated sorting genetic algorithm II (NSGA-II).

Initially, a parent population P_0 is arbitrarily generated in the NSGA-III, thus the two objective values corresponding to each individual in P_0 can be evaluated. Then, each individual is ranked by the nondominated sorting procedure [35], where its nondomination rank (i_{rank}) and perpendicular distance to the reference line (i_{dist}) are also calculated according to the objective values. Afterward, the l^{th} generation of NSGA-III can be described by the following step-by-step loop.

1) Given the parent population P_l with N individuals from $(l-1)^{\text{th}}$ generation, the offspring population Q_l of size N is created from P_l using crossover and mutation operators.

2) Form a combined population of size $2N$ from P_l and Q_l as: $R_l = P_l \cup Q_l$.

3) Evaluate objective values for each individual in R_l, then compute its nondomination rank (i_{rank}) and perpendicular distance to the reference line (i_{dist}).

4) Go through the nondominated sorting procedure, then form a new population P_{l+1} for the next generation by the reference-point-oriented elitist selection approach [35].

5) Increment the generation counter: $l \leftarrow l+1$.

The step-by-step loop above is iterated until the counter l reaches the maximum number of generations, and the detailed formulation of NSGA-III can be found in [34] and [36].

To satisfy the requirements of optimizing multiple objective functions, it is necessary to select an optimal solution $\boldsymbol{X}_p$ from the optimal Pareto set $\boldsymbol{P}$ derived from NSGA-III. Hence, the generational distance metric in [37] is adopted to evaluate the optimality of different solutions in $\boldsymbol{P}$. According to (20), the vector corresponding to a solution $\boldsymbol{X}_p \in \boldsymbol{P}$ is defined as the objective vector, given by (26). Such objective vectors are combined to form the Pareto front.

$$\left\langle R_p^{Sys} = \sum_{k=1}^{N_K} R_k^{CO}, \tau_p^D = \sum_{k=1}^{N_K} \tau_k^D \right\rangle \tag{26}$$

where R_p^{Sys} and τ_p^D are the sum of security risks and the sum of defense resources under all the N_K cyber attacks, respectively.

A random vector in the Pareto front can be seen as a scatter point in the two-dimensional space, where the x-axis and y-axis are represented by R_p^{Sys} and τ_p^D, respectively. Then, the generational distance metric measures the proximity between a random objective vector and the ideal vector, thus the optimality of the corresponding solution $\boldsymbol{X}_p$ in the optimal Pareto set $\boldsymbol{P}$ can be quantitively evaluated. As shown in (20), the minimum value of each objective in the Pareto front constitutes the ideal vector, described by:

$$\left\langle \min_{\forall \boldsymbol{X}_p \in \boldsymbol{P}} R_p^{Sys}, \min_{\forall \boldsymbol{X}_p \in \boldsymbol{P}} \tau_p^D \right\rangle \tag{27}$$

Then, each objective vector is normalized based on the ideal vector value in the two-dimensional space:

$$\begin{cases} \overline{R}_p^{Sys} = \left(R_p^{Sys} - \min_{\forall \boldsymbol{X}_p \in \boldsymbol{P}} R_p^{Sys} \right) \Big/ \left(\max_{\forall \boldsymbol{X}_p \in \boldsymbol{P}} R_p^{Sys} - \min_{\forall \boldsymbol{X}_p \in \boldsymbol{P}} R_p^{Sys} \right) \\ \overline{\tau}_p^D = \left(\tau_p^D - \min_{\forall \boldsymbol{X}_p \in \boldsymbol{P}} \tau_p^D \right) \Big/ \left(\max_{\forall \boldsymbol{X}_p \in \boldsymbol{P}} \tau_p^D - \min_{\forall \boldsymbol{X}_p \in \boldsymbol{P}} \tau_p^D \right) \end{cases} \tag{28}$$

where $\overline{R}_p^{Sys}$ and $\overline{\tau}_p^D$ are the normalized values of R_p^{Sys} and τ_p^D, respectively.

Finally, the $\mathcal{L}_2$-norm of the normalized objective vector is computed to derive the generational distance metric Dis as:

$$\left\| Dis(\boldsymbol{X}_p) \right\|_2 = \sqrt{(\overline{R}_p^{Sys})^2 + (\overline{\tau}_p^D)^2} \tag{29}$$

Remark 3: according to the generational distance metric, different solutions in the optimal Pareto set can be prioritized. The solution with the minimum distance metric is the optimal one, since it enables the corresponding objective vector closest to the ideal vector in the two-dimensional space.

C. Atomic Allocation Approach for Defense Resources

Based on prioritized optimal solutions, the defense resource allocation budget τ^D can be specified for the subsequent defensive countermeasure design. However, it is note-

worthy that defense resources are equally allocated for each measurement in the previous step, which is not applicable in the face of varying coordinated cyber attacks. To allocate the limited budget more efficiently, an atomic allocation approach is proposed in this subsection for the defender to further trim down the overall system risk.

Referring to [38], defense resources should be deployed according to the fastest descent direction of the overall system risk R^{Sys}. In such cases, the problem can be categorized as an atomic allocation, where the term "atomic" indicates that the defense budget has reached the minimum unit and cannot be divided further. As the atomic unit is repeatedly allocated, the system risk can be mitigated as the cost of defense resources gradually increases. In this study, supposing the defense budget τ^D is divided into multiple atomic units, whose base number can be arbitrarily presumed as a small value in any currency. At each allocation step, a single atomic unit is deployed to the measurement with the highest risk reduction value through all the coordinated cyber attacks. The flow chart of the proposed atomic allocation approach for defense resources is shown in Fig. 3, and detailed procedures are illustrated in the following.

