This article has been accepted for publication in IEEE Transactions on Power Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3078730

A Coalitional Cyber-Insurance Design Considering Power System Reliability and Cyber Vulnerability

Pikkin Lau, *Student Member, IEEE*, Lingfeng Wang, *Senior Member, IEEE*, Zhaoxi Liu, *Member, IEEE,* Wei Wei, and Chee-Wooi Ten, *Senior Member, IEEE*

***Abstract*—Due to the development of cyber-physical systems for modernizing power grids, vulnerability assessment has become an emerging focus in power system security studies. With the increasing deployment of cyber-enabled technologies in power systems, modern power system is prevalently exposed to a wide gamut of cybersecurity threats. Thus, there is an urgent need to develop effective cyber risk management mechanisms to mitigate the growing cyberthreats. Recently cyber insurance is emerging as a promising financial instrument for cyber risk management of critical infrastructures such as power grids. In this paper, a new cyber-insurance design framework is proposed to hedge against the risk of massive monetary losses due to potential cyberthreats. Traditionally, insurance companies serve as third-party risk-bearers offering aggregate design of the insurance policy which may stipulate high premiums. However, unusual loss patterns may still lead to excess financial risk for insurance companies. In this paper, coalitional insurance is introduced as a promising alternative or supplement to the traditional insurance plans provided by insurance companies. Under the proposed cyber-insurance model, several transmission operators form an insurance coalition, where the coalitional premiums are derived considering system vulnerabilities and loss distributions. The indemnity which covers the loss of TOs complies with the budget sufficiency. Overall, this study proposes a novel coalitional platform based cyber-insurance design that estimates the insurance premiums via cybersecurity modeling and reliability implication analysis.**

***Index Terms*—Cyber-physical energy systems, cyber-insurance, cyber risk management, power system reliability, power system security, actuarial design, probabilistic methods.**

NOMENCLATURE

A. Acronym

ICTs	Information and Communication Technologies
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
CPSs	Cyber-Physical Systems
SCADA	Supervisory Control And Data Acquisition
DMs	Defense Mechanisms
TTC	Time-To-Compromise
TO	Transmission Operator
LAN	Local Area Network
BN	Bayesian Network
BTTC	Bayesian Time-To-Compromise
CVSS	Common Vulnerability Scoring System
BCT	Beta Compromise Time
SSG	Stackelberg Security Game
DRA	Defense Resource Allocation
MILP	Mixed Integer Linear Programming
(T)VaR	(Tail)Value-at-Risk
TCE	Tail Conditional Expectation
ERW	Expected Reliability Worth
DFS	Depth-First Search
SMC	Sequential Monte Carlo
L/HDC	Low/High Defense Coverage
SDs	Standard Deviations
CoVs	Coefficients of Variation
RLC	Risk-Loading Coefficient

B. Notation

V	Set of the vulnerabilities
T_b	Bayesian Time-To-Compromise
t_β	Bayesian Compromise Time
t^*	Compromise Time
$\{G, A, C, S\}$	Gate, Authentication, Countermeasure, Substation
$\{t_1, t_2, t_3\}$	Mean times of the BCT processes
$\{P_1, P_2, P_3\}$	Probabilities of the BCT processes
v_h	A known or zero-day vulnerability
c_h	Successful vulnerability exploitation of v_h
$p(v_h)$	Probability of exploiting v_h
$p(v_h \wedge c_h)$	Probability that v_h is exploited by c_h
$p(c_h \mid v_h)$	Conditional probability of successfully exploiting v_h
$\mathbf{1}_{\{\cdot\}}$	True/false binary indicator of a conditional statement
$U(\cdot)$	Uniform distribution
$N(\cdot)$	Normal distribution
$\Phi(\cdot)$	Cumulative Density Function of $N(\cdot)$
s	Skill factor of the intruder
$\lvert v \rvert$	Number of known vulnerabilities of the component
σ	Total number of vulnerabilities
$m(s)$	Number of available exploits
$f(s)$	Usable exploits
$E(s, \lvert v \rvert)$	Number of estimated tries
$p(DM_w)$	Strength of the DMs
L_j	An attack leaf
$p(L_j)$	Probability that L_j is active
$p(L_j \wedge e_{DM})$	Probability that a set of DMs are attacked by L_j
τ_x	Target substation x
γ_x	Substation impact index of τ_x
α, β	Intruder and Defender
$\{U^c_{\beta,\tau_x}, U^u_{\beta,\tau_x}, U^c_{\alpha,\tau_x}, U^u_{\alpha,\tau_x}\}$	Covered/uncovered payoffs of α, β
$\mathcal{C}$	Defense coverage sequence
$p_{DC}(\tau_x)$	Defense coverage of τ_x
r	Correlation coefficient of the sampling copula
λ_x	Random sampling applied τ_x
$T_{b,x}$	BTTC of τ_x
$\boldsymbol{M} = \{M_q\}$	Defense resource budget vector
$\mathcal{L}_q$	Monetary loss of TO q
$\pi(\mathcal{L}_q)$	Premium of TO q
φ_q	Occurrence probability of the loss event
$\delta_{q,\varsigma}$	Probability TO q out of ς submits the claim

This work was supported by U.S. National Science Foundation (NSF) under awards ECCS1739485 and ECCS1739422.

P. Lau, L. Wang, and Z. Liu are with Department of Electrical Engineering and Computer Science, University of Wisconsin-Milwaukee, Milwaukee, WI 53211, USA.

W. Wei is with Department of Mathematical Sciences, University of Wisconsin-Milwaukee, Milwaukee, WI 53211, USA.

C.-W. Ten is with Department of Electrical and Computer Engineering, Michigan Technological University, Houghton, MI 49931, USA.

Π_q	Claim of TO q
Γ_q	Indemnity of TO q
$\mathbb{C}_q$	Commitment of TO q
$\rho(\mathcal{L}_q)$	RLC of TO q
$\underline{\Omega} = \{\Omega\}$	Load loss event set
K_Ω	Probability density kernel of loss event Ω
D_Ω	Duration of loss event Ω
$W(D_\Omega)$	Cost mapping function of loss event Ω

I. Introduction

THE looming cybersecurity issue on power grids due to the broad integration of ICTs has attracted extensive attention in recent years [1]. In response to the increasing cyber vulnerability, NERC has stipulated a series of cybersecurity standards [2], and NIST updated the framework for improving critical infrastructure cybersecurity in 2018 [3], respectively. To de-risk the integration of innovative ICTs in CPSs including electric power grids, much research effort has been dedicated to efficient cyber-vulnerability assessment. Ten *et al.* [4] integrated the cyber-physical information of substations into evaluating vulnerability of the SCADA systems. DMs for the vulnerabilities have been proposed to reduce the potential losses. Based on the attack cost, the power system vulnerability can be quantified by the security mechanisms [5]. With the vulnerability data, quantitative metrics could be developed to predict system compromises caused by random cyber adversaries. Probabilistic approaches can be applied in the security assessment of cyber-physical systems. For example, attack graph is used as a hierarchical graphic tool for vulnerability assessment combining intrusion scenarios and corresponding DMs. Various attack graphs are proposed to examine the network hardening options, the dependency, and the network security [6]-[8].

Meanwhile, various quantitative security metrics have been proposed to measure the impact of cyberthreats. McQueen *et al.* [9] proposed TTC modeling based on the data of vulnerability and exploits. Zieger *et al.* [10] eliminated arbitrary values by modeling the distribution of the attackers' proficiency. Given the vulnerability and skill level of an attacker, TTC quantifies various defense mechanisms against the long-term impact of risks and cyberattacks by predicting the time required to compromise a system. Zhang *et al.* [11] addressed the attacker's aspect in reliability evaluation by assessing the cybersecurity using TTC derived from attack graphs. The k-Zero Day Safety metric estimates the number of unknown vulnerabilities required to compromise the network system [12]. To gauge the capability of CPS to recover from multiple system contingencies, resilience metrics were developed to integrate graph theory with the vulnerability scoring system in power grids [13].

More recently, different from the emerging technological or regulatory solutions (e.g., grid hardening, attack-tolerant operational and planning strategies, and industry best practices), cyber-insurance is considered a promising financial instrument to enable efficient cyber risk management. For example, a holistic reliability assessment based cyber-insurance design has been demonstrated in [14]. Moreover, coalitional cyber-insurance has been proposed for the general network security, where a coalition is formed to distribute cyber risks among the cooperative organizations without transferring the risk to a third party [15]. As cyber-insurance for critical energy infrastructures is still an infant field so far, further exploration would be needed to effectively quantify the impacts of cyber vulnerability on the power supply reliability and their actuarial implications.

The coalitional insurance [15] can be viewed as a variation of the mutual insurance considering individual characteristics. While its core idea is similar to the mutual insurance design [16], coalitional insurance also concerns specific characteristics. More specifically, in determining the amount of contribution (premium) from each participant, mutual insurance relies on the statistical characteristic of the population while coalitional insurance emphasizes more on the individual characteristics. This paper presents a coalitional cyber-insurance design applied to cyber-physical power systems.

A. Contributions

In this study, a novel cyber-insurance framework is proposed based on a coalition platform concept for the modern cyber-physical power grids. To the best knowledge of authors, it is the first time that a coalitional cyber-insurance premium design is tailor-made for the power system networks. We design an actuarial premium principle that effectively reflects the security investment of TOs based on an integrated reliability and cyber-vulnerability analysis of power grids. The major contributions of this paper are listed as follows:

- A novel coalitional cybersecurity-insurance framework for power systems is devised. The proposed framework performs reliability analysis accounting for the cyber vulnerability and estimates the premiums of TOs based on reliability worth analysis.
- A new graphic security assessment approach is developed where cyber-vulnerability is estimated by considering all feasible nodal routes from the intruder's perspective. It is critical to distribute the security-enhancing budget in each TO judiciously through proper defense resource allocation scheme.
- A coalitional cyber-insurance design is proposed as an alternative or supplement to the conventional insurance administered by third-party insurers. In the proposed coalitional insurance model, TOs serve as both insurers and insureds.

