FlipIt Game Model-Based Defense Strategy Against Cyberattacks on SCADA Systems Considering Insider Assistance

Zhaoxi Liu, *Member, IEEE*, and Lingfeng Wang, *Senior Member, IEEE*

***Abstract*— The industrial internet of things (IIoT) is emerging as a global trend to dramatically enhance the intelligence and efficiency of the industries in recent years. With the emphasis on data communication by IIoT, cyber vulnerabilities are introduced at the same time. As a key subsystem of the industrial automation systems, the supervisory control and data acquisition (SCADA) system is becoming one of the primary targets for cyberattacks in the IIoT paradigm. In this paper, the semi-Markov process (SMP) is employed to model and evaluate the cyberattacks against the SCADA systems considering the insider assistance. Based on the SMP model, the probability distribution of the time-to-compromise the system of the attacks is derived with the Monte Carlo simulation (MCS). Then, a FlipIt game model is developed to investigate the defense and attack strategies of the defender and attacker, and analyze the impacts of the insider assistance. Case studies were carried out to verify the proposed model. The results of the case studies show that the insider assistance will improve the payoff of the attacker and increase the defense action frequency of the system defender. With a high enough defense action frequency, the defender can force the attacker to drop out and eliminate the attack actions.**

***Index Terms*— SCADA, cybersecurity, FlipIt game, industrial internet of things (IIoT), insider.**

I. Introduction

THE internet of things (IoT) has a wide range of applications, and among the most important ones are the applications in industries [1]. The industrial IoT (IIoT) is emerging as one of the most promising paths to enhance the operation efficiency of the industrial automation systems to a new level by widely integrating innovations in computing, communication, big data analytics and machine learning in recent years. It is believed to bring a new wave of industrial revolution and transform nearly every industry in the modern society [2].

In order to achieve higher efficiency and better quality of operations, IIoT depends heavily on the communication to achieve a highly interconnected industrial automation system. Devices in the automation systems (e.g., sensors, actuators, controllers, motors, workstations and remote cloud servers) are connected through the industrial communication systems to enable real-time data exchange and more intelligent applications [3]. The information and communication technology (ICT) is playing an increasingly significant role due to the growing demand for high-speed high-capacity data communication and information processing in the IIoT paradigm. A direct consequence of the highly interconnected architecture of IIoT and tight integration of ICT is the introduced cyber vulnerability and increasing cybersecurity threats to the industrial control systems (ICS) [4], [5]. Thus, the cybersecurity of the ICS has become an important topic and recent efforts have been paid to access and enhance the cybersecurity of the ICS [6], [7]. The supervisory control and data acquisition (SCADA) systems are widely used for the data acquisition and supervisory control of equipment and processes in industries which are critical for IIoT [8], [9]. Hence, the SCADA systems are potential targets for adversaries, and effective cyberattacks on the SCADA systems can have serious financial and security consequences. A recent example is the cyberattacks against the SCADA systems in the Ukraine power grids in December 2015, in which about 225 thousand customers and more than 50 substations were affected [10]. Thus, improving the reliability of the SCADA systems under potential cyberattacks becomes critical for enhancing the trustworthiness of the industrial automation systems for IIoT.

In recent years, more and more attention is being paid to the insider threats in the area of cybersecurity analysis. It is well accepted that insiders have significant impacts to the cybersecurity. Generally, cyberattacks by malicious insiders are more covert, and are more costly and take longer time to be resolved with respect to external attacks [11]. Statistics show that insiders have already been a substantial threat to many organizations [12]. Although the SCADA systems may employ exclusive protocols and use firewalls to get isolated from the external network, the insider threats may still be fatal to the cybersecurity of the SCADA systems. Insiders have intimate knowledge of the security settings of the SCADA network and how the SCADA system operates, which is important information for the attacker to formulate valid attack vectors. Meanwhile, an external attacker must gain access to the SCADA network before exploiting the vulnerabilities of the protocols or devices in the SCADA system. The remote access or even physical access to the network can be achieved

Manuscript received June 24, 2020; revised October 18, 2020 and December 23, 2020; accepted February 15, 2021. Date of publication March 10, 2021; date of current version April 16, 2021. This work was supported in part by the U.S. National Science Foundation under Award ECCS1711617 and in part by the Research Growth Initiative Program of University of Wisconsin-Milwaukee under Award 101 × 360. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Wei Yu. *(Corresponding author: Lingfeng Wang.)*

The authors are with the Department of Electrical Engineering and Computer Science, University of Wisconsin–Milwaukee, Milwaukee, WI 53211 USA (e-mail: zhaoxil@uwm.edu; l.f.wang@ieee.org).

Digital Object Identifier 10.1109/TIFS.2021.3065504

by the attacker through the insider who has privileged access to the SCADA network. Further, the vulnerabilities of the protocols or devices in the SCADA system can be exploited by the attacker by implanting malware in the SCADA system via the insider. The insider can also provide attacker with the backdoor in the system (e.g., the backdoor intended for remote support from the vendor). As such, the insiders reduce the difficulty and increase the successful rates of the malicious attempts. Thus, it is particularly critical to analyze the insider threats in the cybersecurity analysis of SCADA systems.

Recently, a series of studies have been conducted to assess and enhance the cybersecurity of the SCADA systems in industries. A major focus in the research is the vulnerability and risk evaluation for the cybersecurity of the SCADA systems. In [8], a cyber-vulnerability assessment for the SCADA systems is proposed, and potential machine learning based counter measures are discussed. The cybersecurity risk of SCADA systems is modeled for IIoT in [9] and the risk metrics are identified. In [13], an attack graph model is developed and generated in an automated manner to identify vulnerabilities and analyze the cybersecurity of SCADA networks. The authors of [14] propose the cyberattack model against the SCADA systems in power systems and calculate the mean time-to-compromise (MTTC) of the cyberattacks to estimate the system reliability. Further, the cybersecurity of the wind farm SCADA systems are considered in [15]. The attack scenarios are proposed to estimate the frequencies of the cyberattacks and evaluate the overall system reliability. In [16], the cyberattack scenarios and Bayesian attack graph models of the SCADA networks are developed to evaluate the probability of successful attacks. As a defense approach, cyber intrusion tolerant models have also been proposed the enhance the cybersecurity of the SCADA systems. In [17], a survivable SCADA system against cyberattacks is designed by integrating the modern intrusion-tolerant protocols with a conventional SCADA architecture. Meanwhile, a number of researches focus on the attack detection of the SCADA systems [18]–[21]. A data-driven clustering method is proposed in [18] to detect the attacks on SCADA systems. In [19], the models of integrity attacks on control systems are developed, and model-based techniques are considered in the proposed models for the attack detection. Aiming to provide a comprehensive solution, the authors in [20] propose an intrusion detection system (IDS) for the multi-layer SCADA network architecture by analyzing multiple attributes of the system. In [21], a filtering system is proposed based on the critical state analysis to detect the attacks composed of SCADA commands.

The mentioned existing studies investigate the vulnerability assessment, cyberattack modeling and attack detection problems for SCADA systems. However, the insider threats are not in the scope of these studies. The impacts of the insider on the cybersecurity of SCADA systems are not analyzed or considered in any of these works. The research on the insider threats against the cybersecurity of SCADA systems is extremely limited in the existing literature. Only very few works in the existing literature about the cybersecurity of SCADA systems cover the insider threats in the research. In [22], a statistical anomaly detection method is proposed to identify potential insider attacks at the power transmission system by studying the SCADA alarms. Thresholds are set by learning the mean and standard deviation of the SCADA alarms to detect potential insider attacks, and the behavior falling outside the thresholds is identified as anomalous. Reference [23] investigates the use of Petri nets to model the insider attacks on SCADA systems. Potential malicious behaviors of the system operator as an insider who tries to resolve incoming alarms and create mis-configuration are modeled with the Colored Petri Nets (CPNs) in the study.

In order to enhance the cybersecurity of SCADA systems, the insider assistance to the attacker is considered in the analysis of the cyberattacks on SCADA systems in this paper. Although the SCADA systems are complicated with various types of protocols, firmware, and vulnerabilities for their corresponding physical systems and processes, it is still possible that there are insiders who can access important information and/or have critical privilege of the SCADA network of a certain system. Further, even if the insider has only information or access to a small part of the SCADA system, it can still be exploited by the attacker to launch the attack on the SCADA system for certain purpose. Thus, potential assistance from the insider to the attacker in the cyberattacks on SCADA systems should be investigated and is assumed in the paper.

In this study, the cyberattacks against SCADA systems are modeled with the absorbing semi-Markov process (SMP). A FlipIt game model is proposed in this paper to study the strategies of the system defender, attacker and insider. In the original FlipIt game model [24], the targeted system is compromised as soon as the attack actions are performed. However, in the proposed model in this paper, the time to compromise the SCADA system is modeled and integrated in the FlipIt game model, which is more realistic and closer to the actual case of cyberattacks on SCADA systems. Further, it allows the analysis on the impacts of the insider in the intrusion process of the cyberattacks on SCADA systems. Meanwhile, the original FlipIt game model is a two-player game model which only considers the strategies of the defender and attacker. In the proposed model in this paper, the strategies of the insider are also considered in the game. Thus, the interaction between the defender, attacker and insider can be analyzed in the proposed game model. In this paper, three different types of insiders are modeled and analyzed in the FlipIt game model. As such, the impacts of the insiders in the cyberattacks on SCADA systems can be studied comprehensively. Meanwhile, a Stackelberg model based method is developed to calculate the optimal defense strategy against the cyberattacks with the insider assistance. In the Stackelberg model, the system defender is assumed to be the leader and determine the defense strategy by optimizing the defender's own payoff considering the response of the attacker to the adopted defense strategy with the insider assistance. The attacker is assumed to be the follower in the Stackelberg model who determines the attack strategy by optimizing his/her own payoff given the defender's strategy. The work in [22] focuses on the attack detection of SCADA systems. In [23], two types of malicious behaviors of the insider are modeled. However,

the defense strategy and interaction between the defender, attacker and insider are not investigated in the research of [22] and [23]. In the studies of [25] and [26], the FlipIt game is also applied for the system security analysis considering insider threats. However, in the studies of [25] and [26], the proposed security analysis is not specified for SCADA systems, and the intrusion process of the attacker to the targeted system is not considered. More importantly, the insider is assumed to trade information with the attacker and reduce the cost of the attacker in the mentioned studies. However, the role and impact of the insider on the intrusion process of the attack on the system is not considered or modeled in detail, which is different from the proposed model in this paper.

