Dependability Analysis of Control Center Networks in Smart Grid using Stochastic Petri Nets

Rongfei Zeng*, Yixin Jiang*, Chuang Lin*, and Xuemin (Sherman) Shen†
*Department of Computer Science and Technology, Tsinghua University, Beijing, 100084, China
Email: {zengrf, yxjiang, clin}@csnet1.cs.tsinghua.edu.cn
†Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, N2L 3G1, Canada
Email: xshen@bbcr.uwaterloo.ca

***Abstract*—As an indispensable infrastructure for the future life, smart grid is being implemented to save energy, reduce costs, and increase reliability. In smart grid, control center networks have attracted a great deal of attention, because their security and dependability issues are critical to the entire smart grid. Several studies have been conducted in the field of smart grid security, but few work focuses on the dependability analysis of control center networks. In this paper, we adopt a concise mathematic tool, stochastic Petri nets (SPNs), to analyze the dependability of control center networks in smart grid. We present the general model of control center networks by considering different backup strategies of critical components. With the general SPNs model, we can measure the dependability from two metrics, i.e., the reliability and availability, through analyzing the transient and steady-state probabilities simultaneously. To avoid the state-space explosion problem in computing, the state-space explosion avoidance method is proposed as well. Finally, we study a specific case to demonstrate the feasibility and efficiency of the proposed model in the dependability analysis of control center networks in smart grid.**

***Index Terms*—Smart grid, dependability analysis, stochastic Petri nets.**

I. Introduction

Smart grid introduces modern information technologies, such as the two-way digital communication networks, the automation control technique and smart metering, into the traditional power grid to provide dependable, efficient, and convenient electricity supply services to customers around the entire country. Smart grid can also achieve the characteristics of rapid demand response, self-healing, accommodation of distributed energy generation, etc. Nowadays, many countries invest a great deal of money into the field of smart grid. For instance, U. S. government invests $3.4 billion in various smart grid related projects in 2009, and the state grid corporation of China plans to invest about 40,000 billion RMB in smart grid before 2020. As expected, smart grid will be widespread implemented around the world in the near future.

Control center networks are to smart grid what brain is to human, and the dependability of control center networks is a significant factor that needs to be seriously considered. For one thing, some critical servers in control center networks, e.g., supervisory control and data acquisition (SCADA), database, and application server, may suffer from Byzantine failures and various malicious attacks initialized by hackers and terrorists. More catastrophically, a variety of attack tools are available on the Internet for free, making it easy for adversaries to destroy critical components. For another thing, the disruption of control center networks may lead to the power outages or even cascading blackouts, which cost billions of dollars each time [9]. Another disastrous consequence of disruption is loss of customer and public trust. Therefore, control center networks should be designed with high dependability.

Recently, there are several studies on the security of smart grid, especially the control center networks. Ericsson discusses the risks of connecting SCADA systems to the 'dangerous' Internet [2]. Fouda et al. present a novel light-weight message authentication scheme using Diffie-Hellman exchange protocol for smart grid [1]. Mclaughlin et al. utilize attack tree to discover the potential ways to perform energy theft in smart grid [3]. Ten et al. use attack tree to identify the vulnerabilities of SCADA system in [4], and they perform the same task using another impressive tool, i.e., stochastic Petri nets (SPNs), at system level, scenarios level, and access points level in [5]. The test beds of SCADA system are implemented to identify vulnerabilities of power infrastructure in [7] and [8]. Bompard et al. present an impressive mathematical framework based on game theory to perform cybersecurity assessment for smart grid [23]. Surveys on these issues can be found in [9] and [22]. In summary, many studies have been conducted in the field of smart grid security, but few work focuses on the dependability evaluation of control center networks, which is also very critical to smart grid.

Dependability analysis, first proposed by Robert Lusser in 1952, evaluates the capability of the target system to avoid service failures which may cause great losses more than is acceptable [10]. Nowadays, dependability analysis has already been applied to many critical systems, such as national defense systems, aircrafts, and computer networks. In these studies, researchers evaluate the global concept of dependability from the attributes of reliability, availability, safety, performability, maintainability, etc. For the control center networks in smart grid, we also concern with reliability and availability, because control center networks bear no disruptions, and high reliability and availability are two design goals. Thus, dependability analysis is necessary for the control center networks in smart grid.

In this paper, we study the dependability issue of control center networks in smart grid. We use SPNs to model the general control center networks, considering two different backup

