Modeling and Simulation of Intelligent Substation Network Under Intrusion Attack

Xiaojuan Huang[1(✉)], Rong Fu[1], Yi Tang[2], Mengya Li[2], and Dong Yue[1]

[1] College of Automation, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
huangxiaojuannj@163.com
[2] College of Electrical Engineering, Southeast University, Nanjing 210023, China

Abstract. Recent advancement in the integration of power systems and information communication technology has brought the key concerns towards security operation of cyber physical power system. This paper focuses on realizing the unified system modeling under intrusion attacks and refining the attack effects on communication network by simulation research. We start this survey with an overview of the system operation and crucial intrusion attacks associated with operational security from fusion system perspective. A novel limited stochastic Petri net (LSPN) graph theory is introduced to establish the unified firewall protection system model of intelligent substation network. By proposing quantitative computational methodology of communication throughput variation, the potential consequence on the communication network is determined with information transmission constraints. The final test on IEEE-30 node power system illustrates the usefulness of the proposed model analysis. The research work would raise awareness of the cyber intrusion threats and provide the basis for security defense.

Keywords: Cyber physical system · Communication throughput variation · Intelligent substation network · Petri net theory

1 Introduction

The modern power systems are evolving to accommodate increased renewable sources of energy and active distribution systems with the integration of communication network overlay by information communication technology (ICT). This integration, however, makes facilities in open network [1] be more vulnerable for cyber attackers to invade system safety operation. Ukraine blackout accident [2] was a typical case of power outage with its secondary network suffering from network intrusion attack.

Significant research exists in modeling network intrusion attacks and assessing their impact on cyber physical system (CPS). Literature [3] attempted to characterize attacks on an Industrial Control System, where does not include several aspects of attacks such as start states, intents, and attack points. Generally, many approaches are to base attacks on traditional models derived from information and network security. Such as

M. Fei et al. (Eds.): LSMS/ICSEE 2017, Part I, CCIS 761, pp. 358–367, 2017.
DOI: 10.1007/978-981-10-6370-1_36

influences on the system stability with error data injection and various cryptographic attacks. Graph based modeling techniques are derived from research in network security [4, 5]. The attack graph model, which fully taking into account the network topology information, not only can visual the attack behavior of the infiltration process, but also make it more suitable for complex network attack modeling with the support of automated tools [6]. As a typical method, Petri net graph theory shows a great deal of flexibility and a limited stochastic Petri net (LSPN) can specific attack source propagation path to quantify the impact on the target system. Literature [7] proposed a concept about Petri-net-based CPS fusion modelling by implementing service specification into CPS service control flow. On the basis of studying the demand of active distribution system, a CPS control model and control method base on hybrid system were presented in literature [8].

In the evaluation of the security performance of CPS, development and implementation of SCADA cyber security testbeds are reported in [9–11]. Although the testbeds enable accurate simulations, the cost is high when to incorporate the entire cyber and power system models. In literature [12], the risk of attacking the system was obtained to evaluate successful attack probability by modeling the communication network and the power network respectively. The authors in [13] proposed the method that suggests the use of public key infrastructure technologies along with trusted computing elements, supported by firewalls, strong user and device authentication. Literature [14–16] analyzed the importance of cyber infrastructure security together with power grid security and the need for intrusion attack prevention. However, there is still a lack of methodologies to model the integration of CPDS for security assessment under cyber intrusion scenes.

In view of theoretical study, limited stochastic Petri nets are used in this paper to describe the attacked network states and attack information transmission process by using state transition graph. A unified firewall protection system model is established with highly abstraction of intrusion process and refinement of component constructions. The communication throughput variation is proposed based on the steady-state probability to quantify the impact on substation network when the corresponding power node loses efficacy due to intrusion attacks.

