IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 26, 2018, accepted June 27, 2018, date of publication July 13, 2018, date of current version June 24, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2855752

Security Assessment for Cyber Physical Distribution Power System Under Intrusion Attacks

RONG FU[1], XIAOJUAN HUANG[1], YUSHENG XUE[2], YINGJUN WU[1], YI TANG[3], (Member, IEEE), AND DONG YUE[1], (Senior Member, IEEE)

[1]College of Automation, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
[2]State Grid Electric Power Research Institute, Nanjing 211000, China
[3]School of Electrical Engineering, Southeast University, Nanjing 210096, China

Corresponding author: Rong Fu (furong@njupt.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61633016, in part by the Communication and Network Technology National Engineering Research Center Open Fund Project under Grant TXKY17006, and in part by the State Grid Technology Project of China (Research on the cooperative operation situation awareness and active defense method for Grid information physical system against network attack).

ABSTRACT A cyber physical distribution power system (CPDS) is a large and complex infrastructure that coordinates the cyber communication system and the physical distribution power system. Because of the increasingly advanced information communication technology, the development of cyber physical distribution power system has caused key cyber security issues related to system operation. This paper is focused on realizing a unified system attack modeling and security assessment of an active distribution power system. In this paper, first we present an overview of the system operation from the fusion system perspective. The significant effects of network intrusion attacks on operational security are evaluated. A new unified cyber physical network model is established using a limited stochastic Petri net graph theory that considers refined firewalls and password components. Then, a security effectiveness evaluation method is proposed to analyze channel throughput variation and system robustness. Overall CPDS security risk values are determined based on physical influence coefficients. Finally, simulations of an improved IEEE-33 bus distribution power system and security assessment under intrusion attacks are described. The research work could raise awareness of the cyber intrusion threats and provide the basis for security defense.

INDEX TERMS Cyber physical distribution system, cyber intrusion attacks, information security indices, limited stochastic Petri net theory.

I. INTRODUCTION

With the development of smart grid construction, information technology has penetrated all aspects of infrastructures and advanced applications in active distribution systems. The cyber-physical system (CPS) is characterized as a multi-dimensional heterogeneous complex system integrating multi-source power networks and multiple information networks using information and communication technology (ICT) [1]–[3]. The interaction between the power devices and ICT increases the interdependence of the distribution power system and cyber system. Although high-quality power supply services are thus realized, the factors causing uncertainty in the information network, such as delay, error, interruption, and network attack, clearly force the CPS system to handle more potential security risks and attack threats, and can even cause serious adverse effects to a nation's livelihood and social stability [4]–[6]. The Ukraine blackout accident, where a secondary network suffered a network intrusion attack, is a typical case of a power outage [7]. Intruders attacked part of the substation Supervisory Control and Data Acquisition (SCADA) system through malicious code, causing a widespread blackout in Ukraine, as well as power equipment failures.

Cyber security for the modern power system is an emerging area of research. Scholars have committed to conducting research of the influence that cyber intrusion attacks may cause on power system's operation [8]–[11]. They added the self-healing ability under attacks in order to find system vulnerabilities of smart grids [8]. Researchers proposed a fusion system based on different event-triggered hybrid control, distributed coordinated control and hierarchical hybrid control models to study the operation securities of cyber-physical microsystems considering network malfunction [9]–[11]. Clark and Zonouz showed that a complex invasion can indeed have an impact on the power system in adversarial environments by a power system case study [12]. They presented a formal definition of resilience and assessment metric and formulated cyber defense policies. Haller and Genge [13] focused on designing intrusion detection systems (IDS) to reduce the number of monitored parameters applied for interactive communication between cyber and physical side.

Recently, many scholars have studied the network graph theory as one of the most effective fusion modeling algorithms [14]–[16]. Huang *et al* proposed a new risk assessment based on Bayesian to quantify the impact of intrusion attacks on the Industrial Cyber-Physical systems, involving the attack information communication process and quantitative probabilities of attacked smart meters [17]. The Petri net, proposed by Carl Adam, is widely known as a useful modeling method for a complex hybrid system. Petri net-based fusion modeling was proposed where service specification was implemented in the CPS service control flow [14], [15]. To evaluate the security performance of CPS, Fu *et al.* [18] analyzed CPS information security risk assessment and index weight values by establishing a Petri net model. Besides, the Petri net theory and the game theory were combined to simulate offense and defense behaviors. quantitative models of CPS security analysis were established [19], [20]. Many researchers utilized the hierarchical Petri nets and stochastic Petri nets to enrich the attack model [21]–[24]. Ten *et al* presented a new unified formalism to model the CPS, including interconnections among cyber and physical components [25].

Due to the openness of modern information and communication technologies, information security has become an important issue that cannot be ignored in distribution power system operations. However, current research methods on CPDS cannot consider actual cyber-physical interaction characteristics. To test the communication failure impact on the power grid, CPS co-simulation testbed was analyzed [26]. False data injection attacks on CPDS was studied, but how cyberattacks spread is undesirable [27].

Previous research on the security risk assessment of attack state and attack process is not detailed, the modeling of the related intrusion attack propagation process is not perfect. What's more, the cooperative simulation platform experiment for distributed network physical system is rarely carried out.

In this paper, based on the Petri net quantization theory, a cyber intrusion attack model is proposed by applying the idea of hierarchical Limited stochastic Petri nets (LSPN). In particular, we have established a unified intrusion attack model for distribution networks in the CPDS environment. Improved LSPN is used to theoretically examine the attacked network states and the process of transmitting attack source information. A network attack model is proposed to realize refined device modelling, and a new LSPN-based unified CPDS model is realized. We also have conducted research on CPDS security assessment by proposing throughput and comprehensive security performance indicators. Specifically, this study is aimed at realizing unified modeling of integrated CPDS and security performance analysis of active distribution power systems based on the reachability states graph by the LSPN.

This paper is structured as follows. Section II presents an overview of the cyber physical distribution power system operation and intrusion attacks. Based on Petri net theory, a unified system model under cyber intrusion attacks and the proposed quantitative theory of communication network are presented in Sections III and IV, respectively. Section V introduces the methodology framework for eliciting the cyber security assessment indicator. In Section VI, the analysis method based on LSPN is verified by simulation results on the improved IEEE-33 bus active distribution power system with various attack scenarios. The conclusions follow in Section VII.

II. NETWORK INTRUSION ATTACK PROCESS

A CPS is an integrated system for controlling, maintaining, and monitoring physical components via cyber network transmission. As illustrated in Figure 1, the electricity is distributed between generators (both traditional power generators and distributed generation sources) and terminal users (industrial, commercial, and residential consumers). Meanwhile, the bi-directional information flow is used to control intelligent appliances at the consumer side, which can reduce energy consumption and the consequent expense, and as a result, increase the system's reliability and operation. The general architecture for smart grid communication infrastructures includes wide area networks (WANs), neighborhood area networks (NANs), SCADA, ICT devices, control centers, and substation automation integration systems [28].

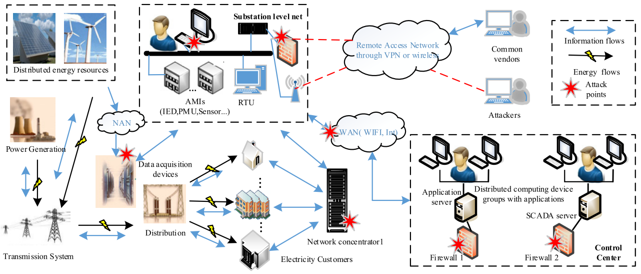


FIGURE 1. Cyber physical system infrastructures.

The SCADA system is used to monitor and control the components distributed from the control center to the substations. Typical hardware comprises components in the control center, such as firewalls, engineering workstations, and various servers that can store and process the data. The hardware also includes communication devices, such as radio, telephone lines, and cables, which can be used as the communication channels. The ICT devices, which realize the interactive operation between a power system and a SCADA system on the network side, consist of remote terminal units (RTUs), sensors, actuators, programmable logic controllers (PLCs), etc. The servers store and process the information sent from the RTUs, and the RTUs or PLCs control the processes of the field devices. The communication hardware allows information to be transmitted between the control center and substation network. For example, the network sensors collect the state variables of a power system, such as voltage and current, and these variables are then transmitted from the RTU to the control system. The RTUs are also responsible for the operation of actuators using the received control commands to adjust the topology and parameters of the dynamic system. The physical systems of generation, transmission, and distribution are interconnected through the transmission lines and substations. The crucial calculations at the control center include status estimation (SE) and optimal power flow (OPF). Moreover, the advanced metering infrastructure (AMI) and PLC have been developed to increase the efficiency, flexibility, and utilization of distributed and localized computations.