Digital Object Indentifier 10.1109/TPDS.2012.68

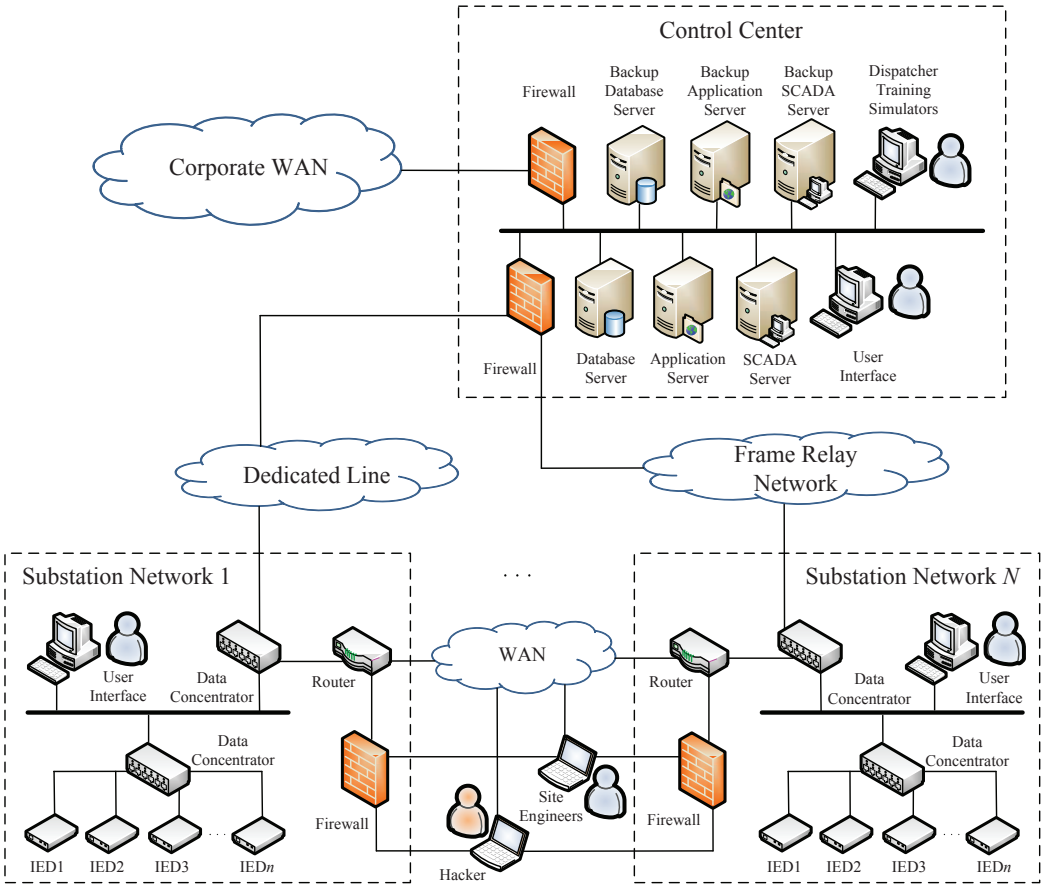


Fig. 1. The system model of control center networks in smart grid

strategies of critical components, i.e., cold backup and hot backup. Compared with other dependability analysis methods, SPNs are the concise and graphic formalization tools which are universally applied to model distributed, asynchronous, and concurrent systems. Subsequently, we measure the dependability from the metrics of reliability and availability through analyzing the transient and steady-state probabilities at the same time. When the size of target network is large, the state space becomes explosive in computing. To address this issue, we present a state-space explosion avoidance method. Finally, we study a specific case to illustrate the proposed method, which also demonstrates the feasibility and efficiency of the proposed scheme in the dependability analysis of control center networks.

The contributions of this paper are three-fold: 1) To the best of our knowledge, this paper is the first work to evaluate the dependability of control center networks in smart grid; 2) We adopt a novel mathematic tool SPNs to analyze two important attributes, i.e., reliability and availability, for control center networks; and 3) Through case study, we demonstrate the feasibility and efficiency of the proposed scheme in dependability analysis of control center networks. We also offer some guidelines for designing control center networks with high dependability.

The remainder of this paper is organized as follows. Section II surveys the related work, and Section III presents the structure of the target control center networks and some preliminaries of SPNs. In Section IV, we propose the general SPNs model of control center networks. Section V defines and computes two attributes of dependability, i.e., reliability and availability. We also address the state-space explosion problem in this section. In Section VI, we present the case study to illustrate the dependability analysis method, followed by the conclusions in Section VII.

II. Related Work

Over the past few years, there have been several works in the fields of smart grid security and dependability analysis. In this section, we discuss some of them, which are closely related to our proposed scheme.

A. Smart Grid

For the security of smart grid, some results have been published in the recent years. Chen [9] reviews the cyber security and privacy issues in smart grid using NIST reference architecture, and he also relates these issues to the cyber security in the Internet. Katz [22] gives some thinkings on the security and architecture issues of smart grid. Amin [21] argues that security awareness and personnel training about supervisory control networks are more important than before. Fleury et al. present a novel approach to classify

attacks against control center networks into a taxonomy based on attack-vulnerability-damage model in [28]. Fouda et al. propose a light-weight message authentication scheme using Diffie-Hellman exchange protocol for smart grid in [1]. Recently, some methods are presented to identify the vulnerability of smart grid. Ericsson [2] identifies the vulnerabilities of connecting SCADA systems to the Internet. Mclaughlin et al. employ attack tree to discover the potential ways to perform energy theft in smart grid [3]. Similarly, Ten et al. use attack tree to identify vulnerabilities of SCADA system in [4], and they also evaluate the same networks using another impressive tool, i.e., SPNs, at system level, scenarios level, and access points level in [5]. Bompard et al. present a mathematical framework based on game theory to perform risk assessment for smart grid [23]. The test beds of SCADA systems are implemented to identify vulnerabilities of power infrastructure in [7], [8]. Impressively, Ferrarini et al. perform the dependability evaluation of the protection schemes of power grid using a computer simulator in [29]. Compared with this work, our proposal models a different target, i.e., control center networks, with a distinct mathematical tool SPNs. In summary, few work focuses on the dependability evaluation of control center networks, which is as significant as the vulnerability assessment.

B. Dependability Analysis Method

There are two types of quantitative dependability analysis methods: combinatorial models and state-space models. Reliability block diagrams [16], fault tree analysis [17], fault mode effect analysis [27], attack tree [4], attack graph [25], and privilege graph [26] are the main representatives of combinatorial models. The easy construction and explicit presentation make the combinatorial methods a good choice for dependability analysis. However, the limitation of capability to model large and complicated networks make them less competitive than state-space models.

State-space models include Markov chain, Markov reward model [19], Markov regenerative process [18], supplementary variable approach, stochastic Petri nets [5], stochastic process algebra [20], etc. Markov chain is the foundation of various state-space methods in dependability analysis. Markov reward process assigns rewards to the transitions of states in CTMC, while Markov regenerative process chooses some regenerative points in CTMC or semi-CTMC to simplify the modeling analysis. Stochastic process algebra [20] uses a process to model the actions of components, making it suitable for modeling resource-sharing systems. As the impressive mathematical tools, SPNs [13] are widely used to the dependability analysis in the recent years. Compared with other dependability analysis methods, SPNs can capture the relationships between actions and states of distributed networks in the simple and concise way, which provides a great advantage over Markov chain and other state-space models. Moreover, various existing results can be applied to SPNs to address the state-space explosion problem faced by all the state-space methods. Thus, we adopt the SPNs model to analyze the dependability of control center networks in smart grid.

III. System Model and Preliminary

A. System Model

In this paper, we consider the control center networks consisting of one control center and N substation networks, as shown in Fig. 1. In the control center, SCADA servers, database, and application servers are linked with local area networks (LAN), which are protected by the firewalls. If a component in the control center suffers from failure or various attackers, it can be repaired rapidly through user interface. Moreover, backup servers are used to improve the dependability. The control center in one region also connects with the control centers in other regions through secure wide area networks (WAN). Since the control center is well protected, we assume that it can not be intruded from other control centers. However, it can be attacked from the substation networks. N substation networks are connected to the control center through dedicated link or frame relay networks. Substation networks are responsible for collecting data from intelligent electronic devices (IEDs). Site engineers can log into the substation networks to restore failed components. Meanwhile, hackers can also intrude into substation networks if they can succeed in passing through the firewalls. These substations networks are connected with unsecure WAN, thus a substation may be at risk when another substation is compromised.

B. Preliminary

Stochastic Petri Nets: Stochastic Petri net is a graphic mathematical tool, which is universally applied to the performance evaluation and dependability analysis of various distributed systems. The definition of SPNs is given as follows.

Definition 1: SPNs can be defined as a five-tuple (P, T, F, M_0, λ), where
(1) $P = \{P_1, P_2, \cdots, P_k\}$ is the place set, which describes the states of networks or the conditions for transitions,
(2) $T = \{T_1, T_2, \cdots, T_l\}$ is the finite set of transitions, the execution of which changes the states of networks,
(3) $F = (P \times T) \cup (T \times P)$ is an arc set, connecting places and transitions,
(4) $\lambda = \{\lambda_1, \lambda_2, \cdots, \lambda_l\}$ is the set of firing rates associated with the transitions. In SPNs, each firing rate $\lambda_i (i = 1, \cdots, l)$ is exponentially-distributed,
(5) $M_0 = \{M_{01}, M_{02}, \cdots, M_{0k}\}$ is an initial marking, which depicts the initial state of networks.

