On Reliability Analysis of Smart Grids under Topology Attacks: A Stochastic Petri Net Approach

BEIBEI LI, Nanyang Technological University, Singapore
RONGXING LU, University of New Brunswick, Canada
KIM-KWANG RAYMOND CHOO, University of Texas at San Antonio, USA
WEI WANG and SHENG LUO, Nanyang Technological University, Singapore

Building an efficient, smart, and multifunctional power grid while maintaining high reliability and security is an extremely challenging task, particularly in the ever-evolving cyber threat landscape. The challenge is also compounded by the increasing complexity of power grids in both cyber and physical domains. In this article, we develop a stochastic Petri net based analytical model to assess and analyze the system reliability of smart grids, specifically against topology attacks under system countermeasures (i.e., intrusion detection systems and malfunction recovery techniques). Topology attacks, evolving from false data injection attacks, are growing security threats to smart grids. In our analytical model, we define and consider both conservative and aggressive topology attacks, and two types of unreliable consequences (i.e., system disturbances and failures). The IEEE 14-bus power system is employed as a case study to clearly explain the model construction and parameterization process. The benefit of having this analytical model is the capability to measure the system reliability from both transient and steady-state analysis. Finally, intensive simulation experiments are conducted to demonstrate the feasibility and effectiveness of our proposed model.

CCS Concepts: • **Security and privacy → Systems security**; **Formal methods and theory of security**; • **Networks → Cyber-physical networks**;

Additional Key Words and Phrases: Cyber-physical systems, smart grids, topology attacks, system reliability, stochastic Petri net

ACM Reference format:
Beibei Li, Rongxing Lu, Kim-Kwang Raymond Choo, Wei Wang, and Sheng Luo. 2018. On Reliability Analysis of Smart Grids under Topology Attacks: A Stochastic Petri Net Approach. *ACM Trans. Cyber-Phys. Syst.* 3, 1, Article 10 (August 2018), 25 pages.
https://doi.org/10.1145/3127021

1 INTRODUCTION

The smart grid is envisioned as a revolutionary alternative of the legacy power grid with the primary expectation to achieve enhanced situational awareness of the enormous, and often

R. Lu is supported in part by Natural Sciences and Engineering Research (NSERC) Discovery Grants (No. Rgpin 04009), NBIF Start-Up Grant (Rif 2017012), and URF Grant (No. 124419), and K.-K.R. Choo is supported by the Cloud Technology Endowed Professorship.

Authors' addresses: B. Li, W. Wang, and S. Luo, School of Electrical and Electronic Engineering, Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798; emails: {bli012, wei001, sluo002}@e.ntu.edu.sg; R. Lu, Faculty of Computer Science, University of New Brunswick, 550 Windsor Street, Fredericton, Canada E3B 5A3; email: rlu1@unb.ca; K. K.-R. Choo, Department of Information Systems and Cyber Security, The University of Texas at San Antonio, 5 Paseo Del Norte, San Antonio, Texas 78249; email: raymond.choo@fulbrightmail.org.

https://doi.org/10.1145/3127021

dispersed, physical infrastructure (Li et al. 2016b; Choo 2014; Li et al. 2017). In addition, by taking full advantage of information and communication technologies, intelligent functionalities such as autonomous demand response, self-healing, self-resilience, and accommodation of renewable energy resources can potentially be achieved (Li et al. 2016a; Moslehi and Kumar 2010; Li et al. 2016a; Liu et al. 2016). Smart grids have also attracted the attention of policymakers and those in governments, as evidenced by the various policy and regulatory initiatives launched in recent years (Farhangi 2010; FERC 2009; Amin and Wollenberg 2005).

Despite these promising benefits, there are a number of underlying issues and challenges (Li et al. 2017; Deng et al. 2017; Wu et al. 2014). System reliability is one of the critical concerns in smart grids, and can be affected by a wide range of grid components (Moslehi and Kumar 2010; Li 2014). Specifically, demand-response strategies and peak load shedding techniques play significant roles in balancing (due to load variability) power demands and generations to preserve grid reliability. Other considerations important in preserving grid reliability include performance and lifetime of the substations, transmission lines, and electrical devices. Renewable resources, such as wind, solar, hydro, and tidal, may also impact on system reliability due to their volatile nature. Similar to other consumer technologies, ensuring the integrity and authenticity of measurement data reported by sensing devices (e.g., line meters, circuit breaker monitors, and smart meters) are also vital to ensure grid reliability (i.e., in terms of system state estimation and informing decision-making). For example, biased or fabricated measurements could potentially result in the system control center issuing erroneous feedback commands, and consequently, compromising the system reliability.

Despite the importance of system reliability, this topic is rarely considered in the power community. With the increasing trend in smart grids being the target of cyber attacks and physical sabotages impacting on the reliability of smart grids (Falliere et al. 2011; Pagliery 2015), it is important to ensure a resilient and reliable system design. A successful attack or compromise can have significant impacts, as illustrated by recent incidents (e.g., Stuxnet (Falliere et al. 2011)). While there has been recent interest in smart grid security research, existing literature generally focus on single-event attacks rather than coordinated attacks. This is partially because existing mathematical tools for modeling and analyzing coordinated attacks are not well developed to handle sophisticated coordinated attacks (Kröger 2008). For example, attack trees are popular tools in existing literature used to describe the conceptual diagram of a single attack. However, attack trees are not suitable for modeling and capturing concurrent and coordinated attacks. In addition, there are only a few studies introducing modeling tools that can adequately capture the dynamics between attacks and defenses, as well as capturing the synthetic idiosyncrasies of a smart grid cyber-physical system (Lee 2017). This is the gap we seek to address in this article.

Specifically, we introduce the topology attacks (Kim and Tong 2013), a typical example of coordinated attacks in the context of smart grids. We then use a stochastic Petri net (SPN) (Dalton et al. 2006; Mitchell and Chen 2016) to model the topology attacks and analyze the system reliability in the presence of both intrusion detection systems and malfunction recovery techniques. Evolving from bad data injection attacks, topology attacks have been the subject of research in recent years. For example, Liu et al. showed in 2011 that by compromising a set of metering devices, attackers are capable of constructing an attack vector that can easily circumvent the conventional bad data detector; thus, launching a successful bad data injection attack (Liu et al. 2011). A key limitation that may impede a successful implementation of such attacks is the need to compromise a large set of metering devices. This is a significantly strong assumption because attackers usually have limited time and capabilities. To avoid these limitations associated with bad data injection attacks, topology attacks have quickly emerged recently with reduced requirements for attacks. Ideally, by concurrently compromising only a very small set of sensing devices such as line meters and circuit breaker monitors, the adversary could initiate a successful topology attack. Petri nets are

tools that have been widely used for modeling various types of asynchronous and concurrent processes; therefore, they are more suitable for modeling the coordinated topology attacks and capturing the concurrent behaviors of both cyber and physical processes in smart grids.

We regard the contributions of this article to be threefold:

- —First, we develop a novel analytical model to assess and analyze the system reliability in the presence of both topology attacks and countermeasures in smart grids (i.e., intrusion detection systems and malfunction recovery techniques). Since topology attacks are commonly considered as "undetectable" attacks, understanding their attack behaviors and corresponding potential impacts contribute to the building of a more resilient and reliable smart grid.
- —Second, we define and characterize two types of topology attacks, namely, conservative topology attacks and aggressive topology attacks. Different attack behaviors and their associated impacts on smart grids are then discussed.
- —Third, we propose a scheme to determine whether the undetected compromised sensing devices can launch a successful topology attack. Following this, different types of the impacts, e.g., system disturbances or failures, of successful attacks are discussed. In addition, an algorithm for construction of a maximum spanning tree (MxST) (McDonald et al. 2005) in a power system is proposed.

This is, to the best of our best knowledge, the first study to use an SPN to study topology attacks in the context of smart grids. The choice of SPN is due to its capability of incorporating features of both the cyber domain (e.g., cyber intrusion process and corresponding state transition process) and the physical domain (e.g., physical measurement data and possible impacts and outages).

We will review related literature in the next section, before presenting the system model, threat model, and our design goals in Section 3. Our proposed analytical model is elaborated in Section 4, and the performance evaluation is presented in Section 5. Section 6 concludes the article.

2 RELATED LITERATURE

2.1 Petri Net Modeling

The Petri net modeling techniques are increasingly popular, partly due to the rapid advancements of networked and distributed systems (Mitchell and Chen 2016). A basic Petri net can be described as a 4-tuple $(\mathcal{P}, \mathcal{T}, \mathcal{F}, \mathcal{M})$, where $\mathcal{P}$ is a finite set of places (or states), $\mathcal{T}$ is a finite set of transitions (or actions, behaviors), $\mathcal{F} \subset (\mathcal{P} \times \mathcal{T}) \cup (\mathcal{T} \times \mathcal{P})$ is a finite set of input and output arcs, and $\mathcal{M}$ is a finite set of markings that denote the number of tokens in each place. A token represents an object that holds a specific condition or the occurrence of a specific event. Tokens can be transferred from place to place when a specific condition changes or event occurs. Since a basic Petri net can only model fairly simple processes, a number of extended Petri nets have been proposed in the literature to support a broader range of applications (Jensen and Rozenberg 2012).

The Petri net technique was first used for modeling cyber attacks by, presumably, McDermott as an alternative tool to traditional attack trees (McDermott 2001). It was demonstrated that Petri nets were more effective than traditional attack trees in describing the concurrent processes. The generalized SPN technique was subsequently introduced by Bause et al. to model cyber attacks (Bause and Kritzinger 2002). An SPN is a timed Petri net, where the firing time between the transitions is assumed to be exponentially distributed. With the SPN, the state transition process can be easily transformed to a reachability graph, and then a continuous time Markov chain. In this way, it facilitates system administrators in performing steady-state analysis. SPNs are increasingly accepted by the research community, and have been used to support diverse applications (Tüysüz and Kahraman 2010; Jensen 2013; Laprie et al. 2007; Zeng et al. 2012; Chen et al. 2011). Another

extension is the colored Petri net, where tokens are represented by different colors. Different from the basic Petri net, a colored Petri net can be used to model more complex systems or processes. For example, Jensen suggested that colored Petri nets can be used for a wide range of practical applications, such as ATM networks, ISDN networks, and naval vessel systems (Jensen 2013).

Petri net modeling techniques have also been used in power systems to describe the state transition processes of physical systems and the communication infrastructures (Laprie et al. 2007; Zeng et al. 2012; Chen et al. 2011). For instance, Laprie et al. used a Petri net to model the interdependence related failures of both electric infrastructure and connected information system. In addition, Zeng et al. analyzed the dependability of control center networks in smart grids using SPN by considering that the servers in control center networks can suffer from Byzantine failures and, thus compromise the network dependability. However, there has been no effective modeling technique developed for modeling topology attacks in smart grids, especially in the presence of system countermeasures.

2.2 Coordinated Attacks

In the increasingly complex and large-scale cyber-physical infrastructures, it is usually far beyond the capability of a single attacker to disrupt such an infrastructure. It is more likely that well-resourced attackers (e.g., state-sponsored actors and organized cyber crime groups) will attempt to launch a coordinated attack collectively, an observation echoed in the report from CERT (Householder et al. 2002).

In the context of smart grid CPS, coordinated attacks include false data injection attacks (Liu et al. 2011; Deng et al. 2017; Li et al. 2017), topology attacks (Weimer et al. 2012; Kim and Tong 2013), and denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks (Liu et al. 2013; Amin et al. 2009). Since Liu demonstrated that a set of coordinated attackers can successfully circumvent the traditional bad data detection mechanisms in power systems (Liu et al. 2011), researchers have started studying such attacks (e.g., see the survey of attack strategies, potential impacts on power systems, and potential countermeasures in Deng et al. (2017)). False data injection attackers can construct an attack vector containing injected false measurement data by compromising an ideal set of data meters. The injected attack vector, if well designed, will easily circumvent bad data detector at the data center without triggering an alarm. Hug et al. introduced a new analytical technique for vulnerability analysis of state estimation, designed to detect hidden false data injection attacks (Hug and Giampapa 2012). A distributed host-based collaborative detection scheme for false data injection attacks in a smart grid cyber-physical system was also recently proposed (Li et al. 2017).