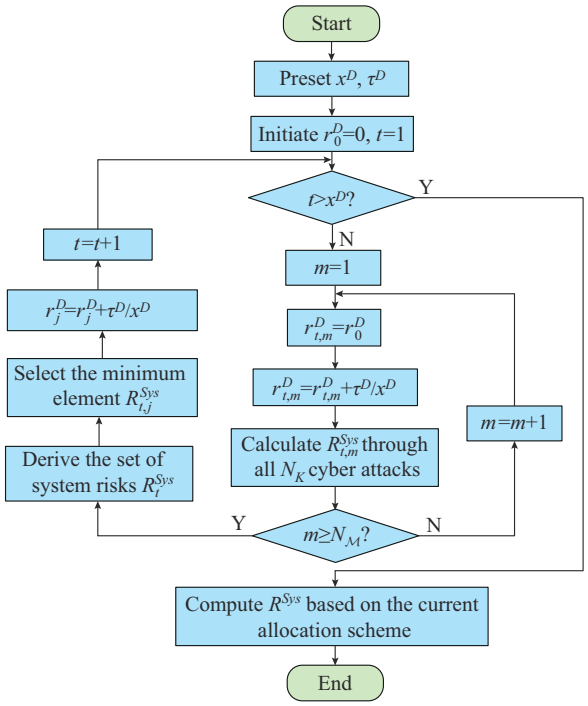

Fig. 3. Flow chart of proposed atomic allocation approach for defense resources.

Step 1: initialization. Initially, the defense resources on all measurement devices are set to be $r_0^D = 0$. The defense resource budget τ^D is divided into multiple atomic units according to the allocation precision x^D, and set the iteration counter $t = 1$.

Step 2: iteration of measurements. At the t^{th} iteration, deploy an atomic unit (i.e., τ^D/x^D) to each measurement as:

$$r_{t,m}^D = r_{t,m}^D + \tau^D/x^D \quad m = 1, 2, \ldots, N_{\mathcal{M}} \tag{30}$$

where $r_{t,m}^D$ is the deployed resource of the m^{th} measurement.

Then, calculate the system risk R^{Sys} under all the N_K possible cyber attacks, and the set of system risks after each measurement is equipped with an atomic unit can be obtained as:

$$R_t^{Sys} = \{R_{t,1}^{Sys}, R_{t,2}^{Sys}, \ldots, R_{t,m}^{Sys}, \ldots, R_{t,N_{\mathcal{M}}}^{Sys}\} \tag{31}$$

where $R_{t,m}^{Sys}$ is the system risk when the m^{th} measurement is equipped with an atomic unit at the t^{th} iteration.

Step 3: atomic unit allocation. Identify the minimum value in R_t^{Sys} (assumed to be the j^{th} element $R_{t,j}^{Sys}$), then assign the t^{th} atomic unit to the j^{th} measurement:

$$r_j^D = r_j^D + \tau^D/x^D \tag{32}$$

where r_j^D is the allocated resource for the j^{th} measurement.

Step 4: terminate evaluation. Except for the j^{th} measurement, defense resources of all the measurements are reset to be $r_0^D = 0$ for the next iteration. Moreover, set $t = t + 1$, if $t > x^D$, the iteration terminates, indicating that all the x^D atomic units have been distributed, and the system risk value R^{Sys} can be determined based on the current allocation scheme. Else, the iteration continues and returns to *Step 2*.

V. Case Study

A. Experimental Setup

The proposed security risk assessment method and risk-oriented defense resource allocation strategy are developed in MATLAB R2022b environment. The simulation is implemented on a PC with an Intel Core i5-10400F CPU and 32 GB RAM. To emulate the CPDN, an unbalanced distribution test feeder consisting of pseudo measurements, SCADA units, and PMUs is employed as the testbed for the proposed method. The standard IEEE 123-node test feeder is modified by integrating several DGs with a *P-Q* controlling strategy. Details of feeder configuration, line impedances, regulator data, and transformer data can be found in [39].

Referring to the U. S. National Vulnerability Database [40], specific information of the exploitable security loopholes at attack portals is tabulated in Table I, where each loophole is unique and denoted by a common vulnerability and exposure (CVE) -ID. The assigned values of CVSS scores are presented in Table II. With the CVSS scores, the exploitability of each loophole can be calculated by (3). Due to the multiplicity and accessibility of IEDs, their loopholes are assigned as L_1, L_4, L_5, L_6, and L_{12}. For routers and the access network, potential loopholes consist of L_2, L_3, L_9, and L_{11} with the moderate exploitability. L_7, L_8, and L_{10} are defined as the loophole of the substation due to its relatively secure cyberspace. Scale and shape parameters of the Pareto distribution are set as: $k_1 = 0.00161$ and $k_2 = 0.26$ [41]. For modeling the transition probability between logical nodes, the attacker's fraction *AF* and cost *AC* are set to be 0.9 and 100, respectively [42]. To derive the measurement vulnerability, the defender resource fraction *DF* is set to be 0.1 for all meter units [41], and the costs *DC* are set to be 100, 200, and 300 for the 127 pseudo measurements, 21 SCADA units, and 4 PMUs, respectively, to address their varying security levels [24].

