Measuring Systemic Risk of Switching Attacks Based on Cybersecurity Technologies in Substations

Koji Yamashita, *Member, IEEE*, Chee-Wooi Ten, *Senior Member, IEEE*, Yeonwoo Rho, Lingfeng Wang, *Senior Member, IEEE*, Wei Wei, and Andrew Ginter, *Member, IEEE*

***Abstract*—This paper describes the derivation of steady-state probabilities of the power communication infrastructure based on today's cybersecurity technologies. The elaboration of steady-state probabilities is established on (i) modified models developed such as password models, (ii) new models on digital relays representing the authentication mechanism, and (iii) models for honeypots/honeynet within a substation network. A generalized stochastic Petri net (GSPN) is utilized to formulate the detailed statuses and transitions of components embedded in a cyber-net. Comprehensive steady-state probabilities are quantitatively and qualitatively performed. The methodologies on how transition *probabilities* and *rates* are extracted from the network components and a conclusion of actuarial applications is discussed.**

***Index Terms*—Actuarial science, cyber-physical security, residual risks, steady-state probabilities, substation technologies.**

I. Introduction

THE year 2019 marked the tenth anniversary of enforcement for North America Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) compliance [1]. The latest version of NERC CIP compliance represents an ongoing refinement in compliance derived from the first draft of CIP002-CIP009 in 2005 [2]. Security violations have been reported recently with fines [3]. Apparently, historical events of cyber anomalies occurred over the past 15 years [4] are rooted in the facts where many believe that these cyber-physical security issues in control centers and substations must be carefully planned for the imminent security threats. In general, there are two groups of asset owners, *i.e.*, ones would either aim to (1) ensure 100% compliance and move on with a minimum investment plan, or (2) comply with a high desire to know how to invest and better protect their cyberinfrastructure with new security technologies. Although the current processes of compliance are thorough and evidence-based, it does not adequately address specific technologies that would enhance security measures to deter potential intrusions. This reflects systemic risk in numbers that can be used for audits [5].

The convenient remote access to Internet Protocol (IP)-based substations elevates security concerns. It becomes a balancing decision between security and maintenance as there are no perfect technologies to thwart uninvited guests effectively [6]. NERC CIP strongly recommends deploying an analytic of anomaly detection features across all IP-based substations. Statistically, the anomalies are the electronic evidence that sometimes can be used for forensic investigation, although the downside would be being subject to tamper if attackers find out where the security logs are stored. This source of security logging can be very useful in establishing a security profile.

Direct security patches and updates are not permitted in a live control system. Hence, the prevention of a cyber attack can be challenging, particularly with the increasing number of unpatched software vulnerabilities that might not effectively reflect on an organization's security posture [7], [8]. One of the key countermeasures is risk management that consists of the associated portfolios and assessment as well as the emergency response. These residual risks require extraction within a cyber network where this information can be consolidated and processed to make a meaningful conclusion for analysis of compliance. With digital protective relaying, the support of IEC61850 can maximize the performance and reliability of the control system. The new deployment of IP-based intelligent electronic devices (IEDs) can post a security threat to be manipulated by attackers [9]–[11].

One security technology that may not be well integrated into critical infrastructure as part of the security solutions is the honeypots/honeynet framework. Such technology has been used to cope with the malware that is a source of spreading security threats [12], [13]. Generally, the honeynet is a fictitious network that consists of a virtual firewall and servers (honeypots) that can be rephrased as a fake network representation, *i.e.*, a decoy. The honeynet was not widely used as compared to the intrusion detection system (IDS); honeynet can be a stepping-stone to facilitate unauthorized access and to spread worms. The

Manuscript received May 29, 2019; revised September 19, 2019 and February 25, 2020; accepted April 5, 2020. Date of publication April 27, 2020; date of current version November 4, 2020. This work was supported in part by the US National Science Foundation (NSF) under the awards "1739422 and 1739485 CPS: Medium: Collaborative Research: An Actuarial Framework of Cyber Risk Management for Power Grids." Paper no. TPWRS-00754-2019. *(Corresponding author: Chee-Wooi Ten.)*

Koji Yamashita and Chee-Wooi Ten are with the Department of Electrical and Computer Engineering, Michigan Technological University, Houghton, MI 49931 USA (e-mail: kyamashi@mtu.edu; ten@mtu.edu).

Yeonwoo Rho is with the Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931 USA (e-mail: yrho@mtu.edu).

Lingfeng Wang is with the Department of Electrical Engineering and Computer Science, University of Wisconsin-Milwaukee, Milwaukee, WI 53211 USA (e-mail: l.f.wang@ieee.org).

Wei Wei is with the Department of Mathematical Sciences, University of Wisconsin-Milwaukee, Milwaukee, WI 53211 USA (e-mail: weiw@uwm.edu).

Andrew Ginter is with the Waterfall Security Solutions, Rosh Haayin 48104, Isreal (e-mail: andrew.ginter@waterfall-security.com).

Color versions of one or more of the figures in this article are available online at https://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TPWRS.2020.2986452

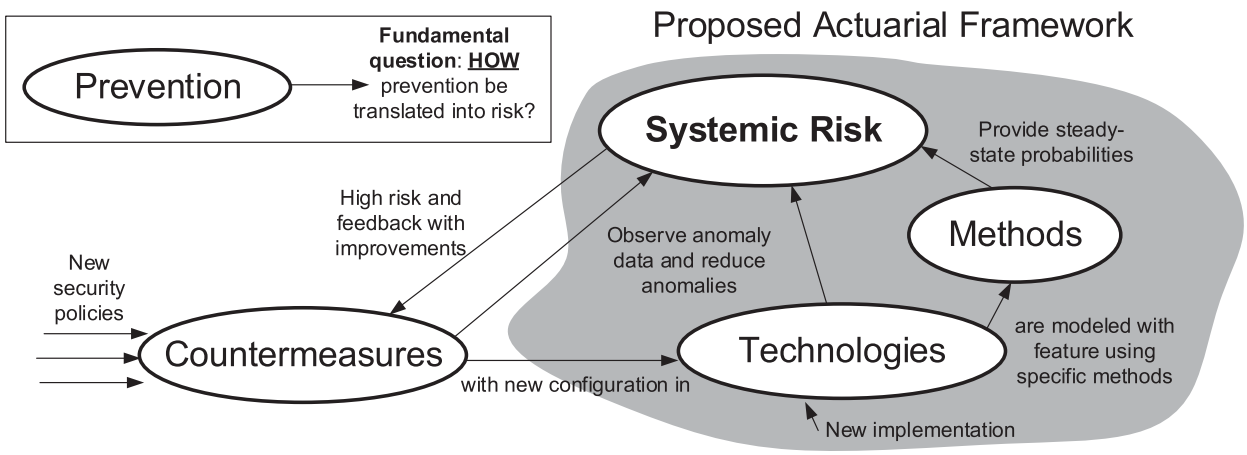

Fig. 1. Systemic risk modeling and anomaly data synthesis.

malware becoming apparent that can be automated to increase the trial-and-error rate to discover network architecture details and entities within a network. This can be revealed through their unauthorized access and footprint. On the contrary, the current countermeasure may not be adopted in a more proactive manner to promote risk awareness, although honeynet can be a technology for deployment [14].

The overarching question here is that how the stakeholder community would conform to a systematic evaluation of the cyber system based on the discrete events of intrusion processes and modeling of hypothetical disruptive attacks at the substations. The primary contribution of this work is to establish an actuarial framework to measure the systemic risk of the cyber system based on security technologies deployed in IP-based substations using four Petri net models: firewall, password, IED, and honeynet models. This work is connected with a discussion in the later section based on industry practice in security logging and how this can be beneficial to redefine grid security. The rest of the paper is organized as follows. Section II introduces the generalized stochastic Petri net (GSPN) representing an enhanced cyber-net with IEDs and the honeynet using the Petri net model. Section III extends the qualitative and quantitative elaboration of the proposed cyber-net. Section IV demonstrates the sensitivity analysis of case studies with discussions of security technologies that affect the steady-state probabilities. Section V discusses industry practice and the transition to the insurance business. Section VI concludes with potential applications.

II. Anomaly Data Synthesis

Fig. 1 shows how systemic risk can be formulated based on countermeasure, technologies, and methods. This paper establishes a comprehensive elaboration of modified and updated cyber-net with new models of IEDs and the honeypot/honeynet connecting the modified password and firewall models, as shown in Fig. 2. It is noted that the switching attack that opens circuit breakers at substations may be performed not only via local substation supervisory control and data acquisition (SCADA),

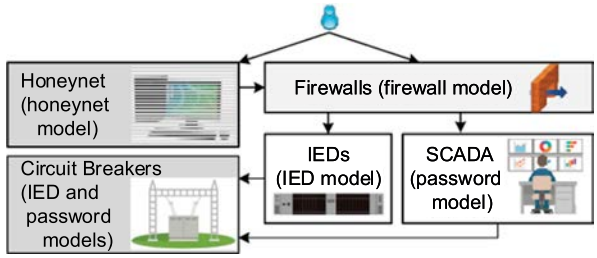

Fig. 2. Interdependencies of abstracted models in a Cyber-Net.

but also through direct IED connections compromised that enables plotting for cyber-physical system (CPS) switching attacks. Capturing the intrusion processes and behaviors of attackers within the private networks with security technologies of defender should be characterized in formalism for the description of concurrency and synchronization for the computational problems [15], [16]. For decades, the Petri net is utilized as an *automata* to model between finite-state and machines as well as to analyze the capabilities [17]. In a more recent development on the cyber-physical system for the power grid, a preliminary model establishment using the steady-state probability was introduced [18], [19]. The disruptive switching substation attack through the server is modeled; however, the switching attack through IEDs such as digital protective relays is not explicitly modeled. The latest security technology, such as new security policies, can be incorporated.

Other applications also gain attention in this subject and extend research in performance evaluation, such as the control system in the nuclear power station [20], the energy control center [21], the impact analysis of the intrusion detection, and the response of cyber-physical systems [22]. References [20]–[23] adopt a Petri net model mainly to derive the reliability and availability of the system for the cyberattack. Although emerging issues on cyber insurance are discussed in [23]–[27], none of those references for the other applications discusses the probability of disruptive switching attack upon a compromised substation from the actuarial point of view.