The remainder of this paper is organized as follows. A graphic model for performing integrated cybersecurity-reliability assessment is proposed in Section II. Section III presents a new coalitional cyber-insurance premium principle. Results of the case studies are discussed in Section IV. Concluding remarks are given in Section V. The Appendix is dedicated to deriving the security game and its equilibrium conditions discussed in Section II.

B. Comparison with Related Work

To further highlight the contributions of this paper, a brief comparison is made with several related studies. Relations of these works are concisely described as follows. In [14], cyber-insurance model was established in light of the loss interdependence in reliability. This paper provides an alternative cyber insurance framework to [14] based on the concept of coalitional insurance platform in [15] and risk estimation in [10]. We propose a novel cyber-insurance design, and the associated premiums are reasonably estimated according to respective cybersecurity scenarios. Inspired by a unified framework of reliability and cyber vulnerability introduced in [11], together with security metrics from [9], [17], our holistic graphic model for cyber systems is tailored for mutual dependence of vulnerability across the operators. The comparison with related work described above is concisely tabulated in Table I. This paper should be considered one of the first endeavors in the development of coalitional cyber-insurance for correlated power system operators.

TABLE I Comparison with Related Work

	This work	**[14]**	**[15]**	**[11]**	**[9],[10],[17]**
RA	O	O		O	
CPE	O	O			
CI	O		O		
LI	O	O			
CSM	O	O		O	O
HGCM	O				

* RA = Reliability Assessment, CPE = Cyber Premium Evaluation, CI = Coalitional Cyber-Insurance, LI = Loss Interdependence, CSM = Cyber-Security Metric, HGCM = Holistic Graphic Cyber Model.

This article has been accepted for publication in IEEE Transactions on Power Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3078730

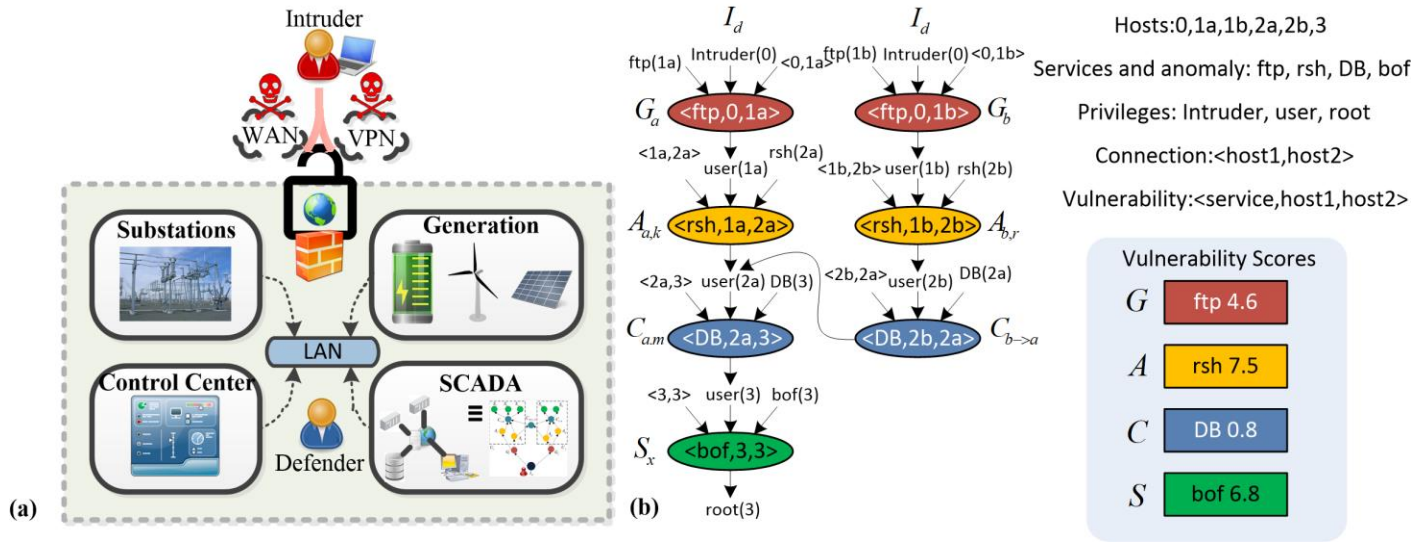


Fig. 1. (a) Graph-based cyber-physical model considering network vulnerabilities. (b) Schematic BN-based attack graph for the cyber-vulnerability in the SCADA systems.

II. Graphic Model for Assessing Cybersecurity

A. Overview of the Cyber Model

Referring to Fig. 1(a), the typical cyber-physical configuration in power systems includes a control center, generation, substations, and the SCADA system interconnected by LAN. Here is a probable attack scenario. The potential intruder initiates a security game with the power system operator/defender by infiltrating the firewall. In this game, the intruder may profit from the ransoms paid by the defender. When the defender fails to pay the demanded ransom, the intruder who obtained the root privilege of the application servers in the SCADA system sends false commands to the relay to trip the breakers of the substations. As a result, the generation units and transmission lines are disconnected, causing load interruption and corresponding monetary loss of the TO.

The cyber model includes vulnerability nodes connected by the networking links. The cyber model of network vulnerability can be represented by an attack graph of BN. BN is a probabilistic approach suited to estimate the combinational impact of the vulnerabilities and synthesize security metrics such as TTC [17], [18]. In cybersecurity assessment, attack graph is a stochastic modeling tool. The intruder targets on the root privilege to sabotage the server commanding a power system substation. To obtain the root privilege of the application server, the intruder needs to exploit n vulnerabilities. The vulnerability nodes are denoted by the ovals with colors corresponding to respective hierarchies. The connection provides a necessary link between two hosts through a vulnerability node. Privilege defines the allowable actions in the host. The intruder utilizes services to access the privilege via the connection. The intruder needs to meet three preconditions to complete a nodal vulnerability exploitation in the BN: Service ($\mathcal{S}_h$), Connection ($\mathcal{N}_h$), and Privilege ($\mathcal{P}_h$) which are assumed to be mutually independent.

As shown in *Definition 1*, the BTTC can be formulated using the BN-based attack graph and t_β of the respective vulnerability nodes. Denote $c_h = \mathcal{S}_h \wedge \mathcal{N}_h \wedge \mathcal{P}_h$ at each vulnerability v_h. The probability of exploiting the known or zero-day vulnerability v_h is $p(v_h)$. The conditional probability $p(c_h|v_h)$ is either determined by a random vulnerability that follows a uniform distribution or synthesized by a series of such vulnerabilities. The probability that the vulnerability v_h is exploited by the successful exploitation condition c_h is $p(v_h \wedge c_h)$, the product of $p(v_h)$ and $p(c_h|v_h)$. The BTTC is synthesized by further taking into account the BCT of all vulnerabilities from the intruder to the root privilege.

***Definition 1*:** Bayesian Time-To-Compromise of the Substations

$$T_b = \frac{\sum_{v_h \in V} t_\beta(v_h) p(v_h \wedge c_h)}{p(c_h)} \tag{1-A}$$

Subject to:

$$t_\beta(v_h) = \begin{cases} t_\beta(|v|), v_h \notin S \ \ (Definition\ 2) \\ t_\beta(C_s), v_h \in S \ \ (Definition\ 3) \end{cases} \tag{1-B}$$

$$p(v_h) = \frac{CVSS}{10} * U(0,1) \tag{1-C}$$

$$p(c_h|v_h) = \begin{cases} U(0.8,1) * \mathbf{1}_{\{c_h=T\}}, h = 1 \\ p\left(c_h \middle| v_h \wedge (v_1 \vee \ldots \vee v_{h-1})\right), n \geq h \geq 2 \end{cases} \tag{1-D}$$

$$p(v_h \wedge c_h) = p(v_h) * p(c_h|v_h) \tag{1-E}$$

$$p(c_h) = \sum_{l=1}^{n} p(c_h|v_l) p(v_l) \tag{1-F}$$

The BTTC evaluates the capability of respective substations to resist against the network adversary.

As shown in Fig. 1(b), to disrupt the substation operation, the intruder I_d Intruder(0) needs to compromise a series of vulnerability nodes $V = \{G, A, C, S\}$ to obtain the root privilege root(3): Gate node (G), Authentication node (A), Countermeasure node (C), Substation node (S).

Feasible attack sequences are:

A1. Within a TO $I_d \to G_a \to A_{a,k} \to C_{a,m} \to S_x$

A2. Across different TOs $I_d \to G_b \to A_{b,r} \to C_{b\to a} \to C_{a,m} \to S_x$

CVSS comprises base score, temporal score, and environmental score that take a wide range of attack factors into account, including confidentiality, integrity, availability, attack complexity, privileges required, and exploit code maturity [19]. Services are designated with respective scores in CVSS, which is an open-access vulnerability evaluation system. For instance, file transfer protocol (ftp), remote shell service (rsh), and database server (DB), together with the anomaly of buffer overflow (bof), are implemented in the vulnerability nodes V. Interested readers are referred to [11], [13] for more detailed descriptions.

B. Exploitation of Cyber-Vulnerability

Referring to Fig. 2, define t^* as the average time that the intruder spends in successfully exploiting the vulnerability. In [9], t^* was decomposed into three mutually exclusive stochastic processes whose mean times and probabilities are $\{t_1, t_2, t_3\}$ and $\{P_1, P_2, P_3\}$, respectively.