ICT devices allow the substation network to communicate with the control center, and the collected field data can be transmitted to the control center based on the ICT interface. By transferring information through the human-machine interface, the SCADA system enables the operator to monitor or control the entire power system operation at the control center. DERs allow the customer-side power generation and management to be more flexible and reliable, reshaping the existing patterns of power flows from unidirectional to bidirectional. Therefore, an AMI system with millions of smart meters in distribution power systems provides innovative two-way real-time communications in smart grids, which can benefit from demand response, energy management, and consumer participation.

Security challenges in the smart grid are on the rise in both the physical and cyber spaces [29]. A virtual private network (VPN) constitutes a network security technology used to form connections with other corporate networks. Remote login programs in the VPN provide the capability to control other machines within the networks. Moreover, intrusion detection systems (IDSs) and password protected firewalls have been deployed against external intrusions [30]. Convenient access to Internet resources and online search capabilities in the open communication network makes it a target for network hackers.

Report No. 7628 of the American Institute of Standards and Technology (NIST) noted that three main elements of cyber security are confidentiality, integrity, and availability [31]. They are commonly referred to as the *Confidentiality*, *Integrity* and *Availability* (CIA) security objectives. In an active distribution power system, when *Availability* is destroyed, failures in data transmission and other issues occur to cause power supply failure and cascading, which has tremendous effects on the system securities [32].

In line with the aims of CIA, various network intrusion attacks against a power system can be divided into three types: 1) password crack attacks and malware installation behaviors, which are intended to obtain information confidentiality. 2) false data injection (FDI) attacks, man-in-the-middle (MITM) attacks, replay attacks, etc., which can destroy data integrity. 3) Denial-of-service (DoS) attacks, black hole attacks in wireless sensor networks, and so on, which threaten communication availability. These attacks are based primarily on using the vulnerabilities and security deficiencies in the network infrastructure without permission. With available information and tools, there are several possible means of perpetrating network intrusion attacks: 1) VPN, 2) dial-up connections, 3) wireless connections, and 4) remote logon programs.

In CPDS, SCADA systems are currently based mainly on open and networked architectures. As a result, private networks in distribution power systems are becoming more vulnerable to IP-based intrusion attacks with TCP/IP and Ethernet technologies. At the beginning of the system operation, initial measurements of state variables are collected by sensors and then transmitted to the communication network at a certain time interval Δt. Usually, analog digital converters in the network are used to convert continuous state variable signals into the corresponding discrete-time digital signals, such as IP addresses. The digital signals are sent across the firewall detection process and then transmitted to the control center as the input values for the SCADA system using the TCP/IP communication protocol. Whenever control commands are sent by the system operator after being processed by the state estimator to the actuators, via SCADA, the control variables are modified accordingly. Thus the receiving distribution power system works in a new operating state. It shows that the coupled system goes into an iterative loop, whereas the modification of the control variable values activates the power flow computation.

Theoretically, to perpetrate an IP-based intrusion attack, the intruder uses the controlled system resources to damage the normal operation of the system equipment, such as the state estimator and the autonomous control function of the substation, and achieves the implementation of target protocols in Figure 2. The combination from substation level networks to other networks allows various attack scenarios with access points. The proposed model could depict the intrusion attack process for refining the firewall and password protection models. Furthermore, the consideration of the firewall and computer logon services is inspired by the necessary steps of invasion.

III. UNIFIED MODEL SETUP

In this section, first the LSPN theory is introduced to qualitatively present the innovative network intrusion attack modeling method. Then, the transition activity of the cyber intrusion

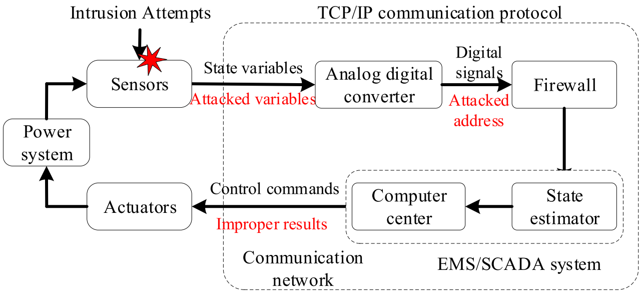


FIGURE 2. Intrusion attack process.

attack is considered in order to build a refined communication network model. Therefore, the property analysis of system modeling is presented and a unified CPDS model is established.

A. TARGET INTRUSION PROCESS

The LSPN is used to model an information processing system with concurrent, asynchronous, distributed, parallel, uncertainty, or random information [33], [34]. It can also evaluate and improve the system by analyzing the dynamic behavior information of the system structure. The dynamic behavior of the LSPN is a local state transition, which involves only the change in the transition state based on the arc connection relation. The occurrence of transition is a stochastic process that considers the time required for completing transition. Moreover, its duration obeys a certain probability distribution. The performance analysis of the LSPN model is based on the isomorphism of its state space and Markov chain (MC). Each location on the LSPN is mapped to its state space in the MC. The start rate of the transition in the reachability graph corresponds to the transfer rate between the MC states.

According to the cyber intrusion activity shown in Figure 2, the exact attributes of the network key components are determined according to the transfer process of the attack source, and the special properties of the system modeling method based on the LSPN are analyzed. This can provide the theoretical basis for the unified modeling of the cyber physical distribution power system.

As intrusion behaviors change with the evolution of security vulnerabilities, it may not be practical to enumerate specific intrusion steps. To detect an anomaly resulting from an intrusion attempt, modeling of the malicious packets flowing through boundary perimeters and the records failed logons to the computer center are necessary to show whether the attack attempts are successful. As this modeling method is a high abstraction for the cyber physical distribution power system, the probability of successful information transmission through the analog digital converter, state estimate, sensor, and actuators is considered to be almost 100% for network infrastructures with point-to-point transmission.

B. FIREWALL PROTECTION RULE

With rapid development of computer network technology, the processing and transmission of information has transcended the limitations of time and region. The firewall is an important component of the network security that is used to protect the network. Further, to perpetrate a successful intrusion attack, the attacker must acquire the necessary information from different tools and resources to determine the IP addresses in the networks. Therefore, an exact rule set is essential for achieving a secure firewall. According to the common security policy, the specific firewall rules for the distribution power system can be implemented according to the priority of the communication protocol level in the case of rule-making priorities.

Considering the reliability of the TCP transmission protocol, a mixed rule set is used to combine a transport layer protocol type and packet IP address to optimize a single rule set and improve filtering efficiency. Because of the diversity of network devices in the cyber network, in view of intrusion attacks on the network side, various protection rules configured by the firewall are considered protecting: 1) Web server class loophole applications, 2) file class vulnerability applications, 3) ActiveX plug-in control class loopholes, and 4) the information refused by a class vulnerability application. The HTTP and FTP protocols are used to transmit communication information. The firewall log records show different types of vulnerability attacks. Specific firewall filtering rules are shown in Table 1.

TABLE 1. Specific firewall filtering rules.

Rule	Protocol	Protection rules	Action
1	HTTP	Protect the Web server class loophole application	Accept I
2	FTP	Protect the file class vulnerability application	Accept II
3	HTTP/ FTP	Protect the ActiveX plug-in control class loopholes	Accept III
4	HTTP/ FTP	Protect the information refused by a class vulnerability application.	Deny

C. COMPUTER PASSWORD PROTECTION RULE

For the intrusion attacker, the computer center is generally the ultimate goal for the purpose of realizing data tampering and then gaining access to economic benefits, etc. Penetration attempts based on repeatedly failed logons without establishing authentication credentials are mainly evaluated. The computer processes for storing these failed logon trials, and other security-relevant logons, are embedded in the computer operation system for analysis. To describe the computer operation, the model includes two parts: failed logon probability and the response rate. The probability expresses the number of failed logon trials. The response rate is regarded as the central processing unit (CPU) clock rate, which represents the performance of a computer system.