In SPNs models, places and tokens are separately drown as circles and black dots, and transitions are denoted by boxes or bars. The transition is enabled when all its input places contain tokens more than the requirements labeled at the corresponding input arcs. The firing of enabled transition removes tokens from input places to its output places, which modifies the distribution of tokens and generates a new marking for SPNs.

There are some extensions of the basic SPNs, e.g., generalized stochastic Petri nets (GSPN) [12], stochastic high-level Petri nets [13], and deterministic and stochastic Petri nets. In this paper, we actually use GSPN to model the target control center networks. Compared with the basic SPNs, GSPN classifies transitions into two types: timed transitions (drown as

boxes) and immediate transitions (drown as bars). The timed transitions have the exponentially-distributed service time, as mentioned in Definition 1, while the immediate transitions are promptly fired if the prerequisites are satisfied. In this paper, we use the term SPNs to cover both SPNs and GSPN for simplicity.

IV. The SPNs Model Formulation

In this section, we first propose the basic failure-repair model of a single server. Then, we study two backup strategies for critical servers and present their SPNs models. Finally, we incorporate the aforementioned models into the general model of the target control center networks.

A. The Failure-repair Model of a Single Server

As a key ingredient of the general model, the failure-repair model of a single component is shown in Fig. 2. Initially, the server is in the operating mode, which is denoted by a token in the place P_{up}. During the operation, the server may suffer from Byzantine failures and various attacks, which leads to the failure of server. The failure state is denoted by the place P_{down}, and the action resulting in this failure is depicted by the transition T_f. When the server fails, it can be repaired by site engineers. The transition T_r of repair operation enables tokens to flow from place P_{down} to place P_{up}. For the transitions T_f and T_r, their firing rates conform to the exponential distribution with parameter λ_f and λ_r, respectively.

In the failure-repair model, we neglect the details of attack and repair and only focus on the impacts of these actions, which is quite different from vulnerability assessment. This feature enables engineers with little knowledge of attacks to perform dependability evaluations.

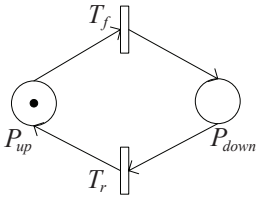
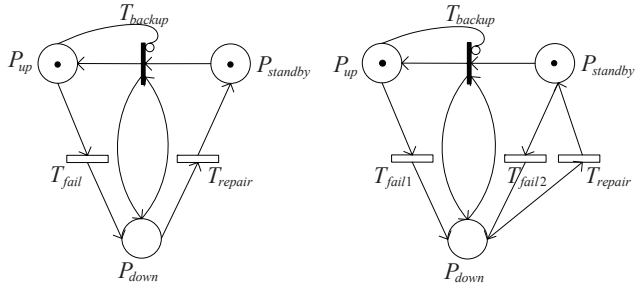


Fig. 2. The failure-repair model of a single component

B. The Models of Backup Strategies

In this paper, we consider two backup strategies, i.e., cool backup and hot backup, for critical servers to improve the dependability of control center networks. For the cool backup strategy, only one of the main server and the backup server is used at one time. In other words, the backup server is started only when the main server is failed. In Fig. 3(a), we use the transition T_{backup} to denote the event that the backup server is started. The prerequisites of T_{backup} are that there is no token in place P_{up} (i.e., the master server is failed) and one token in place $P_{standby}$ (i.e., there is a backup server). For the hot backup strategy, both the main server and backup server work simultaneously, and the backup server is used as a slave server. In terms of the SPNs model, the only difference is that there is an additional transition T_{fail2} between places $P_{standby}$ and P_{down} in the hot backup model, as shown in Fig. 3(b).



(a) Cool Backup (b) Hot Backup

Fig. 3. The models of backup strategies

C. The General Model of Control Center Networks

With the above ingredients, we can construct the general SPNs model of dependability for control center networks in Fig. 4. In this model, there are $(N + 1)$ submodels: N submodels of substation networks and 1 submodel of control center. For each substation network, there are two ways for attackers to intrude into the network: destroying the firewall and attacking from other compromised substation networks, which are separately denoted by transitions $T_{i\_fw\_f}$ and T_{sn_f}. When the substation network i is compromised, meaning that there is a token in the place P_{i_fail}, hackers can launch the following attacks: (1) destroying the data concentrator (DC) or IEDs; (2) intruding other substation networks; and (3) attacking the control center. These attacks are respectively denoted by the transitions $T_{i\_DC\_f}$, $T_{i\_IEDi\_f}$, T_{from_i}, and $T_{fw\_f\_i}$. If the firewall of control center is disrupted, the state of which is denoted by the place P_{fw_down}, then the attacker can further destroy the application servers, SCADA server or database. Note that two backup strategies are used for critical servers in the general model, as shown in the dotted box.

V. Dependability Analysis

In this section, we present the dependability analysis method to evaluate control center networks with the proposed SPNs model. We define two metrics of dependability and provide the detailed method to calculate them. We address the issue of state-space explosion in computing as well.

A. Metrics

In this paper, we consider two dependability metrics, i.e., reliability and availability, for control center networks in smart grid. Reliability is used to evaluate the capability to continuously provide services without failures [10]. In detail, it can be defined as the probability that the control center networks work correctly during the period $[0, t]$, i.e.,