This article has been accepted for publication in IEEE Transactions on Power Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3078730

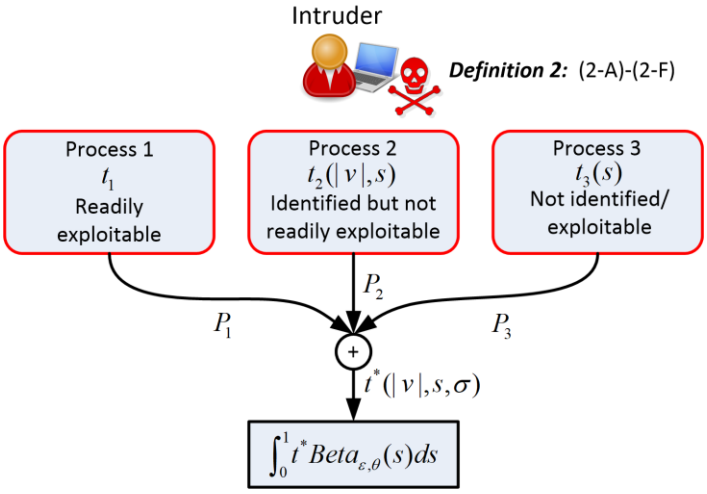


Fig. 2. Block diagram of the processes estimating Beta Compromise Time (Definition 2).

In Process 1, at least one exploit (readily exploitable vulnerability) is available to the intruder. Process 2 indicates at least one vulnerability is identified, while no exploit is available to the intruder. In Process 3, the intruder searches new vulnerability since no vulnerability can be exploited or identified by the intruder. One of the processes is active only when the other two are inactive. Note that the unidentified vulnerabilities may include, but not be limited to, eavesdropping a legitimate password through social engineering, obtaining a stolen password from an insider, and any coordination between the insider and the intruder.

In *Definition 2*, when calculating the stochastic metrics of these processes, a few variables should be taken into consideration: $|v|$ is the number of known vulnerabilities of the component; m is the number of available exploits; σ is the total number of vulnerabilities; $s \in [0,1]$ is the skill level factor; and E is the number of estimated tries, with auxiliary variables u and ξ. E is redefined in [10] to be a monotonically decreasing function with $|v|$. The rationale for E is that less estimated tries are needed given more vulnerabilities.

Ultimately, various degrees of the skill level s curve-fitted by a Beta distribution are accounted for. The Beta Compromise Time (BCT) t_β over the distribution in exploiting the vulnerability is calculated with $(\varepsilon,\theta) = (1.5,2.0)$ according to [10]. Interested readers are referred to [9] and [10] regarding the selection of other constants. Since the cyber model preserves the flexibility for TOs to stipulate defense mechanisms, BCTs of the countermeasure nodes are estimated in a different fashion, with details to be discussed in the next subsection.

C. Modeling of the Countermeasure Nodes

The attack tree in Fig. 3 describes the attacks based on the combinational event sets of countermeasure nodes that may result in substation failure [6], [11]. The defense mechanisms DM1-DM8 are the frontmost entries that safeguard the substations. In *Definition 3*, the defense coverage $p_{DC}(C_s)$ is the manageable resilience at each countermeasure node C_s. The relative strength of the DM is $p(DM_w)$, where η is the number of levels of the countermeasure, χ is the normalizing constant, and p_u is the randomness adjustment following a uniform distribution. Following this design, $p(DM_w)$ lies in [0,1] and manifests η discrete levels of defense strengths against the cyber adversary.

***Definition 2*:** Beta Compromise Time Estimation (except Countermeasure Nodes)

$$t_\beta(|v|) = \int_0^1 t^*(|v|,s,\sigma) * Beta_{\varepsilon,\theta}(s)ds \quad (2\text{-A})$$

Subject to:

$$t^* = t_1P_1 + t_2P_2 + t_3P_3 \quad (2\text{-B})$$

$$\begin{cases} P_1 = 1 - e^{-|v|*\frac{m(s)}{\sigma}} \\ P_2 = (1-P_1)(1-u) \\ P_3 = 1 - P_1 - P_2 \end{cases} \quad (2\text{-C})$$

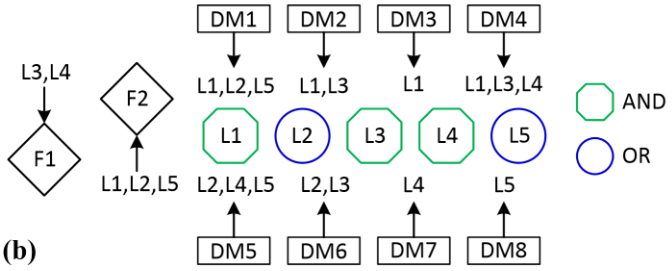
$$\begin{cases} t_1 = 1 \\ t_2 = 5.8E(s,|v|) \\ t_3 = (\frac{1}{f(s)} - 0.5)30.42 + 5.8 \end{cases} \quad (2\text{-D})$$

$$\begin{cases} m(s) = 83 * 3.5^{4s/2.7} - 82 \\ f(s) = 0.145 * 2.6^{2s+0.07} - 0.1 \\ u = \left(1 - f(s)\right)^{|v|} \\ \bar{f} = f(s) * |v| \end{cases} \quad (2\text{-E})$$

$$\begin{cases} E(s,|v|) = E_1(s,|v|) + E_2(s,|v|) \\ E_1(s,|v|) = \xi(\lfloor \bar{f} \rfloor, |v|) * (\lceil \bar{f} \rceil - \bar{f}) \\ E_2(s,|v|) = \xi(\lceil \bar{f} \rceil, |v|) * (1 - \lceil \bar{f} \rceil + \bar{f}) \\ \xi(b,|v|) = \frac{b}{|v|} + \frac{b(|v|-b)!}{|v|!}\bar{\xi} \\ \bar{\xi} = \sum_{t=2}^{|v|-b+1} \left[\frac{t(|v|-t+1)!}{(|v|-b-t+1)!(|v|-t+1)}\right] \end{cases} \quad (2\text{-F})$$

(a) Defense Mechanism (DM), Attack leaves(L), and Failure goals(F)

DM1	Configure LAN firewall
DM2	IP policy, filter rules and address rearrangment
DM3	Install intrusion tolerant system with backup capacity
DM4	Audit the user privileges to application server
DM5	Network analyzer, forensic tool, and traffic scanner
DM6	Digital token, certificate, and biometric verification
DM7	Data integrity check, security patch and anomaly record
DM8	Enact password policy: age, length, and character types
L1	Intercept TO command
L2	Duplicate substation information
L3	Gain the privilege of the targeted server
L4	Launch the active attack
L5	Exhaust the communication bandwidth
F1	Island the substation
F2	Trigger unexpected generation offline



(b)

Fig. 3. (a) Description of the (b) attack tree of the countermeasure nodes including defense mechanisms against attack leaves resulting in failure goal (Definition 3).

Define e_{DM} as the exploits of the DMs. Since DMs are mutually independent, the probability that all/one of a set of DMs are attacked by a local attack leaf L_j. Specifically, logical AND L_j triggered is conservatively activated by the most robust DM. Logical OR L_j triggered is aggressively activated by the most vulnerable DM. The countermeasure node C_s is compromised if either of the failure goals (F_1, F_2) is activated by all the preceding attack leaves $\{L_j\}$.

***Definition 3*:** Beta Compromise Time of Countermeasure Nodes

$$t_\beta(C_s) = \min(t_{\beta,F1}, t_{\beta,F2}) \tag{3-A}$$

Subject to:

$$\begin{cases} t_{\beta,F1} = t_{\beta,L3} + t_{\beta,L4} \\ t_{\beta,F2} = t_{\beta,L1} + t_{\beta,L2} + t_{\beta,L5} \end{cases} \tag{3-B}$$

$$t_{\beta,L_j} = \frac{t_\beta(v_j)p(L_j \wedge e_{DM})}{p(L_j)} \tag{3-C}$$

$$p(DM_w) = \chi * [\eta * p_{DC}(C_s)] + p_u \tag{3-D}$$

$$\begin{cases} p_{AND}(L_j \wedge e_{DM}) = \prod_w p(DM_w) \\ p_{OR}(L_j \wedge e_{DM}) = 1 - \prod_w [1 - p(DM_w)] \end{cases} \tag{3-E}$$

$$\begin{cases} p_{AND}(L_j) = \max\limits_w \{p(DM_w)\} \\ p_{OR}(L_j) = \min\limits_w \{p(DM_w)\} \end{cases} \tag{3-F}$$

In the following subsection, the algorithm for allocating the defense resources on the countermeasure nodes will be introduced.

D. Physical Model and Defense Resource Allocation

Applications of the game theory vary from reducing the variation of the local network load profile [20], managing the inter-grid energy exchange [21] to bargaining energy prices [22], among many others. Game-theoretic algorithms have been applied to distribute the security resources or alleviate possible load curtailments based on the cyber-physical network connection subject to cyberattack intrusion [23]. SSG is a hierarchical approach to arrange the security resources. Marginal strategy representation of the SSG can relieve the computational burden for the defense resource allocation [24].

Compact-form SSG algorithms have been developed to facilitate protection of the targets subject to attacks. Each TO conducts its own DRA optimization. In a two-player compact SSG, rival agents carry out strategies sequentially. The defender specifies its strategy preceding the best strategy selected by the intruder. Either player in the game can be an exact one entity or a group of entities. In the target set $\{\tau_x\}$, a target substation τ_x in service is either covered or uncovered by the defender. The respective payoff values are the expected values calculated based on the payoffs of covered and uncovered attacks, $\{U^c_{\alpha,\tau_x}, U^u_{\alpha,\tau_x}\}$ for the intruder α, and $\{U^c_{\beta,\tau_x}, U^u_{\beta,\tau_x}\}$ for the defender β. The payoffs can be assigned according to the criticality of the substation or the substation load. The defense coverage investment on the respective countermeasure nodes corresponding to the target substations can be allocated up to the defense resource budget $\boldsymbol{M}$ that quantifies the security sparsity against the potential cybersecurity hazards experienced by the respective TOs.