A similar type of attack has been addressed as a cyber-physical switching or system reconfiguration attack [28], [29]. A compromise of the controllers for a generating unit is also categorized as a switching attack [30], [31]. The influence of such attacks reflecting grid vulnerability is clarified using the sliding mode trajectory [28], [29]. Such detection of anomalies can be achieved through game-theoretic analysis or the multiple-model inference algorithms [30], [31].

The recent research studies for cyber-physical switching attacks highlight a coordinated attack that consists of the false data injection attack, reconfiguration attack, and distributed denial of service (DDoS) attack. Considerable coordinated attacks are the plot against multiple component failures through a compromised network that connecting multiple components, such as lines or substations. With the coordination of the DDoS attack, there are combinations of attack scenarios that can be translated into false data injection attacks on wrong measurements of generators, lines, or loads. It is common to relate bi-level modeling for the Load Redistribution (LR) attack, bi-level model for coordination of LR attack, and all sorts of other attacks [32]. Such strategies can lead to an optimal strategy with well-coordinated planning by attackers that can potentially weaken grid operating conditions [32].

Among those possible coordinated switching attacks, this paper focuses on the coordinated attack against substations because the impact of this type of cyberattack becomes larger than others. It should be noted that this paper does not explicitly demonstrate the false data injection attack nor denial of information access. However, those are indirectly included in the proposed Petri net model as the probabilities, which will hereinafter be described in detail. The contribution of this paper is to elaborate on the steady-state probability for a cyber-physical attack at any IP-based substations, *i.e.*, the probability will converge over a long time upon successful intrusions to the internal networks.

III. Cyber-Net Modeling

Although the systemic risk of cybersecurity has been studied as a potential data breach, mainly in security businesses [33], their primary interests are to estimate the number of attacks in the near future. A recent paper proposes a timed Petri net to estimate the steady-state probability of attacks on the special protection scheme (SPS) [34]. Modeling the risk of intrusion and its processes based on security technologies is highly desirable. Technologies of deployed cyberinfrastructure and its associated anomalous events can be modeled in generalized stochastic Petri net (GSPN). The cyber-net defined in this paper is the construction of (bipartite) directed graph based on specific security technology, which can model the interdependencies of cyber components within a network. We define compromised IED-initiated (CII) attacks as the digital protective relays that connect to one or more breakers in substations that are manipulated by attackers.

In this section, three fundamental models are introduced: (1) Modified firewall model, (2) modified password model, (3) extended password model on IED. Those three models are assembled to represent the cyber-net with new technologies shown in Fig. 2. The technical details of the honeynet model in the same figure are introduced in the next section. As depicted in Fig. 3, each of the technology is modeled in GSPN. All of these are represented as a subgraph where a cyber-net is a complete graph, that is elaborated analytically in this section. Figure 4 illustrates the enumeration of marking states, $M_{i|i=0,1,2,\ldots}$ that is mapped to a Markov chain, corresponding to each of the security technologies deployed in IP-based substations. For each marking, all non-zero numbers represent the number of tokens. The 1 s, representing in each row vector of marking, can be increased to 2 or more, which is useful when the simultaneous steady-state probabilities of multiple states are of interest in the modeling. It is noted that weights for the reachability graph, *i.e.*, transition probabilities and rates for the Petri net in Fig. 4, are imputed with values within reasonable ranges. The models of security technologies are illustrated in the following subsections.

A. Modified Firewall Model

The proposed firewall model has been enhanced based on the original establishment [18]. Although the size of the model is slightly larger, the modified firewall model characterizes two advantages: 1) allow repetition of the successful cracking of firewall rules, 2) allow cracking of multiple firewall rules in a sequential manner. The tuple of describing the cyber-net model quantitatively and qualitatively is as follows:

$$\begin{aligned}
\text{GSPN} &= \{P, T_1, T_2, A, W, M_0\} \\
P &= \{p_{\text{begin}}, p_{\text{rule1},\alpha}, p_{\text{rule1},\beta}, p_{\text{rule2},\alpha}, \\
&\quad p_{\text{rule2},\beta}, p_{\text{rule3},\alpha}, p_{\text{rule3},\beta}, p_{\text{pass}}\} \\
T_1 &= \{t_{1,a}, t_{1,b}, t_{2,a}, t_{2,b}, t_{3,a}, t_{3,b}\} \\
T_2 &= \{\tau_{\text{rate},1}, \tau_{\text{rate},2}, \tau_{\text{rate},3}, \tau_{r,4}, \tau_{r,5}\} \\
M_0 &= (1,0,0,0,0,0,0,0) \\
W &= \{w_1, w_2, w_3, w_4, w_5, w_6, w_7, w_8, w_9, w_{10}, w_{11}\},
\end{aligned}$$

where p_{begin} denotes the initiation of the firewall rule cracking, and $p_{\text{rule1},\alpha}$, $p_{\text{rule2},\alpha}$, and $p_{\text{rule3},\alpha}$, denote the successful cracking of firewall rules 1, 2, and 3, respectively. Places, $p_{\text{rule1},\beta}$, $p_{\text{rule2},\beta}$, and $p_{\text{rule3},\beta}$, denote the failure to crack firewall rules 1, 2, and 3, respectively. The place, p_{pass} denotes reaching to password input screen of the server. Variables, $t_{1,a}$, $t_{2,a}$, and $t_{3,a}$, denote the transition probabilities of the successful cracking of firewall rules 1, 2, and 3. Variables, $t_{1,b}$, $t_{2,b}$, and $t_{3,b}$ denote the transition probabilities of the failure to crack firewall rules 1, 2, and 3. The sum of transition probabilities that connect the same place always needs to be one. Variables, $\tau_{\text{rate},1}$, $\tau_{\text{rate},2}$, and $\tau_{\text{rate},3}$, denote the transition rate of responding to attackers opening a port. Variables, $\tau_{r,4}$ and $\tau_{r,5}$, denote the transition rates denying attackers of opening any ports and to attackers with the status of password input, respectively.

The password cracking part shows only two possibilities, *i.e.*, the successful login or the login failure. Those probabilities are modeled as the immediate transition, and the sum of the two probabilities is one. On the other hand, the response time of the server is not immediate, and such time delay is modeled as the timed transition. Therefore, the GSPN is applied to this model and the rest of the proposed models.

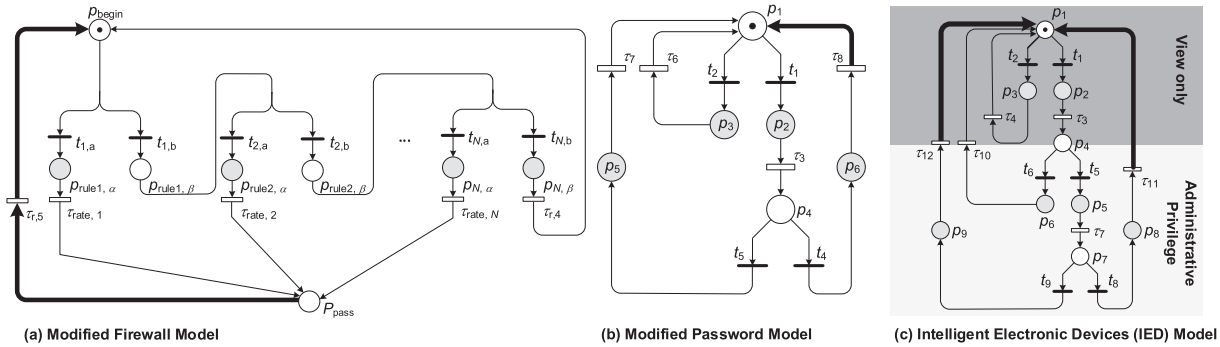

Fig. 3. Modified cyber-net shown in figures 1(a) and 1(b) and new addition shown IED model on figure 1(c).

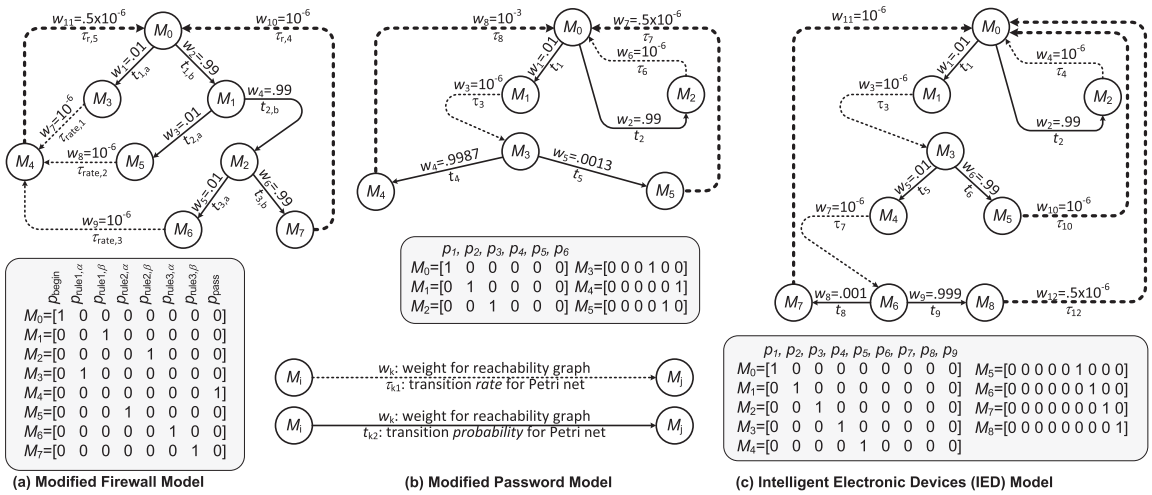

Fig. 4. Reachability graph corresponding to Fig. 1 under the same sequence, respectively.