$$R(t) = Pr\{X > t\}, \tag{1}$$

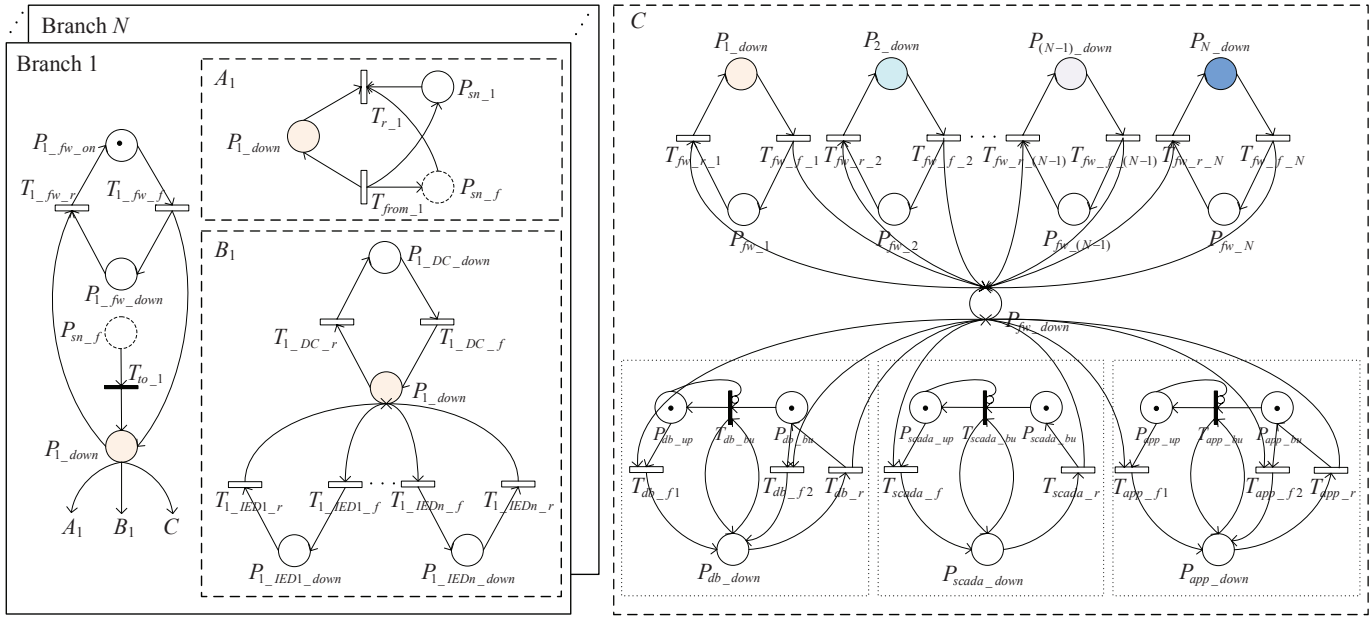


Fig. 4. The general SPNs model of control center networks

where X is the continuous random variable of correct operation time for control center networks. Availability describes the readiness of correct services for some critical components [10]. It can be defined as

$$A(t) = Pr\{\text{Services are available at time } t\}. \tag{2}$$

In the above definitions, both reliability and availability are transient, which means that they focuses on the reliability and availability at the time t. In practical, we are also interested in the steady-state dependability. According to the definition of reliability, its steady-state value is zero, i.e.,

$$Rel = \lim_{t\to\infty} R(t) = 0. \tag{3}$$

The steady-state availability can be defined as

$$Ava = \lim_{t\to\infty} A(t). \tag{4}$$

B. Model Analysis

In this subsection, we present the calculation method of reliability and availability from both steady-state and transient aspects. The proposed method involves two steps: the analysis of the equivalent continuous time Markov chain (CTMC) and the computation of reliability and availability.

Theoretically, Molly et al. have proved that k-bounded SPNs are isomorphic to CTMC due to the memoryless property of the exponentially-distributed service time [14]. Then, we could associate SPNs' markings with the CTMC's states to achieve the isomorphism property [24]. In detail, we can obtain the equivalent CTMC by constructing the reachability graph of SPNs and labeling arcs with the sum of the firing rates of transitions whose firings produce the changes of the corresponding states. Note that we delete the vanishing states and only consider tangible states in CTMC.

There are two equivalent methods to compute the steady-state probability of CTMC. In the first approach, which is suitable for calculations on clusters, we have to define the infinitesimal generator $Q = [q_{ij}]$, where $q_{ij}(i \neq j)$ is the transition rate from states M_i to M_j. If there is no arc from states M_i to M_j, then $q_{ij} = 0$. It should be noted that the element on the diagonal is the negative of the sum of elements in that line, i.e., $q_{ii} = -\sum_{j=1}^{j=n,j\neq i} q_{ij}$. Define the steady-state probability as a vector $\Pi = (\pi_1, \pi_2, \cdots, \pi_n)$. Then, we have

$$\begin{cases} \Pi \times Q = 0 \\ \sum_{i=0}^{n} \pi_i = 1 \end{cases} \tag{5}$$

We can get the steady-state probability by solving these linear equations.

The other method of computing the steady-state probability relies on the birth-death process, which is easy to manually derive analytical solutions. For any marking $M_i \in [M_0 >$, and all the $M_j, M_k \in [M_0 >, M_i \in [t_j > M_j, M_k \in [t_k > M_i$, we can have

$$(\sum_j \lambda_j)\pi_i = \sum_k \lambda_k \pi_k, \tag{6}$$

In addition to the $(n-1)$ equations, we also have $\sum_i \pi_i = 1$. Thus, we can get the vector Π by solving the n equations.

To calculate the transient probability of each state, we define $\pi(t) = [\pi_1(t), \pi_2(t), \cdots, \pi_n(t)]$ and have n first order linear differential equations as

$$\frac{d\pi(t)}{dt} = \pi(t)Q. \tag{7}$$

We can get the transient probabilities by solving these differential equations.

Before computing the reliability, we classify all the states into two categories: the states $\mathcal{M}_{\mathcal{R}}$ that the control center networks are reliable and the states $\widetilde{\mathcal{M}_{\mathcal{R}}}$ that the target

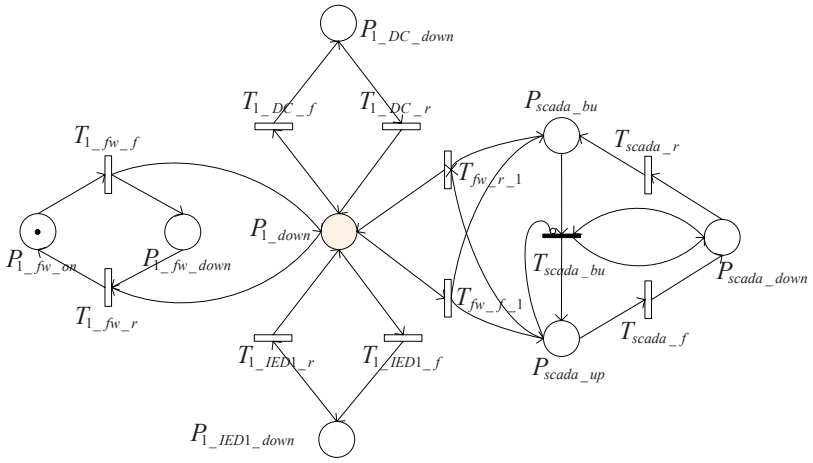


Fig. 5. The SPNs model of the case

networks are not. According to the literature [20], we can have the transient reliability

$$Rel(t) = 1 - Ex(\sum_{i=1}^{t} \lambda_i, t) = e^{-\sum_{i=1}^{t} \lambda_i, t}, \tag{8}$$

where λ_i is the firing rate of transition whose firing causes the target networks to leave the reliable states. From this definition, we can get that $Rel(\infty) = 0$.

For the availability, we can also have two types of states, i.e., the states $\mathcal{M}_{\mathcal{A}}$ that the target networks are available and the states $\widetilde{\mathcal{M}_{\mathcal{A}}}$ that the control center networks are not available. Then, the steady-state availability and the transient availability are respectively

$$Ava = \sum_i b_i \pi_i, M_i \in \mathcal{M}_{\mathcal{A}}, \tag{9}$$

$$A(t) = \sum_i b_i \pi_i(t), M_i \in \mathcal{M}_{\mathcal{A}}, \tag{10}$$

where b_i is the coefficient.