The focus of this article is on the topology attacks that have not yet been widely investigated. Topology attacks are generally considered evolved false data injection attacks, where meter data and breaker status data used for determining the current system topology need to be manipulated. Similar to false data injection attackers, topology attackers also try to blind the bad data detector by constructing matched meter data and breaker status data. A small number of existing studies have discussed such attacks. For example, Weimer et al. proposed a distributed detection and isolation method for topology attacks in power networks (Weimer et al. 2012). Kim and Tong proposed a graph theory based scheme to counter topology attacks by placing the phasor measurement units across the power gird in an optimal way (Kim and Tong 2013). Apart from the above-mentioned few studies that focus on topology attacks, one particular relevant area that is understudied is topology attack modeling and system reliability analysis when subject to such attacks. Thus, in this article, we provide an SPN-based analytical model for smart grids to model the attack behaviors of topology attacks and analyze the system reliability in the presence of such attacks.

Table 1. Summary of Notations

Notation	Description
$\mathbf{z}$	Vector of measurement data collected by line meters
$\mathbf{s}$	Vector of circuit breaker status data collected by breaker monitors
$\mathbf{x}$	Vector of real system status data
$\boldsymbol{\eta}$	Vector of measurement error
$\mathbf{C}$	Covariance matrix of $\boldsymbol{\eta}$
$\mathbf{r}$	Vector of measurement residual
m	Number of measurements
n	Number of real system status
$\mathcal{G}$	Topology graph of a power grid
$\mathbf{H}_{\mathcal{G}}$	Jacobian matrix of measurement data associated with $\mathcal{G}$
$\mathcal{S}$	Maximum spanning tree of a grid topology $\mathcal{G}$
$\mathcal{P}$	Set of places in a Petri net
$\mathcal{T}$	Set of transitions in a Petri net
$\mathcal{F}$	Set of input and output arcs in a Petri net
$\mathcal{M}$	Set of markings in a Petri net
$\mathcal{W}$	Set of weights assigned for all the branches in a power grid
$\mathcal{L}$	Set of compromised line meters
$\mathcal{B}$	Set of compromised breaker monitors
O	Decision outcome
N	Total number of branches in a power grid
R	System reliability of a power grid

3 MODELS AND DESIGN GOALS

In this section, we formalize both the system and threat models, as well as describe the design goals. The notations used in this article are summarized in Table 1.

3.1 System Model

In existing power systems, state estimation is the most widely used technique for estimating system operating status as well as detecting bad collected measurement data. In this article, we use the power system state estimation workflow as our system model (see Figure 1).

In state estimation, the system control center collects two types of data from the sensing devices throughout the grid. One type of data is the line flow and nodal injection analog measurement data $\mathbf{z} = \{P_i, Q_i, P_f, Q_f, V, \theta\}$ provided by line meters, where P_i, Q_i, P_f, Q_f, V, and θ denote real power injection, reactive power injection, real power flow, reactive power flow, bus voltage magnitude, and bus voltage angle, respectively. Another type of data is the circuit breaker on/off status data $\mathbf{s} = s_i^N$, where $s_i \in \{0, 1\}$ and N is the total number of branches in a power grid. The status data $\mathbf{s}$ is provided by circuit breaker monitors (Djekic 2007) and then analyzed by the topology processor to determine the current grid topology $\mathcal{G}$, that is, $\mathcal{G} = f(\mathbf{s})$. After that, both measurement data $\mathbf{z}$ and grid topology $\mathcal{G}$ are fed into the state estimator for further data processing. Using an alternating current (AC) or direct current (DC) power flow model, the state estimator produces the estimated real system status data $\mathbf{x} = \{\hat{V}, \hat{\theta}\}$. At the last step, through residual checking, the bad data detector determines whether any bad data is collected by the sensing devices.

Let us take the DC power flow model as an example to introduce the detailed procedure of state estimation. According to this model, the relationship between the measurement data $\mathbf{z} \in \mathbb{R}^{m\times 1}$ and

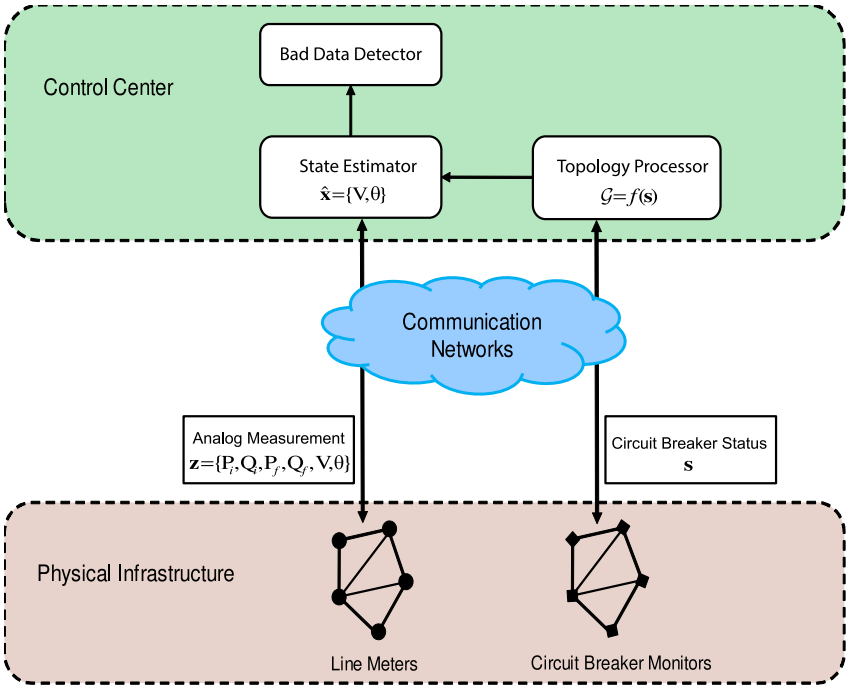

Fig. 1. System model: power system state estimation.

real system status data $\mathbf{x} \in \mathbb{R}^{n\times 1}$ is given by Deng et al. (2017):

$$\mathbf{z} = \mathbf{H}_{\mathcal{G}}\mathbf{x} + \boldsymbol{\eta}, \tag{1}$$

where $\mathbf{H}_{\mathcal{G}} \in \mathbb{R}^{m\times n}$ is the measurement Jacobian matrix associated with the current system topology $\mathcal{G}$. m and n are the numbers of measurement data and real system status data, respectively, and $m > n$ indicates that redundant measurements are introduced. $\boldsymbol{\eta} \in \mathbb{R}^{m\times 1}$ is the measurement noise vector with zero mean and covariance $\mathbf{C}$, a diagonal matrix.

Generally, we cannot directly observe the real status data $\mathbf{x}$, but we can infer from the measurement data $\mathbf{z}$. Due to the measurement noise $\boldsymbol{\eta}$, the optimal estimated $\hat{\mathbf{x}}$ is the vector that generates the minimum weighted square error. According to the DC flow model, the objective function is as follows:

$$\mathbf{J}(\mathbf{x}) = \min_{\mathbf{x}} [\mathbf{z} - \mathbf{H}_{\mathcal{G}}\mathbf{x}]^T \mathbf{C}^{-1} [\mathbf{z} - \mathbf{H}_{\mathcal{G}}\mathbf{x}]. \tag{2}$$

Then, the estimated $\hat{\mathbf{x}}$ is given by

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}} [\mathbf{z} - \mathbf{H}_{\mathcal{G}}\mathbf{x}]^T \mathbf{C}^{-1} [\mathbf{z} - \mathbf{H}_{\mathcal{G}}\mathbf{x}]. \tag{3}$$

The linear DC state estimation has a closed-form solution, which is obtained through a non-iterative procedure by solving Equation (3). The result is given by

$$\hat{\mathbf{x}} = [\mathbf{H}_{\mathcal{G}}{}^T \mathbf{C}^{-1} \mathbf{H}_{\mathcal{G}}]^{-1} \mathbf{H}_{\mathcal{G}}{}^T \mathbf{C}^{-1} \mathbf{z} \triangleq \Lambda \mathbf{z}, \tag{4}$$

where

$$\Lambda \triangleq [\mathbf{H}_{\mathcal{G}}{}^T \mathbf{C}^{-1} \mathbf{H}_{\mathcal{G}}]^{-1} \mathbf{H}_{\mathcal{G}}{}^T \mathbf{C}^{-1}. \tag{5}$$

Then, the estimated measurement data $\hat{\mathbf{z}}$ can then be given by

$$\hat{\mathbf{z}} = \mathbf{H}_{\mathcal{G}}\hat{\mathbf{x}} = \mathbf{H}_{\mathcal{G}}\Lambda\mathbf{z}. \tag{6}$$

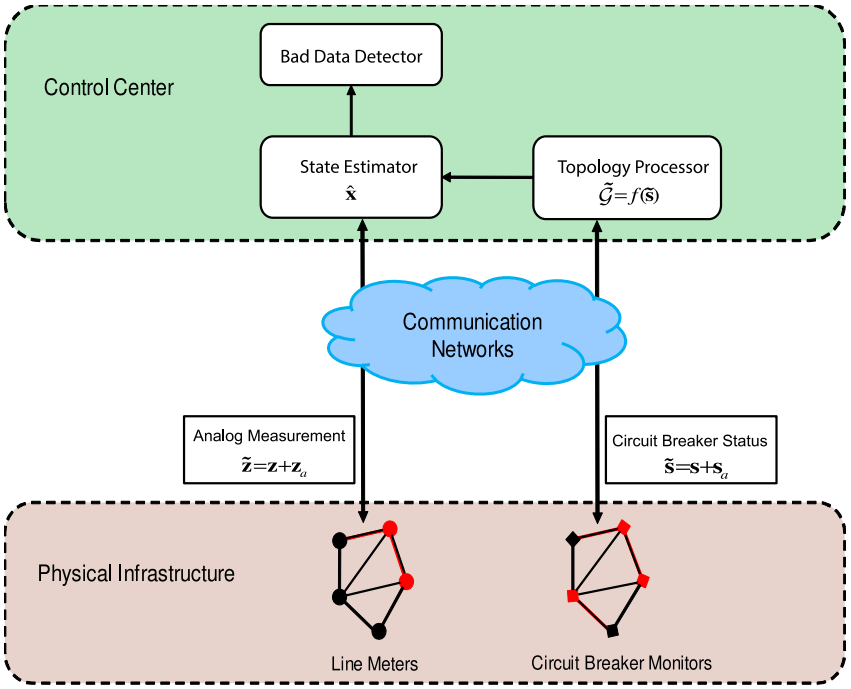

Fig. 2. Adversary model.

Once the system real status data $\hat{\mathbf{x}}$ has been identified, the largest normalized residuals (LNR) can be used to detect the biased measurement data. Specifically, the measurement residual $\mathbf{r} \in \mathbb{R}^{m\times 1}$ is calculated based on the difference between the measurement data $\mathbf{z}$ and the estimated measurements $\hat{\mathbf{z}}$, i.e.,

$$\mathbf{r} = \mathbf{z} - \hat{\mathbf{z}} = \mathbf{z} - \mathbf{H}_{\mathcal{G}}\Lambda\mathbf{z} = (\mathbf{I} - \mathbf{H}_{\mathcal{G}}\Lambda)\mathbf{z}, \tag{7}$$

where $\mathbf{I} \in \mathbb{R}^{m\times m}$ is the identity matrix. The LNR test is to compare the Frobenius norm $\|\mathbf{r}\|_2$ of the measurement residual $\mathbf{r}$ with a predefined threshold τ. $||\mathbf{r}||_2 > \tau$ indicates that anomalous residuals exist; hence, bad measurement data presents in $\mathbf{z}$. Otherwise (i.e., $||\mathbf{r}||_2 <= \tau$), it implies that there is no bad measurement data.