The marking M_0 denotes the initial marking that is the starting point of the behavioral dynamics characterized in the Petri net. As shown in Fig. 3, a token, *i.e.*, a dot is shown only in the place, p_{begin}. Therefore, M_0 contains 1 s in the first column, as shown in Fig. 4. The reachability graph in Fig. 4 is an extended semi-Markovian Process because the holding time (that is the sojourn time) in each state is restricted to be either zero or exponentially distributed.

$$U^T = \begin{array}{c} \\ M_3^T \\ M_4^T \\ M_5^T \\ M_6^T \\ M_7^T \end{array} \begin{array}{c} \begin{array}{cccc|cccc} M_0^V & M_1^V & M_2^V & M_3^T & M_4^T & M_5^T & M_6^T & M_7^T \end{array} \\ \left(\begin{array}{cccc|cccc} 0 & 0 & 0 & 0 & 10^{-6} & 0 & 0 & 0 \\ 5\times10^{-7} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 10^{-6} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 10^{-6} & 0 & 0 & 0 \\ 10^{-6} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \end{array}$$

$$= \left(U^{TV} \middle| U^{TT}\right), \tag{1}$$

The matrix defined is embedded with two sub matrices, describing the transition rate from each tangible marking to each vanishing/tangible marking. It is noted that the superscripts, V and T, denote the vanishing marking and tangible marking, respectively. When only timed transitions are used to transit from the current marking to other markings, this is referred to tangible marking. Similarly, the immediate transitions are used to transit from the current marking to other markings, this type of transition is marked as "vanishing."

The transition probability matrix, $\mathbf{P}$, can be represented as:

$$\mathbf{P} = \begin{array}{c} \begin{array}{cccc|cccc} M_0^V & M_1^V & M_2^V & M_3^T & M_4^T & M_5^T & M_6^T & M_7^T \end{array} \\ \left(\begin{array}{cccc|cccc} 0 & .99 & 0 & .01 & 0 & 0 & 0 & 0 \\ 0 & 0 & .99 & 0 & 0 & .01 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & .01 & .99 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \end{array}_{(8\times8)}$$

$$= \left(\frac{P^V}{P^T}\right) = \left(\begin{array}{c|c} P^{VV} & P^{VT} \\ \hline P^{TV} & P^{TT} \end{array}\right), \tag{2}$$

where $P^V = (P^{VV} | P^{VT})$ denotes a matrix describing the transition probability from each vanishing marking to each vanishing or tangible marking, while $P^T = (P^{TV} | P^{TT})$ denotes a matrix describing the transition probability from each tangible marking to each vanishing or tangible marking. P^T is calculated from U^T normalizing the sum of each row to one. For example, the first row of U^T corresponds to the fourth row of $\mathbf{P}$ as a non-zero element of the first row of U^T is only shown in the fifth column. This element is set as one by normalizing the entire first row of U^T.

The expected holding (sojourn) time h_j at state j can be derived from the transition *rate* matrix U^T:

$$h_j = \begin{cases} \dfrac{1}{\sum_{k\in V\cup T} U^T_{j,k}}, & \text{if } j \in \text{Tangible Markings} \\ 0, & \text{if } j \in \text{Vanishing Markings.} \end{cases} \tag{3}$$

Only tangible markings have non-zero positive values because the holding time is always zero for vanishing markings according to the definition of the immediate transition. In the modified firewall model, the rates corresponding to each timed transition can be written as a row vector

$$\begin{aligned} \boldsymbol{h} &= \left[0 \;\; 0 \;\; 0 \;\; \frac{1}{\tau_{\text{rate},1}} \;\; \frac{1}{\tau_{r,5}} \;\; \frac{1}{\tau_{\text{rate},2}} \;\; \frac{1}{\tau_{\text{rate},3}} \;\; \frac{1}{\tau_{r,4}}\right] \\ &= [0.0 \;\; 0.0 \;\; 0.0 \;\; 1.0 \;\; 2.0 \;\; 1.0 \;\; 1.0 \;\; 1.0] \times 10^6. \end{aligned} \tag{4}$$

Only the vector h in each state and the transition *probability* matrix, $\mathbf{P}$ are needed to obtain the steady-state probability of each state in the semi-Markovian process. The steady-state distribution, $\tilde{\pi}$ of the semi-Markov chain is expressed as

$$\tilde{\pi}\mathbf{P} = \tilde{\pi}; \sum_{M_j\in T\cup V} \tilde{\pi}_j = 1. \tag{5}$$

Since $h_1 = h_2 = h_3 = 0$, the transition probability matrix, $\mathbf{P}$ may be reduced to a 5×5 matrix, $\mathbf{P}'$ using

$$\mathbf{P}' = P^{TT} + P^{TV}(I - P^{VV})^{-1}P^{VT}, \tag{6}$$

and thus

$$\mathbf{P}' = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ .01 & 0 & .0099 & .009801 & .9703 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ .01 & 0 & .0099 & .009801 & .9703 \end{pmatrix}_{(5\times 5)}. \tag{7}$$

This reduction of the transition matrix, with removal of vanishing markings, has contributed to computational efficiency. We formulate this problem with the continuous Markov chain instead of the semi-Markov chain. The steady-state distribution, $\tilde{\pi}$ of the continuous-time Markov chain is expressed by:

$$\tilde{\pi}\mathbf{P}' = \tilde{\pi}; \sum_{M_j\in T} \tilde{\pi}_j = 1. \tag{8}$$

The steady-state distribution, $\tilde{\pi}$, for the tangible markings is as follows:

$$\tilde{\pi} = [.009712 \;\; .02884 \;\; .009614 \;\; .009518 \;\; .94231]. \tag{9}$$

The steady-state probability $\pi_{j|j=1,\ldots,8}$ is calculated from both the steady-state distribution, $\tilde{\pi}_j$, and the corresponding holding times, h_j. For any j in tangible markings, the steady-state probability is

$$\begin{aligned} \pi_{j|j=1,2,\cdots 8} &= \frac{\tilde{\pi}_j h_j}{\sum_{k\in V\cup T} \tilde{\pi}_k h_k} = \frac{\tilde{\pi}_j h_j}{\sum_{k\in T} \tilde{\pi}_k h_k} \\ &= \frac{\tilde{\pi}_j h_j}{\tilde{\pi}_4 h_4 + \tilde{\pi}_5 h_5 + \tilde{\pi}_6 h_6 + \tilde{\pi}_7 h_7 + \tilde{\pi}_8 h_8} \\ &= .972 \cdot \tilde{\pi}_j h_j \times 10^{-6}. \end{aligned} \tag{10}$$

From (4) and (9), the steady-state probability is calculated as follows:

$$\pi = [.009439 \;\; .05607 \;\; .009345 \;\; .009251 \;\; .9159]. \tag{11}$$

B. Modified Password Model (Server Computer)

To analyze the steady-state probability of intruding the server cracking passwords, the password model is defined as follows based on the GSPN representation:

$$\begin{aligned} \text{GSPN} &= \{P, T_1, T_2, A, W, M_0\} \\ P &= \{p_1, p_2, p_3, p_4, p_5, p_6\} \\ T_1 &= \{t_1, t_2, t_4, t_5\}; \;\; T_2 = \{\tau_3, \tau_6, \tau_7, \tau_8\} \\ W &= \{w_1, w_2, w_3, w_4, w_5, w_6, w_7, w_8\} \\ M_0 &= (1, 0, 0, 0, 0, 0), \end{aligned}$$

where p_1 denotes the initiation of the password cracking of local SCADA systems, p_2 denotes the successful login, p_3 denotes the failed login to the local SCADA, p_4 denotes the knowledge discovered from the SCADA, p_5 denotes the executed sequence of disruptive switching attacks from the SCADA, and p_6 denotes the failure to execute switches due to interlocking blocks sequentially. Variables, t_1, t_2, t_4, and t_5, denote the transition *probabilities* of the successful login to the SCADA, of failure to login to the SCADA, of failing to execute, and of successful execution of the sequential switching in the targeted substation, respectively. Variables, τ_3, τ_6, τ_7, and τ_8, denote the transition *rates* of learning to discover the cyber-physical relation, the response to attackers indicating the failed login, response to attackers about successful switching attacks, and response to attackers indicating the failure of the sequential switching due to the interlocking rules, respectively.

Once the reachability graph is obtained, the transition probability matrix $\mathbf{P}$ and its reduced form $\mathbf{P}'$ are

$$\mathbf{P} = \left(\begin{array}{cc|cccc} 0 & 0 & .01 & .99 & 0 & 0 \\ 0 & & 0 & 0 & .9987 & .0013 \\ \hline 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{array}\right), \tag{12}$$

$$\mathbf{P}' = \begin{pmatrix} 0 & 0 & .9987 & .0013 \\ .01 & .99 & 0 & 0 \\ .01 & .99 & 0 & 0 \\ .01 & .99 & 0 & 0 \end{pmatrix}$$

respectively. Using a similar argument as in Section III-A, the steady-state distribution, $\tilde{\pi}$, and the steady-state probability, π, are derived as follow:

$$\tilde{\pi} = [.00990 \;\; .9802 \;\; .00989 \;\; .000013], \tag{13}$$

$$\pi = [.0099996 \;\; .98996 \;\; .000010 \;\; .000026]. \tag{14}$$

C. Extended Password Model (IED Authentication)

Below is the tuple of the cyber-net representation to quantify the statuses with transitions representing the model:

$$\begin{aligned}\text{GSPN} &= \{P, T_1, T_2, A, W, M_0\}\\ P &= \{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9\}\\ T_1 &= \{t_1, t_2, t_5, t_6, t_8, t_9\};\ T_2 = \{\tau_3, \tau_4, \tau_7, \tau_{10}, \tau_{11}, \tau_{12}\}\\ W &= \{w_1, w_2, w_3, w_4, w_5, w_6, w_7, w_8, w_9, w_{10}, w_{11}, w_{12}\}\\ M_0 &= (1,0,0,0,0,0,0,0,0)\end{aligned}$$

where p_1 denotes the initiation of password crackings of IEDs, p_2 and p_3, denote the failure to access and the successful access to the IED with the viewing mode, individually, p_4 denotes the attempt to access to the IED with the control mode, p_5 and p_6, denote the failure to access and the successful access to the IED with the control mode, individually, p_7 denotes obtaining the knowledge to manipulate IEDs, p_8 denotes the executed sequence of disruptive switching actions via IEDs, and p_9 denotes the failure to execute switching actions due to the maintenance or disabling remote relay settings or remote switching operations.