2 System Model and Network Attacks

Cyber Physical System (CPS) is built from, and depends upon the integration of computational algorithms and physical components [17, 18]. Figure 1 illustrates the communication architecture of the cyber-physical power system model, corresponding to the simulation environment. For the power system, the usual power model is showed. With regard to general communication infrastructures, they include wireless transmission networks, SCADA, control center, etc. Typical hardware is known as components in the control center, such as isolated firewall, engineering workstations, and various servers which can store and process the data. And the IEDs reside usually consist of the remote terminal units (RTU), advanced metering infrastructure and the programmable logic controller (PLC). The servers store and process the information

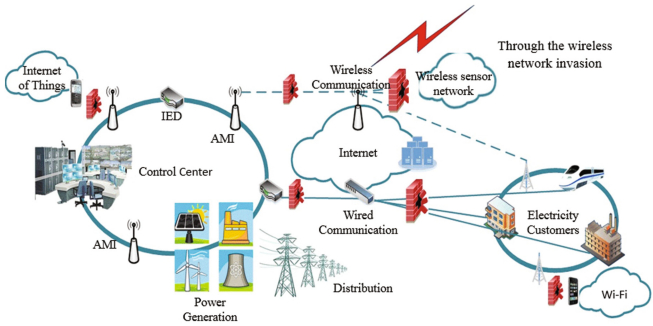

Fig. 1. Cyber physical power system communication infrastructures

sent from and to the RTUs, and the RTU or PLC controls the process of the field devices.

The Report No. 7628 《American Institute of Standards and Technology》 [19] points out that the three elements of cybersecurity are confidentiality, integrity and availability, commonly referred to as "CIA" security objectives [20]. Concerning CIA, private networks in power system are becoming more vulnerable to IP-based intrusion attacks with TCP/IP and Ethernet technologies.

At the beginning of the network operation, the initial measurements of state variables are collected by IEDs and then transmitted to the communication network at a certain interval time. After crossing the firewall detection process, the converted digital signals, such as IP address, then are transmitted to the control centre as the input values with TCP/IP communication protocol. Whenever control commands are sent by control centre after being processed by the state estimator to the actuators, the control variables are modified accordingly and the substation network shows a new operating state. For an IP-based intrusion attack, the proposed graph-theoretic system model in Fig. 2 enables the detailed firewall and password protection model analysis for information transfer process in the communication part to substation network. Such behaviors are studied based on the methodological modelling that provides the boundary inspection of malicious packets and intrusion attempts on each computer system.

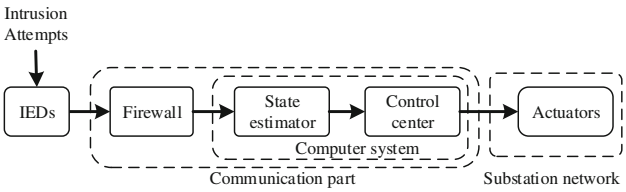

Fig. 2. Proposed intrusion model

3 Unified System Model Setup Under Intrusion Attacks

A. Limited Stochastic Petri Net (LSPN) theory

A basic LSPN consists of the following marks: places, tokens, black spots, transitions and the arc. The relationship between the local states is determined by arc. The directed arcs formed by the direct reachability relation are called the reachable marking states. In this paper, the performance analysis of the LSPN model is based on the isomorphism of its state space and Markov Chain (MC). Each place of LSPN is mapped to state space in MC and the rate of change in the reachability graph corresponds to the transition rate between MC states.

B. Component construction extensions

According to the cyber intrusion activity model introduced in Fig. 2, the modelling method is a high level of abstraction for the intelligent substation network. For the network infrastructures with point-to-point transmission that involve no monitoring capabilities, such as state estimate, IEDs and actuators in this paper, the probability of successful information transmission is considered to be 100%.

A successful intrusion attack means that necessary information needs to be acquired from different tools and resources to determine IP addresses in the network firewalls. So, an exact rule set for a secure firewall is very necessary. A mixed firewall filtering rules combining transport layer protocol type and packet IP address are shown in the following Table 1. The computer control center is generally the ultimate goal to realize data tampering. The password model is used to show the monitoring ability of the computer, which includes two parts: failed logon probability and the response rate.

