Power System Reliability Analysis Considering External and Insider Attacks on the SCADA System

Sirui Tang, Zhaoxi Liu, and Lingfeng Wang
Department of Electrical Engineering and Computer Science
University of Wisconsin-Milwaukee, Milwaukee, WI 53211, USA
Email: l.f.wang@ieee.org

***Abstract*—Cybersecurity of the supervisory control and data acquisition (SCADA) system, which is the key component of the cyber-physical systems (CPS), is facing big challenges and will affect the reliability of the smart grid. System reliability can be influenced by various cyber threats. In this paper, the reliability of the electric power system considering different cybersecurity issues in the SCADA system is analyzed by using Semi-Markov Process (SMP) and mean time-to-compromise (MTTC). External and insider attacks against the SCADA system are investigated with the SMP models and the results are compared. The system reliability is evaluated by reliability indexes including loss of load probability (LOLP) and expected energy not supplied (EENS) through Monte Carlo Simulations (MCS). The lurking threats of the cyberattacks are also analyzed in the study. Case studies were conducted on the IEEE Reliability Test System (RTS-96). The results show that with the increase of the MTTCs of the cyberattacks, the LOLP values decrease. When insider attacks are considered, both the LOLP and EENS values dramatically increase owing to the decreased MTTCs. The results provide insights into the establishment of the electric power system reliability enhancement strategies.**

***Index Terms*--Cybersecurity, insider attacks, mean time-to-compromise (MTTC), Monte Carlo Simulation (MCS), power system reliability.**

I. INTRODUCTION

As the new generation of electric power systems, the smart grid widely deploys the cyber-physical systems (CPS) which provide high capacity, efficiency, and reliability. In CPS, the communication and computation based on the supervisory control and data acquisition (SCADA) system perform vital operations for monitoring and controlling the power grid. However, the scale and complexity of the power systems are further increased owing to the real-time integration of both the physical system and the information computing system, while it is much easier for the cyber components to be exposed and attacked. As a result, cyberattacks are among the main impacts on the electric power system reliability [1]. The SCADA systems in power systems are vulnerable to different network security threats at different stages and at different levels of the data and control command transmission due to different network transmission methods [2]. Fig. 1 shows the different network security threats to the SCADA system and energy manage system (EMS).

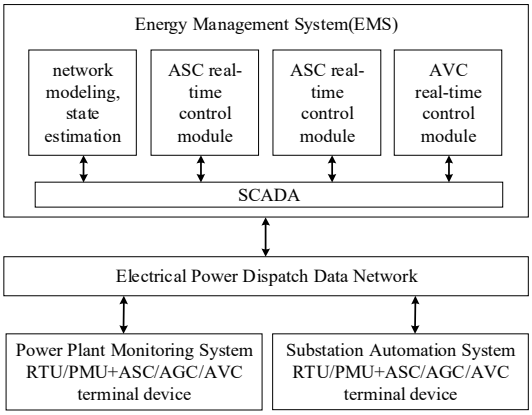

Figure 1. Cyber threats against SCADA/EMS systems.

To protect the cybersecurity of the SCADA system and the reliability of the power system, safeguarding the SCADA network is critical which can be achieved by analyzing and studying its security architecture, combining the universal network security system principles with the characteristics of the SCADA network, effectively ensuring the integrity and effectiveness of the network security strategy and better meeting the security requirements of the power system. In [3], the impact of the attacks which occurred on the generators and transmission lines was estimated. To carry out the security strategy, the evaluation model was built in which the loss was evaluated when the generators were out of service, and the exponential function and the Mean-Time-to-Attack (MTTA) were used to model the cyberattacks on the generators. Meanwhile, assuming that the security strategies of the transmission lines were advanced relaying, various MTTAs were used to simulate the cyber threats. Further, the cyber threats on the SCADA were considered when penetrations were performed to affect the statuses of the controls of the generators, transmission lines and loads. To simulate the cyber threats of the SCADA systems, exponentially distributed random variables and a Bernoulli random variable presented by the Average Percentage of Tripped Breakers (APTB) were used. By applying these simulations in the Roy Billinton Test System (RBTS) [4], it was found that cyberattacks on the SCADA system resulted in times more serious impacts than on the original components [3], [5]. In [6], Monto Carlo Simulations (MCS) were used to estimate the reliability of an electric