D. UNIFIED MODEL FOR CYBER PHYSICAL DISTRIBUTION SYSTEM

With the above Petri net theory modeling, the following related special properties are satisfied to realize the network intrusion attack modeling in the distribution power system:

1) The LSPN is an extended Petri net, and each transition is associated with a start rate, which means the average start number of transition events at a certain time under the effective conditions, namely, the number/unit time.

2) Assuming that the LSPN identifier is reversible, the performance of the system is analyzed based on the MC stable state probability system. Since LSPN is a dynamic process, each state has a certain possibility. When the time is infinite, the system achieves a dynamic equilibrium. Then, the state probability is the stable system state probability in this time.

Thus, an LSPN network consists of two types of transitions: instantaneous transition and delay transition. The instantaneous transition gives the relevant probability value and the delay transition gives the relevant delay time. If there is a number of transitions constituting an enforceable transition set O in an identifier M, there are two cases:

1) If set U is composed of all time transitions, the implementation probability p of transition T_T at any time is

$$p(T_{Ta}) = \lambda_a / \sum_{T_{Tk} \in U} \lambda_k \quad T_{Tv} \in U \tag{1}$$

where λ_a, λ_k are the start rates of time transition a and k, respectively.

2) If set U, with a number of instantaneous transitions and time delay transitions, or only with instantaneous transitions, can be implemented, the specific choice is executed according to the corresponding probability distribution function.

In the modeling process, it is necessary to determine, for each substation node, whether the communication network with ICT devices acquires state variables or sends control commands in the cyber side. Based on the LSPN theory, the communication network is modeled to describe the state of the random process, and the cyber intrusion attack is estimated according to abnormal activity, which includes malicious packet flow in the firewall and password login failures. Thus, a unified system model composed of a firewall protection model and interactive process is formed to analyze malicious intrusion activity. As shown in Figure 3, the model includes the firewall i based on information security defense technology and the realization of authentication login encryption protection. The time of the transition delay is consistent with the time required by the attacker to obtain the system response. Tokens are used to represent the intrusion attempts after the attack begins.

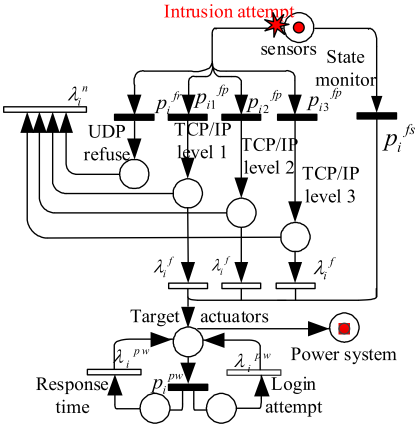


FIGURE 3. Firewall protect model for the CPDS.

In the model, the locations of "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. These components indicate that the intruder can choose four possible paths respectively corresponding to different penetration probabilities p to cross the firewall i. Further, "UDP refuse" means that the intrusion attempt is invalid with a certain penetration probability, because it is blocked by the firewall. Each transient transition of the firewall in the firewall protect model adds a firewall penetration probability, which can be calculated based on the firewall log [16], [25]. This means that when a network intrusion attack occurs, the probability p of firewall penetration for each rule is

$$p_{i,j}^{fp} = \frac{f_{i,j}^{fp}}{N_{i,j}^{fp}}, \quad p_i^{fr} = \frac{f_i^{fr}}{N_i^{fr}}, \quad p_i^{fs} = \frac{f_i^{fs}}{N_i^{fs}} \tag{2}$$

where $f_{i,j}^{fp}$ represents the transition frequency of the firewall, $N_{i,j}^{fp}$ is the total recorded transition times 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, and f_i^{fs} is the number of packets passing directly through the state monitor. The firewall execution speed λ_i^f is the number of instructions executed per second. This speed can be used to estimate the rules validation and the time required to pass through the firewall. The average response speed λ_i^{nr} depends on the network transmission status, which is estimated by the connection trials.

Equation (2) concerns only malicious packages that use a false IP address to cross the firewall. When the firewall has been crossed, the corresponding description of the password login process is shown, including the remaining three locations. They respectively represent the computer response time, login attempt, and the final target system, i.e., the control center. For any computer login authentication interface, an intrusion attack attempting to cross a firewall is represented as a continuous transition probability. To build a firewall protection model, the ability to lock an account after a limited number of attempts can be simulated by initializing the number of N tokens, i.e., the password login threshold limit. In Figure 3, the transition probability p_i^{pw} can be estimated by

$$p_i^{pw} = \frac{f_i^{pw}}{N_i^{pw}} \tag{3}$$

where f_i^{pw} is the number of intrusion attempts, N_i^{pw} is the total number of records, except a repeated login attempt within a specific time interval, which is regarded as a result of common user input error. The response speed λ_i^{pw} is the delay of the repeated login. It can estimate the time of the next attempt, which is assumed to be an automatic process achieved by certain tools.

In particular, when the power node is a DER in an active distribution power system, it may be an energy storage device, wind turbine (WT), solar energy installation, or micro gas turbine. It is considered that different DER units can switch their operation mode according to the different trigger conditions. Similarly to the above system modeling, we use LSPN theory to describe and model the switching process of the operating mode effectively. First, we establish the general communication model of the DER unit. It is divided into a work and a stop mode. In addition, the initial operation mode of each DER unit that has suffered a network intrusion attack is marked as a token, and the black spots are described as discrete positions. The protection model based on firewall equipment is shown in Figure 4.

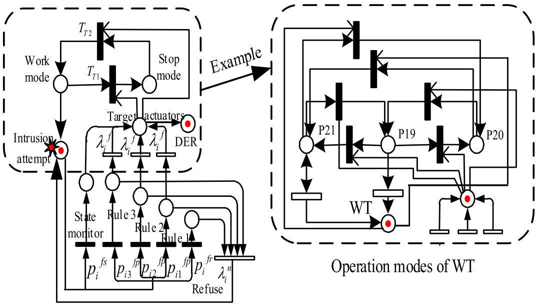


FIGURE 4. Unified firewall protect model with DER node.

The transition conditions T_{T1} and T_{T2} indicate that the malicious packet crosses the firewall and triggers the operation mode of the DER to change between the normal operating mode and stop mode. An example of the operation modes, when the DER node is a WT, is shown in the virtual box of the Figure 4. When the wind speed v is higher than the rated wind speed v_R, which means $v \geq v_R$, the WT works in the constant power output (CPO) mode. When the wind speed satisfies $v < v_R$, the operation mode of the WT is maximum power point tracking (MPPT). If the wind speed is $v \notin (v_{\min}, v_{\max})$, the WT is switched to the stop mode. These modes are represented by P19,P20 and P21 respectively.

IV. QUANTITATIVE ANALYSIS

A. COMPUTATIONAL THEORY

According to the analysis of the communication networks on the cyber side, the intelligent devices integrated on the computer can be mapped to the communication data points. The steps that a successful network intrusion attack must complete are: 1) obtain the availability of computer systems in the network, 2) attempt to invade the computer, and 3) understand how to attack through the communication network using the appropriate attack access point. The reachability states are shown in Figure 5, where the M labels in the circles represent the reachable states. We can acquire eight reachable states from the top of the graph by moving the token. The transition probability and rate are on an arc.

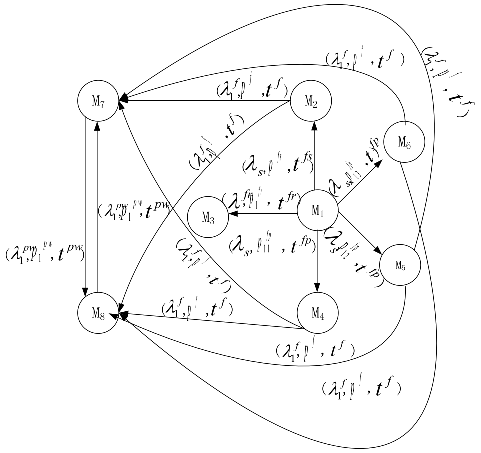

M1
M2
M3
M4
M5
M6
M7
M8
$(\lambda_1^f, p_1^f, t^f)$
$(\lambda_s, p_{13}^{fp}, t^{fs})$
$(\lambda_1^{fr}, p_1^{fr}, t^{fr})$
$(\lambda_s, p_{11}^{fp}, t^{fp})$
$(\lambda_s, p_{12}^{fp}, t^{fp})$
$(\lambda_1^{pw}, p_1^{pw}, t^{pw})$

FIGURE 5. The reachability states graph of the LSPN.