C. The Avoidance of State-space Explosion

When the size of control center networks increases, the potential states of CTMC will be exponentially increased, which makes it impossible to compute the steady-state probability and transient probability. In this subsection, we address the state-space explosion problem faced by all the state-space models. In the proposed model, the firing rates of some transitions (e.g., repair transitions $T_{i\_fr\_r}$, T_{scada_r}, and T_{db_r}) are larger than those of other transitions. From fast transitions point of view, it seems that slow transitions never fire. Based on these observations, we apply the time scale decomposition (TSD) method, first proposed by Ammar and Islam in [15], to reduce the number of states of CTMC. TSD decomposes the SPNs model into several sub-level models, which only have transitions with the firing rates of the same order of magnitude. The TSD method is detailed as follow:

(1) We classify transitions into two types: fast transitions T_f and slow transitions T_s, where $T_s \cup T_f = T$ and $T_s \cap T_f = \emptyset$. Fast transitions include both immediate transitions and fast timed transitions.

(2) In the time scale of fast transitions, slow transitions are assumed not to be fired. Then, the SPNs model can be decomposed into several isolated submodels by deleting slow transitions.

(3) The submodel k is denoted as place P_k in the aggregated SPNs model. For the transitions in the aggregated SPNs, if there is a transition $t \in T_s$ from any place in the submodel i to any place in the submodel j, then the transition t also exists in the aggregated model to connect places P_i and P_j.

(4) The initial marking of the aggregated model is determined by the initial marking of the original SPNs model. In detail, the number of initial tokens in place P_i of the aggregated model equal with the total number of initial tokens in the submodel i. Note that we do not consider tokens that cannot be transferred to other submodels by the firing of transitions in T_s.

(5) The firing rate of transition in the aggregated model is the firing rate of corresponding transition in T_s multiplied by the steady-state probability distribution of local marking in the submodel. We can obtain the steady-state probability of local marking by analyzing each submodel in isolation with the current marking of the aggregated model.

VI. Case Study and Discussions

In this section, we study the virtual control center networks with one IED ($n = 1$) in one substation ($N = 1$) and only SCADA servers, which are assumed to illustrate the dependability analysis procedure and the state-space explosion avoidance method.

In Fig. 5, we present the SPNs model of this example. The explanations of places and transitions are omitted for the space limitation. We respectively set the parameters $\lambda_1, \lambda_2, \cdots, \lambda_{10}$ as the firing rates of transitions $T_{1\_fw\_f}$, $T_{1\_fw\_r}$, $T_{1\_DC\_f}$, $T_{1\_DC\_r}$, $T_{1\_IED1\_f}$, $T_{1\_IED1\_r}$, $T_{fw\_f\_1}$, $T_{fw\_r\_1}$, T_{scada_f}, and T_{scada_r}. These parameters can be obtained by analyzing a large volume of statistics and computed as the average of occurrence frequency of events. From this model, we can have

TABLE I
THE MARKINGS OF THE SPNS MODEL AND THE STATES OF CORRESPONDING CTMC

	$P_{1\_fw\_on}$	$P_{1\_fw\_down}$	P_{1_down}	$P_{1\_DC\_down}$	$P_{1\_IED1\_down}$	P_{scada_up}	P_{scada_bu}	P_{scada_down}
M_0	1	0	0	0	0	0	0	0
M_1	0	1	1	0	0	0	0	0
M_2	0	1	0	1	0	0	0	0
M_3	0	1	0	0	1	0	0	0
M_4	0	1	0	0	0	1	1	0
M_5	0	1	0	0	0	1	0	1

the entire markings of SPNs, which can be mapped to the states of CTMC, as shown in Table I. Then, we can have the equivalent CTMC shown in Fig. 6 and its infinitesimal generator Q as

$$Q = \begin{pmatrix} q_{00} & \lambda_1 & 0 & 0 & 0 & 0 \\ \lambda_2 & q_{11} & \lambda_3 & \lambda_5 & \lambda_7 & 0 \\ 0 & \lambda_4 & q_{22} & 0 & 0 & 0 \\ 0 & \lambda_6 & 0 & q_{33} & 0 & 0 \\ 0 & \lambda_8 & 0 & 0 & q_{44} & \lambda_9 \\ 0 & 0 & 0 & 0 & \lambda_{10} & q_{55} \end{pmatrix}, \quad (11)$$

where $q_{ii} = -\sum_{j=0}^{j=5, i\neq j} q_{ij} (i = 0, \cdots, 5)$. Consequently, we can get the steady-state probability by solving the Eq. (5). For the other method, we can base on the birth-death process and have Eq. (12) to calculate the steady-state probability.

$$\begin{cases} \lambda_1\pi_0 = \lambda_2\pi_1 \\ (\lambda_2 + \lambda_3 + \lambda_5 + \lambda_7)\pi_1 = \lambda_1\pi_0 + \lambda_4\pi_2 + \lambda_6\pi_3 + \lambda_8\pi_4 \\ \lambda_4\pi_2 = \lambda_3\pi_1 \\ \lambda_6\pi_3 = \lambda_5\pi_1 \\ (\lambda_8 + \lambda_9)\pi_4 = \lambda_7\pi_1 + \lambda_{10}\pi_5 \\ \lambda_{10}\pi_5 = \lambda_9\pi_4 \\ \pi_0 + \pi_1 + \pi_2 + \pi_3 + \pi_4 + \pi_5 = 1 \end{cases} \quad (12)$$

To get the transient reliability and availability at time t, we should compute the transient probability of each state. According to Eq. (7), we can have Eq. (13). The initial conditions are $\pi_0(0) = 1$, $\pi_1(0) = 0$, $\pi_2(0) = 0$, $\pi_3(0) = 0$, $\pi_4(0) = 0$, and $\pi_5(0) = 0$. The transient probability can be computed by solving these linear differential equations.

$$\begin{cases} \frac{d\pi_0(t)}{dt} = -\lambda_1\pi_0(t) + \lambda_2\pi_1(t) \\ \frac{d\pi_1(t)}{dt} = -(\lambda_2 + \lambda_3 + \lambda_5 + \lambda_7)\pi_1(t) + \lambda_1\pi_0(t) + \lambda_4\pi_2(t) \\ \qquad +\lambda_6\pi_3(t) + \lambda_8\pi_4(t) \\ \frac{d\pi_2(t)}{dt} = -\lambda_4\pi_2(t) + \lambda_3\pi_1(t) \\ \frac{d\pi_3(t)}{dt} = -\lambda_6\pi_3(t) + \lambda_5\pi_1(t) \\ \frac{d\pi_4(t)}{dt} = -(\lambda_8 + \lambda_9)\pi_4(t) + \lambda_7\pi_1(t) + \lambda_{10}\pi_5(t) \\ \frac{d\pi_5(t)}{dt} = -\lambda_{10}\pi_5(t) + \lambda_9\pi_4(t) \end{cases} \quad (13)$$