3.2 Adversary Model

In this article, we consider the adversaries are topology attackers whose objective is to compromise the system reliability and survivability. As previously discussed, topology attacks can be regarded as evolved false data injection attacks. With regard to false data injection attacks, adversaries generally tamper with only the measurement data $\mathbf{z}$. In practice, these false data can often be detected by the bad data detector due to mismatches with the current system topology $\mathcal{G}$. However, topology attackers may also attempt to falsify both measurement data $\mathbf{z}$ and circuit breaker status data $\mathbf{s}$ associated with the system topology $\mathcal{G}$ (i.e., $\mathcal{G} = f(\mathbf{s})$ (Kim and Tong 2013). In other words, they attempt to construct a pair of matched measurement data and the grid topology. Such an attack strategy can be more effective to blind the bad data detector.

In our adversary model as shown in Figure 2, we assume that the sensing devices (i.e., line meters and circuit breaker monitors) deployed throughout the power grid can be compromised by malicious attackers (including malicious insiders and external attackers). These attackers are

capable of controlling the sensing devices to report false measurement data. In Figure 2, compromised line meters and circuit breaker monitors, represented by red circles and squares, construct attack vectors $\mathbf{z}_a$ and $\mathbf{s}_a$. Then, the reported measurement data $\tilde{\mathbf{z}}$ and circuit breaker status data $\tilde{\mathbf{s}}$ are, respectively, expressed as the following:

$$\tilde{\mathbf{z}} = \mathbf{z} + \mathbf{z}_a, \tag{8}$$

and

$$\tilde{\mathbf{s}} = \mathbf{s} + \mathbf{s}_a. \tag{9}$$

Correspondingly, the processed grid topology is given by

$$\tilde{\mathcal{G}} = f(\tilde{\mathbf{s}}) = f(\mathbf{s} + \mathbf{s}_a), \tag{10}$$

where $f(\cdot)$ is the system function of the topology processor.

Likewise, according to the DC power flow model, the relationship between the measurement data $\tilde{\mathbf{z}}$ and real system status data $\mathbf{x}$ is described as follows:

$$\tilde{\mathbf{z}} = \mathbf{H}_{\tilde{\mathcal{G}}}\mathbf{x} + \boldsymbol{\eta}. \tag{11}$$

Then, the estimated $\hat{\mathbf{x}}$ is given by

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}}[\tilde{\mathbf{z}} - \mathbf{H}_{\tilde{\mathcal{G}}}\mathbf{x}]^T\mathbf{C}^{-1}[\tilde{\mathbf{z}} - \mathbf{H}_{\tilde{\mathcal{G}}})\mathbf{x}] = [\mathbf{H}_{\tilde{\mathcal{G}}}{}^T\mathbf{C}^{-1}\mathbf{H}_{\tilde{\mathcal{G}}}]^{-1}\mathbf{H}_{\tilde{\mathcal{G}}}{}^T\mathbf{C}^{-1}\tilde{\mathbf{z}} \triangleq \tilde{\Lambda}\tilde{\mathbf{z}}, \tag{12}$$

where

$$\tilde{\Lambda} = [\mathbf{H}_{\tilde{\mathcal{G}}}{}^T\mathbf{C}^{-1}\mathbf{H}_{\tilde{\mathcal{G}}}]^{-1}\mathbf{H}_{\tilde{\mathcal{G}}}{}^T\mathbf{C}^{-1}. \tag{13}$$

Thus, the estimated measurement data $\hat{\mathbf{z}}$ is calculated by

$$\hat{\mathbf{z}} = \mathbf{H}_{\tilde{\mathcal{G}}}\hat{\mathbf{x}} = \mathbf{H}_{\tilde{\mathcal{G}}}\tilde{\Lambda}\tilde{\mathbf{z}}. \tag{14}$$

The residual $\tilde{\mathbf{r}}$ is then given by

$$\tilde{\mathbf{r}} = \tilde{\mathbf{z}} - \hat{\mathbf{z}} = (\mathbf{I} - \mathbf{H}_{\tilde{\mathcal{G}}}\tilde{\Lambda})\tilde{\mathbf{z}}. \tag{15}$$

One last and critical step is to detect the bad data. The Frobenius norm $\|\tilde{\mathbf{r}}\|_2 = \|(\mathbf{I} - \mathbf{H}_{\tilde{\mathcal{G}}}\tilde{\Lambda})\tilde{\mathbf{z}}\|_2$ can be seen as a function of $\tilde{\mathbf{z}}$ and $\tilde{\mathbf{s}}$ (recall that $\mathcal{G} = f(\mathbf{s})$). In this way, as long as the constructed vectors $\mathbf{z}_a$ and $\mathbf{s}_a$ can lead to

$$\|\tilde{\mathbf{r}}\|_2 = \|(\mathbf{I} - \mathbf{H}_{\tilde{\mathcal{G}}}\tilde{\Lambda})\tilde{\mathbf{z}}\|_2 < \tau, \tag{16}$$

the adversaries can launch successful topology attacks without being detected; otherwise, the injected bad data can be detected.

In this article, we define two types of topology attacks in terms of the attack strategies, which are shown as follows:

- *Conservative topology attacks:* such attacks aim to manipulate a single or a few transmission lines or buses by compromising a small number of sensing devices. Accordingly, manipulation of these limited resources results in minor impact on the power system (e.g., disturbances).
- *Aggressive topology attacks:* such attacks attempt to manipulate as large an area of power grid as possible (e.g., by compromising as many sensing devices as possible). These attacks usually result in devastating damages to the power system (e.g., system failures), if successful.

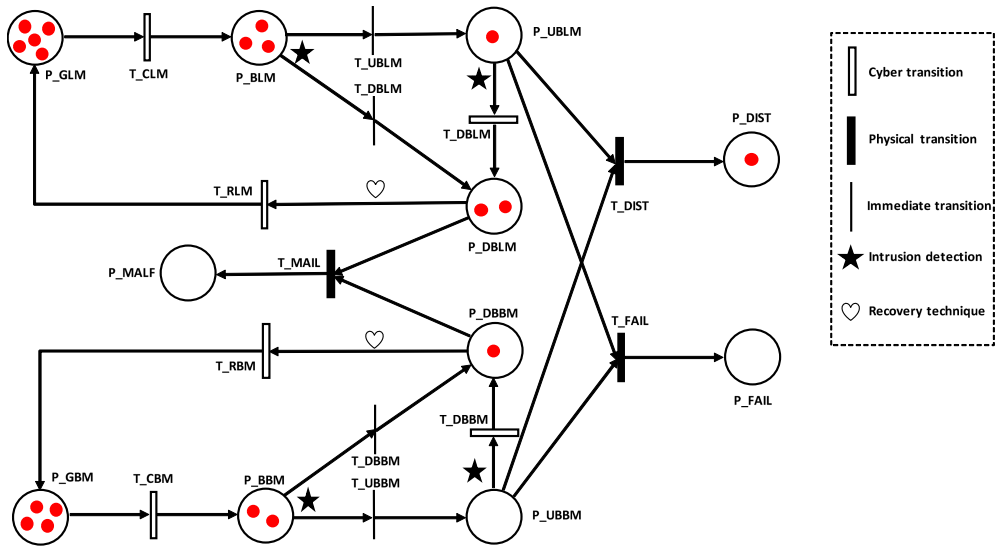

Fig. 3. Analytical SPN model.

3.3 Design Goals

The key objective of our work is to provide an analytical model for studying topology attacks in smart grids, as well as analyzing the system reliability in the presence of such attacks. Specifically, our design goals are as follows:

(1) Carrying out in-depth analyses on the attack strategies of different types of topology attacks and potential impacts on the power system they may cause.
(2) Establishing an SPN-based state transition model for smart grids to describe the system behaviors in the presence of topology attacks.
(3) Defining credible metrics to accurately assess the system reliability of smart grids.

4 PROPOSED ANALYTICAL MODEL

In this section, we present our SPN-based analytical model (see Figure 3) to describe the system behaviors in the presence of both topology attacks and system security countermeasures (e.g., intrusion detection systems and malfunction recovery techniques).

4.1 Construction of the Proposed SPN Model

We now present the construction of the proposed SPN model. Tables 2 and 3 annotate the physical meanings of places and transitions in the SPN model, respectively. Cyber transitions are denoted using blank bars, while physical transitions are shown as filled bars. Note that, in particular, immediate transitions also appear in our model, which belongs to cyber transitions and they are presented by slim vertical bars. In this SPN model, we mainly consider two types of sensing devices, namely, line meters and circuit breaker monitors. Small filled circles in red (tokens) are used to represent the sensing devices holding specific conditions. In terms of countermeasures, we use filled black stars ★ to denote the presence of intrusion detection systems. The intrusion detection systems are deployed for periodical detection of sensing device malfunctions. In addition, the malfunction recovery techniques, represented by blank hearts

Table 2. Places in the SPN Model

Place	Meaning
P_GLM	Place of good line meters
P_BLM	Place of bad line meters
P_GBM	Place of good breaker monitors
P_BBM	Place of bad breaker monitors
P_DBLM	Place of detected bad line meters
P_UBLM	Place of undetected bad line meters
P_DBBM	Place of detected bad breaker monitors
P_UBBM	Place of undetected bad breaker monitors
P_DIST	Place of system disturbance: 0 before and 1 after
P_FAIL	Place of system failure: 0 before and 1 after
P_MALF	Place of system malfunction: 0 before and 1 after

Table 3. Transitions in the SPN Model

Transition	Meaning
T_CLM	Transition that the attacker compromises a line meter
T_CBM	Transition that the attacker compromises a breaker monitor
T_DBLM	Transition that the intrusion detection system detects a bad line meter
T_UBLM	Transition that the intrusion detection system fails to detect a bad line meter
T_DBBM	Transition that the intrusion detection system detects a bad breaker monitor
T_UBBM	Transition that the intrusion detection system fails to detect a bad breaker monitor
T_RLM	Transition that the system operator recovers a line meter
T_RBM	Transition that the system operator recovers a breaker monitor
T_DIST	Transition that the power grid encounters a system disturbance
T_FAIL	Transition that the power grid encounters a system failure
T_MALF	Transition that the power grid encounters a system malfunction

♡, are designed for recovering the malfunction devices identified by the intrusion detection systems.

The SPN model has an 11-element set of place $\mathcal{P}$ = {P_GLM, P_BLM, P_GBM, P_BBM, P_DBLM, P_UBLM, P_DBBM, P_UBBM, P_DIST, P_FAIL, P_MALF}. Specifically, places P_GLM, P_BLM, P_GBM, and P_BBM hold the counts for good line meters, bad line meters, good breaker monitors, and bad breaker monitors, respectively. Likewise, places P_DBLM, P_UBLM, P_DBBM, and P_UBBM hold the counts for detected bad line meters, undetected bad line meters, detected bad breaker monitors, and undetected bad breaker monitors, respectively. Place P_DIST, if holding a token, represents a system disturbance event resulting from places P_UBLM and P_UBBM when transition T_DIST is enabled. Similarly, place P_FAIL, if holding a token, represents a system failure event resulting from places P_UBLM and P_UBBM when transition T_FAIL is enabled. In particular, if place P_MALF holds a token, the whole power system is encountered with a system malfunction transferred from places P_DBLM and P_DBBM when detected bad line meters and breaker monitors are unable to be timely recovered.

We use the following events to show how this SPN model is constructed, and how the system behaves under various event triggers.