Variables, t_1 and t_2, denote transition probabilities of the successful access to IEDs with the viewing mode and of the failed access due to wrong passwords, respectively. Variables, t_5 and t_6, denote transition probabilities of the successful access to IEDs with the control mode and of the failed access due to wrong passwords, respectively. Variables, t_8 and t_9, denote the transition probability of the successful execution of sequential switching actions of circuit breakers in the targeted substation via the IED and of failing to execute the operation of the IED. The variable, τ_3, denotes the transition rate of exploring available IEDs with the control mode. Variables, τ_4 and τ_{10}, denote the transition *rate* of the response to attackers indicating the failed attempt to access to the IED. The variable, τ_7, denotes the transition rate of learning to discover the knowledge of how to manipulate relay settings of IEDs. The variable, τ_{11}, denotes the transition rate of the response to attackers about successful switching attacks. The variable, τ_{12}, denotes the transition rate of the response to attackers indicating the out of service state. The configuring remote relay settings or switching operations can also be disabled.

Once the reachability graph is obtained, the transition probability matrix is derived as (15), and its reduced form is derived as (16).

$$\mathbf{P} = \left(\begin{array}{ccc|cccccc} 0&0&0 & .01 & .99 & 0 & 0 & 0 & 0\\ 0&0&0 & 0 & 0 & .01 & .99 & 0 & 0\\ 0&0&0 & 0 & 0 & 0 & 0 & .001 & .999\\ \hline 0&1&0 & 0 & 0 & 0 & 0 & 0 & 0\\ 1&0&0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0&0&1 & 0 & 0 & 0 & 0 & 0 & 0\\ 1&0&0 & 0 & 0 & 0 & 0 & 0 & 0\\ 1&0&0 & 0 & 0 & 0 & 0 & 0 & 0\\ 1&0&0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)_{(9\times 9)}, \tag{15}$$

$$\mathbf{P}' = \begin{pmatrix} 0 & 0 & .01 & .99 & 0 & 0\\ .01 & .99 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & .001 & .999\\ .01 & .99 & 0 & 0 & 0 & 0\\ .01 & .99 & 0 & 0 & 0 & 0\\ .01 & .99 & 0 & 0 & 0 & 0 \end{pmatrix}_{(6\times 6)}. \tag{16}$$

The corresponding steady-state distribution and the steady-state probability are derived as (17) and (18), respectively.

$$\tilde{\pi} = [9900.0, 980100.0, 99.0, 9800.0, .1, 98.9] \times 10^{-6}, \tag{17}$$

$$\pi = [9899.0, 980004.0, 99.0, 9800.0, .1, 197.8] \times 10^{-6}. \tag{18}$$

D. Model Enhancement Toward Coordinated Attack

The modified and extended password model can represent the coordinated attack, *i.e.*, switching substation attack with DoS/DDoS attacks. The effect of DoS/DDoS attacks can be indirectly reflected in variables, t_4 and t_5 of the modified password model, and in variables, t_8 and t_9 of the extended password model. Once system operators or the intrusion detection system perceive that attackers intrude the substation network, they are highly likely to disable the remote relay settings and remote switching maneuver for the circuit breakers. However, DoS/DDoS attacks prevent system operators and the intrusion detection system from taking such corrective actions. Therefore, the DoS/DDoS attack leads to the higher t_4 and t_8, and lower t_5 and t_9 under the condition, $t_4 + t_5 = t_8 + t_9 = 1$. Thus, the developed model can be extended to analyze how DoS/DDoS affects the overall steady-state probability of the switching substation attack by changing those transition probabilities either with or without DoS/DDoS.

IV. Honeynet Model in Cyber-Net

The first subsection introduces sensitivity analyses for honeynet using the developed cyber-net model in Fig. 5. The second subsection provides the steady-state probabilities of the substation outages due to disruptive switching attacks for SCADA and IEDs using the IEEE 14-bus system model [35]. The attack from outside is applied for all case studies.

A. Establishing a Cyber-Net Model

The proposed cyber-net model contains the modified password model and the IED model in the previous section as well as the developed honeynet model. The honeynet is assumed to have the following functions: 1) collect passwords, 2) update the firewall rule to prevent the attackers from connecting to the Internet from the honeynet. Generally, a honeypot should "trap" intruders' anomaly that captures security events. The features of logging are captured in the cyber-net modeling, where it can interact with firewalls within the network to coordinate substation's anomalous events.

The discerned statistics stay in the event logging that can be purged once every audit cycle. The modeling of a particular type of honeypots can mimic the IEDs, where attackers may use it as a

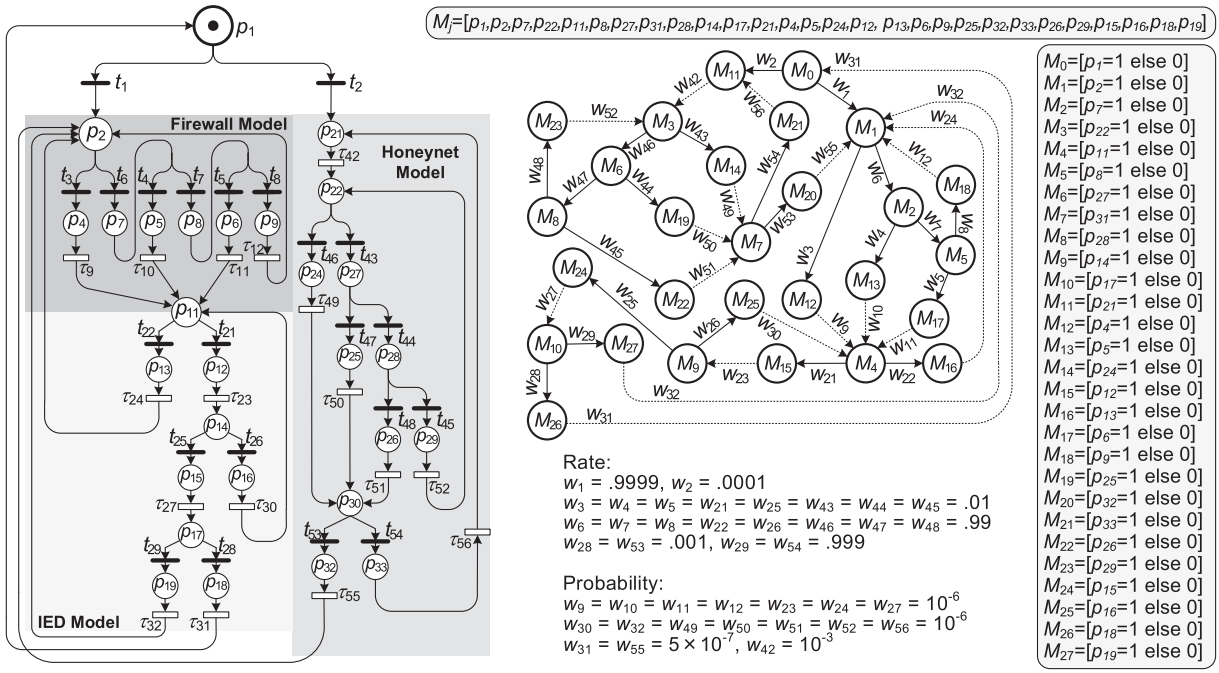

Fig. 5. Honeynet model of a cyber-net.

steppingstone to further a plot. However, the advanced honeynet has a prevention function that enables automatic updates of the statistics reflecting the new rules, resulting in preventing attackers from using the honeynet server. Thus, the prevention function plays an essential role in capturing the risk within a substation network, together with other security technologies.

Variables, t_1 and t_2, denote transition probabilities of the intrusion attempt for the honeypot and IEDs, respectively. Variable, τ_{42} denotes the transition rate of copying the tools to the honeynet for the intrusion attempt. Variables, t_{43} through t_{45}, denote transition probabilities of the failure to crack a designated firewall rule. Variables, t_{46} through t_{48}, denote transition probabilities of the successful cracking of firewall rules. Variables, τ_{49} through τ_{51}, denote transition rates of responding to attackers opening a designated port. Variable, τ_{52}, denotes the transition rate of response to the attackers indicating failure to open any ports. Variables, t_{53} and t_{54}, denote transition probabilities of the successful communication to the Internet from the honeynet and of the failure to communicate to the Internet from the honeynet, respectively. Variables, τ_{55} and τ_{56}, denote the transition rate of exploring the available IED and of failure to reaching to the IED due to the prevention function that is implemented in the advanced honeynet, respectively. It is noted that the rest of the transition probabilities and rates in the firewall model and the IED model have defined in the previous section.

The enhanced cyber-net model establishes several useful indicators. The steady-state probability of cracking the firewall is calculated from the sum of the probabilities of p_{12} and p_{13}. The steady-state probability of cracking the first authentication is calculated from the sum of the probabilities of p_{15} and p_{16}. The steady-state probability of cracking the second authentication is calculated from the sum of the probabilities of p_{18} and p_{19}. The steady-state probabilities of disruptive switching actions and of the successful transmission of the outgoing packets from the honeynet to attack other servers, (*i.e.*, using the honeynet as the steppingstone) are obtained from p_{18} and p_{32}, respectively.

