IET Communications

Research Article

Towards insider threats detection in smart grid communication systems

ISSN 1751-8628
Received on 30th July 2018
Revised 31st January 2019
Accepted on 9th April 2019
doi: 10.1049/iet-com.2018.5736
www.ietdl.org

Beibei Li[1,2], *Rongxing Lu*[2] ✉, *Gaoxi Xiao*[1], *Haiyong Bao*[3], *Ali A. Ghorbani*[2]
[1]*School of Electrical and Electronic Engineering, Nanyang Technological University, 50 Nanyang Avenue, Singapore*
[2]*Faculty of Computer Science, University of New Brunswick, ITC Building, 550 Windsor Street, Fredericton, NB, Canada*
[3]*School of Computer Science and Information Engineering, Zhejiang Gongshang University, Hangzhou, Zhejiang, People's Republic of China*
✉ *E-mail: rlu1@unb.ca*

Abstract: In today's communication systems, the most damaging security threats are not originating from the outsiders but from the trusted insiders – both malicious insiders and negligent insiders. Always endowed with high privileges, insiders are significantly prone to conduct acts that can cause catastrophic damages to the whole system either intentionally or unintentionally. Characterised by the full and rapid integration of information and communication technologies, smart grid – arguably the largest national critical engineering infrastructure – is suffering from a multitude of security threats initiated from both outsiders and insiders. Without security guarantee, the promising benefits of achieving an efficient, green, and reliable power grid would not be a success. In this study, the authors investigate the insider threats and summarise the existing threats detection solutions in smart grid communication systems. In addition, a novel hybrid insider threats modelling, analysis, and detection framework, which is based on stochastic Petri net and behaviour rule specifications, is proposed to contain insider threats in smart grid communication systems.

1 Introduction

The rapid advances in information and communications technologies (ICTs) and the exponential proliferation of intelligent electronic devices (IEDs) have considerably facilitated the emergence of the smart grid, which has been widely believed as a revolutionary alternative for the existing power grid. To meet the ever-increasing demands of electricity in the 21st century and overcome the shortages of the existing power grid, the concept of smart grid has been rolled out with the expectation of achieving an efficient, green, and reliable power generation, transmission, and distribution system [1]. Smart grid is a primary representative of cyber-physical systems (CPSs). A CPS [2] is defined as a fusion system incorporating physical infrastructure (physical space) with communication and control system (cyber space) – see the conceptual architecture of a CPS in Fig. 1. Through close interactions between the cyber space and physical space, i.e. data sensing and commands execution via communication networks, CPSs are envisioned to enable real-time monitoring, accurate coordination, and automatic control objectives over the physical infrastructure.

However, despite these promising benefits, contemporary development of the smart grid (like any other CPSs) is still in its infancy stage facing many critical challenges. Particularly, cyber security issues have been rapidly emerged as primary concerns of the smart grid communication systems over the years [3–7]. The increasing interconnectivity and openness to the outside world inevitably expose the potential vulnerabilities of not only the conventional communication system in existing power grids but also the newly-introduced ICTs. Without security guarantee, the smart grid is susceptible to malicious penetrations and can easily suffer from dire consequences, e.g. catastrophic physical damages, enormous revenue losses, and immeasurable social impacts. The potential adversaries in contemporary communication systems, who can launch malignant cyber assaults by fully exploiting the system vulnerabilities, can be classified into two categories: insiders and outsiders [8]. Although in many industries the absolute numbers of outsiders are still higher than those of insiders in being responsible for publicly reported security incidents, the percentage of insiders is experiencing a rapid rise in recent years [9]. More importantly, the insiders are contributing to increasingly damaging impacts during security incidents, compared to outsiders. According to IBM X-Force Threat Intelligence Index 2018 [10], misconfigured cloud servers and networked backup incidents unintentionally exposed more than two billion records, which is approximately 70% of the total number of compromised records being tracked. There were 424% more records compromised as a result of these types of incidents in 2017 than those in the previous years. This implies that an increasing number of attackers may have shifted their attack paradigms to employing the insiders over the recent years. Insiders always have overwhelming superiorities over the untrusted external adversaries in terms of conducting malignant acts. Specifically, insiders are well aware of the existing security mechanisms (e.g. firewalls, cyber access controls, physical access controls etc.), thus they can fully utilise such knowledge to easily circumvent the defenses in place. This is, however, intractable for untrusted outsiders.