—The first event is model initialization. We use tokens in a place to represent the sensing devices that meet the conditions specified by this place. Particularly, as for places

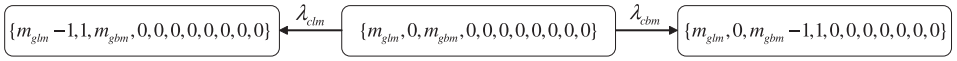

Fig. 4. System state transitions triggered by the second event: a good sensing device in place P_GLM or P_GBM is compromised by an attacker.

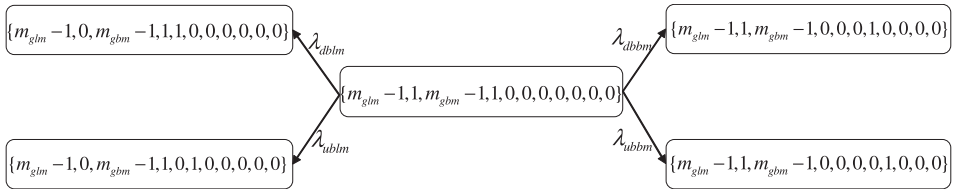

Fig. 5. System state transitions triggered by the third event: a compromised bad sensing device in place P_BLM or P_BBM is detected or undetected by the intrusion detection system.

P_DIST, P_FAIL, and P_MALF, holding a token represents the occurrence of this event; otherwise, empty places denote no occurrence of such events. A marking is a sequence of token states in all the places, which is denoted by $\mathcal{M} = \{m_{glm}, m_{blm}, m_{gbm}, m_{bbm}, m_{dblm}, m_{ublm}, m_{dbbm}, m_{ubbm}, m_{dist}, m_{fail}, m_{malf}\}$, where, particularly as mentioned above, m_{dist}, m_{fail}, and m_{malf} can only take values of either 0 or 1. Initially, all the devices are uncompromised/good, thereby the marking can be initialized as $\mathcal{M}_0 = \{m_{glm}, 0, m_{gbm}, 0, 0, 0, 0, 0, 0, 0, 0\}$.

—The second event is an attacker compromising a line meter or a breaker monitor. We use the compromising rates λ_{clm} and λ_{cbm} to denote, for each token in good places, the average number of tokens per unit time that can be transferred to bad places. Such transitions can be seen from Figure 4. Firing a transition will move one token from the input place to the output place. For example, firing T_CLM in state $\{m_{glm}, 0, m_{gbm}, 0, 0, 0, 0, 0, 0, 0, 0\}$ will move one token from P_GLM to P_BLM, transforming to state $\{m_{glm} - 1, 1, m_{gbm}, 0, 0, 0, 0, 0, 0, 0, 0\}$.

—The third event is concerned with detecting or failing to detect a compromised bad sensing device from place P_BLM or P_BBM using the intrusion detection system. For a newly compromised device within a detection interval, the intrusion detection system may fire two kinds of transitions. For example, as shown in Figure 5, if the intrusion detection system successfully detects a bad line meter in state $\{m_{glm} - 1, 1, m_{gbm} - 1, 1, 0, 0, 0, 0, 0, 0, 0\}$, T_DBLM will be fired transforming the system into state $\{m_{glm} - 1, 0, m_{gbm} - 1, 1, 1, 0, 0, 0, 0, 0, 0\}$ with rate λ_{dblm}; otherwise, T_UBLM will be fired transforming the system into state $\{m_{glm} - 1, 0, m_{gbm} - 1, 1, 0, 1, 0, 0, 0, 0, 0\}$ with rate λ_{ublm}. Similar transitions for bad breaker monitors transitions are also shown in Figure 5.

—The fourth event is concerned with detecting a compromised bad device from place P_UBLM or P_UBBM using the intrusion detection system. Devices (tokens) in place P_UBLM or P_UBBM are compromised bad devices that, heretofore, have not been detected yet. The intrusion detection system runs periodically to check all the devices, perhaps by trust reputation (Li et al. 2016b); thus, the compromised devices may be identified at any detection interval or even undetected for a significantly long period. As shown in Figure 6, if the intrusion detection system successfully detects a bad line meter in state $\{m_{glm} - 2, 0, m_{gbm} - 1, 0, 1, 1, 0, 1, 0, 0, 0\}$, T_DBLM will be fired transforming the system into state $\{m_{glm} - 2, 0, m_{gbm} - 1, 0, 2, 0, 0, 1, 0, 0, 0\}$ with rate λ_{dblm}. Similarly, if transition T_DBBM is fired, a bad breaker monitor will be detected transforming the system into state $\{m_{glm} - 2, 0, m_{gbm} - 1, 0, 1, 1, 1, 0, 0, 0, 0\}$ with rate λ_{dbbm}.

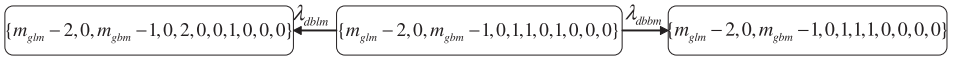

Fig. 6. System state transitions triggered by the fourth event: a compromised bad sensing device in place P_UBLM or P_UBBM is detected by the intrusion detection system.

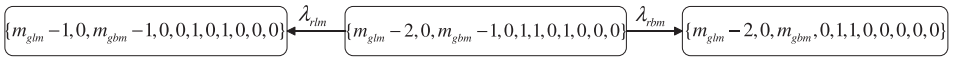

Fig. 7. System state transitions triggered by the fifth event: a detected bad sensing device in place P_DBLM or P_DBBM is recovered by the malfunction recovery technique.

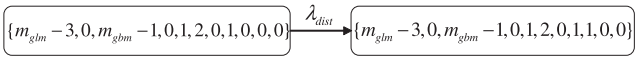

Fig. 8. System state transitions triggered by the sixth event: a system disturbance is caused by a, most probably conservative, topology attack.

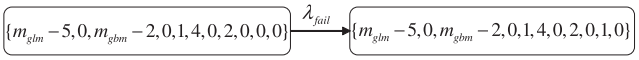

Fig. 9. System state transitions triggered by the seventh event: a system failure is caused by a, most probably aggressive, topology attack.

—The fifth event is concerned with recovering a detected bad device using malfunction recovery techniques. When a bad device is successfully detected by an intrusion detection system, the system administrator will carry out the malfunction recovery techniques to record and reset the compromised bad device. As shown in Figure 7, if transition T_RLM is fired with rate λ_{rlm} in state $\{m_{glm}-2,0,m_{gbm}-1,0,1,1,0,1,0,0,0\}$, a detected bad line meter is recovered to a good line meter, transforming the system state into $\{m_{glm}-1,0,m_{gbm}-1,0,0,1,0,1,0,0,0\}$. Likewise, if transition T_RBM is fired with rate λ_{rbm} in state $\{m_{glm}-2,0,m_{gbm}-1,0,1,1,0,1,0,0,0\}$, a detected bad breaker monitor is recovered to a good breaker monitor, transforming the system state into $\{m_{glm}-2,0,m_{gbm},0,1,1,0,0,0,0,0\}$.

—The sixth event considers a successful topology attack, usually conservative, causing a system disturbance. A small number of undetected bad line meters and breaker monitors can construct a conservative topology attack to fire transition T_DIST. An example is shown in Figure 8, where a system disturbance occurs with state $\{m_{glm}-3,0,m_{gbm}-1,0,1,2,0,1,1,0,0\}$ resulting from state $\{m_{glm}-3,0,m_{gbm}-1,0,1,2,0,1,0,0,0\}$ when T_DIST is enabled. The enabling function is a complex process based on the spanning tree of the power grid topology, which is detailed in the unreliability enabling scheme that will be introduced in the next subsection.

—The seventh event considers a successful topology attack, usually aggressive, causing a system failure. A multitude of undetected bad line meters and breaker monitors can collectively construct an aggressive topology attack to fire transition T_FAIL. An example is shown in Figure 9, where a system failure occurs with state $\{m_{glm}-5,0,m_{gbm}-2,0,1,4,0,2,0,1,0\}$ resulting from state $\{m_{glm}-5,0,m_{gbm}-2,0,1,4,0,2,0,0,0\}$ when T_FAIL is enabled. Likewise, the enabling function is a complex process based on the spanning tree of the power grid topology, which is detailed in the unreliability enabling scheme that will be introduced in the next subsection.

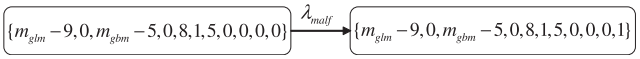

Fig. 10. System state transitions triggered by the eighth event: a system malfunction is caused by insufficient good sensing devices.

Table 4. Weights Assigned to Each Bus

Bus type	Description	Weight assigned
Type 1	Bus with line(s) only but no generator or load	1 unit
Type 2	Bus with line(s) and load(s) but no generator	2 units
Type 3	Bus with line(s) and generator but no load	3 units
Type 4	Bus with line(s), generator and load(s)	4 units

—The last event considers a system malfunction caused by insufficient good sensing devices. If the system has a low recovery rate (i.e., λ_{rlm} and λ_{rbm} are significantly small values), the detected bad sensing devices cannot be recovered in time leaving many detected bad devices remaining in places P_DBLM and P_DBBM. In this case, insufficient good sensing devices can operate normally to support the wide area monitoring functionality. Then, the power system malfunctions because the system states are no longer fully observable to the system control center (Huang et al. 2014). As we see, a number of unrecovered bad line meters and breaker monitors can collectively fire transition T_MALF to cause a system malfunction. As shown in Figure 10, a system malfunction with state $\{m_{glm} - 9, 0, m_{gbm} - 5, 0, 8, 1, 5, 0, 0, 0, 1\}$ may occur from state $\{m_{glm} - 9, 0, m_{gbm} - 5, 0, 8, 1, 5, 0, 0, 0, 0\}$ with rate λ_{malf} when T_MALF is enabled. The enabling function is straightforward and integrated in the unreliability enabling scheme that will be introduced in the next subsection.

4.2 Maximum Spanning Tree Based Unreliability Enabling Scheme

We will now present the proposed scheme composed of two algorithms to determine under what conditions the power system will fall into the unreliability status (i.e., disturbance, failure, or malfunction).

4.2.1 MxST Construction Algorithm. In our scheme, we use the spanning tree in graph theory to determine the most critical measurements. According to the contraction-deletion theorem (Vildhϕj and Wind 2016), there may be multiple spanning trees for a graph $\mathcal{G}$. To obtain the best results, we use the MxST (McDonald et al. 2005). MxST is a spanning tree of a weighted graph $\mathcal{G}$, where the weight sum of all edges is the maximum over all $\mathcal{G}$'s spanning trees. In our scheme, we allocate weights toward the branches to indicate the different levels of significance to the power grid, in terms of its observability and reliability. This is how we use the MxST of a grid topology to determine the most critical branches of a power grid.

There may be various methods to determine the weights assigned to each line. In this article, we use a straightforward approach to achieve this goal as shown in Table 4. Buses can be classified into four types, namely: (1) buses with line(s) only but no generator or load; (2) buses with line(s) and load(s) but no generator; (3) buses with line(s) and generator but no load; and (4) buses with line(s), generator, and load(s) (Grigg et al. 1999). From the system administrator's perspective, the system administrator may be more interested in buses with generators and/or loads than those with only transmission lines; and in buses with generators than those with loads, due to cost savings and

reliability concerns. As such, we simply assign branches connected to a bus with a total weight of 1, 2, 3, and 4 units, respectively, for the four types of buses. Then, the total weight is equally divided among all connected branches. For example, if a type 2 bus has four branches, then this bus is assigned a total weight of $\omega = 2$ units, and each of its four branches is allocated a weight of $\omega_i = 2/4 = 0.5$ unit, where $i \in \{1, 2, 3, 4\}$.