TABLE I
EXPLOITABLE SECURITY LOOPHOLES AT ATTACK PORTALS

No.	CVE-ID	CVSS score	Exploitability
L_1	CVE-2016-5053	C^{AV}: N, C^{AC}: L, C^{AU}: N	0.5403
L_2	CVE-2020-10923	C^{AV}: A, C^{AC}: L, C^{AU}: N	0.3848
L_3	CVE-2015-7599	C^{AV}: N, C^{AC}: H, C^{AU}: N	0.3088
L_4	CVE-2018-5678	C^{AV}: N, C^{AC}: L, C^{AU}: N	0.5387
L_5	CVE-2018-19524	C^{AV}: N, C^{AC}: L, C^{AU}: N	0.5368
L_6	CVE-2020-8958	C^{AV}: N, C^{AC}: L, C^{AU}: N	0.5282
L_7	CVE-2018-0453	C^{AV}: L, C^{AC}: L, C^{AU}: S	0.1398
L_8	CVE-2015-4684	C^{AV}: N, C^{AC}: L, C^{AU}: S	0.1626
L_9	CVE-2014-8684	C^{AV}: A, C^{AC}: L, C^{AU}: N	0.3857
L_{10}	CVE-2014-3569	C^{AV}: A, C^{AC}: H, C^{AU}: N	0.2146
L_{11}	CVE-2015-4879	C^{AV}: N, C^{AC}: L, C^{AU}: S	0.4064
L_{12}	CVE-2015-2822	C^{AV}: N, C^{AC}: L, C^{AU}: N	0.5056

TABLE II
ASSIGNED VALUES OF CVSS SCORES

Metric	Level	Value
AV C^{AV}	Local (C^{AV}: L)	0.55
	Adjacent network (C^{AV}: A)	0.62
	Network (C^{AV}: N)	0.85
AC C^{AC}	High (C^{AC}: H)	0.44
	Medium (C^{AC}: M)	0.58
	Low (C^{AC}: L)	0.77
AU C^{AU}	Multiple (C^{AU}: M)	0.27
	Single (C^{AU}: S)	0.61
	None (C^{AU}: N)	0.85

B. Study of Security Risk Assessment

The CPDN is assumed to be exposed to external attacks in this subsection, whereby the budget value τ^D is initialized to zero without deploying defense resources. Load profiles are distributed in CPDN in the form of pseudo measurements, represented by all the nodal power injections except for the reference node at the slack bus in Fig. 4. Besides, the set of real-time measurements is constituted by SCADA units and PMUs, which are marked in yellow and pink in Fig. 4, respectively. Faced with realistic constraints, the attacker is assumed to possess a limited resource budget $\tau^A = 2000$ and distribute it evenly for each attack considering a bounded rationality. For each measurement, success probabilities of single-target cyber attacks are calculated and shown in Fig. 5. As can be observed, attacks against pseudo measurements generally yield a higher success rate of about 0.2, while the ones for SCADA units and PMUs are at relatively low levels (about 0.08 to 0.15). For a single-target attack, the success probability of each attack path is shown in Fig. 6. In Fig. 6(a), with more exploitable attack paths, pseudo measurements are more susceptible to cyber intrusions in contrast with SCADA units and PMUs in Fig. 6(b) and 6(c). This is because attack paths of pseudo measurements (40 paths) are significantly more than those against SCADA units or PMUs (24 paths). Since the success probabilities are computed by accumulating multiple paths according to (6), load profile attacks are therefore more likely to succeed in the CPDN.

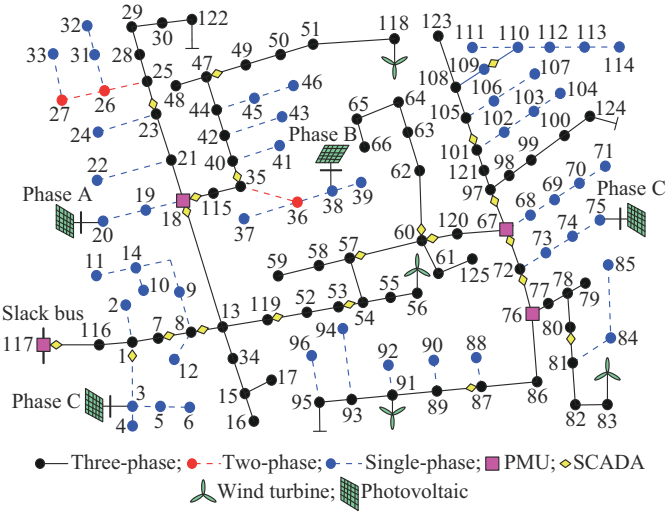

Fig. 4. Modified IEEE 123-node test feeder and its network topology.

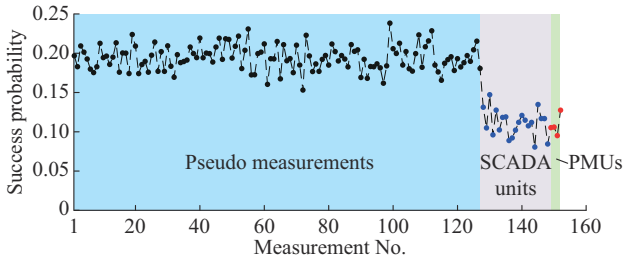

Fig. 5. Success probabilities of single-target cyber attacks for each measurement.

Coordinated cyber attacks can be categorized according to the number of targets, i.e., the attack indexed by $N_{\mathcal{M}}$ indicates that it randomly chooses $N_{\mathcal{M}}$ targets out of all the vulnerable measurements. This study considers coordinated cyber attacks indexed from 1 to 10 ($N_{\mathcal{M}} = 1, 2, \ldots, 10$), where each index is randomly launched 100 times against pseudo measurements, SCADA units, or PMUs. The risk $R^{CO}_{N_{\mathcal{M}}}$ and probability $P^{CO}_{N_{\mathcal{M}}}$ are cumulatively and averagely computed under different $N_{\mathcal{M}}$, respectively. Utilizing the security risk assessment method in Section III-B, success probabilities and induced risks of coordinated cyber attacks are summarized in Table III. It can be observed that attacks with a smaller index tend to yield a higher success possibility. This is because when $N_{\mathcal{M}}$ is greater than 2, calculating the success probability of a coordinated attack needs to involve a cumulative multiplication in (9), i.e., the success probability is inversely proportional to the number of attack targets, which is coincident with Remark 1. Overall, it can be concluded that the overall system risk R^{Sys} is mostly dominated by the first three attacks ($N_{\mathcal{M}} = 1, 2, 3$) since $\sum_{i=1}^{3} R_i^{CO} \Big/ R^{Sys} = 99.10\%$.