Optimization 1 achieves optimal DRA by maximizing the defender's payoff [25] in each of the TOs. Benefitting from the MILP formulation, DRA via *Optimization 1* can be completed in polynomial time. TO operators can invest defense resource coverage $\mathcal{C} = \{p_{DC}(\tau_x)\}$ to individual substations based on the available security budget and the rank of criticality.

E. State Duration Sampling

The BTTC T_b quantifies the duration in which individual substations would be compromised. To emulate the randomness of the cyberattacks, the exponential variate for each substation τ_x is generated through a simple logarithmic operation. $T_{b,x}$ has exponential sample $\hat{T}_{b,x}$. Substituting into cumulative distribution function of the standard normal distribution Φ, a set of uniform variates can be obtained. In this paper, λ sampled from the uniform distribution is replaced by a sample extracted from a correlated set $\{\lambda_x\}$, with correlation coefficient r. The same set produces the correlated loss pattern in the respective TOs.

Optimization 1: DRA via Maximal Defender Payoff
Input: $U^c_{\beta,\tau_x}, U^u_{\beta,\tau_x}, U^c_{\alpha,\tau_x}, U^u_{\alpha,\tau_x}, \boldsymbol{M}$
Output: $\{p_{DC}(\tau_x)\}$
/* $\boldsymbol{M} = \{M_q\}$ */

$$\max d \tag{4-A}$$

Subject to:

$$a_{\tau_x} \in \{0,1\} \tag{4-B}$$

$$\textstyle\sum_{\tau_x} a_{\tau_x} = 1 \tag{4-C}$$

$$p_{DC} \in [0,1] \tag{4-D}$$

$$\textstyle\sum_{\tau_x} p_{DC}(\tau_x) \le M_q \tag{4-E}$$

$$d - U_\beta(\mathcal{C}, \tau_x) \le (1 - a_{\tau_x})Z \tag{4-F}$$

$$0 \le k - U_\alpha(\mathcal{C}, \tau_x) \le (1 - a_{\tau_x})Z \tag{4-G}$$

where $d \ge U_\beta(\mathcal{C}, \tau_x), \forall \tau_x$ and Z is an arbitrarily large number.

Algorithm 1: BTTC State Duration Sampling

Input: $P_{L,x}, P_{L,total}, \mu_v, U^c_{\beta,\tau_x}, U^u_{\beta,\tau_x}, U^c_{\alpha,\tau_x}, U^u_{\alpha,\tau_x}, \boldsymbol{M}, r$
Output: $\hat{T}_{b,x}$

/*Assign the defense coverage using the security game*/
FOREACH TO q
  FOREACH target substation x
    Compute Substation Impact Index γ_x using (5)
    Compute the defender's and intruder's payoffs:
      $U_\beta(\mathcal{C}, \tau_x) \leftarrow \gamma_x\{p_{DC}(\tau_x)U^c_{\beta,\tau_x} + (1 - p_{DC}(\tau_x))U^u_{\beta,\tau_x}\}$
      $U_\alpha(\mathcal{C}, \tau_x) \leftarrow \gamma_x\{p_{DC}(\tau_x)U^c_{\alpha,\tau_x} + (1 - p_{DC}(\tau_x))U^u_{\alpha,\tau_x}\}$
  END
  Designate $\mathcal{C} = \{p_{DC}(\tau_x)\}$ using *Optimization 1*.
END
/*Estimate Beta Compromise Time*/
Evaluate $t_\beta(|v|)$ using *Definition 2*
Evaluate $t_\beta(C_s)$ using *Definition 3*
/*Sample the stochastic state duration for each target substation*/
FOREACH TO q
  $N_{cq} \leftarrow rN_t + \sqrt{1 - r^2}N_{nq}$
/* $N_t, N_{n1}, \ldots, N_{ny} \sim N(0,1)$, $r \in [0,1]$ */
END
/*Generate correlated set $\{\lambda_x\}$ of uniform distribution*/
/*Generate state duration sampling $\hat{T}_{b,x}$*/
FOREACH target substation x
  $\lambda_x \leftarrow \Phi(N_x)$
  Calculate $T_{b,x}$ using *Definition 1*
  $\hat{T}_{b,x} \leftarrow -T_{b,x} \ln \lambda_x$
END

Algorithm 1 summarizes the procedure of state duration sampling by evaluating the BTTC over cyber vulnerabilities. To indicate the load criticality of the substation τ_x, a substation impact index is devised as a weighting coefficient:

$$\gamma_x = (1 + \frac{P_{L,x}}{P_{L,total}})^{\mu_v} \tag{5}$$

where $P_{L,x}$ is the load at the substation τ_x, $P_{L,total}$ is the total load in the system, and μ_v is the number of adjacent substations.

Following *Optimization 1*, BCT of the vulnerability nodes can be synthesized into BTTCs according to *Definitions 2,3*. BTTCs serve as the mean values in state duration sampling.

***Optimization 2*:** Reliability Load Curtailment Estimation

$$\min \{\textstyle\sum_x \boldsymbol{K}_x\}_v \tag{6-A}$$

Subject to:

$$\boldsymbol{B\theta + G + K_x = D_{cap}} \quad \text{(6-B)}$$

$$\boldsymbol{|F| \le F_{cap}} \quad \text{(6-C)}$$

$$\boldsymbol{0 \le K_x \le D_{cap}} \quad \text{(6-D)}$$

$$\boldsymbol{0 \le G \le EN(\tau_x) * G_{cap}} \quad \text{(6-E)}$$

$$EN(\boldsymbol{\tau_x}) = \mathbf{1}_{\{\nu \in \hat{T}_{b,x}\}} \quad \text{(6-F)}$$

where

$\boldsymbol{K_x}$	Load curtailment vector (MW)
ν	Time step of the reliability assessment
$\boldsymbol{B}$	Substation susceptance vector
$\boldsymbol{\theta}$	Vector of the substation voltage angles (rad)
$\boldsymbol{G}$	Vector of the available generation (MW)
$\boldsymbol{G_{cap}}$	Generation capacity vector (MW)
$\boldsymbol{D_{cap}}$	Load capacity vector (MW)
$\boldsymbol{F}$	Transmission power flow vector (MW)
$\boldsymbol{F_{cap}}$	Thermal limit vector of the transmission lines (MW)
$EN(\boldsymbol{\tau_x})$	Enabling function of the substations
$\mathbf{1}_{\{\cdot\}}$	True/false binary indicator of a conditional statement
$*$	Element-wise product operator

F. Reliability Assessment

Based on the respective strengths against cyberattacks, a stochastic $\hat{T}_{b,x}$ sampled in **Algorithm 1** is assigned to individual substations, determining the online generation capacity. Specifically, if the intruder compromises the root privilege of the substation server, a false tripping command is assumed to be sent to the substation relays, leading to generation offline. For further clarification, *Optimization 2* is used to explain the minimization of aggregate substation load loss $\sum_x \boldsymbol{K_x}$ subject to cybersecurity threats in each observed time step ν. In each substation server, an enabling function $EN(\cdot)$ is implemented to set the upper bound $EN(\boldsymbol{\tau_x}) * \boldsymbol{G_{cap}}$ of the generation $\boldsymbol{G}$ by checking whether the time step ν lies in the interval defined by $\hat{T}_{b,x}$, returning 1 if true and 0 otherwise. In addition, the feasible load curtailment $\boldsymbol{K_x}$ and the power flow must never exceed the load capacity $\boldsymbol{D_{cap}}$ and the transmission thermal limit $\boldsymbol{F_{cap}}$, respectively.

Finally, the equality constraint of energy conservation between generation supply and load demand should be met at all time. In the following section, the cyber-insurance premium devised for different TOs and the indemnity mechanism will be presented.

III. Design of Cyber-Insurance Premium

Cyber-insurance is envisioned as a promising financial instrument for the TOs against unpredictable losses. The cyber insurance is in place as a safety net for the power system operators who could otherwise suffer unpredictable monetary losses due to blackouts or load interruption induced by consequential cyberattacks. To incorporate the financial impact of cyberattacks on the economically related entities, it is essential for the premium package to encompass the statistics across the insured entities. However, implementing cyber insurance is difficult in practice due to a relatively small insured pool with large indemnities. Thus, novel insurance principles customized for the cyber-insurance are proposed to resolve the dilemma. A desirable cyber insurance design should allow sufficient total premiums to substantially, if not completely, cover all claims and fairly distribute premiums among the insureds.

To this end, two risk measures, VaR and TVaR, are introduced below. Specifically, VaR measures the riskiness of a portfolio through percentile, which is defined as follows:

$$VaR_{\varpi}(\mathcal{L}) = \inf\{\ell : P(\mathcal{L} > \ell) \le \varpi\}, \varpi \in (0,1). \quad (7)$$

TVaR measures the riskiness of a portfolio through the average of the worst $100\varpi\%$ scenarios. It is defined as follows:

$$TVaR_{\varpi}(\mathcal{L}) = \frac{1}{\varpi}\int_0^{\varpi} VaR_p(\mathcal{L})dp \quad (8)$$

Intuitively, TVaR is the average of all the possible values of $\mathcal{L}$ that are greater than VaR, so it is greater than VaR. In other words, $TVaR_{\varpi}(\mathcal{L}) > VaR_{\varpi}(\mathcal{L})$, and TVaR is a more conservative risk measure than VaR.