ALGORITHM 1: MxST Construction

Input: Initial graph $\mathcal{G} = \{\mathcal{V}_\mathcal{G}, \mathcal{E}_\mathcal{G}\}$ of a power grid topology; set of weights $\mathcal{W}$ assigned for all the branches

Output: A MxST $\mathcal{S} = \{\mathcal{V}_\mathcal{S}, \mathcal{E}_\mathcal{S}\}$

Initialization: $\mathcal{V}_\mathcal{S} = \emptyset, \mathcal{E}_\mathcal{S} = \emptyset$
Step 1: Weight Assignment for each branch.
  (1.1). Assign a total weight to each bus according to Table 4.
  (1.2). Equally divide the weight assigned for each bus into k parts, where k is the number of branches connected to this bus.
  (1.3). Assign the divided weights to each connected branch.
  (1.4). Add the weights for each branch assigned from the two end buses.
Step 2: Arrange all branches in their decreasing order of weights.
Step 3: Add to $\mathcal{E}_\mathcal{S}$ with ϵ_{ij} that has the maximum weight $\omega_{ij} \in \mathcal{W}$; add to $\mathcal{V}_\mathcal{S}$ with v_i and v_j that is connected by ϵ_{ij}.
Step 4: Remove v_i and v_j from $\mathcal{V}_\mathcal{G}$, and ϵ_{ij} from $\mathcal{E}_\mathcal{G}$.
Step 5: Loop over all the remaining edges $\epsilon_{kt} \in \mathcal{E}_\mathcal{G}$ connecting to vertices $v_k \in \mathcal{V}_\mathcal{S}$. Add the edge ϵ_{kt} has currently the maximum weight $\omega_{kt} \in \mathcal{W}$ to $\mathcal{E}_\mathcal{S}$; add $v_t \in \mathcal{V}_\mathcal{G}$ but $v_t \notin \mathcal{V}_\mathcal{S}$ to $\mathcal{V}_\mathcal{S}$.
Step 6: Remove the edge ϵ_{kt} from $\mathcal{E}_\mathcal{G}$ and v_t from $\mathcal{V}_\mathcal{G}$ concerned in the last step.
Step 7: Repeat Steps 5 and 6 until $\mathcal{V}_\mathcal{G} = \emptyset$.
Step 8: Add all generators to $\mathcal{V}_\mathcal{S}$, and generator and load edges to $\mathcal{E}_\mathcal{S}$.
return $\mathcal{S} = \{\mathcal{V}_\mathcal{S}, \mathcal{E}_\mathcal{S}\}$

Based on this method, we develop an algorithm to show the construction of a MxST in a power grid (see Algorithm 1). In Algorithm 1, the weights for all branches are calculated by equally dividing the total weights of each bus and adding the two component weights for each branch. Then, MxST is constructed for the weighted graph step by step. Starting from a branch with the highest weight, branches and buses of interest are added to MxST following decreasing order of weights, until all bus nodes are added to MxST but avoiding that the buses are repeatedly added. Lastly, put in all generators, and generator and load edges to MxST as well, because generators and loads are always important to a power grid.

Let us take the IEEE 14-bus power system (as shown in Figure 11) as an example to introduce the construction of a MxST in a power system. Based on our proposed scheme, the bus types of this power system and the total weights assigned to each bus are summarized in Table 5. Then, the weights of all branches in the power system are calculated and listed in Table 6. According to Algorithm 1, we construct the MxST of the IEEE 14-bus system as shown in Figure 11, wherein all the MxST branches are denoted by solid red lines and the weights of all the MxST branches are annotated.

4.2.2 Unreliability Enabling Algorithm. We employ MxST in our analytical model with the expectation to find the most critical branches, which combined with all the buses, provide the most useful measurement and status data for system operations. As such, we can define the *critical devices* and *critical data*.

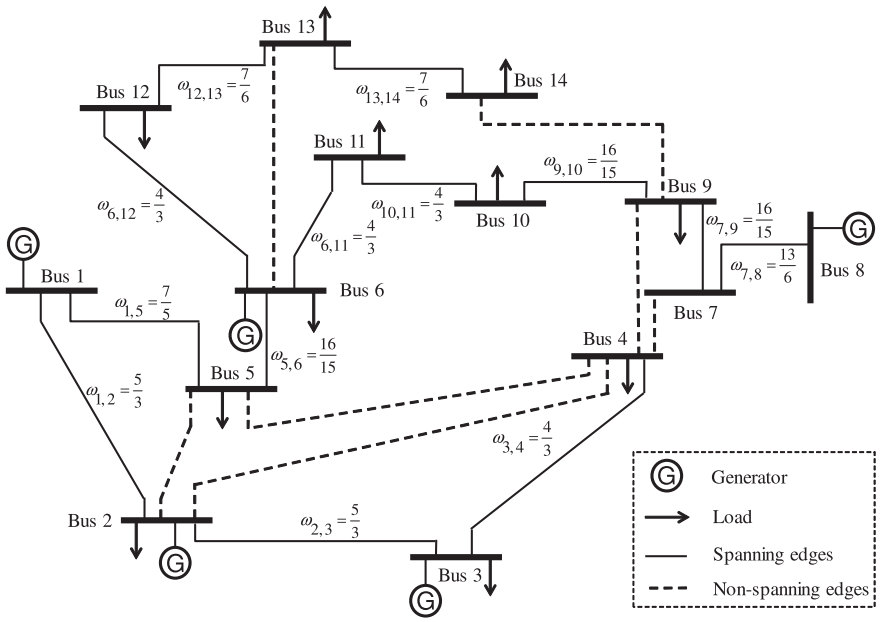

Fig. 11. The MxST of the IEEE 14-bus system.

Table 5. The Bus Type and Total Weight Assigned in IEEE 14-Bus System

Bus index	Bus type	Weight assigned	Bus index	Bus type	Weight assigned
#1	Type 3	3 units	#8	Type 3	3 units
#2	Type 4	4 units	#9	Type 2	2 units
#3	Type 4	4 units	#10	Type 2	2 units
#4	Type 2	2 units	#11	Type 2	2 units
#5	Type 2	2 units	#12	Type 2	2 units
#6	Type 4	4 units	#13	Type 2	2 units
#7	Type 1	1 unit	#14	Type 2	2 units

Definition 4.1. Given a MxST $\mathcal{S}$ of a power grid topology $\mathcal{G}$, sensing devices are said to be *critical devices* if they host on branches ϵ_{ij} that are involved in $\mathcal{S}$, that is,

$$\epsilon_{ij} \in \mathcal{G} \cap \mathcal{S},\ i,j \in \{1,2,\ldots,N_S\} \text{ and } i \neq j, \tag{17}$$

where N_S is the number of edges in $\mathcal{S}$; otherwise, they are said to be *non-critical devices* if

$$\epsilon_{ij} \in \mathcal{G} \setminus \mathcal{S},\ i,j \in \{1,2,\ldots,N_S\} \text{ and } i \neq j. \tag{18}$$

Accordingly, the measurement data or status data generated by these *critical devices* are said to be *critical data*, and data generated by the *non-critical devices* are said to be *non-critical data*.

With the constructed MxST and the above definitions, we design an unreliability enabling algorithm to show under what circumstances can transitions T_DIST, T_FAIL, and T_MALF be fired to cause system unreliability. As described in Algorithm 2, the first step is to check whether the compromised devices have the capability to collectively construct a topology attack. We consider a most optimistic condition from the attackers' perspective that, if the line meter and the circuit

Table 6. Weights Assigned for Each Branch in IEEE 14-Bus System
(g Denotes Generator and l Denotes Load)

Branch index	Weight assigned	Branch index	Weight assigned	Branch index	Weight assigned
$\epsilon_{1,2}$	3/3+2/3=5/3	$\epsilon_{4,7}$	2/6+2/3=1	$\epsilon_{8,g}$	3/2
$\epsilon_{1,5}$	3/3+2/5=7/5	$\epsilon_{4,9}$	2/6+2/5=11/15	$\epsilon_{9,10}$	2/5+2/3=16/15
$\epsilon_{1,g}$	3/3=1	$\epsilon_{4,l}$	2/6=1/3	$\epsilon_{9,14}$	2/5+2/3=16/15
$\epsilon_{2,3}$	4/6+4/4=5/3	$\epsilon_{5,6}$	2/5+4/6=16/15	$\epsilon_{9,l}$	2/5
$\epsilon_{2,4}$	4/6+2/6=1	$\epsilon_{5,l}$	2/5	$\epsilon_{10,11}$	2/3+2/3=4/3
$\epsilon_{2,5}$	4/6+2/5=16/15	$\epsilon_{6,11}$	4/6+2/3=4/3	$\epsilon_{10,l}$	2/3
$\epsilon_{2,g}$	4/6=2/3	$\epsilon_{6,12}$	4/6+2/3=4/3	$\epsilon_{11,l}$	2/3
$\epsilon_{2,l}$	4/6=2/3	$\epsilon_{6,13}$	4/6+2/4=7/6	$\epsilon_{12,13}$	2/3+2/4=7/6
$\epsilon_{3,4}$	4/4+2/6=4/3	$\epsilon_{6,g}$	4/6=2/3	$\epsilon_{12,l}$	2/3
$\epsilon_{3,g}$	4/4=1	$\epsilon_{6,l}$	4/6=2/3	$\epsilon_{13,14}$	2/4+2/3=7/6
$\epsilon_{3,l}$	4/4=1	$\epsilon_{7,8}$	2/3+3/2=13/6	$\epsilon_{13,l}$	2/4=1/2
$\epsilon_{4,5}$	2/6+2/5=11/15	$\epsilon_{7,9}$	2/3+2/5=16/15	$\epsilon_{14,l}$	2/3

breaker monitor on the same branch are unfortunately compromised by the adversary and undetected by the intrusion detection system, the attackers are considered to have the capability to launch a topology attack. Otherwise, the injected false meter data can be easily detected by the bad data detector. Then, for cases where the attackers have the capability to launch a topology attack, further classification is conducted to determine whether a system failure or disturbance happens. Note that, this classification procedure also, to a large extent, successfully differentiates between conservative topology attacks and aggressive topology attacks. The reason is that, according to the definition provided in Section 3.2, conservative topology attacks usually cause system disturbances while aggressive topology attacks usually cause system failures.

5 PERFORMANCE EVALUATION

5.1 Metrics

In this article, the reliability performance of the smart grids using our analytical model is analyzed using both transient analysis and steady-state analysis.

5.1.1 Transient Analysis. The metrics for transient analysis are the mean time to disturbance (MTTD) and mean time to failure (MTTF). Specifically, MTTD is the average time before the power system functions into a system disturbance. Likewise, MTTF is the average time before the power system functions into a system failure. They are given by

$$\text{MTTD} = \int_0^\infty t[1 - Q_D(t)]dt, \tag{19}$$

and

$$\text{MTTF} = \int_0^\infty t[1 - Q_F(t)]dt, \tag{20}$$

where $Q_D(t)$ is the probability of the first visit to a system disturbance, and $Q_F(t)$ is the probability of the first visit to a system failure. Note that in the transient analysis, we ignore the mean time to malfunction (MTTM). The reason is that compared to MTTD and MTTF, MTTM is considerably large due to the negligible probability of a system malfunction occurrence.