Table 1. The specific firewall filtering rules

Rule	Protocol	S_IP	Action
1	TCP/IP	123.45.67.89	Accept I
2	TCP/IP	123.45.67.88	Accept II
3	TCP/IP	123.45.67.87	Accept III
0	UDP/IP	123.45.67.86	Deny

C. Unified model for substation level network

Based on properties of the transient and time delay transitions in a LSPN network, the system dynamic equilibrium can be achieved. With regard to unified network modelling, system elements can be grouped into substation nodes considering that a transmission line connects two substations. Such as the generators, DERs, transmission lines and load nodes, can be grouped into substation nodes. Based on the LSPN theory, the unified model is concerned with refined communication network components in B part. The state of the random process reflects the cyber intrusion abnormal activity which includes the malicious packet flow in firewall and the password login failure. As shown in the Fig. 3, the firewall protection model includes the firewall based on information detection technology and the realization of authentication login protection. The time transition is consistent with the time required by the attacker to obtain the

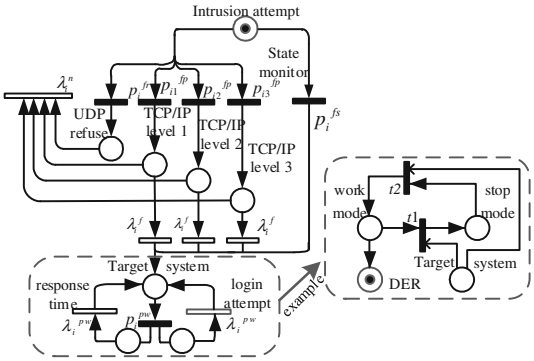

Fig. 3. Unified firewall protect model for substation network

system response. The tokens are used to represent the intrusion attempts after the attack begins. Especially for distributed energy resource (DER) node, we use LSPN theory to describe and model the switching process of the operating mode effectively that includes work and stop mode.

In the model, the places 'TCP/IP level 1, 2 and 3' represent the specific firewall filtering rules and the 'state monitor' means the information state monitoring function for malicious packets. Also, 'UDP refuse' means that the intrusion attempt is invalid with certain penetration probability. Each transient transition of the firewall can be calculated based on the firewall log [12]. The probability of passing the firewall through each rule is Eq. (1):

$$P_{i,j}^{fp} = \frac{f_{i,j}^{fp}}{N_{i,j}^{fp}},\ P_i^{fr} = \frac{f_i^{fr}}{N_i^{fr}},\ P_i^{fs} = \frac{f_i^{fs}}{N_i^{fs}},\ P_i^{pw} = \frac{f_i^{pw}}{N_i^{pw}} \tag{1}$$

Where $f_{i,j}^{fp}$ represents the frequency through the firewall. $N_{i,j}^{fp}$ is the total recorded number of the firewall rule j. f_i^{fr} is the number of rejected packets. N_i^{fr} and N_i^{fs} both are the total number of firewall records. f_i^{fs} is the number of packets directly through state monitoring. The firewall execution speed λ_i^f is the number of instructions executed per second. The average response speed λ_i^{nr} depends on the network transmission status which is estimated using the ping command. For computer system i, the transition probability which respectively represents the computer response time, login attempt and the final target system. The f_i^{pw} is the number of intrusion attempts. N_i^{pw} is the total number of records except the login attempt within a specific time interval which is regarded as an common user input error. The response speed λ_i^{pw} is the delay of the repeated login.

4 Quantitative Analysis on Substation Network

The proposed security assessment methodology can be summarized as a two-step approach. (1) The first step is to analyse the computer network topology in the system for deriving possible intrusion attack paths to the control centre. The net modelling with LSPN defines the intrusion scenarios and quantifies the steady invasion state probability. (2) In the second step, the consequence severity of the communication malfunctions of the substation nodes is determined with communication throughput variation. The integration of these two steps makes it possible to quantify the impacts caused by a potential cyber intrusion attack.