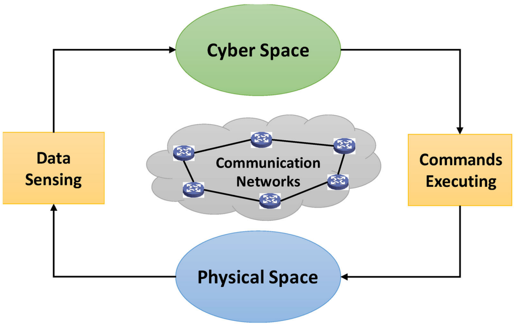


Fig. 1 *Conceptual architecture of a CPS*

In smart grid communication systems, intensive research efforts in recent years have been devoted towards detecting the outsider threats, e.g. denial-of-service (DoS) attacks, man-in-the-middle attacks, and eavesdropping, but seldom on insider threats [11]. As a result, there must exist many limitations when applying existing threats detection solutions directly to insider threats in smart grid communication systems, because insider threats may have completely distinct attack strategies and behaviours. To address these limitations and provide useful insights for future research studies, this paper focuses on insider threats detection solutions in

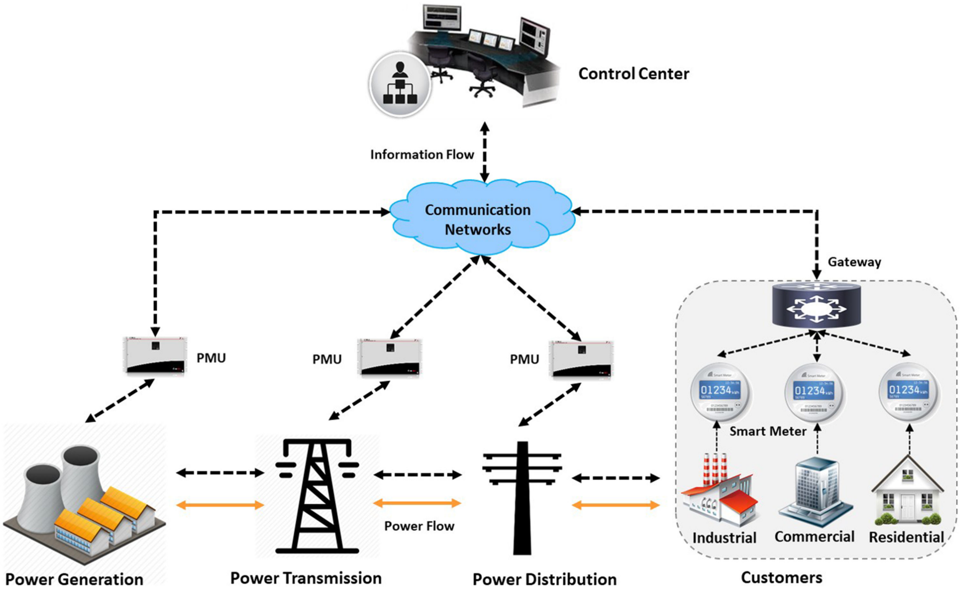


Fig. 2 *Architecture of a smart grid*

smart grid communication systems. Our research contributions are in three-fold:

- We carefully investigate the insider threats in smart grid communication systems and summarise the existing threats detection solutions.
- Most importantly, we propose a novel hybrid insider threats modelling, analysis, and detection framework for smart grid communication systems, which is based on stochastic Petri net and behaviour rule specifications. The effectiveness of the proposed model is validated by PIPE2 [12].
- A learning algorithm of transition rates in the proposed stochastic Petri net-based model is designed to achieve near real-time evaluation of the system risk degree.

The remainder of this paper is organised as follows. Section 2 gives a high-level overview of the smart grid architecture with its specific security requirements. Section 3 showcases a taxonomy of existing insider attacks in smart grid communication systems. Following this, existing threats detection solutions in smart grid communication systems are categorised in Section 4. Our proposed framework for insider threats modelling, analysis, and detection is elaborated in Section 5, followed by the numerical results in Section 6. Finally, Section 7 concludes this paper with future research directions.