In Figure 5, $\prod = \{\lambda, p, t\}$ is defined to describe the process of the states change, λ represents the firewall execution speed, p represents the transition probability, t represents the execution time. The response time t^{pw} is the delay of the repeated login, t^f is the firewall execution time, p^f is the probability of entering the password model.

In LSPN, the transition probability can be represented by matrix $\mathbf{W}$ that includes the instantaneous transition and the time delay transition. The instantaneous transition gives the relevant probability value, and the time delay transition gives the relevant delay time. Each column corresponds to the five labels M_1, M_2, M_4, M_5, M_6 caused by the instantaneous transitions and three labels M_3, M_7, M_8 generated by time delay transitions. The first column in $\mathbf{W}$ represents transfer behavior from M_1 to instantaneous transitions M_1, M_2, M_4, M_5, M_6 and time delay transitions M_3, M_7, M_8.

LSPN is an extension of the basic Petri net, and each transition is associated with a start rate (indicating the average number of starts per unit time under effective conditions, i.e. times/unit time). The basic Petri net can be seen as a special case where all transition start with delays being zero. The difference is that all valid transitions in the basic Petri net can be initiated, whereas in LSPN, there are a few possibilities for a transition with a large effective transition start rate, and a small possibility of a transition with a small start speed.

In general, the LSPN tokens are limited and the labels are all reversible. In this way, the LSPN analysis problem can be transformed into the Markov chain based steady-state probabilistic system performance analysis. As LSPN is a dynamic process, the possibility of each state is certain. When the time becomes infinity, the system will reach a dynamic equilibrium. At this time, the probability of the system state is the so-called stable state probability.

The state transition matrix is used to describe the intrusion attack behaviors. Consider a discrete time version of this LSPN model:

$$\tilde{\pi}_{k+1} = \mathbf{W}\tilde{\pi}_k \tag{4}$$

where $\tilde{\pi}$ is the probability vector, k is the time step and matrix $\mathbf{W}$ represents a transfer matrix formed under different attacks.

Each transition in the system is constrained by the place with a specific probability, and the Markov equilibrium equation is solved to determine the corresponding Markov chain state, which is the steady state probability of the number of variations. Then the specific steady-state probability equation is:

$$\tilde{\pi}\mathbf{W} = \tilde{\pi}\mathbf{I} \tag{5}$$

It represents that $\tilde{\pi}$ is the embedded MC state gained by the LSPN, where $\sum\limits_{M\in M_q\cup M_u} \tilde{\pi} = 1$, M_q and M_u are the set of identities of transient changes and latency changes, respectively. As in the Figure 5, $q = \{1, 2, 4, 5, 6\}$, $u = \{3, 7, 8\}$.

The identification generated by an instantaneous transition requires the time to be 0, which simplifies matrix $\mathbf{W}$ to a matrix $\mathbf{W}'$ that contains only the number of time delay transitions. In order to reduce the embedded MC state transition probability matrix $\mathbf{W}$, the $\mathbf{W}'$ matrix is

$$\mathbf{W}' = \mathbf{F} + \mathbf{E}(\mathbf{1} - \mathbf{C})^{-\mathbf{1}}\mathbf{D} \tag{6}$$

where matrix $\mathbf{C}$ is expressed as the label moved from instantaneous transition to instantaneous one, matrix $\mathbf{D}$ is expressed as the label moved from instantaneous transition to delay transition, matrix $\mathbf{E}$ is expressed as the label moved from delay transition to instantaneous one, and matrix $\mathbf{F}$ is expressed as the label moved from delay transition to delay one.

The linear equation (5) is solved to obtain $\tilde{\pi}$, which means that the steady-state probability π is the weighted sum of the required duration time of each corresponding identifier. In the LSPN system, if $M_j \in M_q$, the probability that information transfer process reaches the steady state is zero; if $M_j \in M_u$, probability π can be calculated by

$$\pi = \frac{t(M_a)}{t_c(M_j)} \tag{7}$$

where $t(M_a)$ is characterized by the time spent in M_1 state when a random process to M_j state is required. $t_c(M_j)$ is the average cycle time in M_j state.

B. INFLUENCE ON COMMUNICATION NETWORK

The proposed network intrusion attack refers to the behavior that it can cross the firewall to reach the control center of the computer and make the corresponding target node fail to receive or transmit information by blocking the communication channel. For example, in a typical DoS attack, the attacker disturbs the normal communication between the network nodes by injecting signals to broadcast meaningless messages in the communication channel. To simulate the real communication network better, it is assumed that each network node can generate, transmit, and receive packets. Specifically, the attacker can directly control the packet size of the channel information transmission by changing the packet loss rate in order to congest the network channel of the destination node.

To quantify the communication volume in the communication network of power node i, the change in the channel throughput variation T is analyzed when the data collected from the node $i$are transmitted directly to the control equipment. In the security period, the packet loss rate is within the acceptable range by default. Packets N_2 can be transmitted successfully. When the data packets N_1 affected by the cyber intrusion attack become malicious, the packet loss rate is similar to the steady state probability value π. Thus, the throughput variation T_i under the intrusion attack can be expressed as

$$T_i{=}(1\text{-}\frac{\pi_i N_2}{N_2 + N_1}) \times \frac{LR}{L+H}{=}(1\text{-}\frac{\pi_i N_2}{1 + N_1/N_2}) \times \frac{LR}{L+H} \tag{8}$$

where π_i is the steady-state probability after an intrusion attack using the appropriate attack access point, which can be obtained by the embedded MC steady-state equation based on Petri net theory. Attack ratio N_1/N_2 describes the characteristics of the interference attack, which means how the attacker knows about the substation network and how skillful the attacker is. L, H are respectively the length of the original data message and the preamble. R is the transmission rate. The smaller the throughput variation, the stronger the operation robustness of the corresponding communication network on the cyber side.

V. CYBER SECURITY ASSESSMENT

The purpose of the proposed methodology is to model intrusion attack behaviors and evaluate the potential consequences of a network intrusion attack in the physical distribution power system through the cyber network. In this section, the framework of our security assessment method for distribution power system is in general divided into two parts: calculation of the communication throughput variation in the unified system model and calculation of the optimal power flow. The unified system model defines the intrusion scenario and the states. Calculation of the optimal power flow is used to evaluate the distribution power system operation state.

A. METHODOLOGY OVERVIEW

The flow chart depicted in Figure 6 illustrates the simulation procedures based on the proposed security assessment method. The security assessment methodology can be summarized as a two-step approach. 1) In the first step, the cyber network topology in the system for deriving possible compromise paths of network intrusion attacks to the control center is analyzed. The net modeling with LSPN defines the intrusion scenarios and quantifies the steady invasion probability. 2) In the second step, the consequence severity of the communication malfunctions of the power nodes with security efficiency indices is determined. The integration of these two steps allows the effects of a potential cyber intrusion attack to be quantified.