With the steady-state and transient probabilities, we can compute the reliability and availability. For the reliability, it can be seen that only the initial state is reliable, and the rate of leaving the reliable state M_0 is λ_1. Thus, we can have the transient reliability as

$$R(t) = e^{-\lambda_1 t}. \quad (14)$$

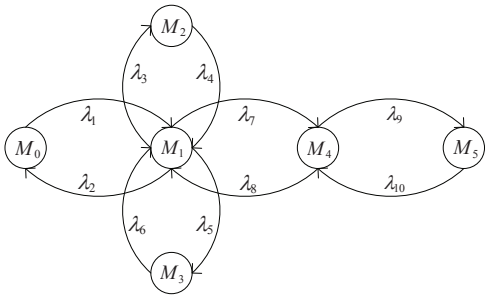


Fig. 6. The equivalent CTMC

For the availability of networks, DC, IED and SCADA server are unavailable in the states M_2, M_3, and M_5, respectively. Then, we can calculate the steady-state and transient availability as

$$Ava = 1 - (a_1\pi_2 + a_2\pi_3 + a_3\pi_5), \quad (15)$$

$$A(t) = 1 - (a_1\pi_2(t) + a_2\pi_3(t) + a_3\pi_5(t)), \quad (16)$$

where a_1, a_2 and a_3 are respectively the weights of DC, IED, and SCADA server.

TABLE II
THE FIRING RATES OF TRANSITIONS

λ_1	λ_2	λ_3	λ_4	λ_5
2	100	0.01	0.02	0.01
λ_6	λ_7	λ_8	λ_9	λ_{10}
0.02	2	100	1	200

In Table II, we present the firing rates of transitions used in the following paper. Note that these parameters are assumed according to the fact that malicious attackers usually need great efforts to destroy the control center networks, while most failures can be promptly repaired by the engineers. We also assume that $a_1 = a_2 = a_3 = 0.3333$. With these settings, we can solve Eq. (12) and get the steady-state probability as

$$\begin{aligned} &\pi_0 = 0.9612, && \pi_1 = 0.0192, \\ &\pi_2 = 9.6117 \times 10^{-3}, && \pi_3 = 9.6117 \times 10^{-3}, \\ &\pi_4 = 3.8447 \times 10^{-4}, && \pi_5 = 1.9223 \times 10^{-5}. \end{aligned}$$

According to Eq. (15), we can get the steady-state availability as

$$Ava = 0.9936.$$

Similarly, we can obtain the transient probability of each

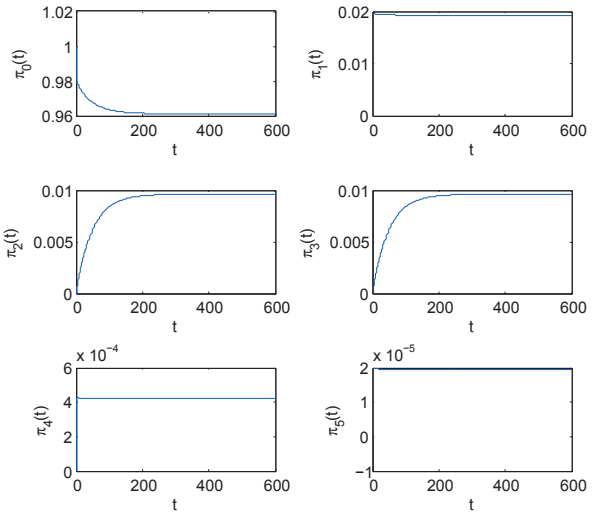


Fig. 7. The transient probability of each state

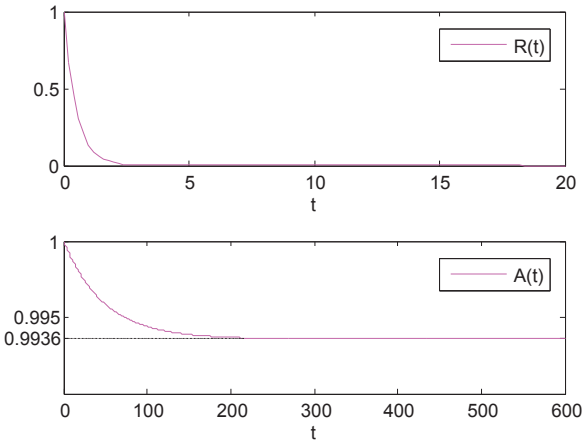


Fig. 8. The transient reliability and availability

state by solving Eq. (13). Considering the space limitations, we omit the detailed analytical solutions and only present the numerical results of the transient probability calculated by the Runge-Kutta method of 4 order in Fig. 7. It can be seen that some transient probabilities (e.g., π_0) are exponentially decreased with time t, while some probabilities (e.g., π_2 and π_3) are exponentially increased with time t. Impressively, each transient probability ultimately approaches to the steady-state probability, which demonstrates the correctness of the proposed analysis method.

In Fig. 8, we present the numerical results of the transient reliability and availability. From this figure, we can see that the transient reliability and availability are exponentially decreased with time t. Moreover, they respectively approach to the steady-state reliability $Rel = 0$ and availability $Ava = 0.9936$. Finally, we should mention that the relationship between two reliability values is more important than the accurate values themselves. In other words, the control center networks with large steady-state availability are more dependable and reliable than those with small steady-state availability.

In the following, we employ TSD to reduce the number of states from 6 to 3. Considering the firing rates of transitions, we could classify the transitions into two types: $T_s = \{T_{1\_DC\_f}, T_{1\_DC\_r}, T_{1\_IED1\_f}, T_{1\_IED1\_r}\}$ and $T_f = \{T_{1\_fw\_f}, T_{1\_fw\_r}, T_{fw\_f\_1}, T_{fw\_r\_1}, T_{scada\_f}, T_{scada\_r}\}$. After deleting the slow transitions, the original SPNs are separated into three sub-models, as shown in Fig. 9. Each sub-model is denoted as a place $P_i (i = 1, 2, 3)$ in the aggregated model. The transitions are selected from the set T_s to connect places in the aggregated model. The initial marking in the aggregated model is $M_2 = (0, 1, 0)$. With the initial marking, transitions T_1 and T_3 can be fired. The firing rates of transitions T_1 and T_3 are associated with both the steady-state probability Pr that there is a token in the place P_{1_down} and the firing rates λ_3 and λ_5, i.e.,

$$\lambda_b = Pr \times \lambda_3,$$

$$\lambda_c = Pr \times \lambda_5.$$

Note that we can apply the proposed analysis method to compute Pr with the submodel in the dashed box of Fig. 9. The firing of transition T_1 generates a new marking $M_1 = (1, 0, 0)$, where only the transition T_2 can be fired. The firing rate of transition T_2 is

$$\lambda_a = \lambda_4.$$

In the marking $M_2 = (0, 1, 0)$, the transition T_3 can be fired, which generates the marking $M_3 = (0, 0, 1)$. In the marking M_3, only the transition T_4 can be fired, and the firing rate of T_4 is

$$\lambda_d = \lambda_6.$$

Now, we can get the aggregated CTMC, as shown in Fig. 9.