2 Smart grid architecture and security requirements

In this section, we formalise the architecture of a smart grid and identify its specific security requirements.

2.1 Architecture of smart grid

Smart grid is a fusion system comprising a physical space of power grid as well as a cyber space of communication and control system (as shown in Fig. 2). The physical space incorporates power generation plants, transmission substations, distribution substations, and customer premises (e.g. residential houses, commercial buildings, and industrial factories). Phasor measurement units (PMUs) are deployed at each bus or substation along the power grid to measure the real-time status of the power grid. In addition, smart meters are positioned at each customer site to collect detailed electricity consumption data. Note that in smart grid, not only the information flow but also the power delivery is no longer restricted to a single direction [13]. Customers with capabilities of producing renewable energies, e.g. solar, wind, hydro etc., are allowed to supply their surplus energy back to the power grid for other customers.

Q1 In the cyber space, a variety of wired and wireless communication networks, such as wireless sensor networks, 3G/4G cellular networks, optical fibre networks etc., are integrated to support diverse communication requirements in different parts of the smart grid. These communication channels are responsible for timely and efficient information transmission across the entire power grid. Specifically, it includes transporting real-time measurement and sensing data from PMUs and smart meters to the system control centre, and delivering control commands from the control centre to IEDs and actuators. The control centre is the core component of the whole power grid, wherein reported data are carefully analysed for multiple applications, e.g. state estimation, event diagnostics, optimal power flow analysis etc. These applications are planned to make optimal feedback decisions to coordinate the demand–supply relations and optimise system operations.

Strictly speaking, the smart grid cannot be distinctly divided into cyber space and physical space, as the heavy interdependence between the two spaces has fused them together as a whole system. Sensing data analysis and control commands execution tightly interconnect the power grid and communication networks, forming into a strict and efficient close-loop control framework. This framework enables automatic real-time supervision and control of the power grid, and thereby boosts the efficiency, reliability, and robustness of the system.

2.2 Security requirements of smart grid

The high reliability, efficiency, and robustness of a smart grid heavily rely on the security guarantee of the entire system. Therefore, a line of high-level security requirements must be satisfied to ensure system security. Here, we discuss a few of these security requirements, and show a few scenarios where inside attackers can breach or misuse these requirements.

- *Integrity:* The integrity in smart grid refers to preventing malicious modification, delay or drop of communication information, such as sensing data, metering readings, and control commands, by unauthorised parties. Inside attackers can conduct false data injection attacks, data replay attacks, data delay or drop attacks over the communication networks to breach this requirement.
- *Availability:* The availability is concerned with ensuring that legitimate access or use of information and/or communication resources for authorised users cannot be delayed or denied by unauthorised parties. For the smart grid, these resources include all the IT elements of the system, like databases, operator

workstations, management systems, defense mechanisms, as well as the communication systems among these elements. Successful implementation of attacks against this requirement may cause significant safety issues and catastrophic physical damages, considering that system operators may lose control of the power grid over the disabled communication channels. This requirement mainly includes defense against DoS attacks, distributed DoS (DDoS) attacks, and delay of service attacks.