To validate the efficacy of the proposed method, two probabilistic risk assessment methods, namely, the method based on resource conversion coefficients (RCCs) [9] and the risk-based contingency screening (RCS) method [14], are used for benchmarking.

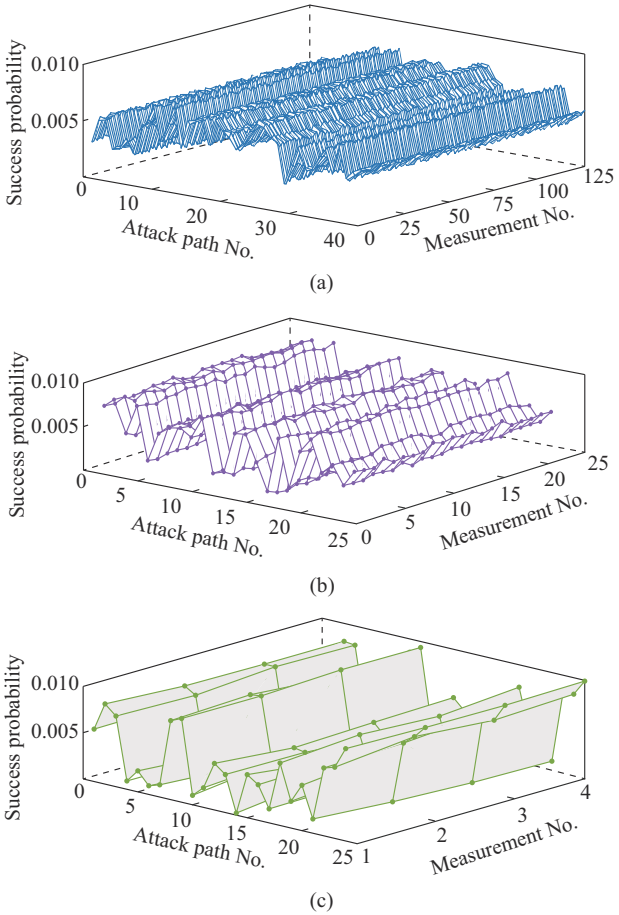

Fig. 6. Success probabilities of different attack paths of single-target attacks for each meter unit. (a) Pseudo measurements. (b) SCADA units. (c) PMUs.

TABLE III
SECURITY RISK ASSESSMENT RESULTS OF COORDINATED CYBER ATTACKS

$N_{\mathcal{M}}$	$P^{CO}_{N_{\mathcal{M}}}$	$R^{CO}_{N_{\mathcal{M}}}$	$N_{\mathcal{M}}$	$P^{CO}_{N_{\mathcal{M}}}$	$R^{CO}_{N_{\mathcal{M}}}$
1	1.7290×10^{-1}	18.1952	6	3.3802×10^{-6}	2.3012×10^{-3}
2	1.9400×10^{-2}	3.8387	7	6.2835×10^{-7}	4.5991×10^{-4}
3	6.1096×10^{-3}	1.2373	8	8.0135×10^{-8}	5.8516×10^{-5}
4	5.3866×10^{-4}	0.1984	9	1.3116×10^{-8}	1.0798×10^{-5}
5	1.1987×10^{-5}	0.0102	10	2.2315×10^{-9}	1.5379×10^{-6}

Cyber attacks with index $N_{\mathcal{M}}=1$ are first adopted against pseudo measurements since such a scenario exhibits the highest risk. Figure 7 shows the success probability of each attack path derived by the three methods. As can be observed, a large number of success probabilities are simply quantified by zero values using RCC and RCS, since the attack propagation process and complex cyberspace topology are not taken into account. By contrast, the attack paths for compromising a pseudo unit are well delineated by the proposed method, whose nonzero probabilities are much more realistic. Table IV presents the cumulative risk assessment results of different methods under one hundred random attacks against pseudo units with $N_{\mathcal{M}}=1,2,3$. The product of load reduction and load outage time is used by RCC as the evaluation metric. Analogously, RCS employs the maximum load shedding as the consequence indicator. However, it is noteworthy that CPDN operates under quasi-steady conditions and the cyber attack against system measurements would not instantly provoke significant load loss. Thus, true risk levels are undoubtedly underestimated by RCC and RCS, as shown in Table IV. In comparison, the number of falsified meter units well quantifies the physical impact of cyber attacks, thereby verifying the superiority of the proposed method.

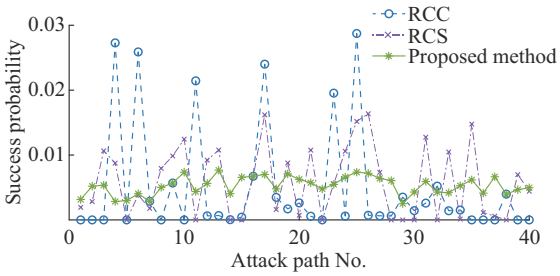

Fig. 7. Success probability of each attack path using different methods.