In the proposed model, the SMP model is used to formulate the cyberattacks against the SCADA systems. Considering the various characteristics of SCADA systems with different configurations, protocols and applications, the SMP based method is applied in this paper for its flexibility in modeling the processes of the cyberattacks. Existing studies in literature show that the Markov process (MP) based method can model the malicious actions and cyberattacks on SCADA systems, e.g., [14], [27]–[29]. The detailed SMP model can be adjusted to cope with the characteristics of the targeted SCADA system with specific configurations, protocols and applications. Thus, the SMP based method is used in the proposed model to formulate the cyberattacks on SCADA systems considering the insider's assistance. In this paper, the proposed work focuses on providing a general method for the optimal strategy to conduct the defense actions against the cyberattacks on SCADA systems considering the existence of the insider's assistance to the attacker. The proposed work in the paper aims to provide a general model against the cyberattacks on various types of SCADA systems and facilitate the analysis on the impacts of the insider on the cybersecurity of the SCADA systems. It does not aim to propose the detailed techniques to defend against the malicious actions in the process of the cyberattacks. It is assumed in the proposed model of the paper that the defender of the SCADA system has effective defense methods against the attacks, and the cyberattacks can be blocked from the SCADA system if the defense actions are conducted by the defender. Meanwhile, in the proposed model, it is assumed that the effects of the defense actions can be noticed by the attacker. Thus, the defense strategy leakage to the attacker by the insider is not considered in the proposed model.

The contributions of this paper are summarized as follows:

- A FlipIt game model for the cyberattacks against the SCADA systems considering the insider assistance is developed. With the proposed FlipIt game model, the interaction between the system defender, attacker and insider can be formulated and analyzed. Accordingly, the impacts of the insider on the system cybersecurity can be analyzed. Moreover, three different types of insiders and their impacts are modeled and investigated with the proposed FlipIt game model. A Stackelberg model based method is developed to derive the optimal defense strategy of the system defender against the cyberattacks in consideration of the response of the attacker with the insider's assistance.
- An absorbing SMP model of the cyberattacks against the SCADA systems with insider's assistance is developed. With the proposed SMP model, the probability distribution of the time-to-compromise the system of the cyberattacks with the insider's assistance can be derived with Monte Carlo simulations (MCS) to facilitate further investigation on the impacts of the insider threats on the system cybersecurity.

TABLE I
MAIN NOTATIONS IN THE SMP MODEL

Notation	Description
$\mathcal{F}$	Failure state in the SMP model.
$\mathcal{G}$	Good state in the SMP model.
$\mathcal{S}$	Set of states in the SMP model.
$\boldsymbol{P}$	SMP Transition probability matrix without insider.
$\boldsymbol{P}'$	SMP Transition probability matrix with insider.
$\boldsymbol{Q}$	Renewal kernel of the SMP model.
p_{ij}	Transition probability from state i to j in the SMP model.
T_{ij}	Sojourn time in state i if the next stat is j of the SMP model.
F_{ij}	Cumulative distribution function (CDF) of T_{ij}.
ξ_n/ξ_{n+1}	State of the SMP model in the $n^{\text{th}}/(n+1)^{\text{th}}$ step.
ϑ_{n+1}	Arrival time of the $(n+1)^{\text{th}}$ step in the SMP model.

The rest of the paper is organized as follows. The absorbing SMP model of the cyberattacks against the SCADA systems with insider assistance is introduced in Section II. The FlipIt game model to formulate the strategies of the defender, attacker and insider in the cyberattacks is proposed in Section III. In Section IV, the case studies are introduced and the results are discussed. Finally, conclusions are presented in Section V.

II. SEMI-MARKOV MODELS OF CYBERATTACKS AGAINST SCADA SYSTEMS

In order to facilitate an in-depth analysis of the cyberattacks against the SCADA systems, it is essential to formulate the intrusion processes theoretically. In this section, the intrusion processes of cyberattacks on SCADA systems considering the insider assistance is developed with the SMP model. SMP is one of the well-established stochastic modeling techniques that has been widely used for analyzing the security intrusion behavior on a system [30]. The SMP model of the intrusion processes is explained below, and the main notations in the SMP model are listed in Table I.

The intrusion process against the SCADA system can be modeled as a semi-Markov process $\{X(t) : t \geqslant 0\}$ with a discrete state space $\mathcal{S}$. The SMP can be defined by the renewal kernel $\boldsymbol{Q}(t) = [Q_{ij}(t) : i, j \in \mathcal{S}], t \geqslant 0$ and the initial distribution $\boldsymbol{p} = [p_i(0) : i \in \mathcal{S}]$, where the renewal kernel $\boldsymbol{Q}(t)$ is defined as follows [31].

$$F_{ij}(t) = P\left(\vartheta_{n+1} \leqslant t \mid \xi_n = i, \xi_{n+1} = j\right), \quad i \in \mathcal{S}, \; j \in \mathcal{S}, t \geqslant 0 \tag{1}$$

$$Q_{ij}(t) = p_{ij} F_{ij}(t) \tag{2}$$

where $F_{ij}(t)$ is the cumulative distribution function (CDF) of the sojourn time T_{ij} in state i if the next state is j. The transition probability matrix $\boldsymbol{P} = [p_{ij} : i, j \in \mathcal{S}]$ shows the probability of transition to state j if the previous state is i.

The intrusion process against the SCADA system is modeled as an SMP in the state space $\mathcal{S}$, which includes the transient states and the failure state. The transient state space is denoted by $\mathcal{S}_{\mathcal{T}}$, and the failure state is denoted by $\mathcal{F}$. The process of an cyberattack starts from the good state $\mathcal{G}$, which represents the secure situation of the SCADA system. The second stage is the intrusion process into the SCADA system which contains a number of intermediate states, and each state represents one phase of the attack activity. Higher privilege of the SCADA system is obtained by the attacker when he/she proceed with the actions sequentially. The last stage is associated with the failure state $\mathcal{F}$, which indicates the target of the attacker in the SCADA system is compromised. In the SMP model of intrusion process, the good state $\mathcal{G}$ and intermediate states are regarded as transient states while the failure state $\mathcal{F}$ is classified as the absorbing state [32]. For instance, the intrusion process of the SQL injection attack against the SCADA system can be divided into four intermediate steps [14], [33], and the SMP model of the intrusion process without considering the insider's assistance to the attacker can be illustrated as Figure 1 (a).

When the insider exists in the attack, the attacker has an opportunity to skip certain intermediate states in the SMP model due to the advantages of the insiders. For example, in the SQL injection attack against the SCADA system, an insider can provide the attacker with critical information about the data structure of the SQL database. As such, the attacker can skip the processes of locating SQL vulnerabilities and reverse engineering the vulnerable application, which are the first two steps of the attack [33]. Thus, the SMP model of the attack with the insider's assist becomes the model shown in Figure 1 (b). Accordingly, the transition probability matrix of the SMP model with insider is changed from $\boldsymbol{P}$ to $\boldsymbol{P}'$, which are shown by (3) and (4) respectively.

$$\boldsymbol{P} = \begin{bmatrix} 1-p_{G1} & p_{G1} & 0 & 0 & 0 & 0 \\ 1-p_{12} & 0 & p_{12} & 0 & 0 & 0 \\ 1-p_{23} & 0 & 0 & p_{23} & 0 & 0 \\ 1-p_{34}-p_{3F} & 0 & 0 & 0 & p_{34} & p_{3F} \\ 1-p_{4F} & 0 & 0 & 0 & 0 & p_{4F} \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{3}$$

$$\boldsymbol{P}' = \begin{bmatrix} 1-p_{G1}-p_{G3} & p_{G1} & 0 & p_{G3} & 0 & 0 \\ 1-p_{12} & 0 & p_{12} & 0 & 0 & 0 \\ 1-p_{23} & 0 & 0 & p_{23} & 0 & 0 \\ 1-p_{34}-p_{3F} & 0 & 0 & 0 & p_{34} & p_{3F} \\ 1-p_{4F} & 0 & 0 & 0 & 0 & p_{4F} \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{4}$$

where p_{ij} $(i, j \in \mathcal{S}_{\mathcal{T}} \cup \mathcal{F})$ is the transition probability of the states in the SMP model. The elements in $\boldsymbol{P}$ and $\boldsymbol{P}'$ indicate the probability of the transition between the corresponding states in the SMP model without and with insider, respectively. For instance, the probability of the transition from the good state $\mathcal{G}$ to transient state 1 is p_{G1} when there is no insider as shown in (3). Accordingly, the probability of the system

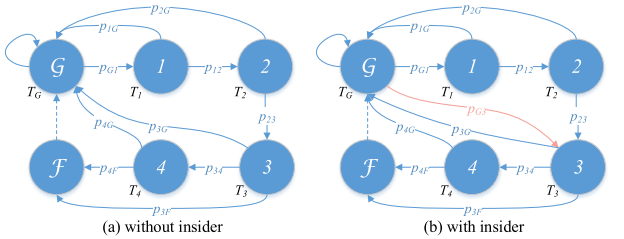


Fig. 1. SMP models of SQL injection attacks.

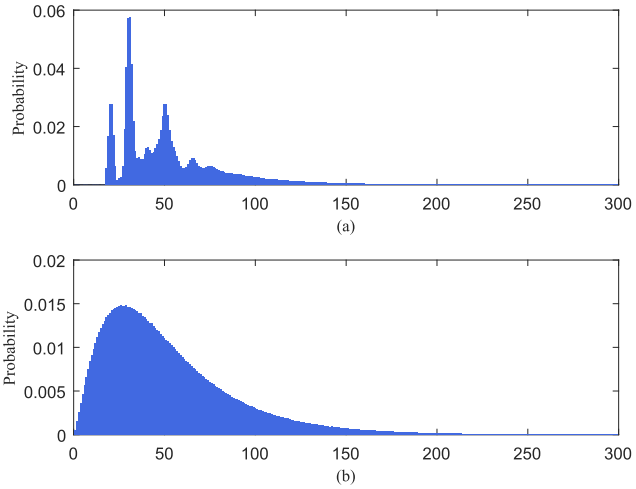


Fig. 2. Probability distribution of time to reach absorbing state in SMP, (a) when T_{ij} follow uniform distributions, (b) when T_{ij} follow exponential distributions.

remaining in the good state $\mathcal{G}$ is $1 - p_{G1}$. However, with the insider, the probability of the system staying in the good state $\mathcal{G}$ is reduced to $1 - p_{G1} - p_{G3}$ as shown in (4), while the probabilities of the transition from the good state $\mathcal{G}$ to transient states 1 and 3 are p_{G1} and p_{G3}, respectively. Thus, the presence of the insider reduces the probability of the system to stay in the good state $\mathcal{G}$. In this case, there is a bigger chance for the system to reach the transient state 3 and consequently the failure state $\mathcal{F}$.

The impacts of cyberattacks are highly dependent on the spent time of a successful attack on the system. It is critical to obtain the probability distribution of the time-to-compromise the system of the attacks in the cybersecurity studies. The time-to-compromise the system of the attack is represented by the time of the SMP to reach the absorbing state $\mathcal{F}$, which depends on the sojourn time in each transient state and the transition probability of the SMP. In general, it does not follow a specific formulated probability distribution. In order to obtain the probability distribution of the time-to-compromise the system of the attack and facilitate further investigation, the MCS is employed in this study to estimate the distribution. Figure 2 shows the probability distribution of the time to reach the absorbing state with different distributions of the sojourn time in the transient states of the SMP model.