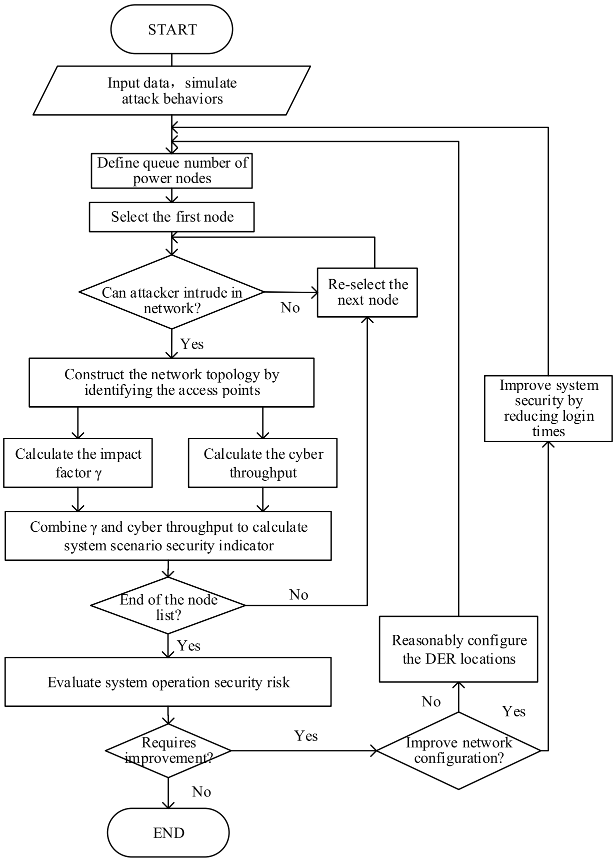

START
Input data，simulate attack behaviors
Define queue number of power nodes
Select the first node
Can attacker intrude in network?
No
Re-select the next node
Yes
Construct the network topology by identifying the access points
Calculate the impact factor γ
Calculate the cyber throughput
Combine γ and cyber throughput to calculate system scenario security indicator
End of the node list?
No
Yes
Evaluate system operation security risk
Improve system security by reducing login times
Reasonably configure the DER locations
No
Yes
Requires improvement?
Yes
Improve network configuration?
No
END

FIGURE 6. Flowchart for proposed security assessment framework.

B. COMPREHENSIVE SECURITY EFFICIENCY INDEX

Traditional power or communication vulnerability calculation methods have been widely studied, including those for determining the safety and stability of power systems and for real-time reliability analysis of communication systems. After determining the type and impact of the communication interruption, certain indices can be used to evaluate the effect on the power operation, such as the system expected load reduction, and the system stability margin. In general, the influence coefficient γ is proposed to characterize the influences on the stability of the whole system after the failure of an attacked node due to a communication network malfunction. When the corresponding node loses efficacy because of a cyber intrusion attack, the loss load of the system is represented by P_{LOL}. The calculation formula of the influence coefficient γ is

$$\gamma = \frac{P_{LOL}}{P_{Total}} E \tag{9}$$

where P_{Total} is the total load of the whole system. The system load level E represents the critical state of the system's stable operation under the influence of the failed node. It can be calculated through the optimal power flow.

Moreover, a security efficiency indicator is also proposed to integrate the topology and operational status better, and the effect of cyber intrusion attacks on the operation stability in the distribution power system:

$$\begin{aligned} V(i) &= \max\{V(i_1), V(i_2)...V(i_k)\} \\ V(i_k) &= \sum_{x\in S} \pi_x \times \gamma_{nodex} + \sum_{y\in S} \pi_y \times \gamma_{CCeny} \quad k = 1, 2, 3...K \end{aligned} \tag{10}$$

$$T_x = (1 - \frac{\sum_{x\in S} \pi_x}{1 + N_1/N_2}) \times \frac{LR}{L+H}, T_y = (1 - \frac{\sum_{y\in S} \pi_y}{1 + N_1/N_2}) \times \frac{LR}{L+H} \tag{11}$$

where K is the number of attack scenes to be evaluated and S is the set of initial points of the network attack. $V(i)$ is the maxim of the security efficiency indicators in different attack scenes with the attacked node i. T_x is the throughput variation affected by the attack steady-state probability π_x with a specific attack access point x. x, y respectively represent the communication network of the power node and control center of the computer that has been invaded. γ_{nodex} and γ_{CCeny} are respectively the influence coefficients of the firewall protection equipment and control center connected with the attacked node i.

The system refers to the wide-area communication network between the control center and the substation node network. Assuming that the attack scenarios performed by the substation-level network are independent of each other, the initial points of the network intrusion attack are not related. For a substation node network, an attack scenario can be defined as the steps of many attack attempts initiated inside the firewall or outside the network with the aim of penetrating the control center in the CPDS. The initial point provides the entry for the intruder to the cyber network. The security efficiency assessment formula in scenario k gives its potential influence, which is the weighted sum of the potential hazards of set S.

VI. PERFORMANCE STUDY

In this section, the security operation on the CPDS is evaluated. Different simulation experiments are described, and the simulation results are then analyzed.

A. SIMULATION EXPERIMENTS

In the IEEE-33 bus active distribution power system, DERs are added as DER 1, 2, and 3 in Node 1, Node 11, and Node 17, respectively. Moreover, to improve the characteristics of the active distribution power system, three DERs are set to supply as much energy as possible. DER 1, 2, and 3 all use PQ mode to control the rated power, which is 1 MW,

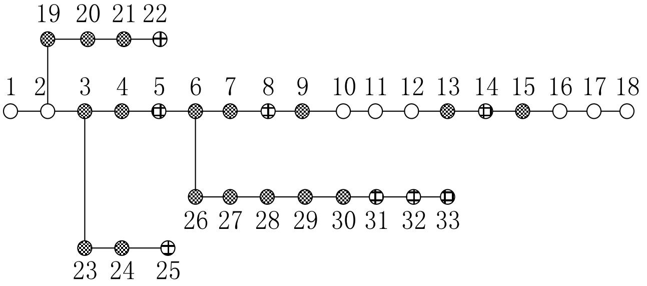


FIGURE 7. Illustration of improved IEEE-33 bus active distribution system architecture.

2 MW, and 2 MW, respectively. Each node has its substation network, and therefore, its firewall protect model is provided by LSPN.

The processes of information communication of the related nodes are defined by three types of modes: Md. 1, where the communication information of a node directly transfers from the substation level network to the control center by the LSPN communication model (represented by ⊕ in Figure 7); Md. 2, where the communication information can choose either the substation level or the distribution load network, and then reach the control center (represented by ◍ in Figure 7); and Md. 3, where the communication information is transmitted via the substation level, distribution load network, or DER network transmission to the control center (represented by ○ in Figure 7). There are three possible access points to the network to be established.

The cyber network connection diagram is shown in Figure 8. There is two-way firewall isolation between the WT DER network, substation level network, and distribution load network. Only the substation level network directly connects to the control center with the firewall model. All the regional networks are assumed to use the same firewall rules and computer password authentication.

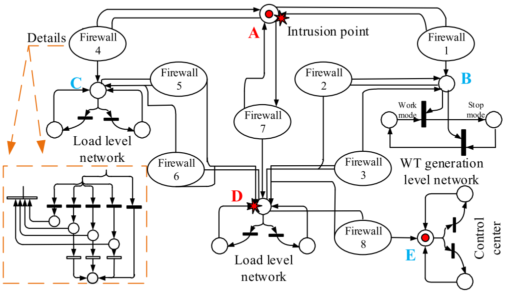


FIGURE 8. Cyber network connection diagram in the CPDS.

A cyber physical simulation platform is built by using Avalanche attack testing devices to exploit the vulnerabilities under intrusion attacks. As shown in Figure 9, the Avalanche testing device connects with the firewall through switches and initiates various vulnerability attacks. The data acquisition request is sent to the measurement terminal from the simulation master station, and the real-time data are uploaded through the firewall from the measurement terminal to the master station.

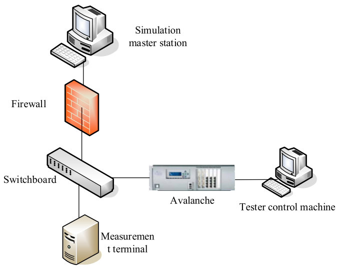


FIGURE 9. Topology of the attack experiment.