ALGORITHM 2: Unreliability Enabling Algorithm

Input: Set of compromised line meter $\mathcal{L}$; set of compromised breaker monitor $\mathcal{B}$; grid topology $\mathcal{G}$; MxST $\mathcal{S}$ of $\mathcal{G}$; number of unrecovered detected bad devices N_L and N_B
Output: Decision outcome O

```
Initialization: threshold N_th, the maximum number of unrecovered detected bad devices a system can tolerate prior to a system malfunction
if N_L > N_th or N_B > N_th then
    O ← system malfunction
else
    if at least one pair of the compromised line meters and breaker monitors are located at the same branch then
        The attacker is capable of launching a topology attack.
        if at least one of the compromised line meters and breaker monitors are critical devices then
            O ← system failure
        else
            O ← system disturbance
        end if
    else
        O ← bad data detected with no system unreliability
    end if
end if
return O
```

5.1.2 Steady-State Analysis. The steady-state analysis is presented by a self-defined metric: *reliability R*, which is defined by

$$R = (1 - p_{malf}) * \left(1 - \frac{\alpha * p_{dist} + \beta * p_{fail}}{\alpha + \beta}\right)^k, \tag{21}$$

where

$$p_{malf} = 1 - \sum_{i=0}^{N_{th}} \sum_{j=0}^{N_{th}} p_{dblm}(i) p_{dbbm}(j), \tag{22}$$

denoting the steady-state probability of a system malfunction occurrence when the number of unrecovered detected bad devices in either place P_DBLM or P_DBBM exceeds the acceptable threshold N_{th}. p_{dist} and p_{fail} denote the steady-state probabilities of system disturbance and failure, respectively. In addition, α and β represent the negative impacts of p_{dist} and p_{fail} posed to the system reliability. k is the average number of pairs of compromised line meter and breaker monitor that host on the same transmission line. k describes the average number of attack events in the power system under the optimistic condition. In practice, the power system usually has a sufficient recovery rate, wherein a really small value can be satisfied; therefore, $p_{dblm}(i)$ and $p_{dbbm}(j)$ always hold large probabilities when i and j are small values (e.g., 0 or 1). According to Equation (22), p_{malf} approaches to zero in steady state, which is negligible. In this case, Equation (21) can be reduced to

$$R = \left(1 - \frac{\alpha * p_{dist} + \beta * p_{fail}}{\alpha + \beta}\right)^k. \tag{23}$$

Since the steady states of P_DIST and P_FAIL are absorbing states, it is hard to find the corresponding steady-state probabilities. Therefore, we transform this problem into several sub-problems. A corresponding workflow is shown in Figure 12. In this workflow, the SPN model is reduced by temporarily removing places P_DIST and P_FAIL (P_MALF as well) and corresponding transitions

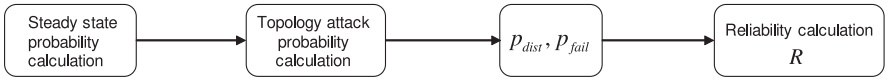

Fig. 12. Workflow of calculating reliability.

T_DIST and T_FAIL (T_MALF as well). Then, the steady-state probabilities of $p_{ublm}(i)$ and $p_{ubbm}(j)$, where $i, j \in \{1, 2, \ldots, N\}$, can be easily obtained using steady-state analysis of the remaining SPN. Next, we determine the expected probability of constructing a topology attack p_{att}, which is given by

$$p_{att} = \sum_{i=1}^{N}\sum_{j=1}^{N} p_{ublm}(i)p_{ubbm}(j) \times \begin{cases} \frac{\sum_{l=1}^{\bar{i}} C_l^{\bar{i}} C_{\bar{j}-l}^{N-\bar{i}}}{C_{\bar{j}}^{N}}, & i+j \le N \\ 1, & i+j > N, \end{cases} \tag{24}$$

where $\bar{i} = \min\{i, j\}$ and $\bar{j} = \max\{i, j\}$. $\frac{C_l^{\bar{i}} C_{\bar{j}-l}^{N-\bar{i}}}{C_{\bar{j}}^{N}}$ calculates the probability of l (out of $\bar{i}$) pairs of undetected compromised line meters and breaker monitors with a same host location. The dual summations then calculate the average probability of at least one pair of undetected compromised line meters and breaker monitors with a same host location, which is the optimistic condition as stated in the above section. After that, the steady-state probabilities p_{dist} and p_{fail} can then be determined by

$$p_{dist} = p_{att}\frac{\overline{N}_S}{N}, \tag{25}$$

and

$$p_{fail} = p_{att}\frac{N_S}{N}, \tag{26}$$

where $\overline{N}_S$ and N_S are the number of non-spanning tree branches and spanning tree branches, respectively. Particularly, when the compromising rate is sufficiently large, there are always enough compromised bad devices in places P_UBLM and P_UBBM. As a result, $i + j > N$ in Equation (24) is always satisfied so that we always have $p_{att} = 1$. In this case, the reliability R is reduced as

$$R = \left(1 - \frac{\alpha * p_{att} * \overline{N}_S/N + \beta * p_{att} * N_S/N}{\alpha + \beta}\right)^k = \left(1 - \frac{\alpha * \overline{N}_S/N + \beta * N_S/N}{\alpha + \beta}\right)^k. \tag{27}$$

Note that k, describing the average number of attack events in the power system, is defined by

$$k = \sum_{x=1}^{N} x * p(x), \tag{28}$$

where

$$p(x) = \sum_{i=x}^{N}\sum_{j=x}^{N} p_{ublm}(i)p_{ubbm}(j) \times \begin{cases} \frac{C_x^{\bar{i}} C_{\bar{j}-x}^{N-\bar{i}}}{C_{\bar{j}}^{N}}, & i+j \le N \\ 1, & i+j > N, \end{cases} \tag{29}$$

calculating the probability of x pairs of undetected compromised line meters and breaker monitors with a same host location. Then, k is determined by the expectation of the probability distribution.

5.2 Numerical Results

In the simulation experiments, we use MATLAB 2015a and PIPE 2 (Dingle et al. 2009) as our simulators for transient and steady-state analysis, respectively. To facilitate comparison, we set the same levels of compromising rates, detection rates, and recovery rates for the two sensing devices, i.e., $\lambda_{clm} = \lambda_{cbm}$, $\lambda_{dblm} = \lambda_{dbbm}$, and $\lambda_{rlm} = \lambda_{rbm}$. The detection interval is set as 10 hours for the

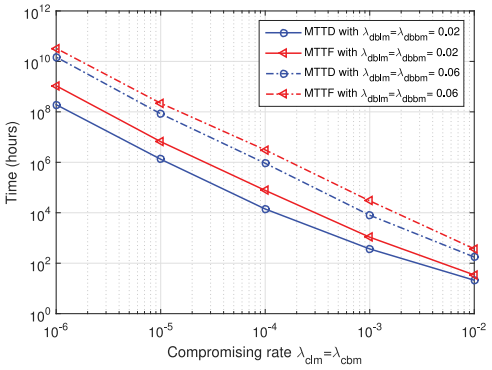

Fig. 13. The MTTD and MTTF versus compromising rate $\lambda_{clm} = \lambda_{cbm}$ for the IEEE 14-bus system ($\lambda_{rlm} = \lambda_{rbm} = 0.08$).

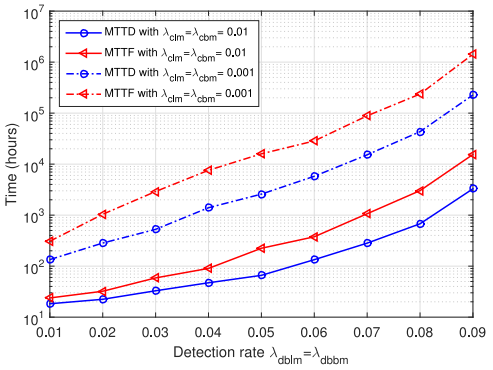

Fig. 14. The MTTD and MTTF versus detection rate $\lambda_{dblm} = \lambda_{dbbm}$ for the IEEE 14-bus system ($\lambda_{rlm} = \lambda_{rbm} = 0.08$).

intrusion detection system. Note that in this section, we do not explicitly differentiate between conservative topology attacks from aggressive topology attacks, because the various compromising levels actually simulate all levels of the attack capability ranging from the conservative topology attacks all the way to aggressive topology attacks. The numerical results of all the simulations are shown as follows.

In Figure 13, we plot the MTTD and MTTF of the IEEE 14-bus test system versus the compromising rate $\lambda_{clm} = \lambda_{cbm}$, for different detection rates $\lambda_{dblm} = \lambda_{dbbm}$. Note that, a sufficient recovery rate of $\lambda_{rlm} = \lambda_{rbm} = 0.08$ is used as a constant parameter while analyzing the compromising rate and the detection rate. Figure 13 shows that when the compromising rate is relatively small, the power system has good operating conditions that both the MTTD and MTTF levels are significantly high. Larger compromising rates result in lower MTTD and MTTF levels as more sensing devices can be compromised by the adversary, increasing the probability to initiate a topology attack. In addition, we observe that MTTF is usually larger than MTTD. This is because when we have constrained knowledge and capability, it is much easier for an adversary to construct a relatively weak attack that causes system disturbances than to construct a complicated strong attack to cause system failures. Also, higher levels of MTTD and MTTF can be obtained by increasing the detection rate, for example, from 0.02 to 0.06.

Figure 14 shows the MTTD and MTTF of the IEEE 14-bus test system versus the detection rate $\lambda_{dblm} = \lambda_{dbbm}$, for different compromising rates $\lambda_{clm} = \lambda_{cbm}$. Clearly, when the detection rate increases, the MTTD and MTTF improve quickly because high detection rates will be more likely to detect compromised bad sensing devices and prevent them from launching topology attacks; thus leading to higher MTTD and MTTF levels. A similar observation is being made in Figure 14, where lower compromising rates can also enhance the MTTD and MTTF levels.

In comparison to the IEEE 14-bus test system, similar experiments pertaining to the MTTD and MTTF are also conducted in the IEEE 24-bus and 39-bus test systems. The results are plotted in Figures 15 and 16 for the compromising rate and detection rate, respectively. As shown in Figure 15, similar to all three test systems, larger compromising rates correspond to lower MTTD and MTTF levels, while smaller compromising rates correspond to higher MTTD and MTTF levels. Most importantly, under the same level of compromising rate, detection rate, and the recovery rate, the IEEE 14-bus system has the highest levels of MTTD and MTTF, followed by the IEEE 24-bus system, and the IEEE 39-bus system. This is because when the total number of sensing devices increases, the average number of sensing devices that can be compromised per unit time also increases; thus,

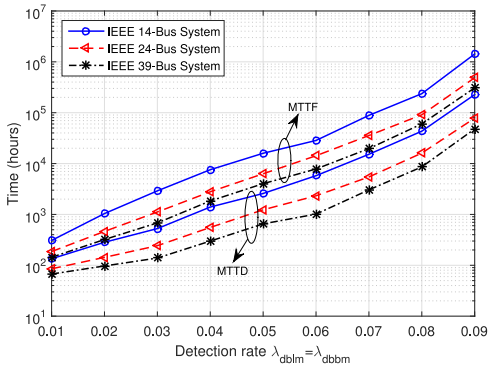

Fig. 15. MTTD and MTTF versus compromising rate $\lambda_{clm} = \lambda_{cbm}$ for the IEEE 14-bus, 24-bus, and 39-bus systems ($\lambda_{dblm} = \lambda_{dbbm} = 0.02$ and $\lambda_{rlm} = \lambda_{rbm} = 0.08$).

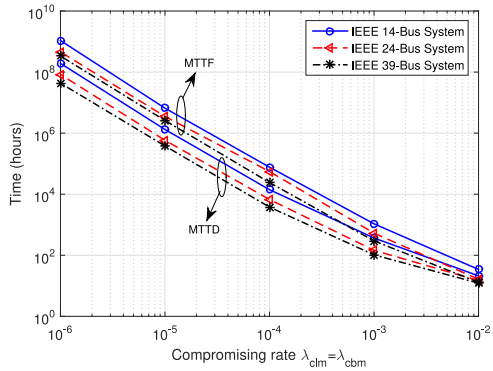

Fig. 16. MTTD and MTTF versus detection rate $\lambda_{dblm} = \lambda_{dbbm}$ for the IEEE 14-bus, 24-bus, and 39-bus systems ($\lambda_{clm} = \lambda_{cbm} = 0.001$ and $\lambda_{rlm} = \lambda_{rbm} = 0.08$).