- *Authentication:* Authentication is a process of determining whether an identity is declared to be a legitimate system user by matching the credentials with those stored in the database. Authentication is required before each communication session starts, and between any two parties that have communication needs. For example, the control centre has the need to authenticate PMUs before accepting the measurement data, or system actuators have the need to authenticate the control centre before executing given commands. Without effective authentication mechanisms in place, malicious attackers, for example, may disguise as a legitimate PMU who can report false measurement data to mislead the control centre into issuing damaging commands. Authentication is of paramount significance to distinguish between legitimate and illegitimate users in smart grid. However, inside attackers can easily misuse their legitimate identities to launch malicious attacks.
- *Confidentiality and privacy:* This requirement in smart grid is concerned with preventing disclosure of secret information, such as system topology and configurations, measurement data, and customer power consumption data etc., to unauthorised parties. Breach of this requirement may contribute to major security issues. On the one hand, leakage of power grid status information (i.e. topology and configurations, measurement data) may cause significant security threats to the system, as malicious attackers can benefit from such information to launch false data injection attacks or more complicated cyber-physical attacks. On the other hand, in case that the detailed customer consumption data is exposed to the outside world, adversaries with vicious intentions can gain insights into users' daily life behaviours by analysing these data with a certain side information. However, insiders with malicious intentions are able to easily break this requirement by stealing and selling such sensitive information to others.
- *Authorisation:* Also known as access control, authorisation in smart grid refers to giving official permissions for specific users or IEDs with full or limited access to certain system resources, say databases, management systems etc. There are many different roles and user groups in the smart grid, and they all have diverse privileges and responsibilities, thereby an effective authorisation mechanism is required to prevent system resources from illegitimate access. Note that, since authorisation is able to distinguish between legitimate and illegitimate users for specific resources, it can also, to a certain extent, protect the integrity and confidentiality. However, similar to that for authentication requirement, insiders with legitimate privileges can easily carry out malicious activities.
- *Non-repudiability:* In the context of smart grid, non-repudiability deals with preserving the undeniable proofs of whom initiated a specific action in the system, say issuing a command or visiting a database. This security requirement expects to establish accountability and liability in smart grid, by which the actors can easily be identified with irrefutable proof of their previous actions. This requirement provides effective proofs to identify insider threats. Unfortunately, in some cases, insiders may be able to ruin these proofs before being disclosed.
- *Auditability:* Auditability allows auditors to reconstruct the complete operation history of a specific user or device based on historical records, e.g. log files, duty schedules, of all its own or relevant performed acts. This security requirement aims to identify the reasons for any malfunction or security incident so that perpetrators can easily be discovered, and the potential vulnerabilities of the system can be identified and further fixed. Such a requirement can be breached by malignant insiders who may access these historical records and delete or ruin them permanently.

3 Insider threats in smart grid

To clearly identify the attack strategies, objectives, and potential impacts of insider threats, here we develop a taxonomy of existing insider threats in smart grid. We then introduce three types of attack behaviours of these insider threats. Note that insiders considered in this paper are those who can play an authorised role in the whole smart grid communication systems. In other words, insiders have authorised entities with legitimate credentials to access the communication system including system operators, utility employees, third-party service providers, end users, and particularly, all IEDs joining in this system.

3.1 Taxonomy of existing insider threats

As summarised in Table 1, we present a taxonomy of existing insider threats in smart grid. In this taxonomy, there are four types of insider threats: false data injection, false command injection, delay of service, and insider data theft. The attack strategies, objectives, and impacts on the system are shown as follows:

3.1.1 False data injection.: A false data injection attack refers to reporting fake measurement data to the control centre from compromised metering devices, say PMUs and smart meters, with a purpose to mislead the control centre into making false decisions [14]. False data injection attacks are able to easily circumvent the traditional false data detection (FDD) system in smart grid, with the assumption that attackers are equipped with the knowledge of system topology and configurations. Through a line of compromised PMUs, these attackers can simultaneously falsify a set of measurement data in a desired manner, which can effectively blind the state estimator used for conventional FDD. Let us brief the state estimation first. Assume that $\boldsymbol{x} = (x_1, x_2, \dots, x_n)'$ is the real system states vector of the power grid, and $\boldsymbol{z} = (z_1, z_2, \dots, z_m)'$ is the measurement data collected from the PMUs, where n and m are positive integers, and $x_i, z_j \in \mathbb{R}$ for $i = 1, 2, \dots, n$ and $j = 1, 2, \dots, m$. With the DC power flow model, the relation between PMU readings and the system real status can be expressed as

$$\boldsymbol{z} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{\eta}, \tag{1}$$

where $\boldsymbol{H}$ is an $m \times n$ measurement Jacobian matrix, implying the knowledge of grid topology and configurations. $\boldsymbol{\eta} = (\eta_1, \eta_2, \dots, \eta_m)' \sim \mathbb{N}(\boldsymbol{0}, \boldsymbol{W})$ is an independent measurement error vector with zero-mean and covariance $\boldsymbol{W}$, a diagonal matrix. Statistical estimation method, like maximum likelihood estimation, is exploited to estimate the real system state variables by

$$\hat{\boldsymbol{x}} = [\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}^{-1}\boldsymbol{H}]^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}^{-1}\boldsymbol{z}\,. \tag{2}$$

The measurement residual $\boldsymbol{r} = \boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}$ is then calculated, and the $\mathbb{L}_2$-norm of the normalised measurement residual $\| \bar{\boldsymbol{r}} \|$ can be utilised to detect the presence of false data.