In the SMP model of the cyberattacks against the SCADA system, the initial state of the system is the good state $\mathcal{G}$. Thus, the initial probability of the good state is 1 and the

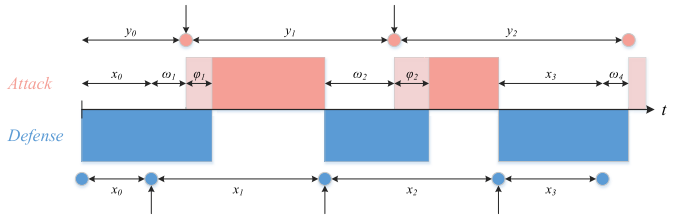


Fig. 3. FlipIt game model of cyberattacks on SCADA systems.

initial probabilities of all the other transient states are 0.

$$p_i(0) = \begin{cases} 1, & \text{if } i = \mathcal{G} \\ 0, & \text{otherwise} \end{cases} \tag{5}$$

With the defined SMP renewal kernel $\boldsymbol{Q}(t)$ and initial distribution $\boldsymbol{p} = [p_i(0) : i \in \mathcal{S}]$, the probability space (Ω, P) of the time-to-compromise the system of the cyberattacks can be modeled and estimated directly using MCS [31].

III. FlipIt Game Model of Cyberattacks Against SCADA Systems

A. FlipIt Game for Cyberattacks Against SCADA Systems

With sufficient resources, the attacker may launch continuous attacks to intrude into the SCADA system instead of a single attempt. Such persistent attacks are classified as Advance Persistent Threat (APT) which is emerging as a major cybersecurity concern of the national infrastructure and information systems [34]. FlipIt game is a novel and effective tool to model and analyze the APT [24]–[26]. In this section, a FlipIt game model is developed to analyze the cyberattacks against the SCADA systems. The main notations of the FlipIt game model are listed in Table II, and the FlipIt game model is illustrated in Figure 3. In the FlipIt game, the system status is either protected or compromised. When the defender performs the defense actions, the system will remain protected or become protected if it is compromised. When the attacker performs the attack actions, the system is assumed to be compromised after the time-to-compromise φ_i which is a stochastic variable. The probability distribution of φ_i can be determined by the SMP model of the cyberattack as presented in Section II. Both the defender and attacker need to pay a cost to perform every defense or attack action. Further, the attacker is assumed to be aware of the action of the defender with a latency of ω_i after the defense action is performed. The awareness time ω_i is assumed to be stochastic and equal to a base awareness latency ω_0 plus an uncertain component $\Delta\omega$. In this paper, the uncertain component $\Delta\omega$ is assumed to be a uniform random variable in the interval $[0, \omega^+]$, $\omega^+ \geqslant 0$. Let α_i and δ_i denote the attack and defense actions in the i^{th} round respectively. When $\alpha_i = 1$ it means the attacker performs the attack action after the awareness of the i^{th} renew action of the defender δ_i, otherwise $\alpha_i = 0$. As shown in Figure 3, the system status in the i^{th} round is determined by the time gap of the defense actions δ_i, the attack actions α_i, the awareness latency ω_i and the time-to-compromise of the attack φ_i.

Due to the awareness of the defense actions by the attackers, the periodic action strategy by the defender is no longer optimal and the exponential strategy in which the intervals between two consecutive defense actions are exponentially distributed is a more desirable choice for the defender [24], [26]. It is because with the awareness of the defense actions, the attacker can estimate the time of the following defense actions if the defender plays actions periodically. Thus, the defender is assumed to play an exponential strategy in this paper. The defense action intervals x_i is assumed to follow an exponential distribution with a rate parameter $\frac{1}{\lambda}$. We note the attack rate of the attacker by r. When $r = 1$, it means the attacker will always perform the attacks in every single round. In contrast, it means the attacker drops out of the attack when $r = 0$. Let $N_{\mathcal{D}}$ and $N_{\mathcal{A}}$ denote the numbers of the defense and attack actions, respectively. The attack rate r is defined by (6) as follows.

$$r = \frac{N_{\mathcal{A}}}{N_{\mathcal{D}}} \tag{6}$$

where $N_{\mathcal{D}} = \sum_i \delta_i$, $N_{\mathcal{A}} = \sum_i \alpha_i$.

TABLE II
Main Notations in the FlipIt Game Model

Notation	Description
$C_{\mathcal{A}}$	Cost coefficient of the attack action.
$C_{\mathcal{D}}$	Cost coefficient of the defense action.
$C_{\mathcal{I}}$	Cost coefficient of the attacker to employ the insider.
η	System coefficient of the insider.
φ_i	Time-to-compromise the system of the attack at the i^{th} round of defense-attack actions over a certain period.
ω_i	Awareness time of the attacker to the defense action at the i^{th} round of defense-attack actions over a certain period.
ω_0	Base component of the awareness time of the attacker to the defense action.
$\Delta\omega$	Uncertain component of the awareness time of the attacker to the defense action.
ω^+	Upper limit of the uncertain component of the awareness time of the attacker to the defense action.
π_j	Probability of the time-to-compromise the system of the j^{th} scenario.
Ω	Sample space of the time-to-compromise the SCADA system.
$N_{\mathcal{A}}$	Number of attack actions over a certain period.
$N_{\mathcal{D}}$	Number of defense actions over a certain period.
r	Attack action rate.
x_i/y_i	Defense/attack action interval at the i^{th} round of defense-attack actions over a certain period.
$U_{\mathcal{A}}$	Expected payoff of the attacker.
$U_{\mathcal{D}}$	Expected payoff of the defender.
$U_{\mathcal{I}}$	Expected payoff of the insider.
λ	Defense action rate coefficient.
α_i	Attack action indicator at the i^{th} round of defense-attack actions over a certain period.
δ_i	Defense action indicator at the i^{th} round of defense-attack actions over a certain period.
ξ	Decision indicator of the attacker's action of employing the insider.
ω_r	Upper bound of the attack action interval with attack action rate r.
ζ	Insider action decision indicator.

B. FlipIt Game Model Without Insider

When there are no insiders in the attacks, the FlipIt game model is formulated as follows.

1) Defender's Payoff: In the FlipIt game model of the attack, the loss of the system defender is evaluated by the time of the system compromised status. The aim of the defender is to minimize the expectation of the average system loss and the cost of defense actions over the time. Therefore the defender's payoff function can be defined as (7).

$$U_{\mathcal{D}} = E\left\{\frac{\sum_{i=0}^{N_{\mathcal{D}}}\left(x_i - [x_i - \omega_i - \varphi_i]^+ \alpha_i\right)}{\sum_{i=0}^{N_{\mathcal{D}}} x_i} - \frac{\sum_{i=0}^{N_{\mathcal{D}}} C_{\mathcal{D}}\delta_i}{\sum_{i=0}^{N_{\mathcal{D}}} x_i}\right\} \tag{7}$$

where $C_{\mathcal{D}}$ is the cost coefficient of the defense action. The first term in (7) is the average time when the system is not compromised. When an attack action is performed, $\alpha_i = 1$ and the time that the system is compromised is determined by the positive part of the defense interval x_i minus the awareness latency ω_i and the time-to-compromise the system of the attack φ_i. The second term in (7) is the average cost of the defense actions. The awareness latency ω_i is a uniform random variable in the interval $[\omega_0, \omega_0 + \omega^+]$. Assume the attack rate of attacker is r. In order to maximize the expectation of the time that the system is compromised, the attacker will choose to attack in the case when the awareness latency is short. Hence, the attack actions will be performed when ω_i falls in the interval $[\omega_0, \omega_r]$, where $\omega_r = \omega_0 + r\omega^+$. Meanwhile, the time-to-compromise the system φ_i is a stochastic variable defined in the probability space (Ω, P). Thus, the defender's payoff can be calculated as (8) below.

$$\begin{aligned} U_{\mathcal{D}} =& \\ & E\left\{\frac{\sum_{i=0}^{N_{\mathcal{D}}} x_i - \sum_{i=0}^{N_{\mathcal{D}}}[x_i - \omega_i - \varphi_i]^+ \alpha_i}{\sum_{i=0}^{N_{\mathcal{D}}} x_i} - \frac{\sum_{i=0}^{N_{\mathcal{D}}} C_{\mathcal{D}}\delta_i}{\sum_{i=0}^{N_{\mathcal{D}}} x_i}\right\} \\ &= 1 - \frac{\sum_{\varphi_j\in\Omega}\pi_j \int_{\omega_0}^{\omega_r}\int_{\omega+\varphi_j}^{+\infty}\frac{1}{\omega^+}\left(x-\omega-\varphi_j\right)\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x\mathrm{d}\omega}{\int_0^{+\infty}\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x} \\ &\quad - \frac{C_{\mathcal{D}}}{\int_0^{+\infty}\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x} \\ &= 1 - \sum_{\varphi_j\in\Omega}\pi_j\frac{\lambda}{\omega^+}\left(e^{-\frac{\omega_0+\varphi_j}{\lambda}} - e^{-\frac{\omega_r+\varphi_j}{\lambda}}\right) - \frac{C_{\mathcal{D}}}{\lambda} \end{aligned} \tag{8}$$

where φ_j and π_j are the value of the time-to-compromise the system and the corresponding probability, $(\varphi_j, \pi_j) \in (\Omega, P)$.

2) Attacker's Payoff: By performing the attack actions, the attacker seeks maximum compromised time of the system taking into consideration the cost of the attacks. Hence, the attacker's payoff is defined as the expected value of the average compromised time of the system minus the average attack action cost over time. It is formulated as (9).

$$U_{\mathcal{A}} = E\left\{\frac{\sum_{i=0}^{N_{\mathcal{D}}}[x_i - \omega_i - \varphi_i]^+ \alpha_i}{\sum_{i=0}^{N_{\mathcal{D}}} x_i} - \frac{\sum_{i=0}^{N_{\mathcal{D}}} C_{\mathcal{A}}\alpha_i}{\sum_{i=0}^{N_{\mathcal{D}}} x_i}\right\} \tag{9}$$

where $C_{\mathcal{D}}$ is the cost coefficient of the attack action. With the probability distributions of the stochastic variables ω_i and φ_i, the attacker's payoff can be calculated as follows.

$$\begin{aligned} U_{\mathcal{A}} &= E\left\{\frac{\sum_{i=0}^{N_{\mathcal{D}}}[x_i - \omega_i - \varphi_i]^+ \alpha_i}{\sum_{i=0}^{N_{\mathcal{D}}} x_i} - \frac{\sum_{i=0}^{N_{\mathcal{D}}} C_{\mathcal{A}}\alpha_i}{\sum_{i=0}^{N_{\mathcal{D}}} x_i}\right\} \\ &= \frac{\sum_{\varphi_j\in\Omega}\pi_j \int_{\omega_0}^{\omega_r}\int_{\omega+\varphi_j}^{+\infty}\frac{1}{\omega^+}\left(x-\omega-\varphi_j\right)\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x\mathrm{d}\omega}{\int_0^{+\infty}\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x} \\ &\quad - \frac{rC_{\mathcal{A}}}{\int_0^{+\infty}\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x} \\ &= \sum_{\varphi_j\in\Omega}\pi_j\frac{\lambda}{\omega^+}\left(e^{-\frac{\omega_0+\varphi_j}{\lambda}} - e^{-\frac{\omega_r+\varphi_j}{\lambda}}\right) - \frac{rC_{\mathcal{A}}}{\lambda} \end{aligned} \tag{10}$$

C. FlipIt Game Model With Insider

When there is insider in the system, the intrusion process of the attack is changed as presented in Section II. Let $(\widetilde{\Omega}, \widetilde{P})$ denote the new probability space of the time-to-compromise the system of the attacks when there is insider in the system. The expected time-to-compromise the system will be shorter due to the insider. As a result, the models of the attacker and defender in the FlipIt game change accordingly. There are a few different types of insiders in the real world. Their impacts on the attacks are analyzed respectively in detail as follows.