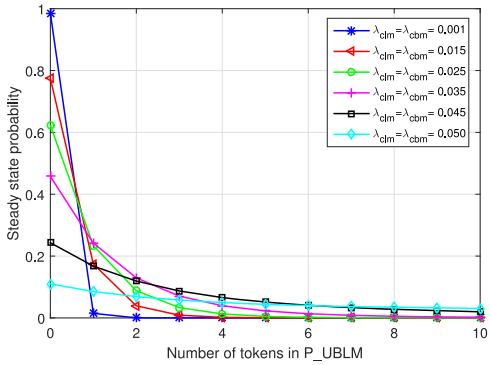

Fig. 17. Steady-state probability distribution of the number of tokens in place P_UBLM (also P_UBBM) of the IEEE 14-bus system, for different compromising rates ($\lambda_{dblm} = \lambda_{dbbm} = 0.04$ and $\lambda_{rlm} = \lambda_{rbm} = 0.08$).

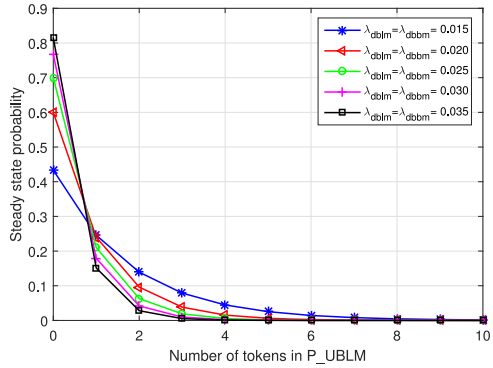

Fig. 18. Steady-state probability distribution of the number of tokens in place P_UBLM (also P_UBBM) of the IEEE 14-bus system, for different detection rates ($\lambda_{clm} = \lambda_{cbm} = 0.01$ and $\lambda_{rlm} = \lambda_{rbm} = 0.08$).

the probability of constructing a topology attack will increase, resulting in relatively lower levels of MTTD and MTTF. Figure 16 presents the parallel results that for all three test systems, MTTD and MTTF grow exponentially as the system detection rate increases, and the IEEE 14-bus system has the highest levels of MTTD and MTTF while the IEEE 39-bus system has the lowest.

After presenting the numerical results of transient analysis, we now present the steady-state analysis. Using the PIPE 2 simulator, the steady-state probability distribution of the number of tokens in each place can be obtained. Figures 17 and 18 present the steady-state probability distribution of the number of tokens in place P_UBLM (also P_UBBM) of the IEEE 14-bus system, for different compromising rates and detection rates, respectively. As observed from Figure 17, when the compromising rate is relatively low, where only a few good devices may be transferred to bad ones and most devices remain in good status, $\Pr\{\#P\_UBLM = 0\}$ is significantly high with narrow probabilities for other number of tokens. $\Pr\{\#P\_UBLM > 0\}$ can be increased by increasing the compromising rate. In contrast, as shown in Figure 18, a smaller detection rate value of, for

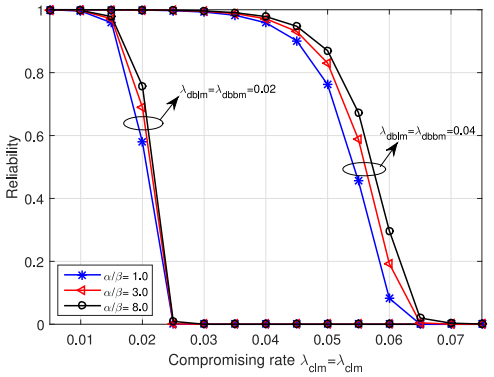

Fig. 19. System reliability of the IEEE 14-bus system versus compromising rate ($\lambda_{rlm} = \lambda_{rbm} = 0.08$).

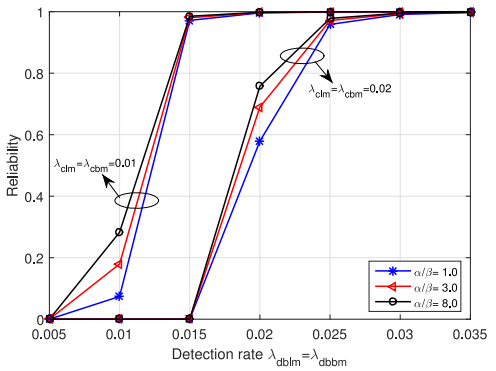

Fig. 20. System reliability of the IEEE 14-bus system versus detection rate ($\lambda_{rlm} = \lambda_{rbm} = 0.08$).

example, $\lambda_{dblm} = \lambda_{dbbm} = 0.015$ ($\lambda_{dblm} = \lambda_{dbbm} = 0.04$ in Figure 17), may result in more bad compromised devices being undetected, and result in relatively larger $\Pr\{\#P\_UBLM > 0\}$. Increasing the detection rate can improve $\Pr\{\#P\_UBLM = 0\}$; thus, reducing the potential for an adversary to construct a topology attack.

With the obtained steady-state probability distribution, system *reliability* can be determined by Equation (23). Figure 19 plots the system reliability of the IEEE 14-bus system versus the compromising rate for various values of α/β. We used the α to β ratio in our experiments because based on Equation (23), the definition of system reliability R can be written as $R = (1 - \frac{\alpha * p_{dist} + \beta * p_{fail}}{\alpha+\beta})^k = (1 - \frac{p_{dist}}{1+\beta/\alpha} - \frac{p_{fail}}{\alpha/\beta+1})^k$. Thus, it is more convenient to use the ratio α/β for analyzing the system reliability. As shown in Figure 19, under the same level of compromising rate, detection rate, and recovery rate, higher values of α/β result in higher reliability. The reason is that, according to Equations (25) and (26), p_{fail} is usually greater than p_{dist} due to $N_S > \overline{N}_S$. Thus, increasing α/β assigns more weight to p_{dist} and less weight to p_{fail}, which as a result decreases the value of $\frac{\alpha * p_{dist} + \beta * p_{fail}}{\alpha+\beta}$. Therefore, the resulting value of reliability will be increased, and vice versa. More interestingly, the reliability decreases gradually from $R = 1$ at the origin and drops quickly to nearly zero with the growth of the compromising rate. This is because when the compromising rate is less than the detection rate, bad devices can usually be detected so that high reliability can be obtained, but when the compromising rate is large enough that it exceeds the detection rate, there are a multitude of bad devices that cannot be successfully detected. In this case, there are always sufficient bad devices together in places P_UBLM and P_UBBM that can easily launch topology attacks, i.e., $p_{att} = 1$ holds all the time. In addition, the higher the compromising rate, the larger the k, which indicates the presence of multiple topology attacks and the large value of k will decrease the reliability in an exponential manner.

The relationship between the system reliability of the IEEE 14-bus system and the detection rate for various values of α/β is plotted in Figure 20. Likewise, this figure shows that under the same conditions, increasing the value of α/β can lead to higher system reliability, while decreasing it can lead to lower system reliability. In addition, the full simulation trace shows that system reliability experiences a slight growth from the beginning and eventually reaches a plateau at around $R = 1$ when the detection rate increases. This indicates that the rise of the detection rate can slowly mitigate the number of undetected compromised devices, reduce the probability of initiating an attack, and further improve the system reliability.

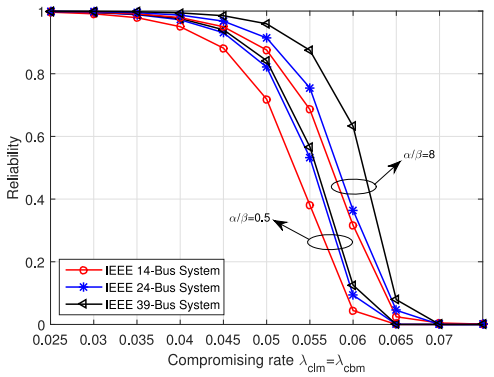

Fig. 21. System reliability versus compromising rate for the IEEE 14-bus, 24-bus, and 39-bus systems ($\lambda_{dblm} = \lambda_{dbbm} = 0.04$ and $\lambda_{rlm} = \lambda_{rbm} = 0.08$).

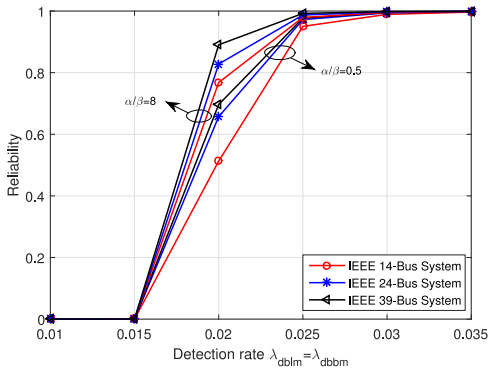

Fig. 22. System reliability versus detection rate for the IEEE 14-bus, 24-bus, and 39-bus systems ($\lambda_{clm} = \lambda_{cbm} = 0.02$ and $\lambda_{rlm} = \lambda_{rbm} = 0.08$).

In addition to the IEEE 14-bus system, simulation experiments concerning steady-state analysis for the IEEE 24-bus and 39-bus systems are conducted as well. Figure 21 presents the system reliability of the three test systems against the compromising rate under different values of α/β. Similar results to the IEEE 14-bus system can be obtained for the IEEE 24-bus and 39-bus systems. Specifically, for all three test systems, the reliability decreases gradually from $R = 1$ as the compromising rate increases, and drops quickly when the compromising rate exceeds the detection rate. In addition, we can also observe that the power systems can have a high system reliability when α/β is set to be high. Furthermore, the numerical results show that the IEEE 39-bus system has generally the highest reliability, followed by the 24-bus system and 14-bus system the last. The reason is that a power system with more redundant branches and higher connection complexity may be more resilient to the attacks.

In Figure 22, the reliability of different power systems against the detection rate is plotted. Similarly, the reliability stabilizes at nearly zero at the original period in each test system, but a slight difference is that the stabilization results from insufficiency of the detection rate to identify the compromised bad devices. While the detection rate increases to a sufficient level, the reliability begins to increase quickly and finally approaches to $R = 1$.

Finally, our simulation experiments focus on steady-state analysis against the recovery rate. The corresponding numerical results are summarized in Figures 23 and 24. As observed in Figure 23, three groups of comparative experiments show that under the same compromising rate and detection rate, the steady-state probability distribution of the number of tokens in place P_UBLM are the same for different recovery rates. This is because the number of detected bad devices arriving in place P_UBLM is determined by the compromising rate and detection rate collectively; thus, the same compromising rate and detection rate will result in the same distribution of tokens in steady states. While, it can also be seen that the recovery rate is of little impact on this distribution, i.e., different values of the recovery rate do not make any difference to the probability of topology attacks. The other curves once again show that the number of compromised devices in place P_UBLM can be further mitigated by increasing the detection rate or reducing the compromising rate.

In Figure 24, we observe that from the two groups of red and blue curves, the system reliability experiences a sharp increase from 0 to 1 as the slight growth of the recovery rate. In such cases, system malfunctions occur when the recovery rate is not sufficient (e.g., $\lambda_{rlm} = \lambda_{rbm} < 0.02$

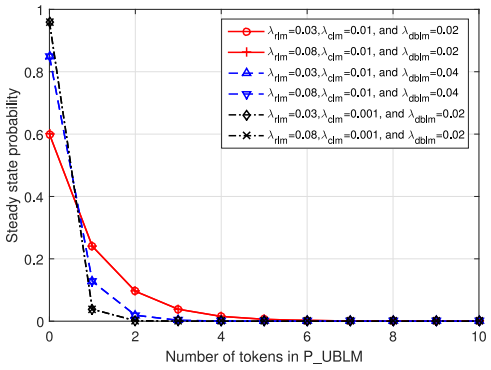

Fig. 23. Steady-state probability distribution of the number of tokens in places P_UBLM and P_UBBM for the IEEE 14-bus system.