On basis of the traditional state estimation, false data injection attackers with knowledge of $\boldsymbol{H}$ can employ a number of

Table 1 Taxonomy of existing insider attacks in smart grid

Name	Description
false data injection	compromised meter devices (e.g. PMUs and smart meters) report fake data to the control centre
false command injection	system operators or local control agents issue fake commands to actuators, say line breakers and generators
delay of service	IEDs create delays in latency-sensitive services, e.g. delayed report of real-time measurement data
confidential data theft	utilities employees or compromised devices steal sensitive information or intellectual property

compromised PMUs to collaboratively construct a set of bad measurement data z_{bad} as

$$z_{\text{bad}} = z + \boldsymbol{Hc}, \tag{3}$$

where $\boldsymbol{c}$ is the desired offset to be injected to $\boldsymbol{x}$. As such, fake system states are estimated by

$$\begin{aligned} \hat{\boldsymbol{x}}_{\text{bad}} &= [\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}^{-1}\boldsymbol{H}]^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}^{-1}z_{\text{bad}} \\ &= [\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}^{-1}\boldsymbol{H}]^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}^{-1}(z + \boldsymbol{Hc}) \\ &= \hat{\boldsymbol{x}} + \boldsymbol{c}\,. \end{aligned} \tag{4}$$

With such a set of fake data being undetected, the system control centre is much likely to issue false feedback commands to the power grid, resulting in serious damages.

3.1.2 False command injection.: A false command injection attack attempts to inject illicit control commands to the system actuators to mislead the normal physical processes [4]. This kind of attack can be implemented by not only inside system operators (say disgruntled employees) but also IEDs (say decentralised control agents). Inside system operators, who oversee the entire power grid with high privileges, can easily inject illicit commands. Likewise, IEDs controlled by remote hackers can also directly inject fake commands, e.g. abnormally opening a circuit breaker to cause power outage, or exceptionally turning on a generator to mess up normal demand–supply relations.

False command injection attacks usually lead to more severe damages for CPSs than false data injection attacks, as attackers can directly manipulate the control units and all its operations. For example, in 2000 an Australia sewage control system was invaded by an ex-contractor, with a motive of revenge, who injected fake commands to open the flood gates. These malignant acts resulted in more than one million litres of raw sewage being poured into two local fresh water streams, which polluted the water for the subsequent three months. Unfortunately, only a few research studies have paid attention to this kind of attacks in the smart grid. One rare example is that Gao *et al.* in 2010 investigated the false command injection attacks in smart grid supervisory control and data acquisition (SCADA) system and the relevant detection techniques [15]. More research efforts are demanded towards preventing and detecting false command injection attacks in smart grid.

3.1.3 Delay of service.: Instead of denying services (e.g. dropping data) or offering bad services (e.g. falsifying data), delay of service attacks prefer to compromise the quality of services by creating delays when offering latency-sensitive services. In other words, similar to DoS attacks, delay of service attacks target at the availability requirement in smart grid [16]. This kind of inside attackers can employ distinct strategies in real-world applications, as various services may have different latency requirements. For example, the power grid can tolerate up to 4 ms for protective relaying service, a few seconds for SCADA data transmission, several minutes for real-time market pricing information, and some hours for smart meter readings etc.

3.1.4 Confidential data theft.: A confidential data theft attack in smart grid is concerned with illicit insider acts of stealing sensitive data stored on database servers, desktop computers, or other internal devices. Specifically, disgruntled employees or compromised IEDs with legitimate access to data resources are able to launch data theft attacks by stealing information such as the system topology and configurations data, user power consumption data, intellectual property etc. Once these data are leaked or sold to the third parties, e.g. marketers, maintenance utilities, household appliance enterprises, or even criminals, they can be exploited for different purposes. For example, customer electricity consumption data may reveal the daily lifestyle of an individual house, as each appliance has a unique electricity usage profile. Criminals, if having such data, may figure out the daily routines of a family and commit burglary when people are absent, or cause personal injuries when someone is at home alone.