The main steps of the experimental test are as follows:

1) Configure the firewall vulnerability rules;

2) Attempt to use the firewall for the server operation class and application service class vulnerability scanning;

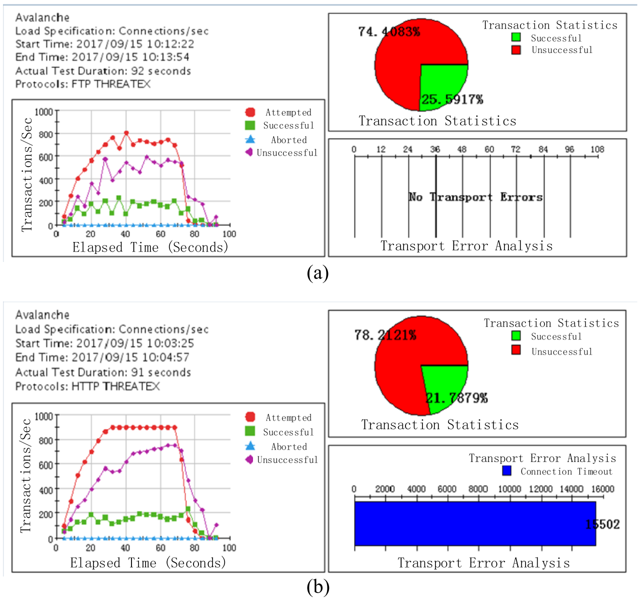
3) After scanning, various vulnerability attack packages are sent to the firewall using Avalanche. For Web server class applications, the firewall SQL injection, XSS scripts, and other attacks are simulated; for file class applications, CVE-2010-0188, CVE-2010-3333, and other vulnerability attacks are simulated; for ActiveX control vulnerability testing, CVE-2009-1534, CVE-2012-1891, and other vulnerability attacks are simulated.

4) Check whether the firewall log records the type of vulnerability attack and whether the client has successfully established a connection with the server.

5) Repeat experiments, and record the statistical quantization values of the penetration probability of firewall rules in the cyber network.

Thousands of experiments are executed. The simulation results for the application of Rule 1 for the Web server class are shown in Figure 10, where the penetration probabilities under FTP and HTTP protocols are shown, respectively.

The experimental results verify that the invasion attacker can affect the firewall defense. When the firewall is attacked by means of different vulnerabilities, the normal transmission of measurement data is destroyed, and then the power system is affected. The abscissa in the graphs on the left hand side of Figure 10 a) and b) shows the attacking time, and the number of successful packet connections in the vertical axis contains attack information and normal user information. The circle line in the graph represents the total number of attempts to connect between the current time points; the diamond line indicates the number of failed connections; the square line is the number of successful connections; and the triangle line represents the number of alarms. In Figure 10 a), the firewall does not open error analysis function, and therefore the value is zero. Because the test experiments need a certain delay time to determine whether the connection is successful, the purple and green lines to a certain extent lag behind the red line, and therefore in the simulation time 75–100*s*, the green and purple lines would exceed the red line.



Avalanche
Load Specification: Connections/sec
Start Time: 2017/09/15 10:12:22
End Time: 2017/09/15 10:13:54
Actual Test Duration: 92 seconds
Protocols: FTP THREATEX

(a)

Avalanche
Load Specification: Connections/sec
Start Time: 2017/09/15 10:03:25
End Time: 2017/09/15 10:04:57
Actual Test Duration: 91 seconds
Protocols: HTTP THREATEX

(b)

FIGURE 10. Results of attack experiments. (a) Attack experiments under FTP protocols. (b) Attack experiments under HTTP protocols.

After thousands of vulnerability attack experimental simulations referring to different firewall rules, the penetration probability of firewall rules and packet status monitors are $p_i^{fp} = (0.0095324, 0.0181514, 0.0019415)$, $p_i^{fs} = (0.0083154)$ respectively. In addition, the rejection probability of malicious packets is $p_i^{fr} = (0.71457)$. In Figure 10 a), the penetration probability under FTP protocols is 0.2559. In Figure 10 b), the penetration probability under HTTP protocols is 0.2179. The logon failure probability for each computer is designed to be 10%. Then, the computer response rates of the computer and firewall are set to $\lambda_1^{pw} = \lambda_2^{pw} = 12 \times 10^{-10}$ and $\lambda_1^{f} = \lambda_1^{nr} = 63 \times 10^{-7}$.

The probability or rate of each transition can be calculated by its weighted sum, i.e.,

$$c_{1,2} = \frac{p_1^{fp}}{p^{fr} + p_1^{fp} + p_2^{fp} + p_3^{fp} + p^{fs}} = 0.01253,$$

$$d_{2,2} = \frac{\lambda_1^f}{\lambda_1^f + \lambda_1^f} = 0.5, \quad f_{2,3} = \frac{\lambda_1^{pw}}{\lambda_1^{pw}} = 1.$$

Thus, matrix **W** can be obtained as follows:

$$\mathbf{W} = \begin{pmatrix} 0 & 0.01253 & 0.0239 & 0.0026 & 0.0318 & 0.93917 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0.5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0.5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0.5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0.5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

According to LSPN theory, the transfer of tokens among states is similar to the Markov process. By calculating the transfer matrix, the probability that the token (i.e., network intrusion attempts) locates in each state can be obtained until the system reaches a steady state.

B. SIMULATION RESULTS

Table 2 shows the transmission probability and influence coefficient in different attack scenarios. The steady-state probability corresponds to the network topology values of the three modes of power communication, namely, Md. 1, Md. 2, and Md. 3 in Figure 7, which reflect the differences in the resistance to attacks of risk levels. The values in rows 1 to 4 of Table 2 represent the steady-state values of each computer system at different locations under monitoring and the steady-state probability values from the firewall. The internal access points are analyzed by comparing different attacks. The steady state value of an external attack scenario is in general less than that of an internal intrusion scenario. The reason is that the internal firewall is the first firewall from outside to the internal network, which increases the probability of a successful penetration of the control center based on the LSPN theory. In addition, because of the firewall and password protection response time set value, the probability of attack from the node network to the control center is very large. The main factor affecting the internal attack vulnerability is the configuration of the communication network model and its more complex structure (Md. 3). The steady-state probability that the attack can successfully reach the control center is lower. Therefore, the network configuration

TABLE 2. Transmission probability and influence coefficient in different attack scenarios.

	Outside the network			Inside the firewall		
	Node 5 (Md. 1)	Node 23 (Md. 2)	Node 11 (Md. 3)	Node 5 (Md. 1)	Node 23 (Md. 2)	Node 11 (Md. 3)
Substation intrusion	0.0218	0.0117	0.0083	0.0002	0.0002	0.0002
Load network intrusion	—	0.0113	0.0116	—	0.0199	0.1670
DER network intrusion	—	—	0.0074	—	—	0.0133
Control center arrival	0.0024	0.0004	0.0002	0.0608	0.0199	0.0132
Loss load P_{LOL} (MW)	0.0600	0.9300	0.0450	0.0600	0.9300	0.0450
Load level E	1.0600	1.3900	1.0500	1.0600	1.3900	1.0500
Impact factor γ	0.7807	0.2344	0.8020	0.7807	0.2344	0.8020

and protection of the key nodes in the actual power grid can refer to the above situation.

Given the steady-state probability value under the invading scenario, the impact of the attack on the network side of the node can be reflected by the linear correlation between the channel throughput and the packet loss caused by the attack. For the network structure shown in Md. 3, the change trend of the throughput variation of the different attack access points is shown in Figure 11. It shows that the network intrusion attacks from outside the firewall have a strong effect on the throughput of data communications. When a node is attacked by an attacker with certain knowledge and skills, the system steady attack probability is high and the initiated low attack probability decreases the effect on the throughput of data transmission caused by the network communication topology. The change range of communication throughput in Md. 3 is more affected by the data transmission path and network topology model, which indicates the greater robustness of the corresponding communication network model.

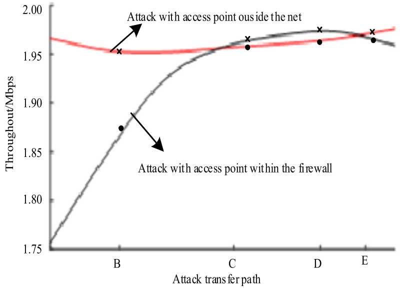


FIGURE 11. Throughput variations in Md. 3.

Row 5 in Table 2 represents the expected load loss for the Nodes 5, 23, and 11 under intrusion attacks, row 6 shows the maximum load level, and row 7 shows the influencing factor. More specifically, assuming the used computer systems are comparable, the use of smaller-scale node networks can lead to higher levels of vulnerability. This is because a smaller computer network could be more likely to identify the target of the attack. The security assessment indicator of Nodes 5 and 11 is 0.0215 and 0.0221, respectively, which means that power Node 5 is more vulnerable and it needs to be given more protection and attention.