1) Volunteer Insider: When the insider is a partner or an ally of the attacker and volunteer to facilitate the cyberattack, no additional cost is placed on the attacker. In this case, the FlipIt game model will be similar to the case but the probability space of the time-to-compromise the system of the attack becomes $(\widetilde{\Omega}, \widetilde{P})$. Thus, the payoff of the defender can be represented as follows.

$$\begin{aligned} \widetilde{U}_{\mathcal{D}} =& \\ & E\left\{\frac{\sum_{i=0}^{N_{\mathcal{D}}} x_i - \sum_{i=0}^{N_{\mathcal{D}}}[x_i - \omega_i - \varphi_i]^+ \alpha_i}{\sum_{i=0}^{N_{\mathcal{D}}} x_i} - \frac{\sum_{i=0}^{N_{\mathcal{D}}} C_{\mathcal{D}}\delta_i}{\sum_{i=0}^{N_{\mathcal{D}}} x_i}\right\} \\ &= 1 - \frac{\sum_{\varphi_k\in\widetilde{\Omega}}\pi_k \int_{\omega_0}^{\omega_r}\int_{\omega+\varphi_k}^{+\infty}\frac{1}{\omega^+}\left(x-\omega-\varphi_k\right)\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x\mathrm{d}\omega}{\int_0^{+\infty}\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x} \\ &\quad - \frac{C_{\mathcal{D}}}{\int_0^{+\infty}\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x} \\ &= 1 - \sum_{\varphi_k\in\widetilde{\Omega}}\pi_k\frac{\lambda}{\omega^+}\left(e^{-\frac{\omega_0+\varphi_k}{\lambda}} - e^{-\frac{\omega_r+\varphi_k}{\lambda}}\right) - \frac{C_{\mathcal{D}}}{\lambda} \end{aligned} \tag{11}$$

where $(\varphi_k, \pi_k) \in (\widetilde{\Omega}, \widetilde{P})$.

As no additional cost is placed on the attacker, the payoff of the attacker can be represented as follows.

$$\begin{aligned} \widetilde{U}_{\mathcal{A}} &= E\left\{\frac{\sum_{i=0}^{N_{\mathcal{D}}}[x_i - \omega_i - \varphi_i]^+ \alpha_i}{\sum_{i=0}^{N_{\mathcal{D}}} x_i} - \frac{\sum_{i=0}^{N_{\mathcal{D}}} C_{\mathcal{A}}\alpha_i}{\sum_{i=0}^{N_{\mathcal{D}}} x_i}\right\} \\ &= \frac{\sum_{\varphi_k\in\widetilde{\Omega}}\pi_k \int_{\omega_0}^{\omega_r}\int_{\omega+\varphi_k}^{+\infty}\frac{1}{\omega^+}\left(x-\omega-\varphi_k\right)\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x\mathrm{d}\omega}{\int_0^{+\infty}\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x} \\ &\quad - \frac{rC_{\mathcal{A}}}{\int_0^{+\infty}\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x} \\ &= \sum_{\varphi_k\in\widetilde{\Omega}}\pi_k\frac{\lambda}{\omega^+}\left(e^{-\frac{\omega_0+\varphi_k}{\lambda}} - e^{-\frac{\omega_r+\varphi_k}{\lambda}}\right) - \frac{rC_{\mathcal{A}}}{\lambda} \end{aligned} \tag{12}$$

2) Financially Motivated Insider Without System Responsibility: When the insider is financially motivated, the attacker needs to pay the insider for his/her assistance in the attack. A cost will be placed on the attacker if the insider is employed. Thus, the payoff of the attacker can be defined as follows.

$$\begin{aligned}\widetilde{U}'_{\mathcal{A}} =& \\ & E\left\{\frac{\sum_{i=0}^{N_{\mathcal{D}}}\left[x_i-\omega_i-\varphi_i\right]^+\alpha_i}{\sum_{i=0}^{N_{\mathcal{D}}}x_i}-\frac{\sum_{i=0}^{N_{\mathcal{D}}}C_{\mathcal{A}}\alpha_i}{\sum_{i=0}^{N_{\mathcal{D}}}x_i}-\xi\frac{\sum_{i=0}^{N_{\mathcal{D}}}C_{\mathcal{I}}\delta_i}{\sum_{i=0}^{N_{\mathcal{D}}}x_i}\right\} \\ &= (1-\xi)\frac{\sum_{\varphi_j\in\Omega}\pi_j\int_{\omega_0}^{\omega_r}\int_{\omega+\varphi_j}^{+\infty}\frac{1}{\omega^+}\left(x-\omega-\varphi_j\right)\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x\mathrm{d}\omega}{\int_0^{+\infty}\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x} \\ &\quad +\xi\frac{\sum_{\varphi_k\in\widetilde{\Omega}}\pi_k\int_{\omega_0}^{\omega_r}\int_{\omega+\varphi_k}^{+\infty}\frac{1}{\omega^+}\left(x-\omega-\varphi_k\right)\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x\mathrm{d}\omega}{\int_0^{+\infty}\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x} \\ &\quad -\frac{rC_{\mathcal{A}}}{\int_0^{+\infty}\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x}-\xi\frac{C_{\mathcal{I}}}{\int_0^{+\infty}\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x} \\ &= (1-\xi)\sum_{\varphi_j\in\Omega}\pi_j\frac{\lambda}{\omega^+}\left(e^{-\frac{\omega_0+\varphi_j}{\lambda}}-e^{-\frac{\omega_r+\varphi_j}{\lambda}}\right) \\ &\quad +\xi\sum_{\varphi_k\in\widetilde{\Omega}}\pi_k\frac{\lambda}{\omega^+}\left(e^{-\frac{\omega_0+\varphi_k}{\lambda}}-e^{-\frac{\omega_r+\varphi_k}{\lambda}}\right)-\frac{rC_{\mathcal{A}}}{\lambda}-\frac{\xi C_{\mathcal{I}}}{\lambda}\end{aligned} \tag{13}$$

where $C_{\mathcal{I}}$ is the cost coefficient of the attacker to employ the insider, and ξ denotes the attacker's action of employing the insider. $\xi=1$ means the attacker chooses to accept the offer from the insider and employ the insider's assist in the attack. Otherwise $\xi=0$.

3) Financially Motivated Insider With System Responsibility: When the insider is free from the responsibility of the system loss as modeled in the previous case, the insider will not hesitate to offer assist to the attacker. Nevertheless, as a part of the system, the insider may be partly responsible for the system security and suffer a loss proportional to the system loss if the SCADA system is compromised. In this case, the insider will evaluate the system loss in the attack and determine whether to offer assist in the attack for the income from the attacker accordingly. Thus, the payoff of the insider can be formulated as (14) below.

$$U_{\mathcal{I}}=E\left\{-\eta\frac{\sum_{i=0}^{N_{\mathcal{D}}}\left[x_i-\omega_i-\varphi_i\right]^+\alpha_i}{\sum_{i=0}^{N_{\mathcal{D}}}x_i}+\zeta\frac{\sum_{i=0}^{N_{\mathcal{D}}}C_{\mathcal{I}}\delta_i}{\sum_{i=0}^{N_{\mathcal{D}}}x_i}\right\} \tag{14}$$

where η is the system coefficient of the insider, ζ denotes the insider's action. $\zeta=1$ means the insider is willing to offer assist to the attacker, otherwise $\zeta=0$. When the insider drops out of the game and does not offer assist to the attacker ($\zeta=0$), the intrusion process of the attack is like the case without insider as described in the previous subsection III-B. However, when the insider offers assist to the attacker ($\zeta=1$), the probability of the time-to-compromised the system of the attack will be changed and the effect of the attack is the same as the case with insider as described above in this subsection. Thus, the payoff of the insider in the FlipIt game can be calculated as (15) below.

$$\begin{aligned}U_{\mathcal{I}} &= E\left\{-\eta\frac{\sum_{i=0}^{N_{\mathcal{D}}}\left[x_i-\omega_i-\varphi_i\right]^+\alpha_i}{\sum_{i=0}^{N_{\mathcal{D}}}x_i}+\zeta\frac{\sum_{i=0}^{N_{\mathcal{D}}}C_{\mathcal{I}}\delta_i}{\sum_{i=0}^{N_{\mathcal{D}}}x_i}\right\} \\ &= (\zeta-1)\,\eta\frac{\sum_{\varphi_j\in\Omega}\pi_j\int_{\omega_0}^{\omega_r}\int_{\omega+\varphi_j}^{+\infty}\frac{1}{\omega^+}\left(x-\omega-\varphi_j\right)\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x\mathrm{d}\omega}{\int_0^{+\infty}\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x} \\ &\quad -\zeta\eta\frac{\sum_{\varphi_k\in\widetilde{\Omega}}\pi_k\int_{\omega_0}^{\omega_r}\int_{\omega+\varphi_k}^{+\infty}\frac{1}{\omega^+}\left(x-\omega-\varphi_k\right)\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x\mathrm{d}\omega}{\int_0^{+\infty}\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x} \\ &\quad +\zeta\frac{C_{\mathcal{I}}}{\int_0^{+\infty}\frac{1}{\lambda}e^{-\frac{x}{\lambda}}\mathrm{d}x} \\ &= (\zeta-1)\,\eta\sum_{\varphi_j\in\Omega}\pi_j\frac{\lambda}{\omega^+}\left(e^{-\frac{\omega_0+\varphi_j}{\lambda}}-e^{-\frac{\omega_r+\varphi_j}{\lambda}}\right) \\ &\quad -\zeta\eta\sum_{\varphi_k\in\widetilde{\Omega}}\pi_k\frac{\lambda}{\omega^+}\left(e^{-\frac{\omega_0+\varphi_k}{\lambda}}-e^{-\frac{\omega_r+\varphi_k}{\lambda}}\right)+\frac{\zeta C_{\mathcal{I}}}{\lambda}\end{aligned} \tag{15}$$