Denote the total losses by $\mathcal{L}^* = \sum_q \mathcal{L}_q$. Using the risk measure TVaR, the total premium can be evaluated as:

$$TVaR_{\varpi}(\mathcal{L}^*) = \frac{1}{\varpi}\int_0^{\varpi} VaR_p(\mathcal{L}^*)dp, \forall\, p \le \varpi \quad (9)$$

After the total premium is determined, individual premiums can be allocated to the individual TOs. With the total premium $TVaR_{\varpi}(\mathcal{L}^*)$, the insolvency (which is the probability that the total losses exceed the total premium) is controlled at the level lower than ϖ.

A TCE premium design π_1 [14] to allocate $TVaR_{\varpi}(\mathcal{L}^*)$ based on individual contributions to the total TVaR, is defined as:

$$\pi_1(\mathcal{L}_q) = E[\mathcal{L}_q | \mathcal{L}^* > VaR_{\varpi}(\mathcal{L}^*)] \quad (10)$$

when is $\mathcal{L}^*$ continuous, it can be easily shown that $\sum_q \pi_1(\mathcal{L}_q) = TVaR_{\varpi}(\mathcal{L}^*)$. Although π_1 is advantageous in controlling insolvency risk, it results in a high premium to indemnity ratio which thus jeopardizes its practicability. The coalitional platform among the TOs can be introduced as a probable alternative to resolve the dilemma. No third-party insurer is involved in the coalition, as each TO who opts to participate in the coalition is both the insurer and the insured [15].

A coalitional premium π_2 can be defined as follows:

$$\pi_2(\mathcal{L}_q) = \varphi_q \sum_{k=1}^{y-1} \delta_{q,k} \psi(\Pi_q + (k-1)\overline{\Pi}_{-q}) \quad (11)$$

where y is the number of TOs in the coalition; φ_q is the occurrence probability of the loss event which is a ratio of the number of time steps with loss occurrence to the total sampled time duration in the reliability assessment; $\delta_{q,\varsigma}$ is the probability that the TO q among ς TOs submits the claim; Π_q is the claim of TO q; and $\overline{\Pi}_{-q} = \frac{(\sum_{k=1}^{y}\Pi_k) - \Pi_q}{y-1}$ is the average of all the claims except for that of TO q.The coalitional premium differs in each claim scenario. ς is the number of TOs which submit their claims. When ς is larger, payments toward claims from other TOs weigh more in the individual premiums.

Define the indemnity as $\Gamma_q = \Pi_q + (\varsigma - 1)\overline{\Pi}_{-q}$ and commitment as $\mathbb{C}_q$ of the TO q, respectively. The scaling function $\psi(*)$ in $\pi_2(\mathcal{L}_q)$ ensures the indemnity sum $\sum_{q\in\sigma}\Gamma_q$ never exceeds the commitment sum $\sum_{q\in(y-\sigma)}\mathbb{C}_q$:

$$\Gamma_q^{\psi} = \psi(\Gamma_q) = \begin{cases} \Gamma_q, when\ \sum_{q\in\sigma}\Gamma_q \le \sum_{q\in(y-\sigma)}\mathbb{C}_q \\ \frac{\sum_{q\in(y-\sigma)}\mathbb{C}_q}{\sum_{q\in\sigma}\Gamma_q}\Gamma_q, otherwise \end{cases} \quad (12)$$

where $\sum_{q\in\sigma}\Gamma_q \le \sum_{q\in(y-\sigma)}\mathbb{C}_q$ ensures the budget sufficiency.

Taking advantage of the abundant loss reimbursement to the potential claims in the TCE premium, the coalitional premium estimates the respective commitment values of TOs by the TCE premiums, and the claims are set to be the respective expected losses in TOs:

$$\mathbb{C}_q = \pi_1(\mathcal{L}_q),\ \Pi_q = E[\mathcal{L}_q] \quad (13)$$

This article has been accepted for publication in IEEE Transactions on Power Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3078730

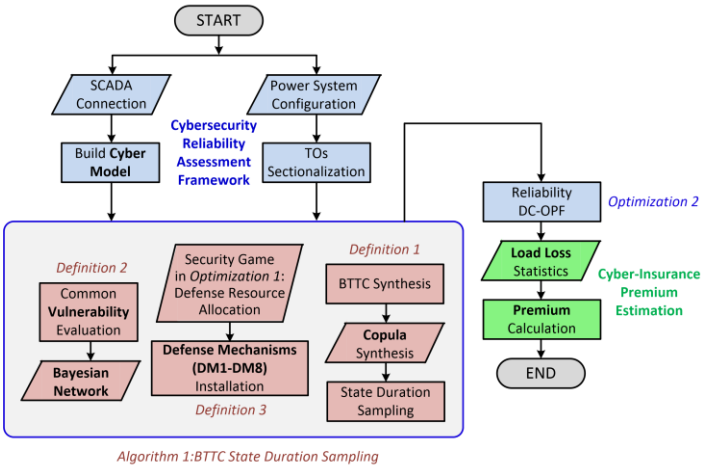


Fig. 4. Flowchart of the proposed reliability-based cyber-insurance model considering cyber vulnerability, comprising (I) Cybersecurity-reliability assessment framework, and (II) Cyber-insurance premium estimation.

The notion of using π_1 as the commitments of π_2 is that π_2 based on a crowdfunding model serves as a remedy of π_1 which deeply penalizes the TOs with heavy-tailed loss distributions. π_2 allows respective TOs to submit the commitments and claims to the coalition. The very motivation of the coalitional premium application is to encourage the risk aversion by reduced premiums for all. The fairness of π_2 is justified by the even distribution of the premiums. In some cases, the indemnities of some TOs may even be allowed to exceed the premiums without violating the budget sufficiency practice, which will be discussed in the case studies. Despite offering reduced premiums, π_2 is cautiously tailored so that the indemnity sum can never exceed the commitment sum, in which the individual indemnities would simply be scaled down by the ratio of the foregoing sums.

To achieve budget sufficiency, the indemnity formed by the claims filed by a group of TOs should never exceed the total commitment of other TOs in the coalition. Note that multiple sets of coalition which satisfy the budget sufficiency may exist. Selection of the coalition is on the discretion of participating TOs. As a rule of thumb, more affordable premiums are desirable so long as it can still cover the claims from the TOs. In other words, the coalition with the lowest total premium is selected.

Fig. 4 depicts the proposed coalitional cyber-insurance model. Stochastic evaluation of the BTTC, state duration sampling, and reliability assessment are shown. Application of the load loss statistics from reliability assessment to cyber-insurance premium computation is introduced. Further details are given in the following.

(I) cybersecurity-reliability assessment framework introduced in Section II. The CPS under study is constructed based on the graph-based cyber model of the SCADA system and the sectionalized physical power system configuration. BTTCs of the substations are composed of BCTs of the cyber nodes synthesized by the Bayesian Network of the vulnerability analysis (*Definition 2*) and BCTs of the game-inspired DRA optimization (*Definition 3, Optimization 1*). With a novel state duration sampling method using the correlated copula of TOs generated using **Algorithm 1**, reliability-assessment-oriented DC-OPF is conducted to obtain temporal load curtailment statistics of the TOs. **(II) cyber-insurance premium estimation presented in Section III.** Developed to handle the load loss statistics of TOs, cyber-insurance premiums are computed by a novel coalitional premium design which takes the interdependence of TOs and the fairness and affordability of the premiums into account. The effectiveness of the proposed cybersecurity assessment framework and the merit of the proposed premium settings in various degrees of TOs' interdependence will be validated in the following section.

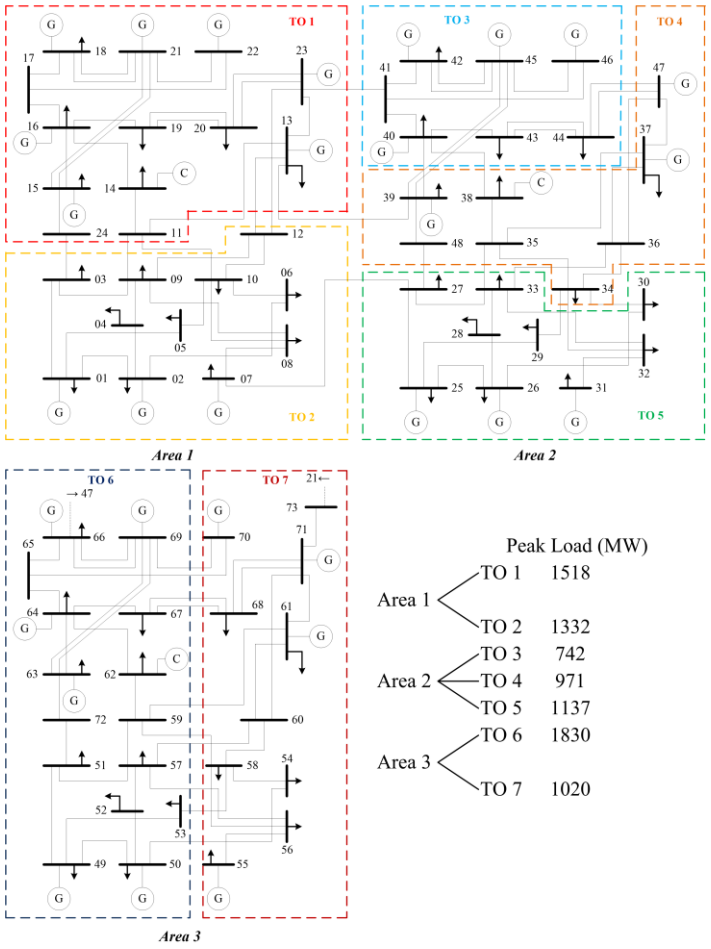


Fig. 5. IEEE Reliability Test system 96 (RTS-96) [26] and associated TOs.