TABLE IV
CUMULATIVE RISK ASSESSMENT RESULTS OF DIFFERENT METHODS

Method	Security risk value $R^{CO}_{N_{\mathcal{M}}}$		
	$N_{\mathcal{M}}=1$	$N_{\mathcal{M}}=2$	$N_{\mathcal{M}}=3$
RCC [9]	4.4702×10^{-5}	2.2640×10^{-6}	9.3206×10^{-7}
RCS [14]	1.3010×10^{-1}	5.0400×10^{-2}	1.8591×10^{-3}
Proposed	2.1133×10^{1}	4.1695×10^{0}	1.2548×10^{0}

C. Study of Defense Resource Allocation

The formulated MOO and solution selection procedure are evaluated under coordinated cyber attacks against arbitrary measurements. Attack settings are the same as in Table III. The population size and maximum iteration numbers of NSGA-III are both set to be 100 [24], while interval limits for resource budget $[\tau^D_{\min},\tau^D_{\max}]$ and allocation precision $[x^D_{\min},x^D_{\max}]$ are $[0,10000]$ and $[2500,5000]$, respectively, to ensure the atomic unit is sufficiently small for accurate allocation. Figure 8 visually shows the obtained optimal Pareto solutions of MOO with $i_{rank}=1,2,3$. As can be observed, the overall risk value R^{Sys} falls off a cliff as the deployed defense resource budget τ^D gradually increases from zero. When the defense resource value is taken over 7500, risk values of all three nondomination ranks are reduced to less than 1. Besides, optimal Pareto solutions with higher i_{rank} yield a strong dominance over those with lower ranks, i.e., the scattered points with higher i_{rank} are generally closer to the origin $(0,0)$ as the MOO intends to simultaneously minimize the overall risk value R^{Sys} and limited resource budget τ^D.

Besides, it is noteworthy in Fig. 8 that when the deployed defense resource value is more than 6000, the corresponding decline in security risk value with $i_{rank}=1,2$ is quite insignificant. Therefore, to avoid excessive resource allocation, it is necessary to address the trade-off between system risk and restricted resource budget. Table V summarizes the optimality evaluation results of candidate strategies $s^D_1,s^D_2,\ldots,s^D_{10}$ from optimal Pareto solutions with $i_{rank}=1,2$, as shown by

the enlarged part in Fig. 8. According to the generational distance metric, the ideal vector is formed by the two minimum objectives in Table V as: $\langle R^{Sys}=1.7547, \tau^D=2270\rangle$. It can be observed that different solutions have been prioritized by the generational distance-based selection procedure in this table. The solution with lower ranks generally exhibits a significantly larger distance value, which indicates its suboptimality and verifies the strong dominance of higher-rank solutions. Among $s_1^D, s_2^D, \ldots, s_{10}^D$, strategy s_5^D with the least $\left\| Dis(\boldsymbol{X}_p) \right\|_2$ metric of 0.6426 is closest to the ideal vector in the two-dimensional space. As a result, the corresponding resource budget $\tau^D=2882$ is adopted for subsequent atomic allocation.

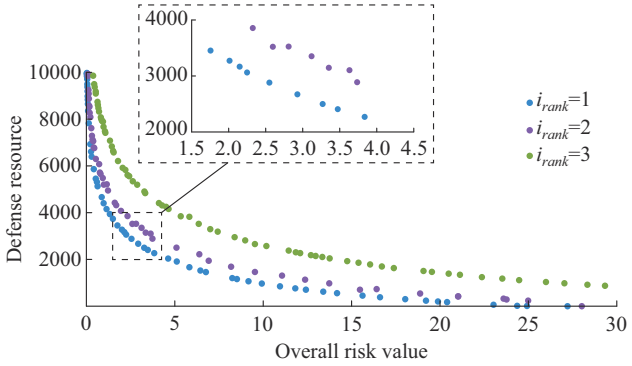

Fig. 8. Optimal Pareto solutions of MOO.

TABLE V
OPTIMALITY EVALUATION RESULTS OF OPTIMAL PARETO SOLUTIONS

Strategy	R^{Sys}	τ^D	$\left\| Dis(\boldsymbol{X}_p) \right\|_2$	i_{rank}
s_1^D	1.7547	3454	1.0000	1
s_2^D	2.0115	3273	0.8560	1
s_3^D	2.1477	3167	0.7808	1
s_4^D	2.2481	3063	0.7105	1
s_5^D	2.5493	2882	0.6426	1
s_6^D	2.9278	2673	0.6584	1
s_7^D	3.1192	3353	1.1253	2
s_8^D	3.2689	2500	0.7529	1
s_9^D	3.4729	2408	0.8336	1
s_{10}^D	3.8363	2270	1.0000	1

Existing allocation approaches [20] and [43] are employed to verify the superiority of the proposed atomic allocation approach. Assume the proposed security risk assessment method has been applied beforehand, and two contrastive approaches are integrated into the CPDN under the varying coordinated cyber attacks ($N_{\mathcal{M}}=1,2,\ldots,10$) in Table III as follows.

Approach I [20]: for a coordinated attack with index $N_{\mathcal{M}}$, the defense resource budget is distributed according to the risk ratio of each cyber attack as $(R^{CO}_{N_{\mathcal{M}}}/R^{Sys})\tau^D$.

Approach II [43]: the budget τ^D is first divided into multiple units by the allocation precision x^D. At each iteration, a single unit τ^D/x^D is assigned for the targets of a certain coordinated cyber attack that triggers the highest risk $R^{CO}_{N_{\mathcal{M}}}$.

Given the same budget value τ^D and allocation precision x^D (set as 5000 for satisfying the upper limit and ensuring accurate allocation), comparative defense resource allocation results for each measurement are presented in Fig. 9. It can be observed from Fig. 9(a) that Approaches I and II distribute the resource budget to specific pseudo measurements, while the vast majority of pseudo units are emplaced with a considerable amount of resource by the proposed approach. Comparing Fig. 9(b) with Fig. 9(a), it is observed that all three approaches allocate less resources for SCADA units and PMUs. The reason for this discrepancy is that numerous pseudo measurements have been introduced to CPDNs to address the low observability. In addition, Section V-B has demonstrated that pseudo units are more susceptible to cyber attacks than SCADA units and PMUs. Therefore, these approaches assign more resources for such measurements to alleviate the overall system security risk. Moreover, it can be observed from Fig. 9(b) that defense resources are not sufficiently deployed for each SCADA unit or PMU by Approaches I and II, e.g., the No. 1, No. 2, No. 3, No. 7, No. 24, and No. 25 measurements with zero resources. On the contrary, the iterative allocation procedure of the proposed approach ensures that each meter unit is equipped with at least one atomic unit of resource budget, thereby enabling system measurements not completely exposed to external attacks.