D. Strategies of the Players in the FlipIt Game Model

In order to derive the optimal defense strategy of the system defender, a Stackelberg model is developed and applied to model the decisions of the players in the FlipIt game. In the Stackelberg model, the defender is regarded as the leader and the attacker is regarded as the follower. The defender considers the optimal attack rate r of the attacker which maximizes the attacker's payoff $U_{\mathcal{A}}$ when he/she notices the defense coefficient λ of the defender. Then, the defender selects the defense coefficient λ to maximize his/her own payoff $U_{\mathcal{D}}$ considering the predicted response of the attacker. As such, the defender's strategy is optimized in consideration of the attacker's response. In the FlipIt game model without insider, the predicted response of the attacker is determined as (16).

$$r^*(\lambda)=\arg\max_r U_{\mathcal{A}}(\lambda,r) \tag{16}$$

Accordingly, the optimal defense strategy of the defender can be expressed as (17).

$$\lambda^*=\arg\max_{\lambda}U_{\mathcal{D}}\left(\lambda,r^*(\lambda)\right) \tag{17}$$

Then, the optimal attack rate r^* of the attacker is determined as (18) when the defense coefficient λ^* is certain.

$$r^*=\arg\max_r U_{\mathcal{A}}\left(\lambda^*,r\right) \tag{18}$$

By considering the first order conditions of (16) and (17), the defender and attacker's strategy (λ^*,r^*) can be determined as follows.

$$\frac{\partial U_{\mathcal{A}}}{\partial r}(r^*)=\sum_{\varphi_j\in\Omega}\pi_j e^{-\frac{\omega_0+r^*\omega^++\varphi_j}{\lambda}}-\frac{C_{\mathcal{A}}}{\lambda}=0 \tag{19}$$

Then, it can be derived from (19) that

$$r^*(\lambda)=\frac{\lambda}{\omega^+}\ln\left(\frac{\lambda\sum_{\varphi_j\in\Omega}\pi_j e^{-\frac{\omega_0+\varphi_j}{\lambda}}}{C_{\mathcal{A}}}\right) \tag{20}$$

By substituting (20) into (17), we have

$$\frac{\partial U_{\mathcal{D}}}{\partial \lambda}\left(\lambda^*\right) = -\sum_{\varphi_j \in \Omega} \pi_j \frac{1}{\omega^+}\left(e^{-\frac{\omega_0+\varphi_j}{\lambda^*}} \cdot \frac{\lambda^* + \omega_0 + \varphi_j}{\lambda^*}\right) + \frac{C_{\mathcal{D}}}{\lambda^{*2}} = 0 \tag{21}$$

Then λ^* is determined by the nonlinear equation (21), and r^* is determined accordingly as follows.

$$r^* = \frac{\lambda^*}{\omega^+} \ln\left(\frac{\lambda^* \sum_{\varphi_j \in \Omega} \pi_j e^{-\frac{\omega_0+\varphi_j}{\lambda^*}}}{C_{\mathcal{A}}}\right) \tag{22}$$

Similarly, when the FlipIt game is modeled with volunteer insider, the defender selects the defense action coefficient λ to maximize the payoff $\widetilde{U}_{\mathcal{D}}$ in consideration of the response of the attacker. Thus, the strategies of the defender and attacker are determined as follows.

$$\widetilde{r}^*(\lambda) = \arg\max_r \widetilde{U}_{\mathcal{A}}(\lambda, r) \tag{23}$$

$$\widetilde{\lambda}^* = \arg\max_{\lambda} \widetilde{U}_{\mathcal{D}}\left(\lambda, \widetilde{r}^*(\lambda)\right) \tag{24}$$

$$\widetilde{r}^* = \arg\max_r \widetilde{U}_{\mathcal{A}}\left(\widetilde{\lambda}^*, r\right) \tag{25}$$

On the one hand, in the defense strategy, the defender needs to determine the optimal defense action coefficient $\widetilde{\lambda}^*$ considering the attack action coefficient r determined by the attacker. On the other hand, in the attacker's strategy, the attacker needs to determine the optimal attack action coefficient $\widetilde{r}^*$ against the defense strategy. Given any defense action coefficient λ, the optimal attack action coefficient is determined by maximizing the attacker's payoff $\widetilde{U}_{\mathcal{A}}$ as indicated in (23). Thus, the optimal attack action coefficient $\widetilde{r}^*$ for the attacker can be expressed as a function of λ. Accordingly, given the expected selection of the attack action coefficient $\widetilde{r}^*(\lambda)$ by the attacker, the optimal defense action coefficient $\widetilde{\lambda}^*$ can be determined by maximizing the defender's payoff $\widetilde{U}_{\mathcal{D}}$ as indicated in (24). Then, with the optimal defense action coefficient $\widetilde{\lambda}^*$ selected by the defender, the optimal attack action coefficient $\widetilde{r}^*$ for the attacker can be determined by maximizing the payoff of the attacker $\widetilde{U}_{\mathcal{A}}$ as indicated in (25). By taking the first order conditions of (23) and (24), it can be easily derived that $\widetilde{\lambda}^*$ is determined by the nonlinear equation (26) and then $\widetilde{r}^*$ can be determined accordingly as (27).

$$\frac{\partial \widetilde{U}_{\mathcal{D}}}{\partial \lambda}\left(\widetilde{\lambda}^*\right) = -\sum_{\varphi_k \in \widetilde{\Omega}} \pi_k \frac{1}{\omega^+}\left(e^{-\frac{\omega_0+\varphi_k}{\widetilde{\lambda}^*}} \cdot \frac{\widetilde{\lambda}^* + \omega_0 + \varphi_k}{\widetilde{\lambda}^*}\right) + \frac{C_{\mathcal{D}}}{\widetilde{\lambda}^{*2}} = 0 \tag{26}$$

$$\widetilde{r}^* = \frac{\widetilde{\lambda}^*}{\omega^+} \ln\left(\frac{\widetilde{\lambda}^* \sum_{\varphi_k \in \widetilde{\Omega}} \pi_k e^{-\frac{\omega_0+\varphi_k}{\widetilde{\lambda}^*}}}{C_{\mathcal{A}}}\right) \tag{27}$$

When the FlipIt game is modeled with the financially motivated insider without responsibility of the system security, a payment from the attacker to the insider is needed. Thus, the attacker will evaluate whether it is beneficial to employ the insider. The attacker's optimal strategy can be determined as follows.

$$\xi^* = \begin{cases} 1, & \text{if } \widetilde{U}'_{\mathcal{A}}\left(\widetilde{\lambda}^*, \widetilde{r}^*\right) > U_{\mathcal{A}}\left(\lambda^*, r^*\right) \\ 0, & \text{otherwise} \end{cases} \tag{28}$$

When the FlipIt game is modeled considering the financially motivated insider with responsibility of the system security, a cost will be placed on the insider for the system loss. Then, the insider will evaluate whether it is beneficial to offer the assist to the attacker. The insider's optimal strategy can be determined as follows.

$$\zeta^* = \begin{cases} 1, & \text{if } U_{\mathcal{I}}\left(\widetilde{\lambda}^*, \widetilde{r}^*, \zeta = 1\right) > U_{\mathcal{I}}\left(\lambda^*, r^*, \zeta = 0\right) \\ 0, & \text{otherwise} \end{cases} \tag{29}$$

In practice, the defense actions of the system operator against the cyberattacks on the SCADA system may include updating the security policy of the SCADA network, updating the access privilege of the personnel and devices in the SCADA network, mandatory reset of the passwords and encryption keys, cybersecurity scanning and re-installing the software in the system. The proposed FlipIt game model can determine the optimal frequency for the system operator to schedule and perform these defense actions against the cyberattacks on the SCADA system. The conceptual costs of performing the defense actions in the proposed model represent the composite costs for the time, labor and resources needed by the system operator to perform the defense actions in practice. In the proposed model, it is assumed that the defender and attacker can estimate and evaluate the costs after a period of time of operation through the response of the defender to the attack strategies. In practice, it takes the attacker time and efforts to perform the attacks and compromise the targeted devices in the SCADA system. Thus, the system operator may increase the frequency of the defense actions to reduce the successful rate of the attacks. However, considering the costs of the defense actions on the system operator, he/she cannot increase the frequency of the defense actions without limit. The proposed FlipIt model in the paper can help the system operator optimally schedule the frequency and interval of the defense actions against the cyberattacks on the system with consideration of the insider's assistance to the attacker.

In this study, it is assumed that the attacker has the probability to employ the insider to assist the attack. With the knowledge and/or privilege of the insider, the attacker can skip certain steps in the intrusion process to the SCADA system, e.g., the insider can provide the attacker with the portal or assess to the SCADA network. Considering the defense actions of the system operator, the action of the insider not only reduces the expected time to compromise the system of the attack, but also increases the successful rate of the attack on the SCADA system. The case when the insider has the highest privilege and full control of the SCADA system to help the attacker will lead the proposed model to the extreme case that the defender's payoff will drop significantly. In this case, the available defense actions against the cyberattacks may not

TABLE III
KEY PARAMETERS IN CASE STUDIES

Parameter	Value
Cost Coefficient of Attacker ($C_{\mathcal{A}}$)	20 (p.u.)
Cost Coefficient of Defender ($C_{\mathcal{D}}$)	60 (p.u.)
Beneficial Coefficient of Insider ($C_{\mathcal{I}}$)	0.1/0.3/0.5 (p.u.)
System Coefficient of Insider (η)	0.1 (p.u.)
Minimal Awareness Time (ω_0)	100 (hour)
Awareness Time Uncertainty (ω^+)	100 (hour)

work as well due to the ability of the insider. In this case, new defense mechanisms need to be introduced on top of the proposed model, which aims to schedule the optimal plan of the defender with the available defense methods of the system that are assumed to be able to block the cyberattacks in this study.

The system defender who performs the defense actions of the SCADA system against the cyberattacks is assumed to be the system operator. In the proposed three-player game model, he/she is an independent player from the insider. The case when the defense policy maker of the system himself/herself is the insider is not covered in the proposed model in this paper. In practice, this case can be prevented by employing a third party to determine or inspect the defense action strategy making of the SCADA system. Then, the group of the third party and the system operator can be viewed as the system defender in the proposed game model.

IV. CASE STUDIES

In order to demonstrate the proposed FlipIt game models of the cyberattacks against SCADA systems in consideration of the insider, case studies were conducted. The details of the case studies are presented in this section.

A. Parameters in the Case Studies

The key parameters of the FlipIt game model of the cyberattacks in the case studies are listed in Table III. Due to the lack of real-world cybersecurity data of the SCADA systems, the values of the parameters in Table III are set hypothetically to showcase the impacts of the insider and validity of the proposed models. The simulations in the case studies were performed using MATLAB on a laptop with Intel Core i5 CPU (1.60-3.90GHz) and 12GB RAM.

In the case studies, the SQL injection attack against the SCADA system was considered and simulated with the SMP model as described in Section II. MCS were conducted to obtain the distributions of the time-to-compromise the system of the attacks. The distributions of the time-to-compromise the system of the attacks with and without insiders are shown in Figure 4. It is shown clearly that the time-to-compromise the system of the attacks is obviously shorter with insiders. The mean time-to-compromise (MTTC) of the attacks without insiders is about 84.2 hours while the MTTC of the attacks with insiders is about 52.3 hours.