Assuming the distributed power DERs are all wind energy, in order to consider the influence of the dynamic mode of DER on the security operation of the system, a comparison of different DER node installation locations in terms of network intrusion attacks is shown in Figure 12. According to the actual maximum power tracking curve of the wind energy of a WT, the working state of the wind energy is distributed as follows. Except for the time when it is in the stop mode, the proportion of time that the WT is in the work mode is 75% during a day, which means the transition probability of WT work mode is 90% * 0.75 = 0.675 under intrusion attacks, where 90% is the predesigned successful logon computer probability value and 0.75 is the probability of work time.

The security performance indices of the power nodes when the DERs are configured at different branch nodes are shown in Figure 12. It shows that the system configuration where all the DER nodes are installed in the main branch is stronger and more stable than that where the DER nodes are decentralized.

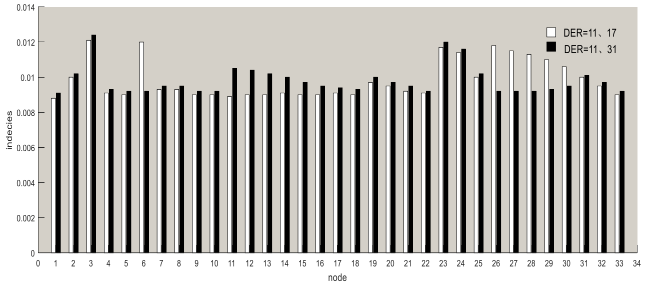


FIGURE 12. Security indices with different DER configurations.

The results of the improved security assessment indicator in the IEEE-33 bus cyber physical distribution system are shown in Figure 13. The countermeasure is improved by setting the IT password login threshold as 3 of tokens. It shows that the improvement reduces the vulnerability indicator for all substation nodes. The logon response strategy is improved by setting the response speed of the password login. This strategy significantly improves the security indicator for all substation nodes. Another interesting point is that the security assessment indicators of Nodes 3 and 6 with the highest level of structure are low in the invasion scenario. This is due to the small size of the network topology, so that an attacker can achieve a higher probability of steady-state malicious packets passing through the firewall and SCADA computer protection system to attempt to log on.

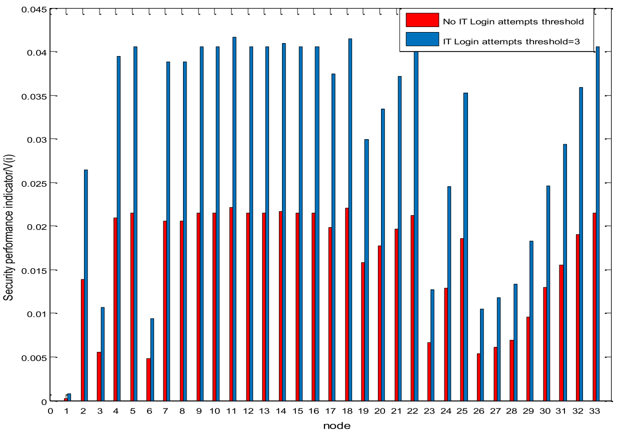


FIGURE 13. Analysis on the security effectiveness of network external attack.

More specifically, the results of node attack scenarios from outside the firewall shows that the power nodes with higher security usually refer to the nodes with the use of a substation model, in a crucial position or having more output in the system. Since the attack access point outside the network to the control center in the network Md. 1 is isolated by only two firewalls, and the others go through more layers of isolation, the attacked nodes that apply Md. 1 are more likely to exert a greater effect on system security, i.e., lead to a greater range of power failure. Some nodes have low security assessment values, such as Node 11 (DER node) and Node 1 (balanced node), because the stability of the entire grid operation is greatly affected by the nodes' failure, although these nodes' network structure with Md. 3 reduces the probability of a successful attack.

Furthermore, the changeable response speeds of the firewall and computer login also affect the security performance evaluation results in the active distribution system. The blue bar in Fig. 13 shows that the security performance evaluation of the power node attacked from outside the network after the response speed of the password protected computer is increased and the response speed of the firewall is reduced. Clearly, the system security is improved when the devices with more vulnerable in the communication models are relatively decreased. Because of the reduced probability of a successful attack against the control center and the greatly increased intrusion probability into the substation-level network, the nodes with large influence factors show a more pronounced influence on the system securities.

VII. CONCLUSION

To ensure the operation security and stability of the contemporary power infrastructure, a key task is to evaluate the system security assessment by considering the possible harm of network intrusion attacks initiated from the communication network side. An analytical framework is proposed in this paper to quantify the steady-state attack probability and the influence on the operational security of an active distribution power system based on LSPN graph theory. Moreover, the descriptions of cyber intrusion attacks, intrusion scenarios, specific evaluation formula for security effectiveness, assessment method and the joint experimental results mentioned can provide a reference for identifying the vulnerability of power system nodes in the face of network intrusion attacks and for improving the security and planning tool to assist the operators in achieving safety analysis.

The main research priorities are as follows.

1) According to the transition process of cyber intrusion attacks, a unified model of an active distribution power system is built to implement the security analysis of system operation. Considering the boundary inspection of malicious packets and intrusion attempts against each computer operation system, the establishment of the model includes primarily a general firewall protection model for monitoring abnormal states using predefined rules and a special network protection model for DERs involving the transformation of the operation mode.

2) Three different levels of communication networks corresponding to the physical nodes are distinguished to describe random attack process. In order to simulate the real data transmission of a communication network, the change in channel throughput in the corresponding network structure is quantitatively analyzed by considering the steady-state probability of the system under different attack access points.

3) A new security efficiency indicator is proposed to comprehensively evaluate the throughput variation in the communication channel and the attack influence on the CPDS when the corresponding power node loses efficacy due to cyber threats. For different attacked power nodes, the effect of the load loss for common nodes and the change in the operation mode for the DER power node are considered, respectively. Simulation results of the IEEE-33 bus distribution power system also demonstrate that the security performance index changes according to different attack scenarios and verify the effectiveness of the improved countermeasures. If the communication network structure becomes more complex, it could have greater effect on communication throughput variation, and the robustness of the system becomes more stronger.

The research work could assess the system securities and raise awareness of the cyber intrusion threats. How to integrate our method to evaluate new target defense technologies is an interesting topic in the future.

ACKNOWLEDGMENT

The authors would like to thank the NARI National Key Laboratory for the facilities and equipment provided. They are also thankful for their participants in the experiments.

REFERENCES

[1] C.-C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *IEEE Power Energy Mag.*, vol. 10, no. 1, pp. 58–66, Jan. 2012.

[2] S.-X. Wang, D. Liang, and X.-D. Wang, "Analytical FRTU deployment approach for reliability improvement of integrated cyber-physical distribution systems," *IET Generat., Transmiss., Distrib.*, vol. 10, no. 11, pp. 2631–2639, Aug. 2016.

[3] Y. Tang and F. Li, "Overview of the co-simulation methods for power and communication system," in *Proc. IEEE Int., Conf. Real-Time Comput. Robot. (RCAR)*, Angkor Wat, Cambodia, Jun. 2016, pp. 94–98.

[4] M. D. Ilic, L. Xie, U. A. Khan, and J. M. F. Moura, "Modeling of future cyber–physical energy systems for distributed sensing and control," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 40, no. 4, pp. 825–838, Jul. 2010.

[5] S.-X. Liu, Q.-H. Wang, and H. Wu, "Traffic scheduling with sustainable cyber physical systems applying in smart grid," in *Proc. 7th Int. Green Sustain. Comput. Conf.*, Hangzhou, China, 2016, pp. 1–6.

[6] Y. Tang, Q. Chen, M.-Y. Li, Q. Wang, and M. Ni, "Challenge and evolution of cyber attacks in cyber physical power system," in *Proc. IEEE PES Asia–Pacific Power Energy Eng. Conf. (APPEEC)*, Xi'an, China, Oct. 2016, pp. 857–862.