TABLE I
PROBABILITIES OF A CYBER-NET IN FIG. 5

Place	Probability	Place	Probability	Place	Probability
P04	9.70590E-03	P15	2.91157E-06	P25	9.70589E-11
P05	9.60884E-03	P16	2.88246E-04	P26	9.60883E-11
P06	9.51275E-03	P18	5.82315E-09	P29	9.51274E-09
P09	9.41763E-01	P19	2.90866E-06	P32	5.82373E-13
P12	2.91157E-04	P21	2.91186E-13	P33	2.90895E-10
P13	2.88246E-02	P24	9.80392E-11		

1) Simulation Results: The steady-state probabilities of each place in Fig. 5 are shown in Table I. The steady-state probability of disruptive switching actions is 5.8×10^{-9}. The steady-state probability at the place, p_9 ranks the highest value of 0.94. The steady-state probability at the place, p_{13} follows to be 0.029 (the second-highest value). These results show imply highly likelihood of intrusion attempts to crack a firewall. Historical data are often used to estimate future cyber-risk. However, invisible/implicit risks such as cracking the firewall cannot be estimated. The proposed cyber-net model provides residual risks that allows to reach steady-state probabilities.

2) Sensitivity Analysis for Honeynet: The steady-state probabilities of disruptive switching attacks with honeynets that do not have the prevention function, and with advanced honeynets that have the prevention function are derived and compared in this case study. In the case of the honeynet with no prevention function, the transition probabilities, t_{53} and t_{54}, are set as 0.999999 and 1.0×10^{-6}, respectively. In the case of the

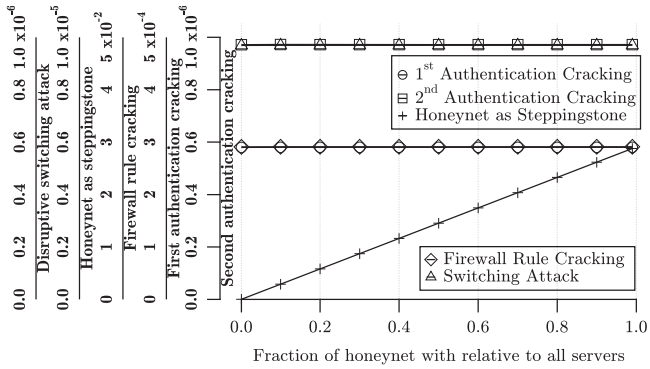

Fig. 6. Probabilities of a cyber-net in response to fraction of honeynet without prevention function.

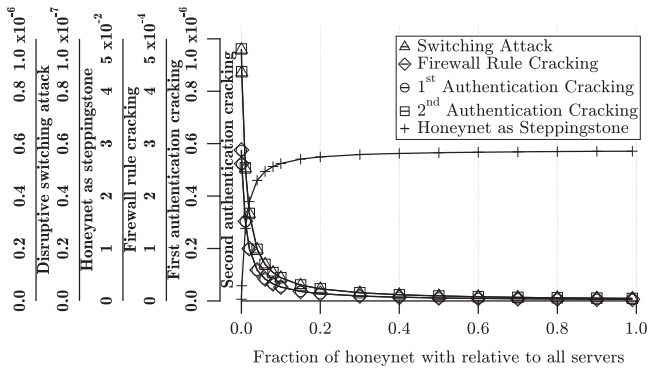

Fig. 7. Probabilities of a cyber-net in response to fraction of honeynet with prevention function.

advanced honeynet, the transition probabilities, t_{53} and t_{54}, are set as 1.0×10^{-6} and 0.999999, respectively. The fraction of the honeynet is set as the transition probability of t_2 in the range of 0 (0%) and 1 (100%), and five indicators are shown in Figs. 6 and 7. As shown in Fig. 6, the steady-state probability of reaching the Internet from honeynets increases linearly as the fraction of honeynets increase, while four steady-state probabilities with honeynets that have no prevention function are almost the same regardless of the fraction of honeynets. On the other hand, Fig. 7 shows five steady-state probabilities with advanced honeynets. The curve in the figure shows exponential changes for the increased number of honeynets and servers deployed in the substation network.

The following are the observations from the simulation with or without prevention function:

a) Honeynet without prevention function: As depicted in Fig. 8, the discrete events from simulations show the two distinct curves of probabilities for each event where all of them converge in the end. If the honeynet without prevention function shares 99% of the servers, the number of attackers who spread outgoing packets gradually increases as time goes (see the second top indicator in Fig. 8). That results in an increased number of attackers who attempt to crack firewall rules, *i.e.*, steady-state probabilities of places, p_4, p_5, p_6, and p_9, consistently rise when it reaches the steady-state condition.

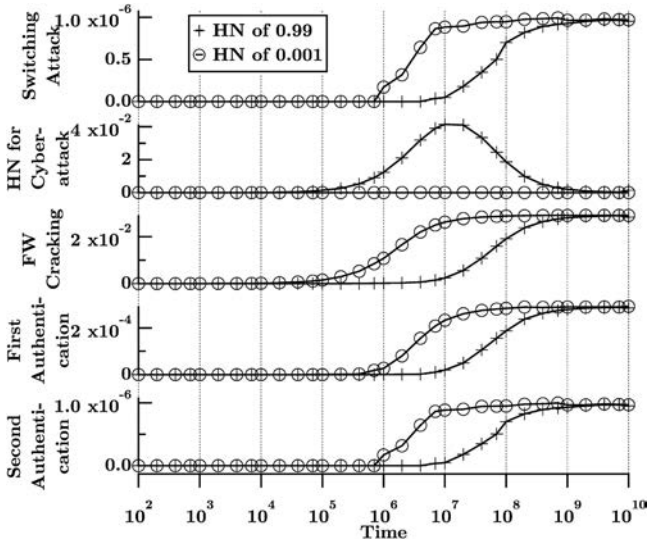

Fig. 8. Time-varying probabilities of a cyber-net in response to fraction of honeynet without prevention function.

It can be observed in Fig. 8 that the imputed value of time at 1×10^7 shows in the third row where the firewall is compromised. The trending of the FW cracking is up with both honeynet parameters of 0.99 and 0.001, reaching the same steady-state values eventually, as observed in the figure. Although the increasing timing of the third top indicator is different depending on the fraction of honeynets, the graph in the third row eventually reaches the same level over a long time. Because steady-state probability only indicates the probability over a long time, steady-state probabilities of cracking firewall rules and passwords and of switching attack are the same, independent from the total numbers of honeypots and servers are modeled.

b) Honeynet with prevention function: If the honeynet has the prevention function, nearly all attackers are trapped in the honeynet (*i.e.*, such attackers fail to infect other servers from the honeynet) once they invade into it. That implies that the honeynet model has a dead-end that does not feedback to the attackers as part of the learning process. On the other hand, the IED model has feedback that enables attackers to learn in trial-and-error discovery. That says some attackers who successfully perform the switching attack can be trapped in the honeynet at the second round or later according to the hypothesized fraction of t_2. Because the steady-state probability discusses the probabilities of each state over an incredibly long time, no loop structure of the honeynet model makes the number of attackers who are trapped in honeynets exponentially accelerated as the fraction of honeynets, t_2 increases. Then, the number of such attackers is saturated, once the probability of the switching attack is small, contributing insignificantly to the overall risk.

B. Cyber-Net Model With Multiple IEDs and SCADA

In order to reach the steady-state probability of substation attacks, the cyber-net model in Fig. 5 is further extended to include multiple IEDs and a SCADA. The major protections that are installed at 220 kV or over substations and power stations are taken into account as IEDs. Readers can refer to the typical

representation of relay types and the number of their settings per each relay in substations from [36]. This reference of the CIGRE report based on the relay experts from around the world is used as the base to set up the case studies here. We deem the number of setting parameters on relaying as potential combinations of tripping associated breaker(s) by experience. This reference is used here in the simulation study.

1) Guidance of Immediate Transition: The installed protections are different between a power station and a substation, and the volume of these protections at each power station/substation varies depending on the number of power equipment such as generators, transformers, buses, and transmission lines. In addition, the type of protective relays can vary depending on the voltage level in the substation.

A distributed control center monitors and controls 6–7 substations in transmission systems on average, according to the real-world example. If the distributed control centers are modeled at a 132 kV/66 kV substation in the IEEE 14-bus system model, two control centers are hypothesized. Because IEDs and the server at the control center have their unique static IP addresses, the risk of the substation attacks via a control server can be diversified at a substation level.

In this study, each relay type is assigned to individual IED, and t_{21} and t_{22} in Fig. 5 are provided according to the fraction of the protective relays at a substation, as shown in Eqs. (19) and (20).

$$t_{21,\text{IED}} = \frac{\times \sum_{j=1}^{n_{\text{equip}}} j}{\sum_{i=1}^{n_{\text{relay}}} i + \frac{n_{\text{CS}}}{n_{\text{SS}}}};\quad t_{21,\text{SCADA}} = \frac{\times \frac{n_{\text{CS}}}{n_{\text{SS}}}}{\sum_{i=1}^{n_{\text{relay}}} i + \frac{n_{\text{CS}}}{n_{\text{SS}}}} \tag{19}$$

$$t_{22,\text{IED}} = \frac{\times \sum_{j=1}^{n_{\text{equip}}} j}{\sum_{i=1}^{n_{\text{relay}}} i + \frac{n_{\text{CS}}}{n_{\text{SS}}}};\quad t_{22,\text{SCADA}} = \frac{\times \frac{n_{\text{CS}}}{n_{\text{SS}}}}{\sum_{i=1}^{n_{\text{relay}}} i + \frac{n_{\text{CS}}}{n_{\text{SS}}}} \tag{20}$$

where n_{equip} denotes the number of same power equipment at a substation, such as buses and lines, n_{relay} denotes the number of same relay type at a substation, n_{CS} and n_{SS} denote the numbers of control centers and substations in the system, respectively ($n_{\text{CS}} = 2$ and $n_{\text{SS}} = 10$ for this study case).

2) Guidance of Timed Transition: This paper proposes a systematic manner of how to provide two specific parameters, τ_{27} and τ_{31} of the developed cyber-net model in Fig. 5. When an IED is compromised by attackers, and the relay settings change, malicious tripping due to the intentional wrong relay settings could occur. In this case, the time to review all relay settings is highly likely to increase as the number of relay settings increases. It is suggested that the time to learn how to deal with the IED for the attack, *i.e.*, the inverse of τ_{27}, is assumed to be proportion to the number of relay settings for each protection scheme. In this case study, τ_{27} is set as the default imputed value of 1.0×10^{-6} for the IED, *i.e.*, the distance relay that has the largest number of relay settings of 19 and derived from Eq. (21). The transition rate τ_{27} for SCADA needs to be initialized as there is a much larger number of switches to be reviewed, it is likely to have a longer time to overview all controllable switches and to get acquainted with the environment of local SCADA system than direct connections to IEDs. In this study, τ_{27} for SCADA is set to be 9.5×10^{-8}.