B. Case Study Results

Four different scenarios were analyzed in the case studies according to the types of insider in the attacks as follows:

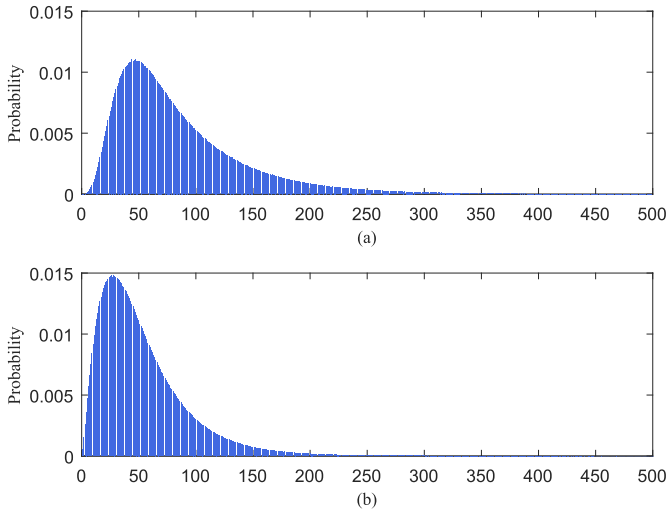


Fig. 4. Probability distribution of time-to-compromise of cyberattacks, (a) without insider assistance, (b) with insider assistance.

- Scenario 1 (S1): without insider. The cost coefficient of the attacker $C_{\mathcal{A}}$, the cost coefficient of the defender $C_{\mathcal{D}}$, the awareness time parameters ω_0 and $\Delta\omega$ are set as shown in Table III. The strategies of the defender and attacker are determined by (21) and (22) as derived in Section III, respectively. The payoffs of the defender and attacker are then calculated by (8) and (10) accordingly.
- Scenario 2 (S2): with volunteer insider. The cost coefficient of the attacker $C_{\mathcal{A}}$, the cost coefficient of the defender $C_{\mathcal{D}}$, the awareness time parameters ω_0 and $\Delta\omega$ are set as shown in Table III. The strategies of the defender and attacker are determined by (26) and (27) as derived in Section III, respectively. The payoffs of the defender and attacker are then calculated by (11) and (12) accordingly.
- Scenario 3 (S3): with financially motivated insider without system responsibility. The cost coefficient of the attacker $C_{\mathcal{A}}$, the cost coefficient of the defender $C_{\mathcal{D}}$, the beneficial coefficient of the insider $C_{\mathcal{I}}$, the awareness time parameters ω_0 and $\Delta\omega$ are set as shown in Table III. The decision of the attacker in employing the insider is determined by (28). If the insider involves, the strategies of the defender and attacker are determined by (26) and (27). The payoffs of the defender and attacker are then calculated by (11) and (13) accordingly. Otherwise, the strategies of the defender and attacker are determined by (21) and (22), respectively. The payoffs of the defender and attacker are then calculated by (8) and (10) accordingly.
- Scenario 4 (S4): with financially motivated insider with system responsibility. The cost coefficient of the attacker $C_{\mathcal{A}}$, the cost coefficient of the defender $C_{\mathcal{D}}$, the beneficial coefficient of the insider $C_{\mathcal{I}}$, the system coefficient of the insider η, the awareness time parameters ω_0 and $\Delta\omega$ are set as shown in Table III. The decision of the insider is determined by (29), and the decision of the attacker in employing the insider is determined by (28). The insider involves in the attack if both the attacker and

TABLE IV
PAYOFFS AND STRATEGIES OF DEFENDER, ATTACKER AND INSIDER WHEN $C_{\mathcal{I}} = 0.1$

Scenario:	S1	S2	S3	S4
Defender's Payoff ($U_{\mathcal{D}}$)	0.4271	0.3702	0.3702	0.4271
Attacker's Payoff ($U_{\mathcal{A}}$)	0.0009	0.0044	0.0035	0.0009
Insider's Payoff ($U_{\mathcal{I}}$)	-	-	-	-0.0020
Defense Coefficient (λ)	108.52	102.64	102.64	108.52
Attack Rate (r)	0.1033	0.2092	0.2092	0.1033
Insider Employment (ξ)	-	-	1	1
Insider Offer Decision (ζ)	-	-	-	0

TABLE V
PAYOFFS AND STRATEGIES OF DEFENDER, ATTACKER AND INSIDER WHEN $C_{\mathcal{I}} = 0.3$

Scenario:	S1	S2	S3	S4
Defender's Payoff ($U_{\mathcal{D}}$)	0.4271	0.3702	0.3702	0.3702
Attacker's Payoff ($U_{\mathcal{A}}$)	0.0009	0.0044	0.0015	0.0015
Insider's Payoff ($U_{\mathcal{I}}$)	-	-	-	-0.0016
Defense Coefficient (λ)	108.52	102.64	102.64	102.64
Attack Rate (r)	0.1033	0.2092	0.2092	0.2092
Insider Employment (ξ)	-	-	1	1
Insider Offer Decision (ζ)	-	-	-	1

TABLE VI
PAYOFFS AND STRATEGIES OF DEFENDER, ATTACKER AND INSIDER WHEN $C_{\mathcal{I}} = 0.5$

Scenario:	S1	S2	S3	S4
Defender's Payoff ($U_{\mathcal{D}}$)	0.4271	0.3702	0.4271	0.4271
Attacker's Payoff ($U_{\mathcal{A}}$)	0.0009	0.0044	0.0009	0.0009
Insider's Payoff ($U_{\mathcal{I}}$)	-	-	-	-0.0020
Defense Coefficient (λ)	108.52	102.64	108.52	108.52
Attack Rate (r)	0.1033	0.2092	0.1033	0.1033
Insider Employment (ξ)	-	-	0	0
Insider Offer Decision (ζ)	-	-	-	1

insider agree on the employment. If the insider involves, the strategies of the defender and attacker are determined by (26) and (27). The payoffs of the defender and attacker are then calculated by (11) and (13) accordingly. Otherwise, the strategies of the defender and attacker are determined by (21) and (22), respectively. The payoffs of the defender and attacker are then calculated by (8) and (10) accordingly.

When the beneficial coefficient of the insider is 0.1, the payoffs and strategies of the players in the FlipIt game model are shown in Table IV. In Table IV (as well as Tables V and VI), the insider employment decision variable ξ indicates whether the attacker chooses to employ the assistance from the insider in the scenario. It equals one if the attacker prefers to employ the insider's assistance. Otherwise, it is equal to zero. The insider offer decision variable ζ indicates whether the insider is willing to assist the attacker in the scenario. It equals one if the insider is willing to assist the attacker. Otherwise, it is equal to zero. As shown in Table IV, due to the existence of the insider, the defender's payoff drops notably and the defender has to reduce the defense interval (indicated by the defense coefficient λ), which means increasing the defense action frequency to protect the system. The attacker's payoff is increased by the existence of the insider as expected. The highest increase happens in Scenario 2 when the insider is a volunteer. The attacker will not hesitate to employ the insider in this case. When a cost is placed on the attacker, his/her payoff drops slightly as shown in Scenario 3. However, when the insider is partly responsible for the system security as assumed in Scenario 4, the insider will consider whether it is beneficial to help the attacker. When $C_{\mathcal{I}} = 0.1$, the insider's payoff is -0.002 if he/she rejects the attacker and the payoff decreases to -0.0045 if he/she facilitates the attack. Thus, the insider turns the attacker down in this case.

When the beneficial coefficient of the insider is 0.3, the payoffs and strategies of the players in the FlipIt game model are shown in Table V. When $C_{\mathcal{I}} = 0.3$, the payment to the insider from the attacker increases. In the case when the insider is system security responsible, the insider's payoff is -0.002 if he/she rejects the attacker and the payoff increases to -0.0016 if he/she helps in the attack. Thus, the insider chooses to facilitate the attack. As a result, the defender's payoff drops and the attacker's payoff increases in Scenario 4.

When the beneficial coefficient of the insider is 0.5, the payoffs and strategies of the players in the FlipIt game model are shown in Table VI. When $C_{\mathcal{I}} = 0.5$, the payment to the insider from the attacker is further increased. In the case when the insider is not volunteer, the attacker's payoff is -0.0004 if he/she employs the insider, while his/her payoff is 0.0009 when the attacker does not employ the insider. Thus, although the insider is willing to facilitate the attack, the attacker chooses not to accept the offer from the insider in both Scenarios 3 and 4.

When $C_{\mathcal{I}} = 0.3$, the insider is willing to facilitate the attack. However, if the system cost coefficient of the insider increases, the insider may turn the attacker down due to a higher evaluation of the system loss. Figure 5 shows the attacker's payoff in the four scenarios when the system cost coefficient of the insider increases from 0.1 in the base case to 0.5, which means the insider takes higher responsibility of the system loss. In this case, the financially motivated insider with system responsibility turns the attacker down due to a higher evaluation of the system loss. As shown in the figure, the attacker's payoff in Scenario 4 drops to the level of Scenario 1 in which there is no insider. Thus, the curve of Scenario 4 overlaps with the curve of Scenario 1. Introducing the system responsibility to potential insiders can be a good method to alleviate the impact of the insider. Further, with a lower defense action cost, the payoff of the attacker drops significantly. When the defense action cost is low, the defender can increase the defense action rate with less cost pressure. In this case, the cost of employing the financially motivated insider is higher than the increase of the attacker's payoff by employing the insider in the game, and therefore the attacker tends not to employ the financially motivated insider. As a result, the curve of Scenario 3 overlaps with the curves of

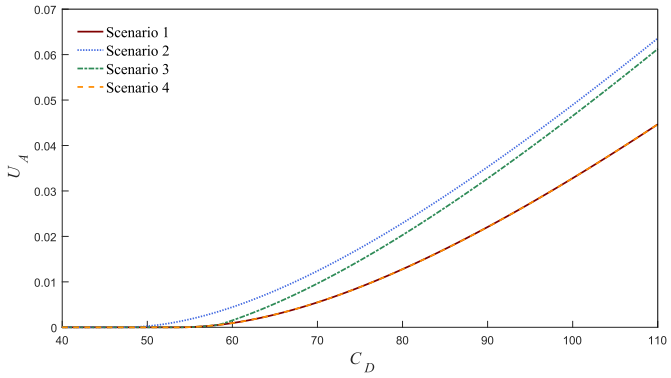


Fig. 5. Attacker's payoff in different scenarios.

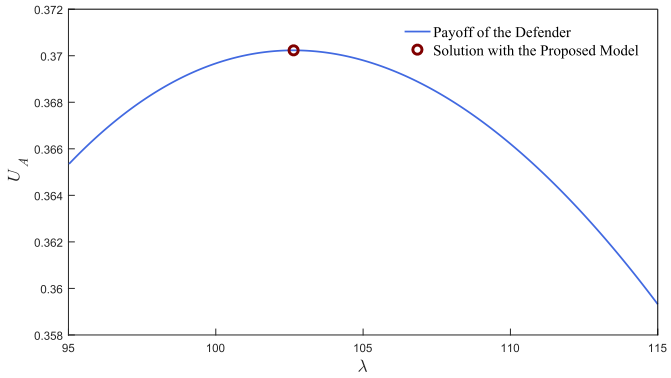


Fig. 6. Defender's payoff with the proposed game model with insider.