[7] G.-Q. Liang, S. R. Weller, and J.-H. Zhao, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[8] T. Koppel, *Lights Out: A Cyberattack, a Nation Unprepared, Surviving the Aftermath*. Danvers, MA, USA: Crown, 2015.

[9] C.-X. Dou, D. Yue, and M. Josep, "Multiagent system-based distributed coordinated control for radial DC microgrid considering transmission time delays," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2370–2381, Sep. 2017.

[10] D. Yue, S.-L. Hu, and C.-X. Dou, "Multiagent system-based event-triggered hybrid controls for high-security hybrid energy generation systems," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 584–594, Apr. 2017.

[11] C. X. Dou and B. Liu, "Multi-agent based hierarchical hybrid control for smart microgrid," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 771–778, Jun. 2013.

[12] A. Clark and S. Zonouz, "Cyber-physical resilience: Definition and assessment metric," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1671–1684, Mar. 2019.

[13] P. Haller and B. Genge, "Using sensitivity analysis and cross-association for the design of intrusion detection systems in industrial cyber-physical systems," *IEEE Access*, vol. 5, pp. 9336–9347, Nov. 2017.

[14] M. A. B. Ahmadon and S. Yamaguchi, "On service orchestration of cyber physical system and its verification based on petri net," in *Proc. IEEE 5th Global Conf. Consum. Electron.*, Las Vegas, NV, USA, Oct. 2016, pp. 1–4.

[15] Y. Wang, D. Liu, and Q.-S. Li, "A hybrid system based cps model and control of loads in active distribution network," in *Proc. Int. Conf. Power Syst. Technol.*, Wollongong, NSW, Australia, 2016, pp. 1–8.

[16] L. K. Singh and H. Rajput, "Dependability analysis of safety critical real-time systems by using Petri nets," *IEEE Trans. Control Syst. Technol.*, vol. 26, no. 2, pp. 415–426, Mar. 2018.

[17] K. Huang, C. Zhou, Y.-C. Tian, S.-H. Yang, and Y. Qin, "Assessing the physical impact of cyberattacks on industrial cyber-physical systems," *IEEE Trans. Ind. Electron.*, vol. 65, no. 10, pp. 8153–8162, Oct. 2018.

[18] Y.-G. Fu, J.-M. Zhu, and S. Gao, "CPS information security risk evaluation system based on Petri net," in *Proc. IEEE 2nd Int. Conf. Data Sci. Cyberspace*, Shenzhen, China, 2017, pp. 514–518.

[19] Y.-Z. Wang, M. Yu, J. Li, K. Meng, C. Lin, and X. Cheng, "Stochastic game net and applications in security analysis for enterprise network," *Int. J. Inf. Secur.*, vol. 11, no. 1, pp. 41–52, Oct. 2011.

[20] X. Xu, H.-Q. Yu, and J.-H. Huang, "Petri net based security quantitative analysis model for cyber-physical system," *Comput. Eng. Appl.*, vol. 50, no. 3, pp. 82–88, Mar. 2014.

[21] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 741–749, Dec. 2011.

[22] W.-Y. Cui and X.-R. Meng, "Security game modeling of cyber-physical systems based on hierarchical Petri nets," *Appl. Res. Comput.*, vol. 34, no. 8, pp. 2439–2442, 2017.

[23] Y.-Z. Wang, C. Lin, X.-Q. Cheng, and B.-X. Fang, "Analysis for network attack-defense based on stochastic game model," *Chin. J. Comput.*, vol. 33, no. 9, pp. 1748–1762, Sep. 2010.

[24] S. Zonouz, C. M. Davis, K. R. Davis, R. Berthier, R. B. Bobba, and W. H. Sanders, "SOCCA: A security-oriented cyber-physical contingency analysis in power infrastructures," *IEEE Trans. Smart Grid*, vol. 5, no. 1, pp. 3–13, Jan. 2014.

[25] C.-W. Ten, C.-C. Liu, and G. Maninaran, "Vulnerability assessment of cyber security for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.

[26] Y. Wang, M. M. Amin, and J. Fu, "A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids," *IEEE Access*, vol. 5, pp. 26022–26033, Nov. 2017.

[27] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2444–2453, Sep. 2015.

[28] R. Yu, Y. Zhang, S. Gjessing, C. Yuen, S. Xie, and M. Guizani, "Cognitive radio based hierarchical communications infrastructure for smart grid," *IEEE Netw.*, vol. 25, no. 5, pp. 6–14, Oct. 2011.

[29] L. Wei, A. I. Sarwat, W. Saad, and S. Biswas, "Stochastic games for power grid protection against coordinated cyber-physical attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 684–694, Mar. 2018.

[30] *Information Security: Technologies to Secure Federal Systems*, Government Accountability Office, Washington, DC, USA, Mar. 2004.

[31] The Smart Grid Interoperability Panel–Cyber Security Working Group, "Guidelines for smart grid cyber security: Supportive analyses and references," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Interagency Rep. 7628, vol. 3, Aug. 2010, p. 219.

[32] R. Fu, X. Huang, J. Sun, Z. Zhou, D. Chen, and Y. Wu, "Stability analysis of the cyber physical microgrid system under the intermittent DoS attacks," *Energies*, vol. 10, no. 5, p. 680, May 2017.

[33] R. Mitchell and I. R. Chen, "Modeling and analysis of attacks and counter defense mechanisms for cyber physical systems," *IEEE Trans. Rel.*, vol. 65, no. 1, pp. 350–358, Mar. 2016.

[34] X.-J. Zhang and S.-Z. Yao, "Fuzzy stochastic Petri nets and analysis of the reliability of multi-state systems," *IET Softw.*, vol. 9, no. 3, pp. 83–93, Jun. 2015.

[35] X.-H. Yu and Y.-S. Xue, "Smart grids: A cyber-physical systems perspective," *Proc. IEEE*, vol. 104, no. 5, pp. 1058–1070, May 2016.

RONG FU received the B.S. degree in electrical engineering from the China University of Mining and Technology, China, in 1994, the M.S. degree in electrical engineering from Hohai University, China, in 1999, and the Ph.D. degree in electrical engineering from Southeast University, China, in 2005. She is currently a Professor with the College of Automation, Nanjing University of Posts and Telecommunications. She currently conducts research on distributed control in cyber physical system and distributed energy management in electricity markets.

XIAOJUAN HUANG received the B.S. and M.S. degrees in electrical engineering from the Nanjing University of Posts and Telecommunications, China, in 2015 and 2018, respectively. She was involved in cyber security analysis in smart grids. She has won three good students from the Nanjing University of Posts and Telecommunications and a second-class scholarship.

YUSHENG XUE received the M.Sc. degree in electrical engineering from the Electric Power Research Institute, China, in 1981, and the Ph.D. degree from the University of Liege, Liege, Belgium, in 1987. He has been an Academician with the Chinese Academy of Engineering since 1995. He is currently the Honorary President of the State Grid Electric Power Research Institute (SGEPRI or NARI), Nanjing, China, an Adjunct Professor in dozens of Chinese universities, and an Adjunct Professor with the University of Newcastle in Australia. He is the Editor-in-Chief of the *Automation of Electric Power System* (in Chinese) and the *Journal of Modern Power Systems and Clean Energy* (in English), as well as the Chairman of the Technical Committee of Chinese National Committee of CIGRE since 2005.

YINGJUN WU received the Ph.D. degree in electrical engineering from the Politecnico di Torino, Italy, in 2013. He is currently an Associate Professor with the Nanjing University of Posts and Telecommunications. His main research directions are active distribution network technology and distributed control of power systems.

YI TANG (M'07) received the Ph.D. degree from the Harbin Institute of Technology, Harbin, China, in 2006. He is currently an Associate Professor with Southeast University, Nanjing, China. His research interest includes smart grid, power system security, power system stability analysis, renewable energy systems, and cyber physical system.

DONG YUE (M'05–SM'08) received the Ph.D. degree from the South China University of Technology in 1999. He is currently the Dean of the Institute of Advanced Technology/Institute of Automation, Nanjing University of Posts and Telecommunications, a Professor, and a Chang Jiang Scholar. The main research directions are networked control systems, power system optimization, and power big data.