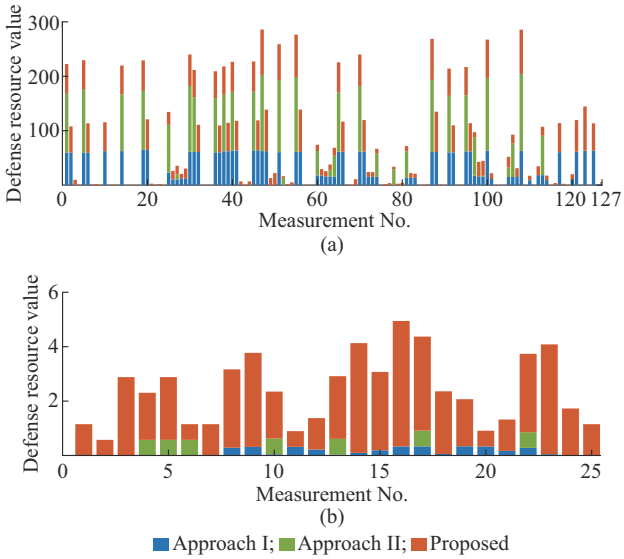

Fig. 9. Defense resource allocation results. (a) Pseudo measurements. (b) SCADA units and PMUs.

By applying the three allocation approaches, the risk incurred by each coordinated cyber attack and the overall system risk are both cumulatively calculated. As shown in Table VI, the overall system risk R^{Sys} is still dominated by attacks with $N_{\mathcal{M}}=1,2,3$, which is consistent with the results in Table III. According to Table VI, it is validated that the proposed approach can reduce the security risk more effectively than the other two benchmarks when $N_{\mathcal{M}}$ ranges from 1 to 10. This is because the iterative allocation mechanism of Ap-

proach I is dependent on the risk ratio of $R^{CO}_{N_{\mathcal{M}}}$ to R^{Sys}. Meanwhile, Approach II focuses on the coordinated cyber attack that triggers the highest risk $R^{CO}_{N_{\mathcal{M}}}$, indicating the low success probability of such an attack has been overlooked. By contrast, in all the attack scenarios, each atomic unit is deployed according to the fastest descent direction of R^{Sys}, thereby the measurement corresponding to the highest risk reduction value is prioritized by the proposed approach. As shown in the bottom row, the minimum overall system risk value can be derived using the proposed approach by contrast with Approaches I and II.

TABLE VI
SECURITY RISK VALUES USING DIFFERENT ALLOCATION APPROACHES

$N_{\mathcal{M}}$	Security risk value			
	No defense	Approach I	Approach II	Proposed
1	1.8195×10^{1}	6.2164×10^{0}	3.9439×10^{0}	1.5791×10^{0}
2	3.8387×10^{0}	2.3025×10^{0}	1.2984×10^{0}	5.1200×10^{-1}
3	1.2373×10^{0}	4.3120×10^{-1}	2.1750×10^{-1}	4.6000×10^{-3}
4	1.9840×10^{-1}	1.3200×10^{-2}	7.5392×10^{-3}	5.3725×10^{-4}
5	1.0200×10^{-2}	8.2942×10^{-4}	3.9350×10^{-4}	7.1204×10^{-5}
6	2.3012×10^{-3}	6.5645×10^{-5}	1.4296×10^{-5}	3.2655×10^{-6}
7	4.5991×10^{-4}	7.2703×10^{-6}	2.0103×10^{-6}	3.0728×10^{-7}
8	5.8516×10^{-5}	5.2238×10^{-7}	1.6333×10^{-7}	1.2726×10^{-8}
9	1.0798×10^{-5}	9.2246×10^{-8}	4.6166×10^{-8}	9.6958×10^{-10}
10	1.5379×10^{-6}	1.6478×10^{-8}	6.8449×10^{-9}	4.7354×10^{-10}
R^{Sys}	2.3483×10^{1}	8.9642×10^{0}	5.4677×10^{0}	2.0963×10^{0}

VI. CONCLUSION

This paper proposes a novel security risk assessment method and risk-oriented defense resource allocation strategy for CPDNs. By constructing an attack graph-based CPDN architecture, the success rate of a coordinated cyber attack and corresponding security risks are properly evaluated using the security risk assessment method. Moreover, the incurred risk is efficiently mitigated by the developed risk-oriented defense resource allocation strategy, in which the prioritized MOO solution is able to reasonably address the trade-off between security risk and limited resource budget. Extensive simulation results on the modified IEEE 123-node test feeder have verified the efficacy of the proposed method and strategy in evaluating security risk, solving the formulated MOO problem, and allocating limited defense resources in the presence of multiple coordinated cyber attacks.

Results derived from this paper can shed some light on the defensive studies for assessing the mounting cyberspace risks in CPDNs. A plausible defense resource allocation framework is also provided for addressing the security issues in modern CPDNs under cyber attacks. In the future, we will focus on taking additional vulnerable system components and a realistic cyber-physical coupling environment into account, so as to devise more comprehensive and representative risk assessment methods in the context of varying attack scenarios. Besides, the scalability of the proposed method and strategy in the variants of CPDNs, e.g., industrial control systems and industrial Internet of Things, is worthy of further investigation.