IV. Case Studies and Discussion

A. Settings of the simulation

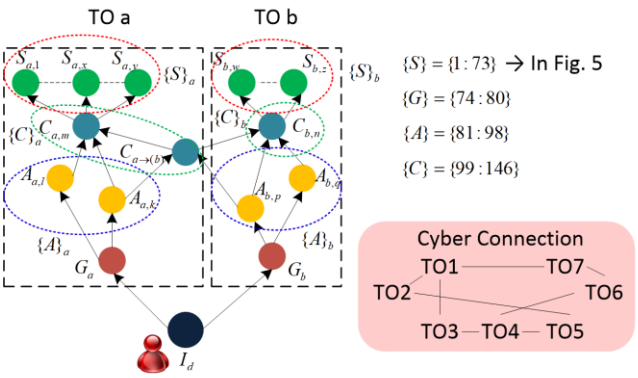
In case studies, the physical impact of cyberattacks is reflected by the load losses in reliability assessment. The crucial interdependence of cyber and physical aspects lies in the server of the SCADA system. If the root privilege of this server is obtained by the intruder, then malicious commands may be sent to trip protection relays and cause generation off-line, resulting in physical load losses.

The effectiveness is examined by case studies of defense resource allocation with tight and abundant budgets. The security budget m only suffices to partially cover substations. For example, 20% security budget is sufficient to cover one-fifth of the substations. In the scenarios of LDC and HDC, the corresponding available security budgets are set to be 20% and 80%, respectively.

A case study for validating the proposed coalitional cyber-insurance framework is performed based on the IEEE Reliability Test System (RTS-96). One-line diagram of the sectionalized RTS-96 is illustrated in Fig. 5, with details listed in [26]. The test system is divided into 3 areas including 7 TOs connected by 6 inter-area lines. No TO operates across the areas. In Area 1, TOs 1-2 are located. TOs 3-5 are situated in Area 2, and TOs 6-7 are located at Area 3. Peak load capacities are also shown in Fig. 5.

The proposed cyber model can be viewed as an attack net whose branches can be extracted as respective attack graphs of the substations.

This article has been accepted for publication in IEEE Transactions on Power Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3078730



Node(s)	TO1	TO2	TO3	TO4	TO5	TO6	TO7
$\{S\}$	$\{S\}_1$	$\{S\}_2$	$\{S\}_3$	$\{S\}_4$	$\{S\}_5$	$\{S\}_6$	$\{S\}_7$
G	74	75	76	77	78	79	80
$\{A\}$	81-83	84-86	87,88	89,90	91-93	94-96	97,98
$\{C\}$	99-107	108-113	114-117	118-122	123-129	130-139	140-146

Fig. 6. Hierarchical vulnerability nodes of the cyber model in IEEE RTS-96.

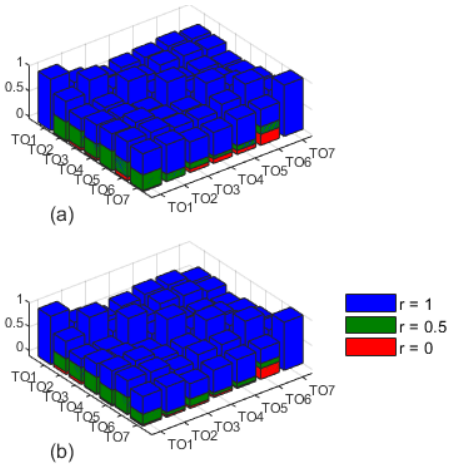


Fig. 7. Load loss correlation matrices of the TOs (a) at LDC (b) at HDC varied with correlated copulas.

The cyber model of the SCADA system developed for the IEEE RTS-96 is shown in Fig. 6, with all feasible routes identified by a DFS algorithm [27]. Case studies are conducted using the SMC method sampling over 500 years with hourly time steps, where expected values of reliability worth are:

$$ERW = E[\mathcal{L}] = \sum_{\Omega} K_{\Omega}\, W(D_{\Omega})\ (\$/yr) \qquad (14)$$

Fig. 7 shows the load correlation matrices. We would like to observe the Pearson correlation between each of the two TOs. Note that the diagonal entries are always 1's, which do not carry information. When $r = 0$, the correlation entries are mostly close to 0 with those belonging to TOs in the same area having slightly higher values, representing the impact induced by physical connection. As r increases to 0.5, the correlations range around 0.35. At LDC, the correlations can go as high as 0.78. In general, each TO at HDC has slightly higher correlation values than the same TO at LDC. The effectiveness of the copula is thus validated.

Figs. 8 and 9 illustrate the expected reliability worth, Standard Deviations SDs, and CoVs subject to LDC and HDC. CoV is a dimensionless ratio of the SD to the expected value. The effectiveness of DMs is validated by the fact that the expected losses of TOs monotonically decrease as the available security budget increases.

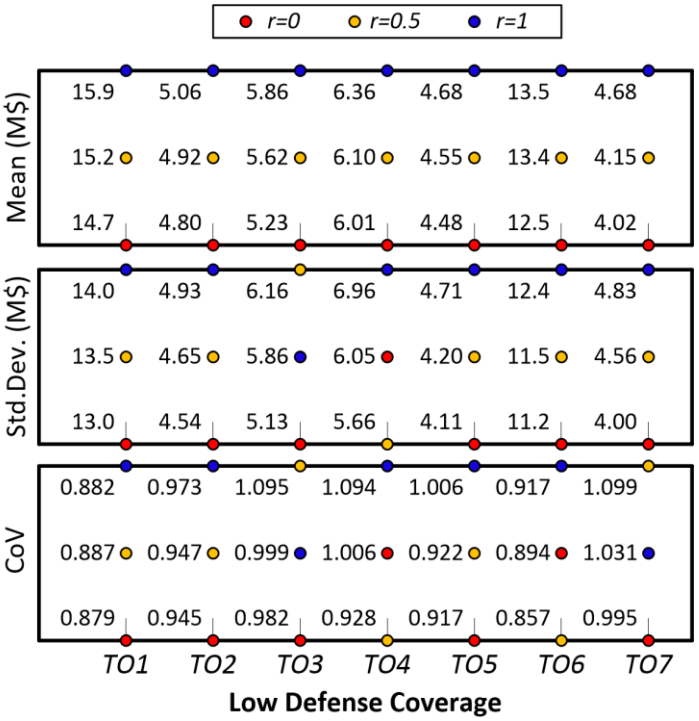


Fig. 8. Expected Values (M$), Standard Deviations (M$) and Coefficients of Variation of monetary loss in the TOs at LDC.

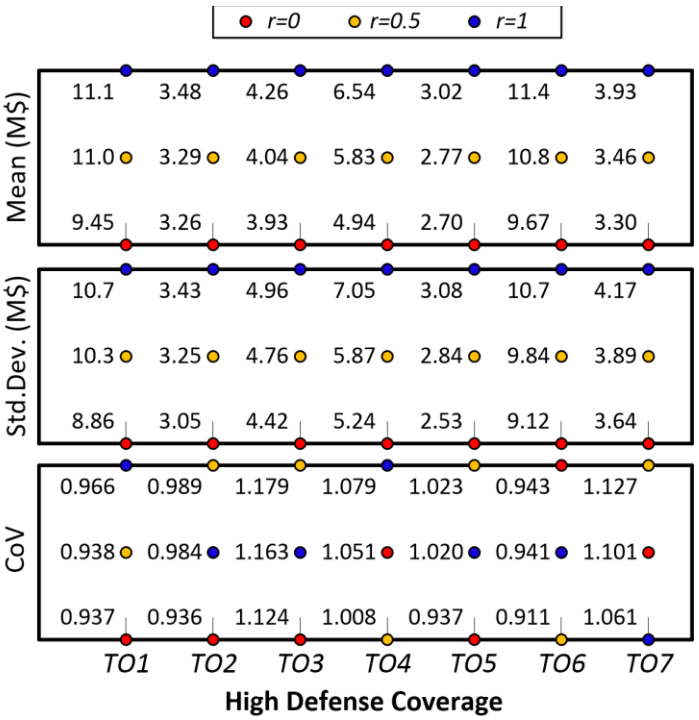


Fig. 9. Expected Values (M$), SDs (M$) and CoVs of monetary loss in the TOs at HDC.

The trend that the expected losses increase with the correlation can also be observed. Since SDs are close to the expected losses, CoVs remain flat across the TOs within the range of [0.86 1.18]. With the obtained monetary loss statistics, the insurance premium can be calculated accordingly. In the next subsection, premium estimation according to the insurance principle will be demonstrated and discussed. We would like to find if the premiums which sample the tail risks capture the same trend as demonstrated by the loss expectation.