A. Quantitative computational theory

According to the analysis of communication network in cyber side, the intelligent devices integrated on the computer can be mapped to the communication data point. The steps a successful network intrusion attack must complete are: (1) obtain the availability of computer systems in the network; (2) attempt to invade the computer; (3) understand how to attack through the communication network with appropriate attack access point.

Generally, the state transition matrix W can be obtained through determining the instantaneous transition and the time delay transitions to describe the intrusion attack behaviours [12]. The Markov equilibrium equation is solved with corresponding Markov chain state. The specific steady-state probability equation is:

$$\begin{cases} \tilde{\pi} W = \tilde{\pi} \\ \sum\limits_{M \in T \cup V} \tilde{\pi} = 1 \end{cases} \tag{2}$$

Where T and V are the set of identities that transient changes and latency changes respectively. W represents a transfer matrix formed under different attacks. The vector π represents the embedded MC states.

B. Attack influence on substation communication network

The focused network intrusion attack refers to the behavior that across the firewall to reach the control center of the computer and make the corresponding target node fail to receive or transmit the correct information by the means of blocking the communication channel. Specifically, the attacker can control the packet size of the channel information transmission directly by changing the packet loss rate to congest network channel. To quantify the communication volume, the change of the channel throughput variation T is analyzed. While the data packets affected by the cyber intrusion attack become malicious, its packet loss rate is seen as the steady state probability value π. Thus, the communication throughput variation under the intrusion attack can be expressed as:

$$T = (1 - \frac{\pi_i N_2}{N_2 + N_1}) \times \frac{LR}{L + H} = (1 - \frac{\pi_i N_2}{1 + N_1 / N_2}) \times \frac{LR}{L + H} \tag{3}$$

Where π_i is the steady-state probability after intrusion attack, which can be obtained by Eq. (2). Attack ratio N_1/N_2 depicts the characteristics of the interference attack, which means how well the attacker knows about the substation network. L, H are respectively the length of the original data message and the preamble. The transmission rate is R. The smaller throughput variation, the stronger the operation robustness of the corresponding communication network in the cyber side.

5 Case Simulations and Implementation

In this section, we evaluate the throughout variation caused by the intrusion attacks on communication networks of the IEEE30 power system. Based on the system wiring diagram, the three-winding transformer bus lines 4, 12, 13 and 6, 9, 10, 11, and the double-winding transformer bus lines 27 and 28 are used as one substation. The system has a total of 24 communication network models. We define the intrusion attack process of each substation into three models: (1) Directly attack the substation network and attempt to reach the control center (as shown ⊞); (2) Attack through the distribution network or substation network (as shown ▨); (3) Jointly attack through the power plant process control network, distribution network and substation network (as shown ◯). Assume that there is two-way firewall isolation among the three networks, and only substation network can directly connect to the control center (Fig. 4).

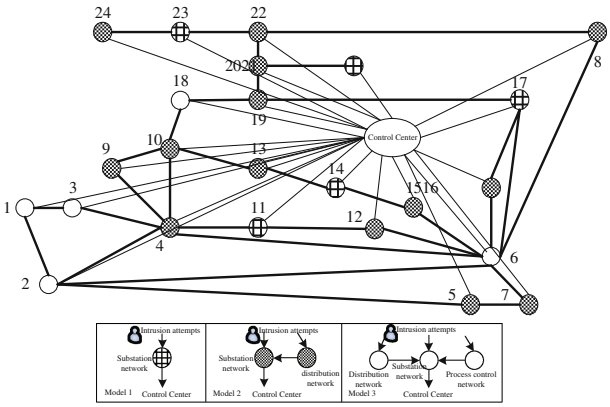

Fig. 4. The communication diagram of substation

According to the above Limited Stochastic Petri net (LSPN) theory, the transfer of tokens among states is similar to the Markov process. The penetration probabilities of firewall rules and packet information state monitors are assumed to be $P_i^{fp} = (0.0095324, 0.0181514, 0.0019415)$, $P_i^{fs} = (0.0083154)$ respectively. Also, the rejection probability of malicious packets is $P_i^{fr} = (0.71457)$. The logon failure probability for each machine is designed to be 10%. The computer response rates of computer and

firewall are set to be $\lambda_1^{pw} = \lambda_2^{pw} = 12 \times 10^{-10}$ and $\lambda_1^{f} = \lambda_1^{nr} = 63 \times 10^{-7}$. The above values are generated by a random number generator.