REFERENCES

[1] Y. Zhang, M. Ni, and Y. Sun, "Fully distributed economic dispatch for cyber-physical power system with time delays and channel noises," *Journal of Modern Power Systems and Clean Energy*, vol. 10, no. 6, pp. 1472-1481, Nov. 2022.

[2] Y. Yang, P. Zhang, C. Wang *et al*., "State transition modeling method for optimal dispatching for integrated energy system based on cyber-physical system," *Journal of Modern Power Systems and Clean Energy*, vol. 12, no. 5, pp. 1617-1630, Sept. 2024.

[3] D. Du, M. Zhu, X. Li *et al.*, "A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems," *Journal of Modern Power Systems and Clean Energy*, vol. 11, no. 3, pp. 727-743, May 2023.

[4] Z. Wei, K. Xie, B. Hu *et al*., "Distribution system restoration with cyber failures based on co-dispatching of multiple recovery resources," *Journal of Modern Power Systems and Clean Energy*, vol. 12, no. 4, pp. 1096-1112, Jul. 2024.

[5] K. Pan, A. Teixeira, M. Cvetkovic *et al.*, "Cyber risk analysis of combined data attacks against power system state estimation," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3044-3056, May 2019.

[6] S. Deng, J. Zhang, D. Wu *et al.*, "A quantitative risk assessment model for distribution cyber-physical system under cyber attack," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 3, pp. 2899-2908, Mar. 2023.

[7] S. Li, C. K. Ahn, and Z. Xiang, "Decentralized sampled-data control for cyber-physical systems subject to DoS attacks," *IEEE Systems Journal*, vol. 15, no. 4, pp. 5126-5134, Dec. 2021.

[8] W. He, S. Li, C. K. Ahn *et al*., "Sampled-data stabilization of stochastic interconnected cyber-physical systems under DoS attacks," *IEEE Systems Journal*, vol. 16, no. 3, pp. 3844-3854, Sept. 2022.

[9] H. Qin, J. Weng, D. Liu *et al.*, "Risk assessment and defense resource allocation of cyber-physical distribution system under denial of service attack," *CSEE Journal of Power and Energy Systems*, doi: 10.17775/CSEEJPES.2020.04550

[10] Y. Zhang, L. Wang, and Y. Xiang, "Power system reliability analysis with intrusion tolerance in SCADA systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 669-683, Mar. 2016.

[11] Z. Liu, W. Wei, L. Wang *et al*., "An actuarial framework for power system reliability considering cybersecurity threats," *IEEE Transactions on Power Systems*, vol. 36, no. 2, pp. 851-864, Mar. 2021.

[12] R. Zeng, Y. Cao, Y. Li *et al*., "A general real-time cyberattack risk assessment method for distribution network involving the influence of feeder automation system," *IEEE Transactions on Smart Grid*, vol. 15, no. 2, pp. 2102-2115, Mar. 2024.

[13] Y. Zhao, Y. Li, Y. Cao *et al*., "Risk-based contingency analysis for power systems considering a combination of different types of cyber-attacks," *Applied Energy*, vol. 348, pp. 1-10, Oct. 2023.

[14] Y. Zhao, Y. Cao, Y. Li *et al*., "Risk-based contingency screening method considering cyber-attacks on substations," *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4973-4976, Nov. 2022.

[15] W. Xia, D. He, and J. Chen, "On the PMU placement optimization for the detection of false data injection attacks," *IEEE Systems Journal*, vol. 17, no. 3, pp. 3794-3797, Sept. 2023.

[16] M. Zhang, Z. Wu, J. Yan *et al*., "Attack-resilient optimal PMU placement via reinforcement learning guided tree search in smart grids," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1919-1929, May 2022.

[17] H. Lei, S. Huang, Y. Liu *et al*., "Robust optimization for microgrid defense resource planning and allocation against multi-period attacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5841-5850, Sept. 2019.

[18] P. Lau, W. Wei, L. Wang *et al*., "A cybersecurity insurance model for power system reliability considering optimal defense resource allocation," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 4403-4414, Sept. 2020.

[19] C. Shao and Y. Li, "Optimal defense resources allocation for power system based on bounded rationality game theory analysis," *IEEE Transactions on Power Systems*, vol. 36, no. 5, pp. 4223-4234, Sept. 2021.

[20] W. Chen, W. Chen, and A. Xue, "Security risk assessment and defense resource allocation of power system under synergetic cyber attacks," *Power System Technology*, vol. 43, no. 7, pp. 2353-2360, Jul. 2019.