On the other hand, at least one AND conditions and many OR conditions are generally included in the relay logic diagram, and many relay settings can be restrained to avoid the improper relay settings coordination. Therefore, as the number of relay settings increases, the possibility of the malicious relay operation can increase against such constraints, *i.e.*, the attackers are likely to shorten the time to operate the targeted IED. In light of this, it is suggested that the time to complete disruptive switching actions, *i.e.*, the inverse of τ_{31} may be assumed to be inversely proportional to the number of relay settings. In this case study, τ_{31} is set as the default imputed value of 0.5×10^{-6} for the IED, *i.e.*, the high impedance voltage differential relay that has the smallest number of relay settings of 2 and all τ_{31} are derived from Eq. (21). In this study, τ_{31} for SCADA is set to be 4.17×10^{-7}.

$$\tau_{27,\text{IED}} = \frac{1.0 \times 10^{-6} \times 19}{n_{\text{ry\_set}}};\ \tau_{31,\text{IED}} = \frac{0.5 \times 10^{-6} \times n_{\text{ry\_set}}}{2} \tag{21}$$

where $n_{\text{ry\_set}}$ denotes the number of relay settings. The rest of the transition parameters are assumed to be the same as the values in Fig. 5. These will be updated based on the observation of the time window from the available event source from the local computer systems.

3) Case Study and Implementation: Figure 10 shows the outline of the created cyber-net model with up to 8 IEDs. In order to elaborate on the installed protections at each power station/substation, the following are considered using [35]:

- A step-up transformer of synchronous generators or condensers are directly connected to the 132-kV bus; they are typically connected to a substation with the voltage level is lower than 132-kV. Step-down transformers of loads are not considered in this study.
- One reactive power compensator is included if a load or a transformer is explicitly shown without reactive power compensators or synchronous condensers.
- A double-circuit line for the one-line diagram shown in general IEEE test cases. Advanced line protection that compensates for the zero-phase circulation current is assumed to be applied to multi-circuit transmission lines that share the same towers.

4) Simulation Result: The probabilities of disruptive switching executed against the substation automation SCADA system or executed by compromised IED-initiated (CII) attacks are shown in Table II. The table shows that the probabilities of IEDs are inversely proportional to the number of relay settings as well as proportional to the number of protective relays, relatively to all relays in the designated substation.

The steady-state probability of the substation attack is the summation of the steady-state probabilities of switching attacks for the SCADA and for IEDs that result in the entire substation outage. A subset of breaker tripping associated IEDs can energize the entire substation, depending on the substation topology. For example, compromising IED6 and IED7 at Bus 1 in Table II can cause the whole substation outage. The steady-state probability of such a simultaneous switching attack is calculated using two initial tokens. In this case, the steady-state probability of the

TABLE II
STEADY-STATE PROBABILITIES OF SUBSTATION ATTACK FOR IEEE 14-BUS SYSTEM WITH HYPOTHESIZED RELAY TYPES

	Substation										Protection type	Relay type	Number of relay settings
	Bus 1	Bus 2	Bus 3	Buses 4&9	Buses 5&6	Bus 10	Bus 11	Bus 12	Bus 13	Bus 14			
IED1	1.563E-07 (1)	1.182E-07 (1)	1.864E-07 (1)	1.729E-07 (2)	1.953E-07 (2)	2.307E-07 (1)	2.307E-07 (1)	2.307E-07 (1)	1.864E-07 (1)	2.307E-07 (1)	Bus	Current differential	12
IED2	–	–	–	2.075E-07 (1)	–	5.537E-07 (1)	5.537E-07 (1)	5.537E-07 (1)	4.473E-07 (1)	5.537E-07 (1)	Reactive power compensator		5
IED3	1.443E-07 (1)	1.091E-07 (1)	1.720E-07 (1)	7.981E-08 (1)	9.013E-08 (1)	–	–	–	–	–	Generator		13
IED4	–	–	–	2.075E-07 (2)	–	–	–	–	–	–	Sub-trans-mission line (multi-circuit)	Advanced transverse differential	10
IED5	–	–	–	–	5.858E-07 (3)	9.228E-07 (2)	9.228E-07 (2)	9.228E-07 (2)	1.118E-06 (3)	9.228E-07 (2)	Sub-trans-mission line	Transversal differential	6
IED6	3.411E-07 (2)	5.158E-07 (4)	–	1.886E-07 (2)	2.130E-07 (2)	–	–	–	–	–	Transmission line (multi-circuit)	Advanced current differential	11
IED7	4.689E-07 (1)	3.546E-07 (1)	1.118E-06 (2)	2.594E-07 (1)	2.929E-07 (1)	–	–	–	–	–	Transmission line	Current differential	4
IED8	1.876E-07 (1)	1.418E-07 (1)	2.236E-07 (1)	2.075E-07 (2)	1.172E-07 (1)	–	–	–	–	–	Transformer	Current differential	10
SCADA	2.927E-09	2.213E-09	3.489E-09	1.619E-09	1.828E-09	4.320E-09	4.320E-09	4.320E-09	3.489E-09	4.320E-09	–	–	–
Total	1.592E-07	1.204E-07	1.899E-07	1.745E-07	1.971E-07	2.350E-07	2.350E-07	2.350E-07	1.899E-07	2.350E-07	–	–	–

Note: figures in brackets denote the number of protective relays

TABLE III
RELAY MODELING: TYPES AND SETTINGS USING FOUR IEEE STANDARD SYSTEM MODELS

IEEE standard system model	14-bus	30-bus	57-bus	118-bus
Number of substation (and power station)	10	24	43	109
Number of SCADA	2	3	4	11
Relay type of high-voltage line protection	Ordinary current differential (4); Advanced current differential (11)			
Relay type of medium-voltage line protection	Ordinary transversal differential (6); Advanced current differential (10)			
Relay type of low-voltage line protection	–	–	Distance (19)	–
Relay type of bus protection for substation	Current differential (12)			
Relay type of bus protection for switching station	High-impedance voltage differential (2)			
Relay type of transformer protection for step-up transformer	Current differential			
	(12)	(12)	(12)	Synchronous generator (12); Synchronous condenser (13)
Relay type of transformer protection for step-down transformer	Current differential			
	(12)	(12)	Autotransformer (13); Ordinary transformer (14)	(14)

Note: figures in brackets denote the number of relay settings for the corresponding relays.

switching attack for IED6 and IED7 is derived as 1.70×10^{-14}, which is 10^4 times smaller than the steady-state probability of switching attacks for the SCADA and negligible. On the other hand, compromising IED1 at Bus 1 in Table II also causes the whole substation outage. This steady-state probability is around 100 times larger than that for the SCADA and is not negligible. Therefore, the only steady-state probability of switching attacks for a single IED that causes the whole substation attack, (*i.e.*, only when all bus protections at a substation are compromised) other than the steady-state probability for the SCADA needs to be included. In other words, the steady-state probability of switching attacks can be negligible when using more than or equal to two different relay types for bus protections. In this case study, the steady-state probability of the switching attack for substation 1 at Bus 1 can be derived as 1.592×10^{-7}(with $1.563 \times 10^{-7} + 2.927 \times 10^{-9}$). The same procedure is applied to derive the steady-state probability of switching attacks at each substation in the different IEEE standard models, such as IEEE 30-Bus, 57-Bus, and 118-Bus systems as shown in Table III and Fig. 9.

V. DISCUSSION

A. Industry Practice in Security Logging

In practice, anomalous statistics for each utility can largely vary. Due to the proprietary information, such datasets are not publicly available. Some values are imputed based on the empirical base that falls within a reasonable range. Although deriving reasonable transition probabilities and rates for the cyber-net model would be a future research study, the considerable approach is shown in Table IV.

The number of commissioned protective relays set up in substations can be directly obtained from the utilities. This is in proportion to the typical deployment of substation equipment, such as associated busbars, transmission lines, and transformers. The attempts resulting in successful intrusion to bypass firewalls or passwords can be inferred from the security event logs from the available sources. That can include honeypots to be modeled [37]–[39]. The frequency of the zero-day attack can also be obtained from the database that is available to the public [40], [41]. As security event logs do not reveal to the

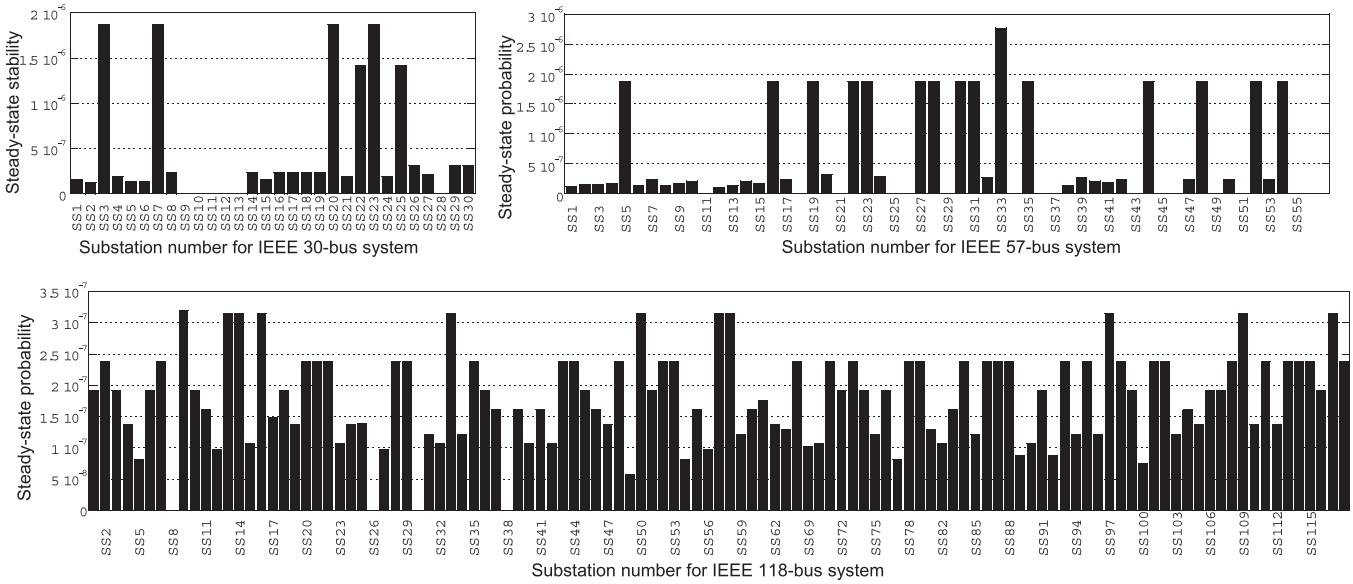

Fig. 9. Steady-state probability for each substation (sequential order) in IEEE 30-, 57-, and 118-bus systems.