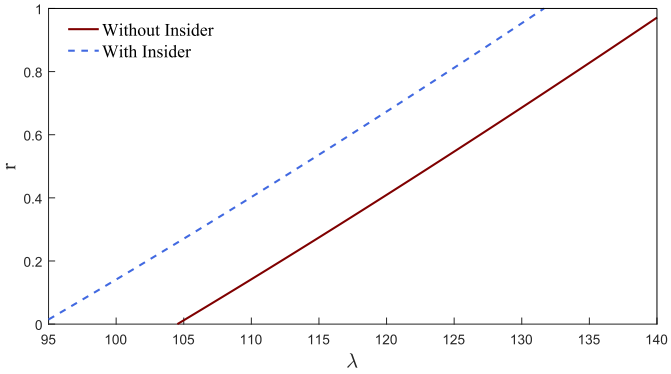


Fig. 7. Relation between attack rate r and defense coefficient λ.

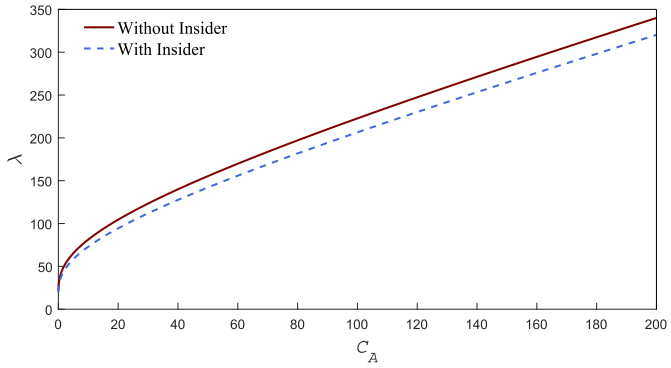


Fig. 8. Necessary defense coefficient λ to force attacker to drop out.

Scenarios 1 and 4 in the left part of the figure where the defense action cost is low.

The results of the case studies also show that the proposed FlipIt game model is able to provide the optimal solution for the defense strategy of the system operator against the cyberattacks with insider. The solution of the proposed model maximizes the payoff of the system operator as the defender considering the attack strategies and the impacts of the insider. Figure 6 shows the defender's payoff with different defense action rate and the solution of the proposed model in the case with the volunteer insider. As shown in the figure, the solution of the proposed model maximizes the payoff of the defender in the presence of the insider in the attacks. If the solution without considering the insider or any other defense action rate is selected by the defender, his/her payoff will be reduced compared with the solution of the proposed model considering the insider in this paper.

In the FlipIt game, the relation of the defense coefficient λ and the attack rate r with and without insider is shown in Figure 7. As shown in the figure, when the defense coefficient λ drops, which means the defense frequency increases, the attack rate r decreases accordingly. It is also shown in the figure that the presence of insider will increase the attack rates by the attacker. Thus, a most effective approach to increase the system security with insider is to reduce the cost of the system defense action and increase the defense action frequency. When the defense action frequency is high enough, the attacker will be forced to drop out of the attack (as $r = 0$) both with and without insider. The necessary defense coefficient λ to force the attacker to drop out is shown in Figure 8.

As shown in the figure, the necessary defense coefficient λ decreases along with the decrease of the cost coefficient $C_{\mathcal{A}}$ in both cases with and without the insider. In other words, when the cost for the attack action decreases, more frequent defense actions should be performed in order to force the attacker to drop out of the attack. However, when the insider exists, the necessary defense coefficient λ is lower with the same cost coefficient $C_{\mathcal{A}}$. Thus, more efforts need to be paid by the defender to force the attacker to drop out in the presence of the insider.

C. An Example in Electric Power Systems

A locational marginal price (LMP) manipulation model by the aggregators in power systems is demonstrated in [35]. By curtailing the generation at certain nodes in the grid purposely, the aggregator may be able to manipulate the LMPs in the grid and profit from the electricity price manipulation. The LMP calculation in the real-time electricity market can be expressed as follows.

$$\min\ c^{\mathrm{T}} B f \tag{30}$$

Subject to

$$\Delta p^{-} \leqslant Bf - p + \alpha + d \leqslant \Delta p^{+},\ \left(\lambda^{-}, \lambda^{+}\right) \tag{31}$$

$$f^{-} \leqslant f \leqslant f^{+},\ \left(\mu^{-}, \mu^{+}\right) \tag{32}$$

$$f \in \text{range}\,(G)\,,\ (\nu) \tag{33}$$

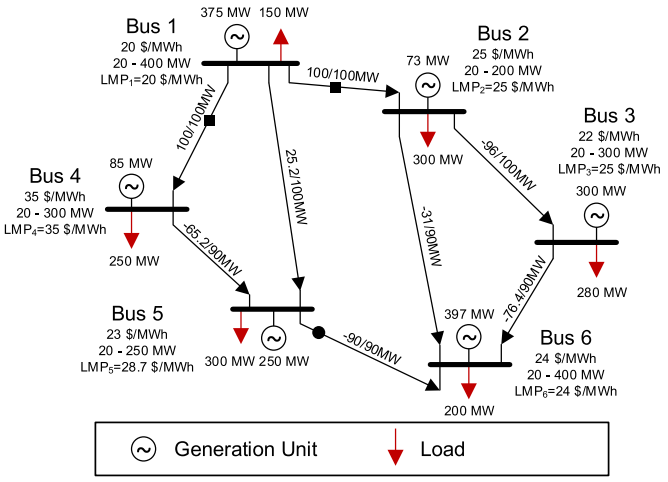


Fig. 9. Single line diagram of the 6-Bus system [35].

where c is the offer price vector of the generation units, B is the branch-to-bus incidence matrix, f is the vector of the flow on the transmission branches, p is the output vector of the generation units, α is the strategic curtailment by the aggregator, Δp^- and Δp^+ are the limits of the power injection change at each bus, f^- and f^+ are the limits of the flow on the transmission branches, and $\lambda^-, \lambda^+, \mu^-, \mu^+, \nu$ are the Lagrange multipliers of the corresponding constraints, respectively. With the solution of the optimization problem above, the LMP at each bus i of the grid can be calculated as (34).

$$LMP_i(\alpha) = c_i + \lambda_i^+(\alpha) - \lambda_i^-(\alpha) \tag{34}$$

Then the profit of the aggregator by manipulating the LMPs can be calculated as follows.

$$\gamma(\alpha) = \sum_{i \in \mathcal{N}_a} \left[LMP_i(\alpha)\left(p_i^a - \alpha_i\right) - LMP_i(0)\, p_i^a \right] \tag{35}$$

where $\mathcal{N}_a$ is the set of buses with generation units of the aggregator, p_i^a is the original output of the generation unit of the aggregator at bus i in the grid. In general, the profit γ can be either positive or negative depending on the state of the grid. When γ is positive, it is profitable for the aggregator to curtail the generation. The case of a 6-bus network in [35] is used here to demonstrate the price manipulation. The 6-bus system is shown in Figure 9.

In the original case, the generation outputs at each bus are 375.19, 72.59, 300.00, 84.81, 250.00 and 397.41 MW, respectively. Accordingly, the LMPs are 20.0, 25.0, 25.0, 35.0, 28.7 and 24.0 \$/MWh. Assume that aggregator a owns the generation units at Bus 1. By curtailing 0.15 MW generation at Bus 1, it can be proofed that the LMPs will be changed to 25.8, 25.0, 25.0, 35.0, 30.6 and 24.0 \$/MWh. As such, the aggregator increases its profit by manipulating the LMPs in the grid as $\gamma = 25.8 \times 375.04 - 20.0 \times 375.19 = 2180\,\$/\text{h}$. In contrast, the grid is originally operated at a cost of $36491.5\,\$/\text{h}$ which is now increased to $39160.7\,\$/\text{h}$ due to the LMP manipulation.

As mentioned above, the curtailment profit of the aggregator is not always positive. It can be either positive or negative depending on the real-time network topology, operational constraints, and estimation of the power injection and loads at the buses of the grid as shown in model (30)-(33). In order to decide whether it is a good opportunity to manipulate the LMPs for profit as (35), the aggregator needs to obtain such information of the grid. Generally, the mentioned information is gathered by the transmission system operator (TSO) SCADA system. In order to access the necessary information of the grid to determine the LMP manipulation strategy, the aggregator may intrude into the TSO SCADA system. A typical TSO SCADA system configuration is shown in Figure 10.

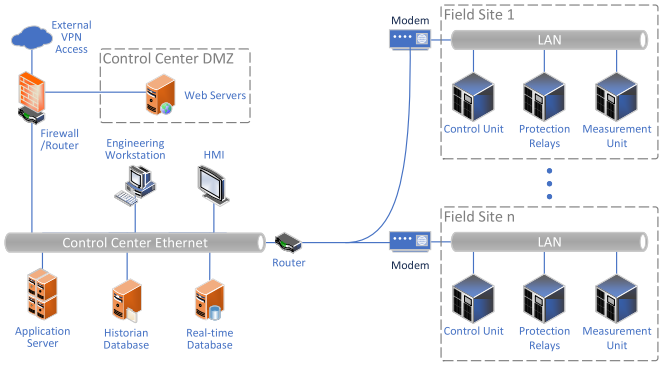


Fig. 10. Configuration of TSO SCADA system.

As the mentioned information may be exchanged between the application servers and the real-time databases, the aggregator may perform the packet sniffing attack on the SCADA system to obtain the information [33]. First, the attacker compromises the remote access. Secondly, it needs to compromise the firewall of the SCADA network. Then the attacker acquires the privilege for its presence in the DMZ to protect the remote access. After that, the attacker can gather reconnaissance to gain the access to the control center LAN. Then, the attacker is able to install a sniffer and sniff the packets in the control center LAN to gather the wanted information. The attack process can be formulated by the SMP model shown in Figure 11 (a). If an insider exists in the system and aids the attacker to gain the remote access and bypass the firewall through the VPN to get connected to the DMZ of the SCADA network, the SMP model of the attack process then becomes Figure 11 (b). The distributions of the time for the attacker to launch the attack and compromise the system with and without the assistance of the insider can be simulated with the SMP models. The distributions without and with insider are shown in Figure 12 (a) and (b), respectively.

In order to eliminate the potential impacts of the eavesdrops from the attacker, the defender may revoke the privilege of the existing remote access to the SCADA network through the VPN and update the authorizations with mandatory secure identity and access management, e.g., multi-factor authentication. Then the optimal time coefficients to perform the defense actions on the SCADA network can be determined according to the proposed FlipIt game based model. When there is no insider's assistance to the attacker, the optimal defense time coefficient is 9.96 h, which means the mean time for the defender to perform the defense actions is about 10 hours.