978-1-7281-4547-1/20/$31.00 ©2020 IEEE

service in the SCADA system and the availability of system control. It is reported that the cyberattacks that can be accurately detected is only occupied by 30%, while more than half of them have resulted in extremely huge economic losses that may be more than one million dollars [7]. However, the most harmful threat is the insider attacks which apply rights for despiteful purposes [8]. It is reported by the US Computer Security Institute (CSI) that the influence of insider attacks has exceeded the impact cause by viruses and worms since 2007 [9].

In this paper, the reliability analysis model of SCADA systems of the power systems considering the cybersecurity issues with different attacks is developed. The SMP based attack models are built considering both external attack and insider attacks. The lurking threats of the cyberattacks are analyzed in the study. Case studies were performed on the IEEE Reliability Test System (RTS-96). Results show that with the increase of vulnerabilities in the system, the values of MTTC decrease, and the LOLP values increase, which indicates that the reliability of the electric power system becomes worse. The EENS values of the scenarios considering the insider attacks greatly increase which indicates that insider attacks cause worse impacts than the external cyberattacks.

II. Attack Modeling Based on Semi-Markov Process

To model the cyberattacks and analyze their impacts on the SCADA systems, the Semi-Markov Process (SMP) is used to model the external and insider attacks. The Mean Time-to-Compromise (MTTC) can be estimated based on the SMP models, as the time which a particularly skilled attacker will use to successfully attack a system. The attacker levels are divided into four categories, i.e., Novice, Beginner, Intermediate and Expert [10].

The SMP model is proposed for a half Markov process that takes the time factor into account [11]-[13]. A discrete state space SMP is a stochastic process $\{X(t): t \geq 0\}$ with the sample path $X(t) = \xi_n(t)$ associated with the Markov renewal process (MRP) $\{(\xi_n, \vartheta_n): n \in \mathbb{N}_0\}$ with the initial distribution $p = [p_i(0): i \in S]$ and the kernel $Q(t) = [Q_{ij}(t): i,j \in S], t \geq 0$, where S is a finite discrete state space. Then the transition probability matrix $Q = [p_{ij}: i,j \in S]$ can be determined as follows.

$$p_{ij} = \lim_{t\to\infty} Q_{ij}(t) \tag{1}$$

Consider the sojourn time of in state *i* if the next state is *j*, which is denoted by T_{ij}. Then the cumulative distribution function (CDF) of T_{ij} can be determined according to the kernel as (2).

$$F_{ij}(t) = P(\vartheta_{n+1} \leq t | \xi_n = i, \xi_{n+1} = j) = \frac{Q_{ij}(t)}{p_{ij}} \tag{2}$$

Fig. 2 illustrates a general SMP model of the intrusion process. G represents the good state which means the targeted system is secure, and states 1 to n are intermediate states with the actions of the attacker. As the process is pushed forward, higher privilege of the targeted system will be obtained by the attacker. Finally, the failure state F is reached when the system is compromised. State G and states 1 to n are transient states, and state F is the absorbing state. The transition probability of state changing from state i to j is set as p_{ij} [14].

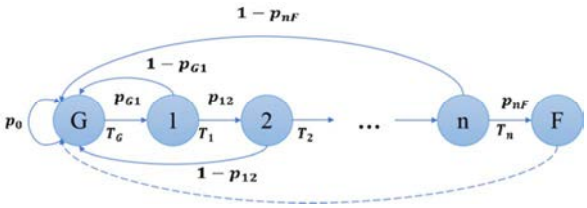

Figure 2. General SMP model of the intrusion process.