Confidential data theft attack has been a growing critical problem for corporations and organisations over the years. According to the 2018 Data Breach Investigations Report [17] by Verizon, the year 2017 has confirmed 2216 data breaches across 65 countries. In particular, the healthcare, education, professional, and public domains have experienced an ever-growing number of data breaches.

3.2 Attack prototypes

In this subsection, we show three attack prototypes in terms of malicious insiders' attack strategies. With different illegitimate intentions and under different circumstances, inside attackers may behave in distinct manners. Some may prefer to lurk behind the power grid as long time as possible by performing less malicious acts, while others may prefer to cause as extensive damages as possible by carrying out malicious acts whenever having an opportunity. In this paper, insider attacks are categorised into three prototypes: reckless, random, and opportunistic attacks [8].

- Reckless attacks are carried out without hesitation whenever the attackers have the capability and have not been detected yet. The attacking probability of a reckless attack can be defined as $P_{\text{att}} = 1$, wherein these attacks behave in a rude manner with the intention to cause as extensive damages as possible. Reckless attacks are, therefore, the easiest type of attacks to be identified by existing detection techniques.
- Random attacks are conducted with a certain attacking probability, i.e. $P_{\text{att}} = \rho$, where $\rho \in [0, 1]$. Unlike reckless attacks, these attacks are performed with consideration to balance between the damages they may cause and the chances they could be identified. Hence, such attacks are carried out in a relatively moderate mode. Usually, it will cost the detection system a certain efforts to detect these random attacks.
- Opportunistic attacks are the most cunning attacks, which are usually implemented based on the system noise level with an attacking probability of

$$P_{\text{att}} = f(\alpha, \beta, \gamma) \cdot P_n^{\epsilon}, \tag{5}$$

where $f(\alpha, \beta, \gamma)$ is a coefficient function. α, β, and γ denote the difficulty level of the attack mission, operating time of the insider (employee or device), and the latent period since the insider has been compromised, respectively. In addition, ϵ denotes a scalar of the system noise level P_n, where $P_n \in [0, 1]$. In particular, $\epsilon > 1$ represents conservative opportunistic attacks, while $\epsilon < 1$ represents aggressive ones. From (5), we see that the higher the system noise level P_n is, the larger the attacking probability P_{att} is, and vice versa. This reveals that opportunistic attackers are good at hiding themselves based on the system noise level. As a result, it is usually hard to detect these attacks.

4 Existing detection countermeasures for security threats in smart grid

In this section, we give an overview of state-of-the-art threats detection approaches in smart grid, including signature-, anomaly-, and specification-based approaches. These detection approaches are all grounded on data forensics and network surveillance techniques, for example by comparing the collected measurement data with the predefined rule specifications, or matching the traffic flow patterns with those stored in databases. Features of different detection approaches usually vary a lot, resulting in a wide variety of superiorities and limitations while solving threats detection problems in smart grid. We summarise and compare the mechanisms, advantages, and disadvantages of the these approaches in Table 2.

Table 2 Comparison of existing threat detection approaches

Detection approach	Signature-based	Anomaly-based	Specification-based
mechanism	data mining methods are utilised to detect possible attacks based on known attack patterns (with a pre-established blacklist)	statistical techniques are utilised to differentiate between the normal and abnormal behaviours (with a pre-established whitelist)	normal behaviour model is built based on either man-made or mined rule specifications to detect non-specification-comply behaviours
advantage	extremely efficient for known-pattern attacks; low false positive rate	capable of detecting both new-pattern and known-pattern attacks although not highly effective	able to effectively detect not only known-pattern but also new-pattern attacks; low false alarms
disadvantage	inefficient for new-pattern attacks; high false negative rate	suffering from heavy computational burden; high false positive rate	costly efforts to manually develop a complete and detailed set of legitimate rule specifications for complicated networks

4.1 Signature-based detection

Signature-based detection approaches, also known as misuse detection approaches, aim to look for patterns of malicious behaviours by matching the observed runtime features with known-attack signatures from a pre-established database. These type of approaches have been widely used in existing CPS communication networks. For example, in order to detect known suspicious or Q2 malicious communication activities in smart grid, Yang *et al.* [18] utilised a signature-based detection scheme by specifying a line of attack behaviours (e.g. spontaneous messages storm, unauthorised interrogation commands to a server, reset process command from unauthorised client etc.), and matching user profiles with these attack behaviours to identify potential cyber attacks.