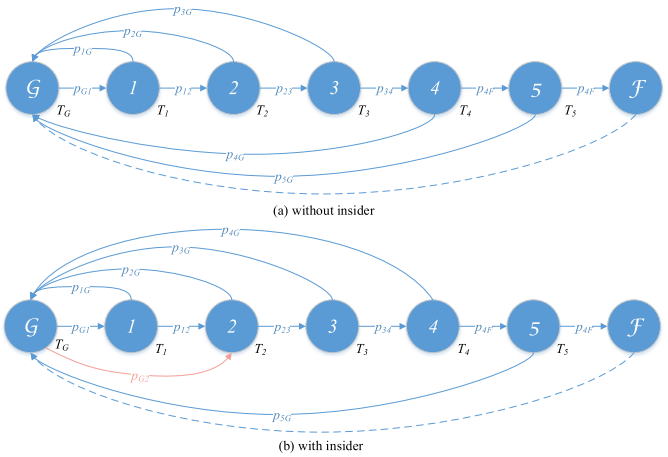


Fig. 11. SMP model of packet sniffing attack on TSO SCADA system.

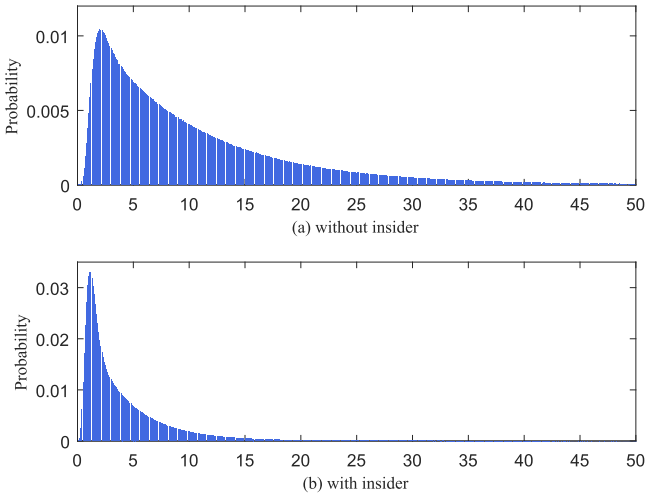


Fig. 12. Probability distribution of time-to-Compromise of Packet Sniffing attack on TSO SCADA system, (a) without insider assistance, (b) with insider assistance.

In this case, the expected ratio of time with information leakage possibility to the attacker is about 0.0715. However, if the insider's assistance to the attacker exists, the attacker gains extra advantages in launching the attack, and a higher frequency of defense actions will be needed. In this case, the defense time coefficient drops to 8.95 h which means more frequent defense actions, and the expected ratio of time with information leakage possibility increases to about 0.3096. In order to force the attacker to drop out of the attempts in this case, the system defender will have to further decrease the defense time coefficient to 6.83 h, which means the mean time for the defender to conduct the defense actions should be lower than seven hours in order to adequately prevent the potential attacks considering the insider's assistance.

V. Conclusion

In this paper, the cyberattacks against the SCADA systems are investigated considering the insider's assistance to the attacker. A SMP model is developed to formulate the intrusion process of the attacks and derive the distribution of the time-to-compromise the system with the impact of the insider. A FlipIt game model is developed to analyze the strategies of the defender, attacker and insider in the attacks. It is shown in the case studies that the presence of the insider will increase the payoff of the attacker while reducing the defender's payoff at the same time. The defender has to pay a higher price and increase the defense action frequency for maintaining the cybersecurity of the SCADA system due to the insider's assistance to the attacker. Among the three different types of insiders, the volunteer insider is most damaging as no cost is placed on the attacker and the attacker does not hesitate to employ the insider's help in the attack. In order to enhance the system security, an effective method is to reduce the cost of the system defense action and increase the defense action frequency. Another beneficial method to mitigate the impact of the insider and enhance the system security is to introduce the system security responsibility to the insiders. As such, the insiders will need to evaluate the system loss in the attack and hesitate to offer help to the attacker.

References

[1] L. D. Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[2] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The future of industrial communication: Automation networks in the era of the Internet of Things and industry 4.0," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 17–27, Mar. 2017.

[3] M. Aazam, S. Zeadally, and K. A. Harras, "Deploying fog computing in industrial Internet of Things and industry 4.0," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4674–4682, Oct. 2018.

[4] M. T. Review. *Industrial Control Systems are Still Vulnerable to Malicious Cyberattacks*. Accessed: Jan. 2019. [Online]. Available: https://www.technologyreview.com/s/612829/industrial-control-systems-are-still-vulnerable-to-malicious-cyberattacks/

[5] NERC Planning, Operating, and Critical Infrastructure Protection Committees, "High-impact, low-frequency event risk to the North American bulk power system," North Amer. Electr. Rel. Corp. (NERC), U.S. Dept. Energy (DOE), Atlanta, GA, USA, Tech. Rep., Jun. 2010.

[6] Y. Qin, Q. Zhang, C. Zhou, and N. Xiong, "A risk-based dynamic decision-making approach for cybersecurity protection in industrial control systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 10, pp. 3863–3870, Oct. 2020.

[7] Q. Zhang, C. Zhou, N. Xiong, Y. Qin, X. Li, and S. Huang, "Multimodel-based incident prediction and risk assessment in dynamic cybersecurity protection for industrial control systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 46, no. 10, pp. 1429–1444, Oct. 2016.

[8] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine learning-based network vulnerability analysis of industrial Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6822–6834, Aug. 2019.

[9] G. Falco, C. Caldera, and H. Shrobe, "IIoT cybersecurity risk modeling for SCADA systems," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4486–4495, Dec. 2018.

[10] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *Proc. 70th Annu. Conf. Protective Relay Eng. (CPRE)*, College Station, TX, USA, Apr. 2017, pp. 1–8.

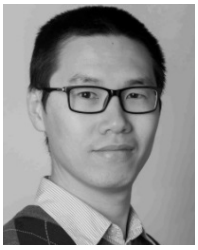
[11] K. Richards, R. LaSall, M. Devost, F. Van Den Dool, and J. Kennedy-White, "2017 cost of cyber crime study," Ponemon Inst. Accenture, Traverse City, MI, USA, Tech. Rep., 2017.

[12] ISACA, "State of cybersecurity: Implications for 2016," ISACA, Rolling Meadows, IL, USA, Tech. Rep., 2016.

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

[14] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation," *IEEE Trans. Power Syst.*, vol. 31, no. 6, pp. 4379–4394, Nov. 2016.

[15] Y. Zhang, Y. Xiang, and L. Wang, "Power system reliability assessment incorporating cyber attacks against wind farm energy management systems," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2343–2357, Sep. 2017.
[16] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Power system reliability evaluation with SCADA cybersecurity considerations," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1707–1721, Jul. 2015.
[17] J. Kirsch, S. Goose, Y. Amir, D. Wei, and P. Skare, "Survivable SCADA via intrusion-tolerant replication," *IEEE Trans. Smart Grid*, vol. 5, no. 1, pp. 60–70, Jan. 2014.
[18] A. Almalawi, A. Fahad, Z. Tari, A. Alamri, R. AlGhamdi, and A. Y. Zomaya, "An efficient data-driven clustering technique to detect attacks in SCADA systems," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 893–906, May 2016.
[19] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 4, pp. 1396–1407, Jul. 2014.
[20] Y. Yang *et al.*, "Multiattribute SCADA-specific intrusion detection system for power networks," *IEEE Trans. Power Del.*, vol. 29, no. 3, pp. 1092–1102, Jun. 2014.
[21] I. N. Fovino, A. Coletta, A. Carcano, and M. Masera, "Critical state-based filtering system for securing SCADA network protocols," *IEEE Trans. Ind. Electron.*, vol. 59, no. 10, pp. 3943–3950, Oct. 2012.
[22] P. M. Nasr and A. Y. Varjani, "Alarm based anomaly detection of insider attacks in SCADA system," in *Proc. Smart Grid Conf. (SGC)*. Tehran, Iran: IEEE, Dec. 2014, pp. 1–6.
[23] P. M. Nasr and A. Y. Varjani, "Petri net model of insider attacks in SCADA system," in *Proc. 11th Int. ISC Conf. Inf. Secur. Cryptol. (ISCISC)*. Tehran, Iran: IEEE, Sep. 2014, pp. 55–60.
[24] M. van Dijk, A. Juels, A. Oprea, and R. L. Rivest, "FLIPIT: The game of 'Stealthy Takeover,'" *J. Cryptol.*, vol. 26, no. 4, pp. 655–713, Oct. 2013.
[25] X. Feng, Z. Zheng, P. Hu, D. Cansever, and P. Mohapatra, "Stealthy attacks meets insider threats: A three-player game model," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Tampa, FL, USA, Oct. 2015, pp. 25–30.
[26] X. Feng, Z. Zheng, D. Cansever, A. Swami, and P. Mohapatra, "Stealthy attacks with insider information: A game theoretic model with asymmetric feedback," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Baltimore, MD, USA, Nov. 2016, pp. 277–282.
[27] H. Gunduz and D. Jayaweera, "Modern power system reliability assessment with cyber-intrusion on heat pump systems," *IET Smart Grid*, vol. 3, no. 5, pp. 561–571, Oct. 2020.
[28] Y. Chen, J. Hong, and C.-C. Liu, "Modeling of intrusion and defense for assessment of cyber security at power substations," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2541–2552, Jul. 2018.
[29] Z. H. Fang, H. D. Mo, and Y. Wang, "Reliability analysis of cyber-physical systems considering cyber-attacks," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manage. (IEEM)*, Singapore, Dec. 2017, pp. 364–368.
[30] B. B. Madan, K. Goševa-Popstojanova, K. Vaidyanathan, and K. S. Trivedi, "A method for modeling and quantifying the security attributes of intrusion tolerant systems," *Perform. Eval.*, vol. 56, nos. 1–4, pp. 167–186, Mar. 2004.
[31] F. Grabski, *Semi-Markov Processes: Applications in System Reliability and Maintenance*. Amsterdam, The Netherlands: Elsevier, 2014.
[32] K. S. Trivedi, *Probability and Statistics With Reliability, Queuing, and Computer Science Applications*. Hoboken, NJ, USA: Wiley, 2001.
[33] S. Young and D. Aitel, *The Hacker's Handbook: The Strategy Behind Breaking into and Defending Networks*. Boca Raton, FL, USA: CRC Press, 2004.
[34] M. Zhang, Z. Zheng, and N. B. Shroff, "A game theoretic model for defending against stealthy attacks with limited resources," in *Proc. Int. Conf. Decis. Game Theory Secur. (GameSec)*, London, U.K., 2015, pp. 93–112.
[35] N. A. Ruhi, K. Dvijotham, N. Chen, and A. Wierman, "Opportunities for price manipulation by aggregators in electricity markets," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 5687–5698, Nov. 2018.



Zhaoxi Liu (Member, IEEE) 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.

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 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. He 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 was a recipient of the Outstanding Faculty Research Award of College of Engineering and Applied Science at UWM in 2018.