The MTTC of the attack is the mean time that the semi-Markov process reaches the absorbing state [14]. It can be calculated from the transition matrix Q which consists of the transition probabilities as (3).

$$MTTC = \sum_{j\in S_T} V_j T_j \tag{3}$$

where V_j is the average number of times that state j has been visited before the final failure state is reached, and T_j is the mean sojourn time of state j [15]. For each state in the transient state set S_T, the average visit number V_j can be expressed as (4) below.

$$V_j = p_j + \sum_i V_i\, p_{ij}, \qquad i,j \in S_T \tag{4}$$

where p_j is the probability that state j is the starting state of the discrete-time Markov chain (DTMC) [16]. It is assumed in this paper that the attack starts from the good state G. Thus $p_G = 1$; otherwise $p_j = 0|_{j\neq G}$. p_{ij} is the element in the transition matrix Q. With (3) and (4), the MTTC of the attack can be calculated accordingly.

III. Attack Scenarios and MTTC Estimation

The control center local area network (LAN) and the corporation LAN are the main targets of the attackers to invade the SCADA systems in power systems by discovering the vulnerabilities among the components in cyber networks. The SMP models of the attacks through both LANs are developed. Besides, in this paper, the external attacks and insider attacks are both considered, and results are compared with each other.

A. Attacks on Control Center LAN

Fig. 3 shows a schematic diagram of the control center LAN. For external attacks, after the attacker bypasses the hardware firewall by using well-planned intrusion strategies, the attacker can access the switch through the port scan method. Then the attacker can scan the network's hosts and servers by invading the historical data server. The application server, which is used to store data and send updated data to other clients like the human machine interface (HMI), is the target of the intrusion [17]. In Fig. 4, the SMP based attack model on the control center LAN is illustrated. State G is the good state, and state F indicates the success of the attack. The SMP will shift to state 1 from state G if the attacker successfully bypasses the hardware firewall. Then state 2 will be reached if the history server is breached. For insider attacks, an insider with knowledge of the SCADA system setting may have the privilege to modify the setting maliciously. In this case, the insider attacker can easily breach the history server without triggering alerts from the intrusion-detection system (IDS). Thus, an additional transition probability from state G to state 2 is added in the

SMP model as shown in Fig. 4. The transition matrix of the SMP model considering the insider threats Q_1 is represented as (5).

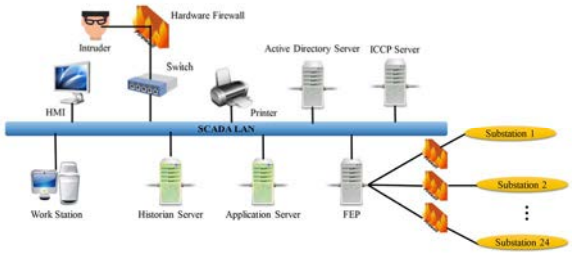

Figure 3. Attack path on the control center LAN.

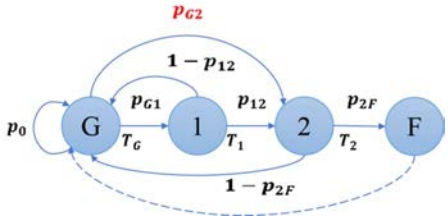

Figure 4. SMP model of attacks on the control center LAN.

$$Q_1 = \begin{bmatrix} (1-p_{G1}-p_{G2}) & p_{G1} & p_{G2} \\ 1-p_{12} & 0 & p_{12} \\ 1-p_{2F} & 0 & 0 \end{bmatrix} \quad (5)$$

B. Attacks on Corporation LAN

Because of the complex communication network between the attackers and substation networks, it is possible for the attackers to firstly access the corporation LAN via the Internet. Fig. 5 illustrates the possible attack path on the corporation LAN. For external attacks, by accessing the communication network between the control center and the substation, an attacker can install an eavesdropping device on a wired or wireless network. Then the attacker can monitor the traffic, intercept the measured values and/or status packets, and replace some of the normal state data with the manufactured anomaly data and/or inject false commands which are fatal to the normal operations of the power system. For insider attacks, there is a probability that the attacker already has the access privilege to the FTP server, and the attacker can immediately affect the database serve to inject the false data. Thus, an additional transition probability from state 2 to the failure state F is added in the SMP model as shown in Fig. 6. The transition matrix of the SMP model considering the potential insider threats Q_2 is represented as (6).