TABLE III
THE COMPARISONS OF RELIABILITY AND AVAILABILITY WITH AND WITHOUT TSD TECHNIQUE

	(a)	(b)	δ
$Rel(t)$	e^{-2t}	e^{-2t}	0
Ava	0.9936	0.9998	0.62%

In Table III, we present the results of reliability and availability, which are computed with the original method (a) and the TSD technique (b). We also present the relative error $\delta = \frac{|x_0 - x|}{x}$, where x computed by the method (a) and x_0 is given by TSD (b), to demonstrate the performance of TSD method. It can been seen that TSD can be applied to address the state-space explosion issue and the error caused by TSD can be neglected. It should also be noted that TSD can achieve better performance when the firing rates of fast transitions are much larger than those of slow transitions. Refer to [15] for the detailed performance analysis of the TSD technique.

VII. CONCLUSIONS

In this paper, we employ SPNs model to study the dependability issue of control center networks in smart grid. We consider two backup strategies for critical components and

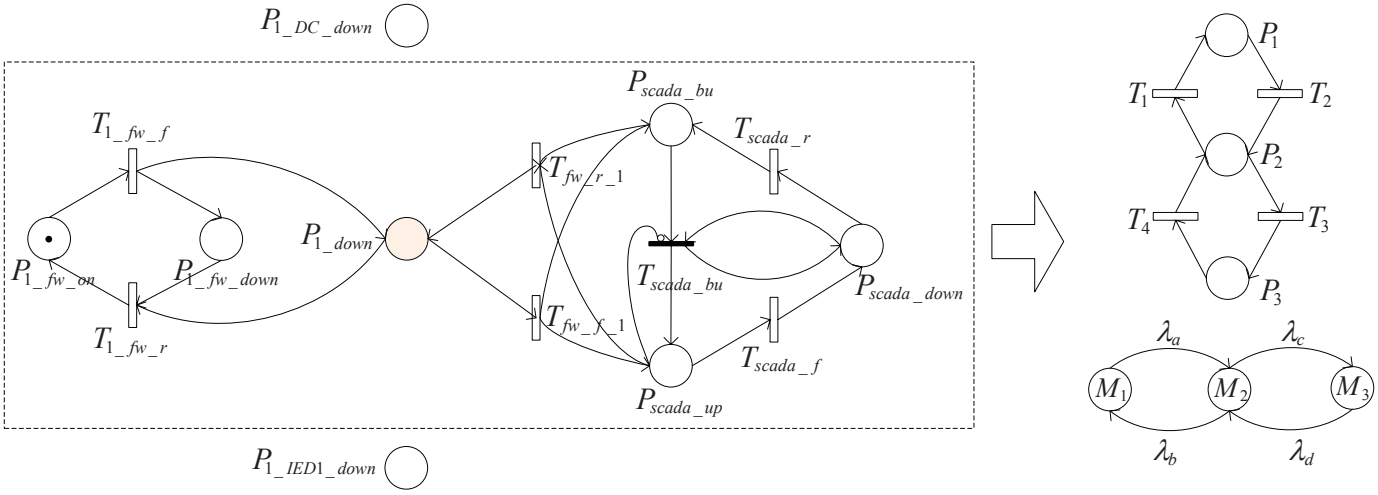


Fig. 9. The aggregated SPNs model

present the general SPNs model for control center networks. Then, we refine dependability into two specific metrics, i.e., reliability and availability, from both transient and steady-state aspects. We also present the detailed analysis method to calculated these metrics. Moreover, an approach to reduce the state number in computing has been given as well. Finally, we use case study to illustrate our proposed scheme, which also demonstrates the feasibility and correctness of the proposed method. In the future work, we will design a light-weight protection scheme to guarantee the dependability of data transmission in control center networks of smart grid. Moreover, we will study how many states have been reduced by the proposed TSD method and give the analytical solutions of the improvement of the scalability.

REFERENCES

[1] M. Fouda, Z. Fadlullah, N. Kato, R. Lu, and X. Shen, "A light-weight message authentication scheme for smart grid communication," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 675-685, 2011.

[2] G. Ericsson, "Toward a framework for managing information security for an electric power utility - CIGRE experiences," *IEEE Transactions on Power Delivery*, vol. 22, no. 3, pp. 1461-1469, 2007.

[3] S. Mclaughlin, D. Podkuiko, and P. Mcdaniel, "Engergy theft in the advanced metering infrastructure," in *Proc. of 4th International Workshop on Critical Information Infrastructures Security*, pp. 176-187, 2009.

[4] C. Ten, C. Liu, and M. Govindarasu, "Vulnerabililty assessment of cybersecurity for SCADA systems using attack trees," in *Proc. of IEEE Power Engineering Society General Meeting*, pp. 1-6, 2007.

[5] C. Ten, C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836-1846, 2008.

[6] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power system," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382-390, 2011.

[7] C. Davis, J. Tate, H. Okhravl, C. Grier, T. Overbye, and D. Nicol, "SCADA cybersecurity test bed development," in *Proc. of 38th North America Power Symposium,*, pp. 483-488, 2006.

[8] J. Tang, R. Hovsapian, M. Richardson, M. Baca, J. Trent, Z. Hartley, and R. Smith, "The CAPS-SNL power system security test bed", in *Proc. of 3rd International Confernece of Critical Infrastructures*, pp. 1-6, 2006.

[9] T. Chen, "Survey of cyber security issues in smart grids," in *Proc. of SPIE*, pp. 1-11, 2010.

[10] A. Avizienis, J. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11-33, 2004.

[11] D. Nicol, W. Sanders, and K. Trivedi, "Model-based evaluation: from dependability to security," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 48-65, 2004.

[12] M. Marsan, G. Conte, and G. Balbo, "A class of generalized petri nets for the performance evaluation of multiprocessor systems," *ACM Transaction on Computer Systems*, vol. 2, no. 2, pp. 93-122, 1984.

[13] C. Lin and D. Marinescu, "Stochastic high level petri nets and applications," *IEEE Transactions on Computer*, vol. 37, no. 7, pp. 815-825, 1988.

[14] K. Molly, "On the integration of delay and throughput measures in distributed processing models," Ph. D. Dissertation, University of California, Los Angeles, 1981.