The main advantage of signature-based detection approach is the high efficiency for known-pattern attacks detection, as it can quickly respond to known attacks with the blacklist database in hand. As a result, this type of approach usually maintains significantly low false positive rates. However, since the pre-established database cannot accommodate all the attack signatures, the major disadvantage is obviously the inefficiency for new-pattern attacks detection, usually yielding high false negative rates.

4.2 Anomaly-based detection

Anomaly-based detection approaches look for deviations from a pre-established database of normal behaviour profiles via statistical methods. These normal behaviour profiles are established based on a collection of historical observations (unsupervised) or a set of training data (semi-supervised). Anomaly-based detection technique is valuable to thwart malicious activities in CPS communication networks. For instance, Faisal *et al.* [19] employed an anomaly-based detection system using data mining techniques to secure the advanced metering infrastructure of the smart grid. Unlike legacy static data mining techniques, they opted to stream data mining technique, which they believe is a more realistic approach in real-world applications.

The key advantage of anomaly-based approaches is that they are capable of identifying new-pattern attacks, as they aim to only differentiate normal and abnormal behaviours regardless of new- or known-pattern attacks. Therefore, this approach eliminates the efforts for collecting as many known attack patterns as those for signature-based approach to keep the database up-to-date. However, the major disadvantage of this category is the susceptibility to false positives. Since the user's normal behaviours may change over time under different circumstances, thus some of these changed behaviours may easily be considered as abnormal. Moreover, this type of approaches may also suffer from heavy computational burden while matching the observed behaviours with nearly all the normal behaviour patterns in the databse.

4.3 Specification-based detection

Specification-based detection approaches look for abnormal behaviours by comparing the actual behaviours with the pre-built normal behaviour model, which is based on a set of either man-made or mined rule specifications. Unlike anomaly-based detection approaches which compare to specific limited normal user profiles, specification-based detection approaches formally define legitimate specification model and identify potential attacks when deviations from this behaviour model is observed. One key advantage of specification-based detection approaches is that they can not only be utilised to effectively detect known-pattern attacks but also new-pattern attacks, with low false alarms. Its major disadvantage, however, is the efforts cost to manually develop a complete and detailed set of legitimate specifications in a complicated network.

BLITHE [8] is a representative work of specification-based detection approaches for smart grid communication systems. In BLITHE, PMUs are assumed to be the possible compromised IEDs that can launch false data injection attacks. To identify the potential compromised PMUs, BLITHE first employs a set of manually developed normal rule specifications for the measurement data, which are then used to build up a normal behaviour model. With this model, BLITHE is able to assess the compliance degree of each PMU. By comparing the compliance degree with a pre-defined threshold for benign PMUs, BLITHE can then identify whether a PMU is compromised or not and further whether a false data injection attack is launched.

5 Proposed framework

In this section, we elaborate our proposed insider threats modelling, analysis, and detection framework. This framework is designed based on stochastic Petri net and behaviour rule specifications (see Fig. 3 for the proposed stochastic Petri net model). A stochastic Petri net [20] is an extended Petri net, where the time intervals of state transitions are characterised by random distributions and usually exponential distributions are used. Stochastic Petri nets have the advantage of being easily transformed to discrete time Markov processes, allowing further steady-state analysis. In our proposed framework, the stochastic Petri net is used to model the behaviours of insiders, analyse the steady-state *risk degree* of the whole system, and detect the malicious insiders including both intentional and unintentional ones.

5.1 Introduction of the proposed stochastic Petri net model

A basic Petri net can be described as a 4-tuple $(\mathbb{P}, \mathbb{T}, \mathbb{F}, \mathbb{M})$, where $\mathbb{P}$ is a finite set of places, $\mathbb{T}$ is a finite set of transitions (or actions), $\mathbb{F} \subset (\mathbb{P} \times \mathbb{T}) \cup (\mathbb{T} \times \mathbb{P})$ is a finite set of input and output arcs, and $\mathbb{M}$ is a finite set of markings denoting the number of tokens in each place at a time instant. Here, a token in a place represents an object that holds a specific condition or the occurrence of a specific event that the specific place defines. Tokens can be transferred from one place to another when a transition is fired once a specific condition changes, or when an event occurs. In our proposed stochastic Petri net model, there are three places and five transitions, which are summarised in Tables 3 and 4.