This article has been accepted for publication in IEEE Transactions on Power Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3078730

TABLE II ACTUARIAL INSURANCE PREMIUMS (M$) OF THE TOS AT LDC

$r=0$	TO1	TO2	TO3	TO4	TO5	TO6	TO7
π_1	45.4	16.1	18.5	22.8	14.8	41.8	14.7
ρ_1	2.09	2.35	2.54	2.79	2.29	2.35	2.65
π_2	13.1	9.51	9.55	9.66	9.43	12.2	9.07
ρ_2	-0.11	0.98	0.83	0.61	1.10	-0.03	1.26
$r=0.5$	**TO1**	**TO2**	**TO3**	**TO4**	**TO5**	**TO6**	**TO7**
π_1	49.5	17.1	22.5	20.4	15.1	41.6	17.2
ρ_1	2.26	2.47	3.01	2.35	2.31	2.10	3.14
π_2	14.3	10.5	10.4	11.0	10.5	13.8	9.79
ρ_2	-0.06	1.13	0.85	0.80	1.30	0.03	1.36
$r=1$	**TO1**	**TO2**	**TO3**	**TO4**	**TO5**	**TO6**	**TO7**
π_1	50.0	17.4	21.1	26.4	16.8	44.9	17.4
ρ_1	2.14	2.43	2.60	3.15	2.59	2.33	2.72
π_2	14.7	10.7	10.8	10.6	10.4	13.7	10.3
ρ_2	-0.07	1.11	0.85	0.67	1.23	0.02	1.21

TABLE III ACTUARIAL INSURANCE PREMIUMS (M$) OF THE TOS AT HDC

$r=0$	TO1	TO2	TO3	TO4	TO5	TO6	TO7
π_1	32.7	10.9	16.4	18.7	8.43	35.1	13.5
ρ_1	2.46	2.35	3.18	2.75	2.12	2.63	3.08
π_2	9.37	7.22	7.09	7.65	7.12	9.36	6.92
ρ_2	-0.01	1.21	0.80	0.53	1.64	-0.03	1.09
$r=0.5$	**TO1**	**TO2**	**TO3**	**TO4**	**TO5**	**TO6**	**TO7**
π_1	37.1	11.2	17.8	21.3	10.5	35.2	14.5
ρ_1	2.37	2.41	3.42	2.66	2.79	2.26	3.20
π_2	10.6	7.82	7.59	8.58	7.45	10.6	7.49
ρ_2	-0.04	1.37	0.88	0.47	1.69	-0.02	1.17
$r=1$	**TO1**	**TO2**	**TO3**	**TO4**	**TO5**	**TO6**	**TO7**
π_1	38.9	12.4	18.9	26.1	11.1	37.9	15.1
ρ_1	2.50	2.55	3.44	3.00	2.68	2.34	2.84
π_2	11.0	8.23	8.04	9.06	8.01	11.1	8.24
ρ_2	-0.01	1.36	0.89	0.38	1.65	-0.02	1.09

B. Estimation of the Premium Design

In the cyber-insurance framework, respective premiums of TOs estimated by marginal statistics of the loss distribution. Due to the interconnection of power grids across the TOs, the premiums should be allocated by synthesizing loss distribution across the TOs. A major motivation for the TOs to engage in the cyber-insurance is to alleviate the unexpected losses resulting from the cybersecurity threats.

The premiums are designed to account for the strength and peak load capacity varied by TOs. Although the premium design π_1 (TCE Premium) guarantees the loss coverage, the estimated premiums are remarkably higher than the expected losses. The low cost-effectiveness may discourage the TOs from participation.

To alleviate the financial burden of TOs, a novel premium package π_2 (termed Coalitional Premium) is designed using the crowdfunding concept. In this subsection, π_1 and π_2 are estimated according to the same set of loss distributions of TOs. Given a potential loss $\mathcal{L}_q$, RLC ρ that further highlights the affordability of the premium relative to the risk expectation is defined as follows:

$$\rho(\mathcal{L}_q) = \pi(\mathcal{L}_q)/\Gamma_q^{\psi} - 1 \tag{15}$$

where $\rho(\mathcal{L}_q) > 0, \forall q$ guarantees the budget sufficiency. While positive RLC provides some margin to cushion against uncertainty, we will show majority of the participating entities provide safety-net margins to cover outliers with negative RLC according to the proposed insurance principle. To provide a viable insurance product, the RLC in the market is usually set relatively low.

The premiums collected from TOs is used as the budget for indemnities. In Table II, ρ_1 ranges from 2.09 to 3.15. Higher ρ_1 is caused by heavy tails of the loss distribution. On the contrary, ρ_2 is dispersed in [-0.11 1.36], mostly without exceeding 1. Note that a few TOs with slightly negative RLCs (TO1 and TO6) are tolerable for the coalition which gains remarkably wider positive margins from the premiums of other TOs. In other words, the total coalitional premium still suffices to cover the claimed total potential losses given the insurance pool. In addition, π_2 also distributes the risks more uniformly than π_1, making the coalition a compelling insurance model. In Table III, premiums are reduced at HDC, and π_2 still serves as a more affordable option, with ρ_2 being lower than 1.70.

The commitment term $\mathbb{C}_q$ can be flexibly replaced so long as the budget sufficiency still holds. The pattern of ρ_2 agrees with the more uniformly distributed π_2 across the TOs. While π_1 guarantees the monetary coverage of the losses by substantial margins at the cost of affordability, π_2 proposed in this paper imposes lower financial threshold and fair premium distribution for the TOs. π_1 is more advantageous for thin tail distributions, while π_2 is more cost-effective in high risk uncertainty. The tradeoff between the two premium designs can be made based on the preference of individual practitioners.

V. CONCLUSION

In this paper, a coalitional cyber-insurance framework is proposed based on power system reliability assessment accounting for cyber-vulnerability. Different from the TCE premium that conservatively ensures loss coverage of the TOs, the coalitional premium is designed to alleviate the RLC across the TOs especially at high defense coverage. Also, the proposed coalitional cyber-insurance design does not involve the third-party insurer. In addition, a graphic intrusion model is proposed to encompass the interdependence of network vulnerabilities and synthesize the stochastic cybersecurity metric based on the intrusion routes.

As shown in the case studies, a higher defense level is incentivized by the reduced premiums according to the proposed actuarial principle. This paper is an attempt to establish an innovative cyber-insurance design incorporating integrated long-term reliability-vulnerability assessment for power grids. Possible future work on this research topic includes insurance package design customized to the needs of individual TOs. Since dependence among the TOs is always one crucial factor when calculating the insurance premiums, the dependence factors of cyber risks may be separately estimated to further improve the fairness of the premium design.

APPENDIX

DETAILED DERIVATION OF THE SSG OPTIMIZATION

In Section II-D, the SSG-based defense resource distribution mechanism is carried out in the planning stage to fortify the resilience of countermeasures within the respective TOs against the cyber adversary. The defense coverage at each target substation is allocated exactly at the maximum payoffs of both the defender and intruder are reached. Derivation of the SSG optimization is further elaborated as follows.

Optimization 1 is essentially a bi-level optimization problem: a defender's problem embedded with an intruder's subproblem where the intruder's payoff is maximized. In this optimization, the defender specifies strategies before the intruder. The bi-level optimization is paired up as one using Karush-Kuhn-Tucker (KKT) conditions. The subproblem, given $\mathcal{C}$ assigned by the defender, can be devised for achieving maximal intruder's payoff:

$$\max \textstyle\sum_{\tau_x} a_{\tau_x} U_\alpha(\mathcal{C}, \tau_x) \tag{16-A}$$

Subject to:

$$a_{\tau_x} \in \{0,1\} \tag{16-B}$$

$$\textstyle\sum_{\tau_x} a_{\tau_x} = 1 \tag{16-C}$$

The problem that accounts for maximal defender's payoff subject to maximal intruder's payoff is formulated as follows:

$$\max \sum_{\tau_x} a_{\tau_x} U_\beta(\mathcal{C}, \tau_x) \quad \text{(17-A)}$$

Subject to:

$$a_{\tau_x} \in \{0,1\} \quad \text{(17-B)}$$

$$\sum_{\tau_x} a_{\tau_x} = 1 \quad \text{(17-C)}$$

$$p_{DC} \in [0,1] \quad \text{(17-D)}$$

$$\sum_{\tau_x} p_{DC}(\tau_x) \le M_q \quad \text{(17-E)}$$

$$a_{\tau_x}\big(k - U_\alpha(\mathcal{C}, \tau_x)\big) = 0 \quad \text{(17-F)}$$

In the bi-level optimization problem (17), the subproblem's objective (16-A) is incorporated as a complementary slackness condition (17-F) of the problem to ensure both objectives of the problem and subproblem can be met simultaneously. For the ease of implementation, expression (17-F) is further replaced with the following inequality constraints:

$$0 \le k - U_\alpha(\mathcal{C}, \tau_x) \le \big(1 - a_{\tau_x}\big)Z \quad \text{(17-G)}$$

The optimization problem (17) is a tedious Mixed Integer Quadratic Programming (MIQP) problem which involves a bilinear objective. To further simplify the problem, the problem can be reformulated into a MILP problem by replacing the objective (17-A) with the following objective bounded by inequality constraints:

$$\max d \quad \text{(18-A)}$$

$$\text{(17-B) - (17-E), (17-G)}$$

$$d - U_\beta(\mathcal{C}, \tau_x) \le \big(1 - a_{\tau_x}\big)Z \quad \text{(18-B)}$$

which is exactly *Optimization 1*.

Remark 1: The Stackelberg equilibrium for the intruder and the defender is guaranteed by the bi-level structure which maximizes payoffs of both the intruder and defender in *Optimization 1*:

$$d = \sum_{\tau_x} a_{\tau_x} U_\beta(\mathcal{C}, \tau_x) \ge \sum_{\tau_x} a^*_{\tau_x} U_\beta(\mathcal{C}^*, \tau_x) \quad \text{(19-A)}$$

$$k = \sum_{\tau_x} a_{\tau_x} U_\alpha(\mathcal{C}, \tau_x) \ge \sum_{\tau_x} a^*_{\tau_x} U_\alpha(\mathcal{C}^*, \tau_x) \quad \text{(19-B)}$$

$\forall \mathcal{C}^* \ne \mathcal{C}, \forall a^*_{\tau_x} \ne a_{\tau_x}$.

Remark 2: Mixed strategy Nash equilibrium between the intruder and the defender can be achieved *iff* $U_\beta(\mathcal{C}, \tau_x) = -U_\alpha(\mathcal{C}, \tau_x)$, $\forall \tau_x$; that is, when the SSG is a zero-sum game.

REFERENCES

[1] N. Kshetri and J. Voas, "Hacking Power Grids: A Current Problem," Computer, vol. 50, no. 12, pp. 91–95, 2017.