[15] H. Ammar and S. Islam, "Timed scale decomposition of a class of generalized stochastic petri net models," *IEEE Transactions on Software Engineering*, vol. 15, no. 6, pp. 809-820, 1989.

[16] M. Malhotra and K. Trivedi, "Power-hierarchy of dependabiliyt-model types," *IEEE Transactions on Reliability*, vol. 43, no. 3, pp. 493-501, 1994.

[17] W. Lee, D. Grosh, F. Tillman, and C. Lie, "Fault tree analysis methods and applications - a review," *IEEE Transaction on Reliability*, vol. 43, no. 3, pp. 194-203, 1985.

[18] A. Bondavalli, S. Chiaradonna, F. Digiandomenico, and I. Mura, "Dependability modeling and evaluation of multiple-phased systems using DEEM," *IEEE Transactions on Reliability*, vol. 54, no. 4, pp. 509-522, 2004.

[19] F. Wang, B. Madan, and S. Trivedi, "Security analysis of SITAR intrusion tolerant system," in *Proc. of ACM Workshop on Survivable and self-Regenerative Systems*, pp. 23-32, 2003.

[20] C. Lin and Y. Wei, "Stochastic process algebra and stochastic petri nets," *Journal of Software*, vol. 13, no. 2, pp. 203-213, 2002.

[21] M. Amin, "Security challenges for the electricity infrastructure," *IEEE Security & Privacy Magazine*, vol. 35, no. 4, pp. 8-10, 2002.

[22] J. Katz, "Smart grid security and architecutral thinking," White Papers, 2010.

[23] E. Bompard, C. Gao, R. Napoli, A. Russo, M. Masera, and A. Stefanini, "Risk assessment of malicious attacks against power systems," *Transactions on System, Man, and Cybernetics*, vol. 39, no. 5, pp. 1074-1084, 2009.

[24] R. Zeng, Y. Jiang, C. Lin, X. Chu, and F. Liu, "Performance analysis of data management in sensor data storage via Stochasitc Petri Nets," in *Proc. of IEEE Globecom*, pp. 1-5, 2010.

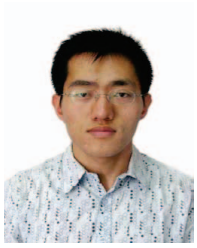
[25] C. Phillips and L. Swiler, "A graph-based system for network vulnerability analysis," in *Proc. of ACM New Security Paradigms Workshop*, pp. 71-79, 1998.

[26] R. Ortalo, Y. Deswarte, and M. Kaaniche, "Experimenting with quantitative evaluation tools for monitoring operational security," *IEEE Transactions on Software Engineering*, vol. 25, no. 5, pp. 633-650, 1999.

[27] O. Henry, B. William, and H. Roger, "Statistical model for a failure mode and effects analyisis and its application to computer fault-tracing," *IEEE Transactions on Reliability*, vol. 27, no. 1, pp. 16-22, 1978.

[28] T. Fluery, H. Kurana, and V. Welch, "Towards a taxonomy of attacks againsts energy control systems," in *Critical Infrastructure Protection II*, pp. 71-85, 2009.

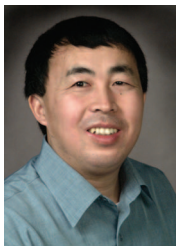
[29] L. Ferrarini, J. Carneiro, S. Radaelli, and E. Ciapessoni, "Dependability analysis of power systems protections using stochastic hybrid simulation with modelica," in *Proc. of IEEE International Conference on Robotics and Automation*, pp. 1584-1589, 2007.



Rongfei Zeng received a B.S. degree (2002) from Northeastern University (China) in computer science and technology. Currently, he is a Ph.D. candidate at Computer Science Department, Tsinghua University, China. His current research interests include wireless network security, smart grid, and performance evaluations.

Yixin Jiang is an associate professor in Tsinghua University. In 2007-2009, he was a Post Doctorial Fellow with University of Waterloo. He received the Ph.D. degree (2006) from Department of Computer Science and Technology, Tsinghua University, China. In 2005, he was a Visiting Scholar with the Department of Computer Sciences, Hong Kong Baptist University. In 2009, he was a Visiting Scholar with the Department of Computer Science and Engineering, the Chinese University of Hong Kong. He has served as the Technical Program Committee (TPC) member for main network conferences, such as IEEE ICCCN, IEEE GLOBECOM, IEEE ICC, IEEE WCNC, etc. He is a member of IEEE CISTC. His current research interests include network coding, clouding computing, security and privacy in wireless communication and mobile computing. He has received Excellent Backbone Talents Fund Award, Outstanding Doctoral Graduate Award, and Excellent Doctoral Thesis Award of Tsinghua University.

Chuang Lin (IEEE SM'04) is a professor of the Department of Computer Science and Technology, Tsinghua University, Beijing, China. He received the Ph.D. degree in Computer Science from the Tsinghua University in 1994. His current research interests include computer networks, performance evaluation, network security analysis, and Petri net theory and its applications. He has published more than 300 papers in research journals and IEEE conference proceedings in these areas and has published three books. Professor Lin is a member of ACM Council, a senior member of the IEEE and the Chinese Delegate in TC6 of IFIP. He serves as the Technical Program Vice Chair, the 10th IEEE Workshop on Future Trends of Distributed Computing Systems (FTDCS 2004); the General Chair, ACM SIGCOMM Asia workshop 2005; the Associate Editor, IEEE Transactions on Vehicular Technology; the Area Editor, Journal of Computer Networks; and the Area Editor, Journal of Parallel and Distributed Computing.



Xuemin (Sherman) Shen (IEEE M'97-SM'02-F'09) received the B.Sc. (1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a University Research Chair Professor, Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research focuses on mobility and resource management in interconnected wireless/wired networks, UWB wireless communications networks, wireless network security, wireless body area networks and vehicular ad hoc and sensor networks. He is a co-author of three books, and has published more than 400 papers and book chapters in wireless communications and networks, control and filtering. He is a Distinguished Lecturer of IEEE Communications Society. He serves as the Tutorial Chair for IEEE ICC'08, the Technical Program Committee Chair for IEEE Globecom'07, the General Co-Chair for Chinacom'07 and QShine'06, the Founding Chair for IEEE Communications Society Technical Committee on P2P Communications and Networking. He also serves as a Founding Area Editor for IEEE Transactions on Wireless Communications; Editor-in-Chief for Peer-to-Peer Networking and Application; Associate Editor for IEEE Transactions on Vehicular Technology; KICS/IEEE Journal of Communications and Networks, Computer Networks; ACM/Wireless Networks; and Wireless Communications and Mobile Computing (Wiley), etc. He has also served as Guest Editor for IEEE JSAC, IEEE Wireless Communications, IEEE Communications Magazine, and ACM Mobile Networks and Applications, etc. He received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004 and 2008 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. He is a registered Professional Engineer of Ontario, Canada.