TABLE IV
MEASURE OF DERIVATION OF TRANSITION PROBABILITY AND RATE FOR SUBSTATION ATTACK WITH USED VALUES FOR IEEE 14-BUS SYSTEM

Transition probability/rate	Measure of setting transition probabilities and rates	Example of reference source	Values for case study
t_1 $(= 1 - t_2)$	Number of honeypot servers with relative to all control servers including honeypot servers	Brochure for control centers	0.0001
t_3 $(= 1 - t_6)$, t_4 $(= 1 - t_7)$, t_5 $(= 1 - t_8)$, t_{43} $(= 1 - t_{46})$, t_{44} $(= 1 - t_{47})$, t_{45} $(= 1 - t_{48})$.	Number of successful attempts to open a port with relative to the total attempts to open the port	Operating system event logs	0.01
τ_9, τ_{10}, τ_{11}, τ_{49}, τ_{50}, τ_{51}.	Inverse of the following sum of the averaged time 1) response time to attempt opening the port 2) response time to confirm that the status of the port is opened 3) response time to reach to the password input screen of the targeted server 4) response time to input the first password	Specification of server performance	1.0×10^{-6}
τ_{12}, τ_{52}	Inverse of the following sum of the averaged time 5) response time to attempt opening the port 6) response time to confirm that the status of the port is closed		1.0×10^{-6}
τ_{23}	Inverse of the following sum of the averaged time 7) response time to reach to the second password input screen 8) response time to input the second password		1.0×10^{-6}
τ_{24}	Inverse of the averaged response time to return to the first password input screen		1.0×10^{-6}
τ_{30}	Inverse of the averaged time to return to the first password input screen		1.0×10^{-6}
t_{21} $(= 1 - t_{22})$	9) Number of successful attempts to log in to the targeted server as the first authentication 10) Fraction of one relay type with relative to all relay types at a substation or a power station	Security event logs of servers	0.01 Eqs. (19)(20)*
τ_{27}	11) Inverse of the averaged time to review and to learn how to change relay settings 12) Fraction of relay settings with relative to maximum/minimum relay settings	Instruction manual of protective relays	1.0×10^{-6} Eq. (21)
τ_{31}	13) Inverse of the averaged time to opening all circuit breakers that are connected to a substation 14) Fraction of relay settings with relative to maximum/minimum relay settings		5.0×10^{-7} Eq. (21)
t_{28} $(= 1 - t_{29})$	15) Fraction of IEDs with relative to all protective relays and/or fraction of digitalized substation with relative to all operating substations 16) Fraction of IEDs without interlocking or a function that can cope with the switching attack	In consultation with manufacturers/utilities	0.0001
τ_{32}	Inverse of the averaged time to give up substation attacks from the attack inception	Substation diagram	5.0×10^{-7}
τ_{42}	Inverse of the averaged time to copying tools into the honeynet for the cyberattack	Event logs of honeypot	1.0×10^{-3}
t_{53} $(= 1 - t_{54})$	Fraction of time between the honeynet infection and application of the new generated rule	Data sources of security vulnerabilities	0.01
τ_{55}	Inverse of the averaged time to apply the new generated rule after the honeynet infection		1.0×10^{-3}
τ_{56}	Inverse of the averaged time to fail to send outgoing packets to infect other servers		5.0×10^{-7}

* The value of 9) is reflected in 10), *i.e.*, Eqs. (19) and (20).

zero-day vulnerability for the honeynet and the data can vary as time goes by, only carefully thought values are imputed in the case studies. Accessing to the proprietary data would strengthen the quality of systemic risk in a practical case study that would allow insurances to better assess utility risk with regards to their readiness in security defense.

B. Transition to Cyber Insurance Business for Power Grids

The creativity of attackers' stratagem can result in different operational implications. Switching attack in the control system would perturb the instability of a power grid. There may be combinations of events with assistance from insiders where an attack can be effective when coordination between insiders

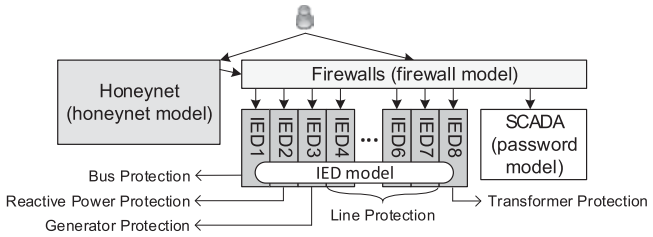

Fig. 10. Case setup for cyber-net with multiple protective IEDs and a SCADA.

and the remote collaborators may create events of disturbance, such as electrical short circuits. Substations are connected with multiple components where an abrupt switching of all of these components can implicate system operation, which is studied in [28]–[31]. Although security is viewed as a *low-probability, high-impact* event, the new perspectives of enterprise risk management in planning should consist of two major components, *i.e.*, assessment of security readiness and remedial/preventive responses. The planning for security investment should be based on the operational bottleneck from historical observations with simulations where it should reflect consequential contingencies associated with each substation and their corresponding outages. On the contrary, this work extensively captures the high level of abstraction with respect to technology implementation, and the events from the first intrusion attempt to execute a switching attack in discrete events successfully. The prevention of such cyber events is described in the proposed models.

C. Establishing Actuarial Framework

Establishing the premium of an insurance policy depends on two fundamental aspects of consideration, *i.e.*, (1) distributions of frequency, and (2) severity of insurance claims. These two distributions are often estimated based on historical observations. This work establishes a systemic risk framework to provide quantities pertaining to what is deployed in substations. To the best of our knowledge, gauging the frequency of event occurrence that captures within a substation has been challenging due to a large number of attack vector combinations. The proposed model estimating the steady-state probabilities of potential case combinations provides a means of adjustment for future protection improvement in security planning. The anomalous incidents can lead to successful intrusion, and the actuarial aspect of the anomalies should be captured in the systemic risk.

VI. Concluding Remarks

The compilation and analysis of anomaly data statistics extracted from the cyber system in IP-based substations are critical to the understanding of security health within the private network. Establishing steady-state probabilities based on the network architecture, security technologies, as well as characterizing intrusion behaviors, are the essential subjects to estimate security risks. This paper advances the procedure to reflect on the steady-state probabilities of switching substation attacks within the existing implementation of security protection, using Petri net models. This also provides a guideline on the estimation of model parameters in the specific substation topology and protective IEDs. However, the developed model has a limitation. It is noted that the proposed Petri net model is based on the Markov property for state transitions. The GSPN is applicable only when the holding time, such as the sojourn time, in each state, is assumed to be either zero or exponentially distributed. Future research includes establishing other statistical distributions. In addition, enhancing the modeling complexity in terms of the size of the specific modeling can increase computational time. Capturing the risks of switching attack can be further extended for estimating cyber insurance premiums because such a risk is generally derived from the steady-state probability of anomalies and the impact of the switching attack. Other combinations, such as one or more outages of interconnected substations due to false data injection attacks, should be considered in proposed risk-based framework. Asset owners can also consider to implement their in-house cyber analytics to understand and implement security policies more effectively.

References

[1] North American Reliability Corporation, "CIP standards," 2020. [Online]. Available: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
[2] Federal Departments and Agencies, "https://fas.org/irp/agency/dhs/nipp110205.pdf protection plan," Nov. 2005. [Online]. Available: https://fas.org/irp/agency/dhs/nipp110205.pdf
[3] R. Heidorn Jr., "NERC seeks $10m fine for duke energy security lapses," Feb. 2019. [Online]. Available: https://www.rtoinsider.com/nerc-fine-duke-energy-cip-110308/
[4] Center for Strategic and International Studies (CSIS), "Significant cyber incidents since 2006," Feb. 2019. [Online]. Available: https://csis-prod.s3.amazonaws.com/s3fs-public/190211_Significant_Cyber_Events_List.pdf
[5] R. Bulbul, P. Sapkota, C.-W. Ten, L. Wang, and A. Ginter, "Intrusion evaluation of communication network architectures for power substations," *IEEE Trans. Power Del.*, vol. 30, no. 3, pp. 1372–1382, Jun. 2015.
[6] The Department of Homeland Security, "Critical infrastructure protection DHS has made progress in enhancing critical infrastructure assessments, but additional improvements are needed," Jul. 2016. [Online]. Available: https://www.hsdl.org/?view&did=796918
[7] NERC Board of Trustees, "Reliability standards for the bulk electric systems of north america," May 2017. [Online]. Available: http://www.nerc.com/pa/Stand/Reliability Standards Complete Set/RSCompleteSet.pdf
[8] Critical Infrastructure Protection Committee (CIPC), "Cybersecurity – BES cyber system categorization," Oct. 26 2012. [Online]. Available: http://www.netsectech.com/wp-content/uploads/2013/05/Version-5-of-the-N ERC-CIP-Cyber-Security-Standards.pdf
[9] H. Wardak, S. Zhioua, and A. Almulhem, "PLC access control: A security analysis," in *Proc. World Congr. Ind. Control Syst. Sec.*, London, UK, Dec. 2016, pp. 1–6.
[10] S. Bricker, T. Gonen, and L. Rubin, "Substation automation technologies and advantages," *IEEE Comput. Appl. Power*, vol. 14, no. 3, pp. 31–37, Jul. 2001.
[11] J. Hong, C.-C. Liu, and M. Govindarasu, "Detection of cyber intrusions using network-based multicast messages for substation automation," in *Proc. IEEE PES Innovative Smart Grid Technol.*, Feb. 2014, pp. 1–5.
[12] L. Spitzner, "The honeynet project: Trapping the hackers," *IEEE Secur. Privacy*, vol. 1, no. 2, pp. 15–23, Mar. 2003. [Online]. Available: http://dx.doi.org/10.1109/MSECP.2003.1193207.
[13] L. R. Even, "Honeypot systems explained," Jul. 2000, [Online]. Available: https://www.sans.org/security-resources/idfaq/honeypot3.php.
[14] M. Nawrocki, M. Wahlisch, T. C. Schmidty, C. Keilz, and J. Schonfelder, "A survey on honeypot software and data analysis. Cornell University," Aug. 2016, [Online]. Available: https://arxiv.org/pdf/1608.06249.
[15] T. Murata, "Petri nets: Properties, analysis and applications," *Proc. IEEE*, vol. 77, no. 4, pp. 541–580, Apr. 1989.
[16] F. Bause and P. S. Kritzinger, *Stochastic Petri Nets*, 2nd ed. Wiesbaden, Germany: Vieweg+Teubner Verlag, 2002.