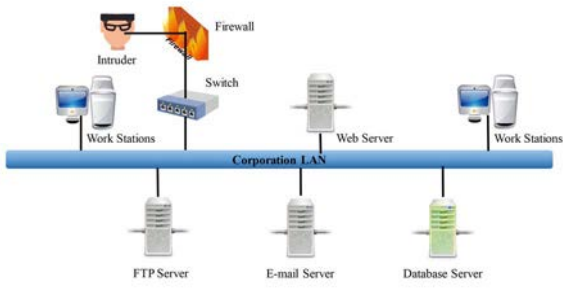

Figure 5. Attack path on the corporation LAN.

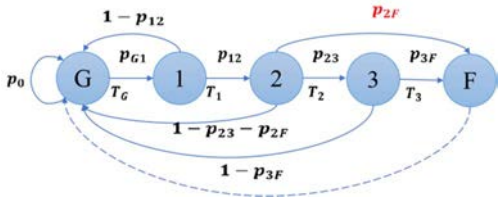

Figure 6. SMP model of attacks on the corporation LAN.

$$Q_2 = \begin{bmatrix} (1-p_{G1}) & p_{G1} & 0 & 0 \\ (1-p_{12}) & 0 & p_{12} & 0 \\ (1-p_{23}-p_{2F}) & 0 & 0 & p_{23} \\ (1-p_{3F}) & 0 & 0 & 0 \end{bmatrix} \quad (6)$$

IV. Power System Reliability Analysis

To analyze the reliability of the electric power system considering the external attack and insider attack models, the Monte Carlo Simulation (MCS) is applied. The steps of the reliability analysis process are shown in Fig. 7. In the simulation, it is assumed that if the SCADA system of a bus is compromised and the attack is launched, all the breakers in this substation will be tripped by the attacker maliciously. The system restoration process is assumed to start when the attack on a bus is launched. The repair time of the system is represented by the mean time-to-repair (MTTR). Then the probability that the SCADA system of a node in the system can be evaluated as (7).

$$p_a = \frac{MTTR}{MTTR+MTTC} \quad (7)$$

With the statuses of all the components in the grid, an optimal power flow (OPF) analysis is performed to determine the load loss considering the external and insider cyberattacks on the power systems. Then the reliability metrics including the loss of load probability (LOLP) and the expected energy not supplied (EENS) are calculated to evaluate the reliability of the power system under the potential cyberattacks.

In the cyberattacks against the power systems, when the SCADA system of a substation is compromised, the attacker may stay hidden intentionally for a period instead of launching the attack immediately. In this way, the attackers can enlarge the damage to the power system by triggering the attacks on multiple substations simultaneously. Thus, the lurking threat is an important issue in the reliability analysis when considering the cyberattacks on the power systems. In this study, the lurking threat of the cyberattacks is studied. The attacker is assumed to lurk for a certain time period to synchronize the attacks on different buses in the case when the lurking threat is considered. As the attacks are regarded as stochastic processes, the attacker does not know the exact time when the attacks will be successful in advance. It is impossible for the attacker to wait forever to synchronize the attacks. Thus, a maximum lurking period T_{max} is assumed for the attacks in the study. Fig. 8 shows an example of the sequence for the lurking actions. The attack processes on four nodes are shown in Fig. 8. It is shown that the attacks on nodes 1 and 3 are not triggered immediately when the nodes are compromised. Instead, they are launched together with node 4 after a certain period. The attack on node 2 is not synchronized because the lurking period limit T_{max} is reached.

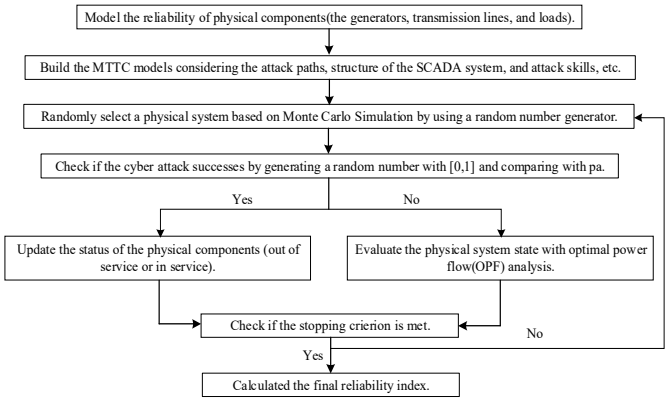

Figure 7. Flow diagram of MCS for reliability analysis.