To support the intuitive judgment, the Table 2 shows the steady-state probability corresponds to the 3 kinds power communication network topologies with different intrusion access points. The values in lines 1 to 4 of the table represent the steady-state values of intrusion behaviors at different locations with different access points A and B. The steady state value of the external attack point is generally less than the internal intrusion scene. Because that the internal firewall is the first firewall from outside to the internal network, which makes the probability of successfully penetrating into the control center increases. The main factor affecting the internal attack vulnerability is the configuration of the communication network and more complex structure (model 3). Therefore, the network configuration and protection of the key nodes in the actual power grid can refer to the above situation.

Table 2. Transmission probability with different intrusion access points

	A (inside the firewall)			B (outside the network)		
	Node17 (model 1)	Node4 (model 2)	Node11 (model 3)	Node17 (model 1)	Node4 (model 2)	Node11 (model 3)
Substation intrusion	0.0000076	0.000796	0.00106	0.00019	0.00019	0.0002
Distribution network intrusion	–	0.00004	0.00442	–	0.0199	0.334
Process control network intrusion	–	–	0.00018	–	–	0.0133
Control center arrival	0.000792	0.000396	0.000176	0.0398	0.0199	0.0133

For the network structure model 3, the change trend of the communication throughput variation with the different attack access points is shown in the Fig. 5. The network intrusion attacks from outside the firewall have a strong effect on the throughput of data communications (strongly opposed to the other two models), and from within the firewall. When the node is attacked, its throughput is changed by the communication topology of the larger impact. Because the low probability attack inside the network makes the throughput of data transmission less affected by the network communication structure. The range of communication throughput changes in model 3 are more affected by the data transmission path and network topology model which indicates the more robustness of the corresponding communication network model.

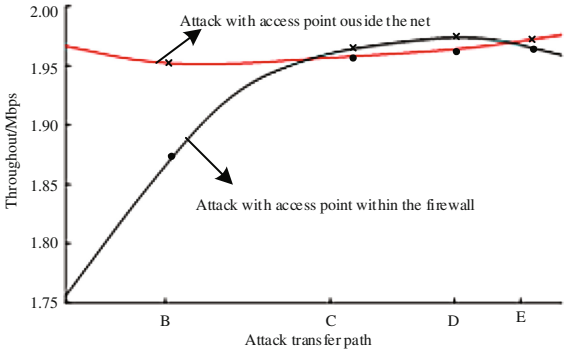

Fig. 5. Throughput variations in model 3

6 Conclusion

In this paper, the intelligent substation network modeling problem has been investigated considering the information transmission process in a cyber-physical system subject to effects of the intrusion attacks. Towards the fine modeling for network components equipped with different protection methods, here the firewall and computer login system protection methods were studied and a unified firewall protection communication model of substation network was established. In the case of distinguishing the three different levels of attack paths with two access points, the proposed analytical framework evaluated the steady-state attack probability of a successful attack based on LSPN graph theory. Then the communication throughput variation is proposed to quantify the impact on intelligent substation network. Moreover, the network intrusion attack definition, intrusion attack scenarios, specific throughput variation formula and its simulation results mentioned in this paper can provide a reference for identifying the vulnerability of substation network in the face of network intrusion attacks.

Acknowledgment. This work was supported by Key project of National Natural Science Foundation of China (Research on complex networked system architecture and system operating state security assessment with fault dynamic evolution mechanism) (Grant No. 61633016), a Communication and Network Technology National Engineering Research Center Open Fund project and an open project of National Key Laboratory (Research on operation security analysis and defense strategy of cyber physical system). We gratefully acknowledge the support from the Professor Fei Minrui of Shanghai University and Professor Hu Songlin.