[2] North American Electric Reliability Corporation, "CIP standards." [Online].Available: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[3] National Institute of Standards and Technology, "Cybersecurity Framework Version 1.1 (April 2018)" [Online]. Available: https://www.nist.gov/cyberframework/framework

[4] C.-W. Ten, C. Liu and G. Manimaran, "Vulnerability Assessment of Cybersecurity for SCADA Systems," in IEEE Transactions on Power Systems, vol. 23, no. 4, pp. 1836-1846, Nov. 2008.

[5] N. Liu, J. Zhang, H. Zhang and W. Liu, "Security Assessment for Communication Networks of Power Control Systems Using Attack Graph and MCDM," in IEEE Transactions on Power Delivery, vol. 25, no. 3, pp. 1492-1500, July 2010.

[6] C.-W. Ten, C. Liu and M. Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees," 2007 IEEE Power Engineering Society General Meeting, Tampa, FL, USA, 2007, pp. 1-8.

[7] H. Holm, K. Shahzad, M. Buschle and M. Ekstedt, "P^2CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language," in IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 6, pp. 626-639, 1 Nov.-Dec. 2015.

[8] L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia. "An attack graph-based probabilistic security metric." In IFIP Annual Conference on Data and Applications Security and Privacy, pp. 283-296. Springer, Berlin, Heidelberg, Germany, 2008.

[9] M. A. McQueen, W. F. Boyer, M. A. Flynn, and G. A. Beitel. "Time-to-compromise model for cyber risk reduction estimation." In Quality of Protection, pp. 49-64. Springer, Boston, MA, USA, 2006.

[10] A. Zieger, F. Freiling and K. Kossakowski, "The β-Time-to-Compromise Metric for Practical Cyber Security Risk Estimation," 2018 11th International Conference on IT Security Incident Management & IT Forensics (IMF), Hamburg, Germany, 2018, pp. 115-133.

[11] Y. Zhang, L. Wang, Y. Xiang and C.-W. Ten, "Power System Reliability Evaluation with SCADA Cybersecurity Considerations," in IEEE Transactions on Smart Grid, vol. 6, no. 4, pp. 1707-1721, July 2015.

[12] L. Wang, S. Jajodia, A. Singhal, and S. Noel. "k-zero day safety: Measuring the security risk of networks against unknown attacks." In European Symposium on Research in Computer Security, pp. 573-587. Springer, Berlin, Heidelberg, Germany, 2010.

[13] V. Venkataramanan, A. K. Srivastava, A. Hahn and S. Zonouz, "Measuring and Enhancing Microgrid Resiliency Against Cyber Threats," in IEEE Transactions on Industry Applications, vol. 55, no. 6, pp. 6303-6312, Nov.-Dec. 2019.

[14] P. Lau, W. Wei, L. Wang, Z. Liu and C.-W. Ten, "A Cybersecurity Insurance Model for Power System Reliability Considering Optimal Defense Resource Allocation," in IEEE Transactions on Smart Grid, vol. 11, no. 5, pp. 4403-4414, Sept. 2020.

[15] I. Vakilinia and S. Sengupta, "A Coalitional Cyber-Insurance Framework for a Common Platform," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 6, pp. 1526-1538, June 2019.

[16] A. Talonen, "Systematic literature review of research on mutual insurance companies", Journal of Co-operative Organization and Management, vol.4, no.2, pp.53-65, 2016.

[17] W. Nzoukou, L. Wang, S. Jajodia and A. Singhal, "A Unified Framework for Measuring a Network's Mean Time-to-Compromise," 2013 IEEE 32nd International Symposium on Reliable Distributed Systems, Braga, Portugal, 2013, pp. 215-224.

[18] N. Poolsappasit, R. Dewri and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs," in IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 1, pp. 61-74, Jan.-Feb. 2012.

[19] M. Schiffman, "Common Vulnerability Scoring System (CVSS)," http://www.first.org/cvss/

[20] L. Han, T. Morstyn and M. McCulloch, "Incentivizing Prosumer Coalitions with Energy Management Using Cooperative Game Theory," in IEEE Transactions on Power Systems, vol. 34, no. 1, pp. 303-313, Jan. 2019.

[21] C. Stevanoni, Z. De Grève, F. Vallée and O. Deblecker, "Long-Term Planning of Connected Industrial Microgrids: A Game Theoretical Approach Including Daily Peer-to-Microgrid Exchanges," in IEEE Transactions on Smart Grid, vol. 10, no. 2, pp. 2245-2256, March 2019.

[22] K. Dehghanpour and H. Nehrir, "An Agent-Based Hierarchical Bargaining Framework for Power Management of Multiple Cooperative Microgrids," in IEEE Transactions on Smart Grid, vol. 10, no. 1, pp. 514-522, Jan. 2019.

[23] M. Touhiduzzaman, A. Hahn and A. K. Srivastava, "A Diversity-Based Substation Cyber Defense Strategy Utilizing Coloring Games," in IEEE Transactions on Smart Grid, vol. 10, no. 5, pp. 5405-5415, Sept. 2019.

[24] A. Sinha, F. Fang, B. An, C. Kiekintveld, and M. Tambe, "Stackelberg security games: Looking beyond a decade of success", Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence (IJCAI-18), Stockholm, Sweden, July 13-19, 2018, pp. 5494-5501.

[25] C. Kiekintveld, M. Jain, J. Tsai, J. Pita, F. Ordóñez, M. Tambe, "Computing Optimal Randomized Resource Allocations for Massive Security Games", In Proc. of 8th Int. Conf. on Autonomous Agents and Multiagent Systems (AAMAS 2009), Budapest, Hungary, May 2009, pp. 689-696.

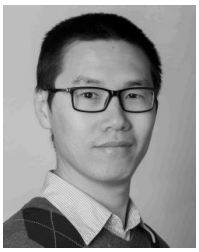
[26] C. Grigg et al., "The IEEE Reliability Test System-1996. A report prepared by the Reliability Test System Task Force of the Application of Probability Methods Subcommittee," in IEEE Transactions on Power Systems, vol. 14, no. 3, pp. 1010-1020, Aug. 1999.

[27] P. Lammich and R. Neumann, "A framework for verifying depth-first search algorithms", Proceedings of the 2015 Conference on Certified Programs and Proofs (CPP-15), Mumbai, India, pp. 137-146, Jan. 2015.

Pikkin Lau (S'13) received the M.S. degree in electrical engineering from Washington State University, Pullman, WA, USA, in 2017. He is currently a Ph.D. candidate with the University of Wisconsin-Milwaukee, Milwaukee, WI, USA. His research interests include reliability analysis, cybersecurity assessment, machine learning, dynamic state estimation, and power system model validation. He is an Engineer in Training certified by the state of Washington.

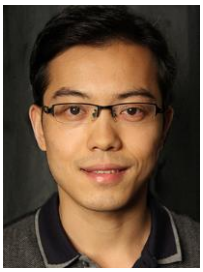
Lingfeng Wang (S'02-M'09-SM'18) received the B.E. degree in measurement and instrumentation from Zhejiang University, Hangzhou, China, in 1997; the M.S. degree in electrical and computer engineering from the National University of Singapore, Singapore, in 2002; and the Ph.D. degree from the Electrical and Computer Engineering Department, Texas A&M University, College Station, TX, USA, in 2008. He is currently a Professor with the Department of Electrical Engineering and Computer Science, University of Wisconsin–Milwaukee (UWM), Milwaukee, WI, USA. His major research interests include power system reliability, security and resiliency.

Dr. Wang is an Editor of the IEEE TRANSACTIONS ON SMART GRID, IEEE TRANSACTIONS ON POWER SYSTEMS, and IEEE POWER ENGINEERING LETTERS, and served on the Steering Committee of the IEEE TRANSACTIONS ON CLOUD COMPUTING. He is a recipient of the Outstanding Faculty Research Award of College of Engineering and Applied Science at UWM in 2018.



Zhaoxi Liu (M'17) received the B.S. and M.S. degrees in electrical engineering from Tsinghua University, Beijing, China, in 2006 and 2008, respectively, and the Ph.D. degree in electrical engineering from the Technical University of Denmark, Kgs. Lyngby, Denmark, in 2016.

He is currently a Research Associate with the Department of Electrical Engineering and Computer Science, University of Wisconsin-Milwaukee, Milwaukee, WI, USA. His research interests include power system operations, integration of distributed energy resources in power systems, and power system cybersecurity.



Wei Wei is an associate professor in Actuarial Science at the University of Wisconsin-Milwaukee. He joined UWM in 2013 after receiving his Ph.D. in Actuarial Science at the University of Waterloo, Canada. His research interests mainly lie in the areas of actuarial science and quantitative risk management, as well as applied probability and operations research. Specifically, he works on the topics of optimal insurance design, dependence modeling, stochastic ordering, cyber risk management, optimal scheduling, and ruin theory.

Chee-Wooi Ten (SM'11) is an Associate Professor of Electrical and Computer Engineering at Michigan Technological University. He received the B.S.E.E. and M.S.E.E. degrees from Iowa State University, Ames, in 1999 and 2001, respectively. He received the Ph.D. degree in 2009 from University College Dublin (UCD), National University of Ireland prior joining Michigan Tech in 2010. Dr. Ten was a Power Application Engineer working in project development for EMS/DMS with Siemens Energy Management and Information System (SEMIS) in Singapore from 2002 to 2006. His primary research interests are modeling for interdependent critical cyberinfrastructures and SCADA automation applications for a power grid. He is an active reviewer for IEEE PES transactions journals and was a member of IEEE PES computer and analytical method for cybersecurity task force. Dr. Ten is currently serving as an Editor for IEEE TRANSACTIONS ON SMART GRID and ELSEVIER JOURNAL SUSTAINABLE ENERGY, GRIDS, AND NETWORKS (SEGAN).