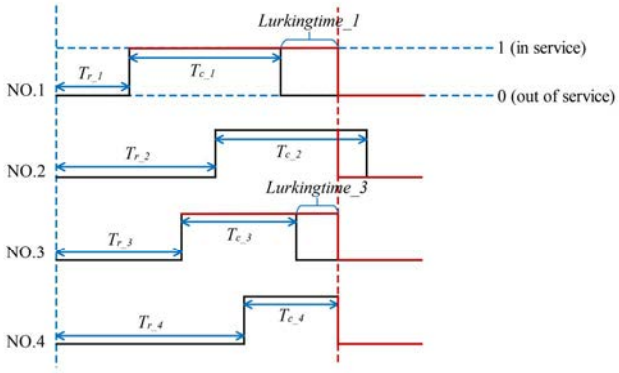

Figure 8. Sequence diagram of lurking actions in cyberattacks.

V. Simulation Results

In order to illustrate the proposed power system reliability evaluation scheme considering the external attack and insider attack models, case studies were conducted based on the IEEE Reliability Test System (RTS-96). The results of the case studies are presented and discussed in this section.

A. MTTC Estimation

According to (3), the MTTCs can be estimated. According to the National Vulnerability Database, 7000 kinds of vulnerabilities are examined. In this paper, the additional transition probabilities of state changing due to the insider attacks (which are P_{G2} and P_{2F} in Fig. 4 and Fig. 6 respectively) are set as 0.5. In contrast, for the external attack models, they are set as 0. Obviously, the insider attacks will change the transition matrix of the SMP models and result in the impacts on the MTTCs. The MTTC estimation is as follows. According to Q_1, the MTTCs of the attacks on the control center LAN are showed in Fig. 9. Corresponding to the 4 attacker levels, about 1039 days, 401 days, 163.5 days, and 44 days are needed respectively to realize the external attacks through the control center LAN. The MTTCs of the insider attacks through the control center LAN are 728, 269, 94, and 20 days respectively, which are much lower. This is because the insider attacks are easier and more likely to be successful than the external attacks with an extra transition probability. It can be seen from the results that the MTTC of insider attacks is much lower than that of external attacks. This is because shorter attack paths are needed for the insider attacks to realize a successful intrusion than the external attacks.

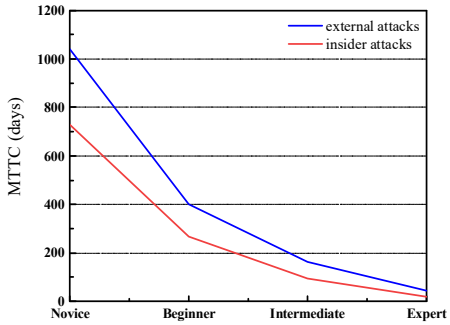

Figure 9. MTTC estimation of attacks through the control center LAN.

The MTTCs at the 4 attacker skill levels for the attacks through the corporation LAN are shown in Fig. 10. 734 days, 289.6 days, 120 days, and 39.3 days are needed respectively to complete a successful external attack on average. The MTTC values under different insider attacks' skill levels are only 441, 103, 52, and 9.8 days, which shows a similar trend with the previous case.

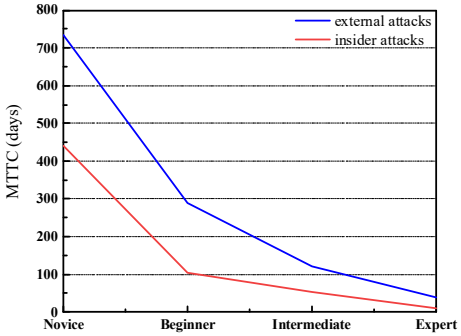

Figure 10. MTTC estimation of attacks through the corporation LAN.