References

1. Liu, Z.: Smart Grid Technology, 4th edn. China Electric Power Press, Beijing (2010). ISBN 9787512302235
2. Liang, G., Zhao, J., Weller, S.R.: The 2015 Ukraine blackout: implications for false data injection attacks. IEEE Trans. Power Syst. **40**, 149–151 (2016)

3. Berman, D., Butts, J.: Towards characterization of cyber attacks on industrial control systems: emulating field devices using Gumstix technology. IEEE Xplore, Resilient Control Systems (ISRCS), pp. 63–68 (2012)
4. Buford, J., Sanchez-Aarnoutse, J.C., Chen, T.M.: Petri net modeling of cyber-physical attacks on smart grid. IEEE Trans. Smart Grid **2**, 741–749 (2011)
5. Tran, B.N., Lakshminarayana, S.: SecureRails: towards an open simulation platform for analyzing cyber-physical attacks in railways. IEEE Xplore, pp. 95–98 (2016)
6. Hong, J., Panciatici, P., Liu, C.-C., Stefanov, A.: Intruders in the grid. IEEE Power Energy Mag. **10**, 58–66 (2012)
7. Ahmadon, M.A.B., Yamaguchi, S.: On service orchestration of cyber physical system and its verification based on petri net. In: 2016 IEEE 5th Global Conference on Consumer Electronics, pp. 1–4 (2016)
8. Liu, D., Li, Q-S., Wang, Y.: A hybrid system based CPS model and control of loads in active distribution network. In: 2016 IEEE International Conference on Power System Technology, pp. 1–8 (2016)
9. Adnan, R., Hahn, A., Higdon, M., Manimaran, G., Sridhar, S.: Development of the power cyber SCADA cyber security testbed cyber security and information intelligence research workshop. Oak Ridge National Lab, vol. 21, pp. 1–4 (2010)
10. Davis, C.M., Tate, J.E., Okhravi, H.: SCADA cyber security testbed development. In: 38th North American Power Symposium NAPS, pp. 483–488 (2006)
11. Xie, X., Hu, Y., Xin, Y.: Power information systems security: modeling and quantitative evaluation. In: Proceedings of IEEE Power Engineering Society General Meeting, vol. 1, pp. 905–910 (2004)
12. Liu, C.-C., Manimaran, G., Ten, C.W.: Vulnerability assessment of cybersecurity for SCADA systems. IEEE Trans. Power Syst. **23**, 1836–1846 (2008)
13. Metke, A.R., Ekl, R.L.: Security technology for smart grid networks. IEEE Trans. Smart Grid **1**, 99–107 (2010)
14. Jajodia, S., Noel, S.: Advanced cyber attack modeling, analysis, and visualization, Final Technical report AFRL-RI-RS-TR-2010-078, George Mason University (2010)
15. Hahn, A., Sridhar, S., Manimaran, G.: Cyber-physical system security for the electric power grid. Proc. IEEE **100**, 210–224 (2012)
16. Bompard, E., Napoli, R., Xue, F.: Vulnerability of interconnected power systems to malicious attacks under limited information. Eur. Trans. Electr. Power **18**, 820–834 (2008)
17. Ernster, T., Morris, T., Pan, S., Srivastava, A., Vellaithurai, C.: Modeling cyber-physical vulnerability of the smart grid with incomplete information. IEEE Trans. Smart Grid **4**, 235–244 (2013)
18. Liu, D., Lu, M.Y., Wang, X.S., Wang, Y.: Key technologies and trends of cyber physical system for power grid. In: Proceedings of the CSEE, vol. 35, pp. 3522–3531 (2015). (in Chinese)
19. National Institute for Standards and Technology (NIST): Guidelines for smart grid cyber security: vol. 3, supportive analyses and references: NISTIR 7628[S] (2010)
20. Li, M.Y., Rahman, S., Wang, Q., Tang, Y.: Framework for vulnerability assessment of communication systems for electric power grids. IET Gener. Transm. Distrib. **10**, 477–486 (2016)