[21] Y. Song, X. Liu, Z. Li *et al*., "Intelligent data attacks against power

systems using incomplete network information: a review," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 4, pp. 630-641, Jul. 2018.
[22] G. Liang, S. R. Weller, J. Zhao *et al*., "The 2015 Ukraine blackout: implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317-3318, Jul. 2017.
[23] M. Zhou, C. Liu, A. A. Jahromi *et al*., "Revealing vulnerability of *N*–1 secure power systems to coordinated cyber-physical attacks," *IEEE Transactions on Power Systems*, vol. 38, no. 2, pp. 1044-1057, Mar. 2023.
[24] Y. Cheng, "State estimation in three-phase unbalanced distribution system with false data injection attacks," M. S. thesis, School of Cyber Science and Engineering, Southeast University, Nanjing, China, 2021.
[25] M. Schiffman. (2023, Sept.). Common vulnerability scoring system (CVSS). [Online]. Available: http://www.first.org/cvss/
[26] A. Ali, P. Zavarsky, D. Lindskog *et al*., "A software application to analyze affects of temporal and environmental metrics on overall CVSS v2 score," in *Proceedings of 2011 World Congress on Internet Security*, London, UK, Feb. 2011, pp. 1-5.
[27] S. Abraham and S. Nair, "Exploitability analysis using predictive cybersecurity framework," in *Proceedings of 2015 IEEE 2nd International Conference on Cybernetics*, Gdynia, Poland, Aug. 2015, pp. 317-323.
[28] N. Fardad, S. Soleymani, and F. Faghihi, "Cyber defense analysis of smart grid including renewable energy resources based on coalitional game theory," *Journal of Intelligent & Fuzzy Systems*, vol. 35, no. 2, pp. 2063-2077, Aug. 2018.
[29] S. Abraham and S. Nair, "Cyber security analytics: A stochastic model for security quantification using absorbing Markov chains," *Journal of Communications*, vol. 9, no. 12, pp. 899-907, Dec. 2014.
[30] NIST. (2023, Oct.). NIST special publication 800-82r3. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-82r3
[31] J. M. Hendrickx, K. H. Johansson, R. M. Jungers *et al*., "Efficient computations of a security index for false data attacks in power networks," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3194-3208, Dec. 2014.
[32] W. Hao, P. Yao, T. Yang *et al*., "Industrial cyber-physical system defense resource allocation using distributed anomaly detection," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22304-22314, Nov. 2022.
[33] Z. Sun, Y. Liu, and L. Tao, "Attack localization task allocation in wireless sensor networks based on multi-objective binary particle swarm optimization," *Journal of Network and Computer Applications*, vol. 112, pp. 29-40, Jun. 2018.
[34] K. Deb and H. Jain, "An evolutionary many-objective optimization algorithm using reference-point-based nondominated sorting approach, part I: solving problems with box constraints," *IEEE Transactions on Evolutionary Computation*, vol. 18, no. 4, pp. 577-601, Aug. 2014.
[35] K. Deb, A. Pratap, S. Agarwal *et al*., "A fast and elitist multiobjective genetic algorithm: NSGA-II," *IEEE Transactions on Evolutionary Computation*, vol. 6, no. 2, pp. 182-197, Apr. 2002.
[36] H. Jain and K. Deb, "An evolutionary many-objective optimization algorithm using reference-point based nondominated sorting approach, part II: handling constraints and extending to an adaptive approach," *IEEE Transactions on Evolutionary Computation*, vol. 18, no. 4, pp. 602-622, Aug. 2014.
[37] S. Jiang, Y. S. Ong, J. Zhang *et al*., "Consistencies and contradictions of performance metrics in multiobjective optimization," *IEEE Transactions on Cybernetics*, vol. 44, no. 12, pp. 2391-2404, Dec. 2014.
[38] G. Chen, Z. Y. Dong, D. J. Hill *et al*., "Exploring reliable strategies for defending power systems against targeted attacks," *IEEE Transactions on Power Systems*, vol. 26, no. 3, pp. 1000-1009, Aug. 2011.
[39] IEEE PES AMPS DSAS Test Feeder Working Group. (2023, Aug.). Resources. [Online]. Available: https://cmte. ieee. org/pes-testfeeders/resources/
[40] NIST. (2024, Jan.). National vulnerability database. [Online]. Available: https://nvd.nist.gov/
[41] S. Frei. (2009, Apr.). Security econometrics: the dynamics of (in) security. [Online]. Available: https://www. research-collection. ethz. ch/bitstream/handle/20.500.11850/151394/eth-154-02.pdf
[42] W. I. A. Mannai, "Development of a decision support tool to inform resource allocation for critical infrastructure protection in homeland security," Ph. D. dissertation, Naval Postgraduate School, Monterey, USA, 2008.
[43] L. Shi and Z. Jian, "Vulnerability assessment of cyber physical power system based on dynamic attack-defense game model," *Automation of Electric Power Systems*, vol. 40, no. 17, pp. 99-105, Sept. 2016.

Shuheng Wei received the B.S. degree in electrical engineering and its automation from Wuhan University, Wuhan, China, in 2020. He is currently pursuing the Ph.D. degree with the School of Electrical Engineering, Southeast University, Nanjing, China. His research interests include state estimation and cybersecurity of power distribution networks.

Zaijun Wu received the B. S. degree in power system and its automation from Hefei University of Technology, Hefei, China, in 1996, and the Ph. D. degree in electrical engineering from Southeast University, Nanjing, China, in 2004. From 2012 to 2013, he was a Visiting Scholar with Ohio State University, Columbus, USA. He is currently working as a Professor with the School of Electrical Engineering, Southeast University. His research interests include microgrid, active distribution network, and power quality.

Junjun Xu received the B. S. degree in power system and its automation from Nanjing Institute of Technology, Nanjing, China, in 2012, the M.S. degree in agricultural electrification and automation from the School of Electrical and Information Engineering, Jiangsu University, Zhenjiang, China, in 2015, and the Ph.D. degree in electrical engineering from Southeast University, Nanjing, China, in 2019. He is currently working as an Associate Professor with the College of Automation, College of Artificial Intelligence, Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests include distribution network state estimation, self-healing control, and uncertainty modeling approaches.

Yanzhe Cheng received the M.S. degree in cyberspace security from Southeast University, Nanjing, China, in 2021. She is currently working as an Engineer with Shenzhen Power Supply Bureau Co., Ltd., Shenzhen, China. Her research interests include cybersecurity and state estimation of cyber-physical distribution networks.

Qinran Hu received the B. S. degree in electrical engineering from the Chien-Shiung Wu Honors College, Southeast University, Nanjing, China, in 2010, and the M. S. and Ph. D. degrees in electrical engineering from the University of Tennessee, Knoxville, USA, in 2013 and 2015, respectively. He was a Postdoctoral Fellow with Harvard University, Cambridge, USA, from 2015 to 2018. He is currently working as a Professor with the School of Electrical Engineering, Southeast University. His research interests include distributed energy resource aggregation and power system operation optimization.