B. MCS Results and Reliability Analysis

In Fig. 11 (a)-(d), the highest LOLP and EENS values of the attacks through both the control center LAN and corporation LAN come from the attacks at the expert level. Additionally, under the insider attacks, the LOLP and EENS are much higher than that in the results of the external attacks.

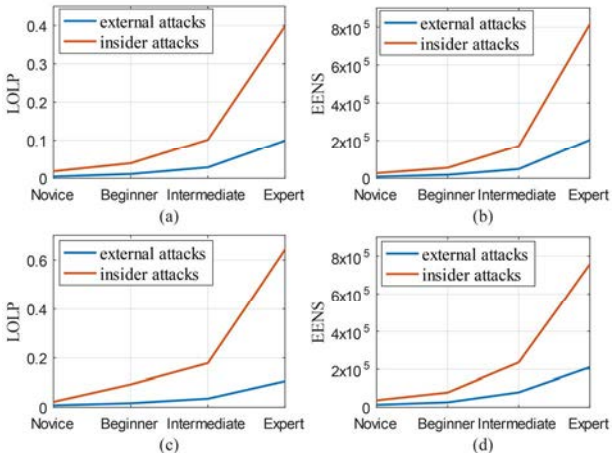

Figure 11. LOLP and EENS values of scenarios: (a) LOLP values of attacks on the control center LAN; (b) EENS values of attacks on the control center LAN; (c) LOLP values of attacks on the corporation LAN; (d) EENS values of attacks on the corporation LAN.

LOLP and EENS change with the variations of the transition probabilities of the attacks on the SCADA systems. Thus, the LOLP and EENS changes among different attack levels and paths. Shorter attacking processes are needed by the insider attacks to compromise the target as they have already certain privilege in the cyber systems. As a result, much higher LOLP and EENS are caused by the insider attacks, which means the system reliability is worse and the overall system is in a more dangerous situation when insider threats exist.

C. *Impacts of Lurking Threats*

In Fig. 12 shows the impacts of the lurking actions in the cases with the external attacks. It is shown that with the luring actions, the EENS of the power system increases for all the four attacker levels, especially the expert level. Further, the maximum lurking period limit also affects the results. In the four scenarios, the case when $T_{max} = 5\ days$ shows the highest EENS of all. Thus, with a proper lurking period limit, the damage of the attacks can be maximized by the lurking threats.

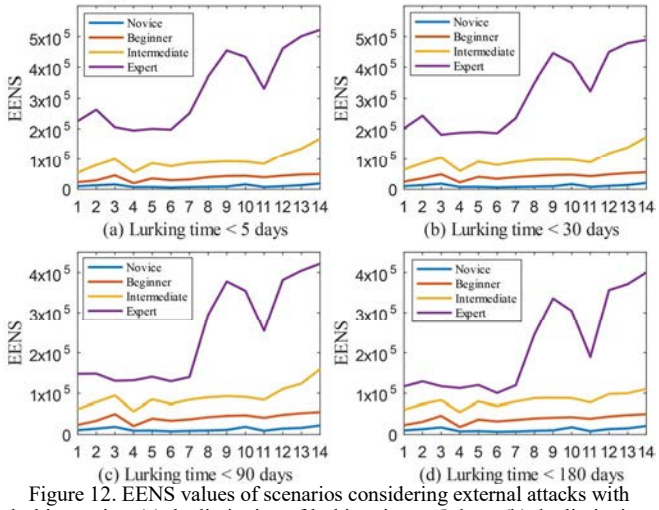

Figure 12. EENS values of scenarios considering external attacks with lurking actions(a) the limitation of lurking time = 5 days, (b) the limitation of lurking time = 30 days, (c) the limitation of lurking time = 90 days, (d) the limitation of lurking time = 180 days.