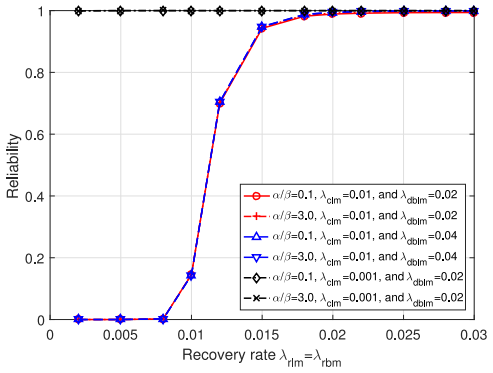

Fig. 24. System reliability versus recovery rate for the IEEE 14-bus system.

here) to recover the detected bad devices under a compromising rate of $\lambda_{clm} = \lambda_{cbm} = 0.01$ and a detection rate of either $\lambda_{dblm} = \lambda_{dbbm} = 0.02$ or 0.04. In contrast, as the two black curves show that under a rather small compromising rate (i.e., $\lambda_{clm} = \lambda_{cbm} = 0.001$), a recovery rate of $\lambda_{rlm} = \lambda_{rbm} = 0.002$ is reasonably sufficient to recover all the detected bad devices. This leads to a full system reliability (i.e., $R = 1$) with no system malfunctions. In previous simulations related to the compromising rate and detection rate, we use a sufficient recovery rate of $\lambda_{rlm} = \lambda_{rbm} = 0.08$ to exclude the impacts on system reliability that insufficient recovery rate may cause. Compared to the compromising rate and detection rate, we observe that, in this figure, the recovery rate has relatively marginal impact on the system reliability as long as it can reach a basic acceptable level. More importantly, the recovery rate highly relies on the compromising rate and, then, the detection rate.

Such observations help inform future design of the system, so that system designers can devote more efforts to significant aspects, such as mitigating the compromising rate and improving the detection rate, rather than focusing too much on the recovery rate.

6 CONCLUSION

Smart grid cyber-physical systems will be increasingly deployed in the foreseeable future, and there are a number of research challenges that need to be addressed.

In this article, we developed an SPN-based analytical model for smart grid cyber-physical systems to assess and analyze the system reliability in the presence of both topology attacks and system countermeasures. We also demonstrated how to construct successful topology attacks in a smart grid. In our analytical SPN model, we took into account two types of sensing devices involving line meters and circuit breaker monitors, and two kinds of typical system countermeasures (i.e., intrusion detection systems and malfunction recovery techniques); we demonstrated how we can use several events to describe the system behaviors under these event triggers. Moreover, using the IEEE 14-bus as an example, we proposed two algorithms pertaining to the construction of a MxST and identification of system disturbances, failures, and malfunctions. Finally, simulation experiments on the IEEE 14-bus, 24-bus, and 39-bus test systems and, correspondingly, both transient- and steady-state analysis demonstrated the utility and efficiency of our proposed analytical model. The findings (e.g., confirming that compromising rate and detection rate are of paramount significance to system reliability) will inform future system design.

Future research includes prototyping the approach presented in this article, and evaluating and refining the prototype in a real-world implementation.

ACKNOWLEDGMENTS

The authors would like to thank the editor and the three anonymous reviewers for providing constructive and generous feedback.

REFERENCES

Saurabh Amin, Alvaro A. Cárdenas, and S. Shankar Sastry. 2009. Safe and secure networked control systems under denial-of-service attacks. In *Proceedings of the International Workshop on Hybrid Systems: Computation and Control (HSCC'09)*. Springer, 31–45.

S. Massoud Amin and Bruce F. Wollenberg. 2005. Toward a smart grid: Power delivery for the 21st century. *IEEE Power and Energy Magazine* 3, 5 (2005), 34–41.

Falko Bause and Pieter S. Kritzinger. 2002. *Stochastic Petri Nets*. Vol. 1. Vieweg, Wiesbaden.

Thomas M. Chen, Juan Carlos Sanchez-Aarnoutse, and John Buford. 2011. Petri net modeling of cyber-physical attacks on smart grid. *IEEE Transactions on Smart Grid* 2, 4 (2011), 741–749.

Kim-Kwang Raymond Choo. 2014. A conceptual interdisciplinary plug-and-play cyber security framework. In *ICTs and the Millennium Development Goals*. Springer Science & Business Media, New York, 81–99.

G. C. Dalton, Robert F. Mills, John M. Colombi, and Richard A. Raines. 2006. Analyzing attack trees using generalized stochastic Petri nets. In *Proceedings of the IEEE Information Assurance Workshop (IAW'06)*. IEEE, 116–123.

Ruilong Deng, Gaoxi Xiao, Rongxing Lu, Hao Liang, and Athanasios V. Vasilakos. 2017. False data injection on state estimation in power systems-Attacks, impacts, and defense: A survey. *IEEE Transactions on Industrial Informatics* 13, 2 (2017), 411–423.

Nicholas J. Dingle, William J. Knottenbelt, and Tamas Suto. 2009. PIPE2: A tool for the performance evaluation of generalised stochastic Petri nets. *ACM SIGMETRICS Performance Evaluation Review* 36, 4 (2009), 34–39.

Zarko Djekic. 2007. *Online Circuit Breaker Monitoring System*. Ph.D. dissertation. Texas A&M University, College Station, TX.

Nicolas Falliere, Liam O. Murchu, and Eric Chien. 2011. W32. Stuxnet dossier. *White Paper, Symantec Corp., Security Response* 5 (2011), 6.

Hassan Farhangi. 2010. The path of the smart grid. *IEEE Power and Energy Magazine* 8, 1 (2010), 18–28.

U.S. Federal Energy Regulatory Commission (FERC). 2009. Smart grid policy. *Docket PL09-4-000*.

Cliff Grigg, Peter Wong, Paul Albrecht, Ron Allan, Murty Bhavaraju, Roy Billinton, Quan Chen, Clement Fong, Suheil Haddad, Sastry Kuruganty, and others. 1999. The IEEE reliability test system-1996. A report prepared by the reliability test system task force of the application of probability methods subcommittee. *IEEE Transactions on Power Systems* 14, 3 (1999), 1010–1020.

Allen Householder, Kevin Houle, and Chad Dougherty. 2002. Computer attack trends challenge internet security. *Computer* 35, 4 (2002), sulp5–sulp7.

Lei Huang, Yuanzhang Sun, Jian Xu, Wenzhong Gao, Jun Zhang, and Ziping Wu. 2014. Optimal PMU placement considering controlled islanding of power system. *IEEE Transactions on Power Systems* 29, 2 (2014), 742–755.

Gabriela Hug and Joseph Andrew Giampapa. 2012. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. *IEEE Transactions on Smart Grid* 3, 3 (2012), 1362–1370.

Kurt Jensen. 2013. *Coloured Petri Nets: Basic Concepts, Analysis Methods and Practical Use*. Vol. 1. Springer Science & Business Media.

Kurt Jensen and Grzegorz Rozenberg. 2012. *High-Level Petri Nets: Theory and Application*. Springer Science & Business Media.

Jinsub Kim and Lang Tong. 2013. On topology attack of a smart grid: Undetectable attacks and countermeasures. *IEEE Journal on Selected Areas in Communications* 31, 7 (2013), 1294–1305.

Wolfgang Kröger. 2008. Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. *Reliability Engineering & System Safety* 93, 12 (2008), 1781–1787.

Jean-Claude Laprie, Karama Kanoun, and Mohamed Kaâniche. 2007. Modelling interdependencies between the electricity and information infrastructures. In *Proceedings of the International Conference on Computer Safety, Reliability, and Security (SAFECOMP'07)*. Springer, 54–67.

Edward A. Lee. 2017. Fundamental limits of cyber-physical systems modeling. *ACM Transactions on Cyber-Physical Systems* 1, 1 (2017), Article 3, 26 pages.

Beibei Li, Rongxing Lu, and Haiyong Bao. 2016a. Behavior rule specification-based false data injection detection technique for smart grid. In *Cyber Security for Industrial Control Systems: From the Viewpoint of Close-Loop*. 119–150.

Beibei Li, Rongxing Lu, Wei Wang, and Kim-Kwang Raymond Choo. 2016b. DDOA: A Dirichlet-based detection scheme for opportunistic attacks in smart grid cyber-physical system. *IEEE Transactions on Infromation Forensics and Security* 11, 11 (2016), 2415–2425.

Beibei Li, Rongxing Lu, Wei Wang, and Kim-Kwang Raymond Choo. 2017. Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system. *Journal of Parallel and Distributed Computing* 103 (2017), 32–41.

Wenyuan Li. 2014. *Risk Assessment of Power Systems: Models, Methods, and Applications*. John Wiley & Sons.

Shichao Liu, Xiaoping P. Liu, and Abdulmotaleb El Saddik. 2013. Denial-of-service (DoS) attacks on load frequency control in smart grids. In *Proceedings of the Innovative Smart Grid Technologies (ISGT'13)*, IEEE PES. 1–6.

Yao Liu, Peng Ning, and Michael K. Reiter. 2011. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security* 14, 1 (2011), Article 5, 33 pages.

Zhi Liu, Cheng Zhang, Mianxiong Dong, Bo Gu, Yusheng Ji, and Yoshiaki Tanaka. 2016. Markov-decision-process-assisted consumerscheduling in a networked smart grid. *IEEE Access* 5 (2016), 2448–2458.

James P. McDermott. 2001. Attack net penetration testing. In *Proceedings of the New Security Paradigms Workshop (NSPW'00)*. ACM, 15–21.

Ryan McDonald, Fernando Pereira, Kiril Ribarov, and Jan Hajič. 2005. Non-projective dependency parsing using spanning tree algorithms. In *Proceedings of the Conference on Human Language Technology and Empirical Methods in Natural Language Processing (HLT/EMNLP'05)*. Association for Computational Linguistics, 523–530.

Robert Mitchell and Ing-Ray Chen. 2016. Modeling and analysis of attacks and counter defense mechanisms for cyber physical systems. *IEEE Transactions on Reliability* 65, 1 (2016), 350–358.

Khosrow Moslehi and Ranjit Kumar. 2010. A reliability perspective of the smart grid. *IEEE Transactions on Smart Grid* 1, 1 (2010), 57–64.

Jose Pagliery. 2015. ISIS is Attacking the U.S. Energy Grid. Retrieved January 8, 2017 from http://money.cnn.com/2015/10/15/technology/isis-energy-grid/.

Fatih Tüysüz and Cengiz Kahraman. 2010. Modeling a flexible manufacturing cell using stochastic Petri nets with fuzzy parameters. *Expert Systems with Applications* 37, 5 (2010), 3910–3920.

Hjalte Wedel Vildhøj and David Kofoed Wind. 2016. Supplementary notes for graph theory 1. 26–26. https://hwv.dk/pdfs/01227-notes.pdf.

James Weimer, Soummya Kar, and Karl Henrik Johansson. 2012. Distributed detection and isolation of topology attacks in power networks. In *Proceedings of the 1st International Conference on High Confidence Networked Systems (HiCoNS'12)*. ACM, 65–72.

Jun Wu, Mianxiong Dong, Kaoru Ota, Zhenyu Zhou, and Bin Duan. 2014. Towards fault-tolerant fine-grained data access control for smart grid. *Wireless Personal Communications* 75, 3 (2014), 1787–1808.

Rongfei Zeng, Yixin Jiang, Chuang Lin, and Xuemin Shen. 2012. Dependability analysis of control center networks in smart grid using stochastic Petri nets. *IEEE Transactions on Parallel and Distributed Systems* 23, 9 (2012), 1721–1730.

Received March 2017; revised May 2017; accepted July 2017