[17] C. A. Petri, "Kommunikation mit automaten," Ph.D. dissertation, Bonn: Institut für Instrumentelle Mathematik, vol. 3, pp. 1–128, Jun. 1962.
[18] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA system," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.
[19] M. A. Berger, *An Introduction to Probability and Stochastic Processes*, 1st ed. Berlin, Germany: Springer, 1993.
[20] C.-S. Cho, W.-H. Chung, and S.-Y. Kuo, "Cyber-physical security and dependability analysis of digital control systems in nuclear power plants," *IEEE Trans. Syst., Man, Cybern.*, vol. 46, no. 3, pp. 356–369, Mar. 2016.
[21] R. Zeng, Y. Jiang, C. Lin, and X. Shen, "Dependability analysis of control center networks in smart grid using stochastic Petri nets," *IEEE Trans. Parallel Distribution Syst.*, vol. 23, no. 9, pp. 1721–1730, Sep. 2012.
[22] R. Mitchell and I.-R. Chen, "Effect of intrusion detection and response on reliability of cyber physical systems," *IEEE Trans. Rel.*, vol. 62, no. 1, pp. 199–210, Mar. 2013.
[23] D. Verneza, D. Buchsb, and G. Pierrehumberta, "Perspectives in the use of coloured petri nets for risk analysis and accident modelling," *Safety Sci.*, vol. 41, no. 5, pp. 445–463, Jun. 2003.
[24] "Behavior and vulnerability assessment of drones-enabled industrial internet of things (IIoT)," *IEEE Access*, vol. 6, pp. 43 368–43 383, 2018.
[25] London Economics International LLC, "Estimating the value of lost load," Jun. 17, 2013. [Online]. Available: http://www.ercot.com/content/gridinfo/resource/2015/mktanalysis/ERCOT_ValueofLostLoad_LiteratureReviewandMacroeconomic.pdf
[26] European Network and Information Security Agency, "Incentives and barriers of the cyber insurance market in europe," Jun. 28 2012. [Online]. Available: http://www.biztositasiszemle.hu/files/201207/cyber_insurance_market.pdf
[27] J. F. Anderson and R. L. Brown, "Risk and insurance. education and examination committee of the society actuaries," 2005, [Online]. Available: https://www.soa.org/files/pdf/P-21-05.pdf
[28] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 2, pp. 273–285, Dec. 2013.
[29] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "A smart grid vulnerability analysis framework for coordinated variable structure switching attacks," in *Proc. Power Energy Soc. General Meeting*, 2012, pp. 1–8.
[30] A. Farraj, E. Hammad, A. A. Daoud, and D. Kundur, "A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1846–1855, Jul. 2016.
[31] S. Z. Yong, M. Zhu, and E. Frazzoli, "Resilient state estimation against switching attacks on stochastic cyber-physical systems," in *Proc. IEEE 54th Annu. Conf. Decis. Control*, Dec. 2015, pp. 5162–5169.
[32] Y. Xiang, L. Wang, and N. Liu, "Coordinated attacks on electric power systems in a cyber-physical environment," *Electric Power Syst. Res.*, vol. 149, pp. 56–168, Aug. 2017.
[33] L. Ponemon, "Calculating the cost of a data breach in 2018, the age of AI and the IoT," Jul. 2018. [Online]. Available: https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/
[34] M. A. H. Kermani1, M. A. Golkar, and S. Zokaei, "Providing a model for a cyber-attack to a special protection scheme based on timed petri net," *J. Energy Manag. Technol.*, vol. 3, no. 2, pp. 22–33, Apr. 2019.
[35] R. D. Christie, "Power systems test case archive," Aug. 1999. [Online]. Available: http://labs.ece.uw.edu/pstca/pf14/pg_tca14bus.htm
[36] W. G. B5.19, "Protection relay coordination," CIGRE, Paris, Tech. Rep. TB432, Oct. 2010.
[37] Bitdefender Labs, "New hide-and-seek IoT botnet using custom-built peer-to-peer communication spotted in the wild," Jan. 2018. [Online]. Available: https://labs.bitdefender.com/2018/01/new-hide-n-seek-iot-botnet-using-custom-built-peer-to-peer-communication-spotted-in-the-wild/.
[38] Akamai, "Upnproxy: Blackhat proxies via NAT injections," 2018. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/white-paper/upnproxy-blackhat-proxies-via-nat-injections-white-paper.pdf
[39] Cisco Talos Intelligence Group, "New VPN filter malware targets at least 500k networking devices worldwide," May 2018. [Online]. Available: https://blog.talosintelligence.com/2018/05/VPNFilter.html
[40] M. Corporation, "CVE details -security vulnerabilities (CVSS score between 9 and 10)," 2019. [Online]. Available: https://www.cvedetails.com/vulnerability-list/cvssscoremin-9/cvssscorem ax-10/vulnerabilities.html.
[41] O. Security, "Exploit database," 2020. [Online]. Available: https://www.exploit-db.com/.

Koji Yamashita (Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Waseda University, Tokyo, Japan, in 1993 and 1995, respectively. He is currently working toward the doctorate degree with Michigan Technological University, Houghton, MI, USA. He was a Visiting Researcher with Iowa State University from 2006 to 2007. He had been a Researcher with the Central Research Institute of Electric Power Industry, Tokyo, Japan and had been with the Department of Power Systems since 1995. His research interests include hypothesized attack scenarios and its resulting impact on system dynamics and stability, wide-area protection and control as well as strategic mitigation of system generation/loads imbalance.

Chee-Wooi Ten (Senior Member, IEEE) received the B.S.E.E. and M.S.E.E. degrees from Iowa State University, Ames, IA, USA, in 1999 and 2001, respectively, and the Ph.D. degree in 2009 from the National University of Ireland, University College Dublin, Dublin, Ireland, prior joining Michigan Tech in 2010. He is currently an Associate Professor of electrical and computer engineering, Michigan Technological University, Houghton, MI, USA. He was a Power Application Engineer working in project development for EMS/DMS with Siemens Energy Management and Information System (SEMIS), Singapore from 2002 to 2006. His primary research interests are modeling for interdependent critical cyberinfrastructures and SCADA automation applications for a power grid.

Yeonwoo Rho received the B.S. degree in mathematics and the B.A. degree in economics from Seoul National University, Seoul, South Korea, in 2006, the M.S. degree in statistics from Seoul National University, Seoul, South Korea, in 2009, and the Ph.D. degree in statistics from the University of Illinois at Urbana-Champaign, Champaign, IL, USA, in 2014. She is currently an Assistant Professor of statistics with the Department of Mathematical Sciences, Michigan Technological University, Houghton, MI, USA. Her primary research interests are in time series analysis and forecasting, econometrics, spatial-temporal dependence modeling, bootstrap and resampling methods, and mixed frequency data.

Lingfeng Wang (Senior Member, IEEE) 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 Department of Electrical and Computer Engineering, 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, Milwaukee, WI, USA. His major research interests include power system reliability, security and resiliency. He is an Editor for the IEEE TRANSACTIONS ON SMART GRID, IEEE TRANSACTIONS ON POWER SYSTEMS, and IEEE POWER ENGINEERING LETTERS, and served on the steering committee for the IEEE TRANSACTIONS ON CLOUD COMPUTING. He is also an editorial board member for several international journals, including *Journal of Modern Power Systems and Clean Energy, Sustainable Energy Technologies and Assessments, and Intelligent Industrial Systems*. He was the recipient of the Outstanding Faculty Research Award of College of Engineering and Applied Science at UWM in 2018.

Wei Wei received the Ph.D. degree in actuarial science from the University of Waterloo, Waterloo, ON, Canada. In 2013, he joined the University of Wisconsin.Milwaukee, Milwaukee, WI, USA, where he is currently an Associate Professor in Actuarial Science. He is an Associate of Society of Actuaries and China Association of Actuaries. 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 applications of ruin theory.

Andrew Ginter (Member, IEEE) received the degree in mathematics and computer science from the University of Calgary, Calgary, AB, Canada, as well as Industrial Security Professional, Information Technology Certified Professional, and Certified Information Systems Security Professional. He is the Vice President of Industrial Security with Waterfall Security Solutions. He spent the first part of his career developing systems level and control system products for a number of vendors, including Honeywell and Hewlett-Packard. He led development of middleware products connecting industrial control systems to the SAP enterprise resource planning systems with Agilent Technologies. As a Chief Technology Officer with Industrial Defender, he led the development of HTE core industrial security product suite.