VI. Discussion and Conclusion

The modern power system is a complex system with CPS, and the SCADA systems are the critical components of the grid. The cybersecurity of the power grid is calling for attention. In this paper, the cyberattacks on the SCADA systems are modeled with SMP. To analyze the scenarios that attacks through the control center LAN and corporation LAN, the detailed SMP models are developed considering both the external attacks and insider attacks. The MTTC model is expounded and used to assess the time interval of successful intrusion into network components. Based on the IEEE RTS-96, the power system reliability considering the external attacks and insider attacks is evaluated. The LOLP and EENS values are calculated via MCS. It is shown that with the increase of vulnerabilities in the system, the values of MTTC decrease, and the LOLP and EENS values increase, which indicates that the reliability of the electric power system is worse. The comparison between the results of the external attacks and insider attacks indicates that insider attacks worsen the system reliability due to the shorter attacking paths. The results also show that the lurking threats of the attacks will affect the reliability of power systems. It should be noted that SMP is a flexible and general stochastic modeling tool which can be modified specifically to include different cybersecurity features in the analysis. For instance, SMP can be tailored to effectively model the security attributes of intrusion tolerant systems [16]. The states and transition probabilities in the proposed SMP models can be adjusted to reflect the enhanced strength of defense of the SCADA system if more advanced protection approaches are adopted. Thus, the proposed framework can efficiently accommodate additional cybersecurity features of the SCADA system in the analysis when necessary. In the future research, the actuarial implications of insider threats will be studied in the cybersecurity insurance premium estimations.

Acknowledgment

This work was supported in part by the National Science Foundation under Award ECCS1739485.

References

[1] Teixeira, A., Sandberg, H., & Johansson, K. H. (2010, June). Networked control systems under cyber attacks with applications to power networks. In *Proceedings of the 2010 American Control Conference* (pp. 3690-3696). IEEE.

[2] Ericsson, G. N. (2010). Cyber security and power system communication—essential parts of a smart grid infrastructure. *IEEE Transactions on Power Delivery*, 25(3), 1501-1507.

[3] Stamp, J., McIntyre, A., & Ricardson, B. (2009, March). Reliability impacts from cyber attack on electric power systems. In *2009 IEEE/PES Power Systems Conference and Exposition* (pp. 1-8). IEEE.

[4] Billinton, R. and Li, W. (2013). *Reliability assessment of electric power systems using Monte Carlo methods*. Springer.

[5] Stamp, J., Laviolette, R., Phillips, L., & Richardson, B. (2009). Impacts analysis for cyber attack on electric power systems (National SCADA Test Bed FY08). SAND2009-1673.

[6] Bruce, A. G. (1997, May). Reliability analysis of electric utility SCADA systems. In *Proceedings of the 20th International Conference on Power Industry Computer Applications* (pp. 200-205). IEEE.

[7] Byres, E., & Lowe, J. (2004, October). The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Kongress* (Vol. 116, pp. 213-218).

[8] Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, 21(6), 526-531.

[9] Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). 2005 CSI/FBI computer crime and security survey. *Computer Security Journal*, 21(3), 1.

[10] Leversage, D. J., & Byres, E. J. 2008. Estimating a system's mean time-to-compromise. IEEE Security & Privacy, 6(1), 52-60.

[11] Pyke, R. (1961). Markov renewal processes: definitions and preliminary properties. The Annals of Mathematical Statistics, 1231-1242.

[12] Limnios, N., & Oprisan, G. (2012). Semi-Markov processes and reliability. Springer Science & Business Media.

[13] Grabski, F., *Semi-Markov processes: applications in system reliability and maintenance*. Elsevier, 2014..

[14] Zhang, Y., Wang, L., Xiang, Y., & Ten, C. W. (2016). Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation. IEEE Transactions on Power Systems, 31(6), 4379-4394.

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

[16] Madan, B. B., Goševa-Popstojanova, K., Vaidyanathan, K., & Trivedi, K. S. (2004). A method for modeling and quantifying the security attributes of intrusion tolerant systems. Performance Evaluation, 56(1-4), 167-186.

[17] Verba, J., & Milvich, M. (2008, May). Idaho national laboratory supervisory control and data acquisition intrusion detection system (SCADA IDS). In *2008 IEEE Conference on Technologies for Homeland Security*, pp. 469-473.