5.2 Behaviour rule specifications

The behaviours of insiders are the essential evidences to assess their operating status. In our framework, we consider two categories of insider behaviours: suspicious and malicious. Specifically, suspicious behaviours are unauthorised behaviours or

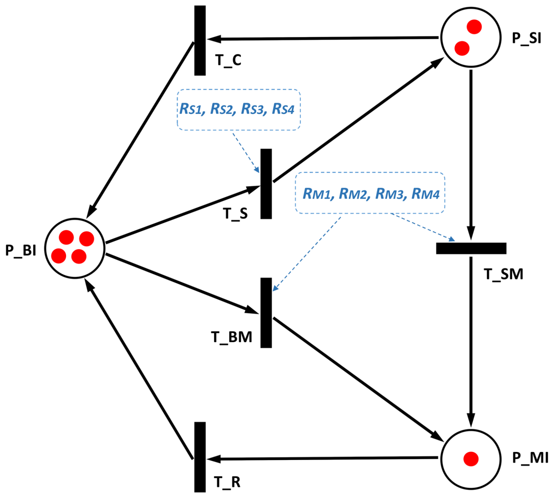


Fig. 3 *Proposed stochastic Petri net model*

Table 3 Places in the proposed stochastic Petri net

Place	Meaning
P_BI	place of benign insiders
P_SI	place of suspicious insiders
P_MI	place of malicious insiders

Table 4 Transitions in the proposed stochastic Petri net

Transition	Meaning
T_BS	transition that a benign insider commits a suspicious act
T_BM	transition that a benign insider commits a malicious act
T_SM	transition that a suspicious insider commits a malicious act
T_SB	transition that a suspicious insider is cleared from suspicion
T_MB	transition that a detected malicious insider is reset to benign

Table 5 Some example suspicious rules

Rule	Description
R_{S1}	a system operator issues an inaccurate control command
R_{S2}	utility employee visits a website w/ untrusted certificate
R_{S3}	third-party service provider keeps secret information w/o authorisation
R_{S4}	IED delays reporting measurement or sensing data

Table 6 Some example malicious rules

Rule	Description
R_{M1}	system operator issues an incorrect control command
R_{M2}	utility employee visits an unsafe/prohibited website
R_{M3}	third-party service provider leaks secret information w/o authorisation
R_{M4}	IED declines or fails to report measurement or sensing data

warned acts that may not cause damages or could only lead to minor impacts, while malicious behaviours are unauthorised behaviours or prohibited acts that can cause great damages or have high risks of contributing to significant impacts. Correspondingly, the behaviour rule specifications used in our framework are also classified into two categories: suspicious rules and malicious rules. Since there are many existing studies introducing the construction of rules, we will not focus on that point, but give some example useful rules to illustrate our framework (see Tables 5 and 6).

5.3 Insiders behaviour modelling, analysis, and detection

In this subsection, we introduce several events to show the construction of the proposed stochastic Petri net model and the transitions of tokens triggered by various insider behaviours.

- *System initialisation*: In the proposed stochastic Petri net model, each token in a place denotes an insider meeting the conditions specified by that place. Assume that there are N insiders in the considered smart grid communication systems, and in the initial stage, all of them are benign. An initial marking is, therefore, given by $M_0 = \{M_0^{\mathrm{P\_BI}}, M_0^{\mathrm{P\_SI}}, M_0^{\mathrm{P\_MI}}\} = \{N, 0, 0\}$, where $M_0^{\mathrm{P\_BI}}, M_0^{\mathrm{P\_SI}}$, and $M_0^{\mathrm{P\_MI}}$ are the numbers of tokens in places P_BI, P_SI, and P_MI at time instant 0, respectively.
- *The first event*: In the first event, we consider a utility employee visiting a website with untrusted certificate after the system initialisation. In this case, complying with rule R_{S2} fires transition T_S, as a result of which one token from place P_BI is transferred to place P_SI. The marking now shall be updated from $M_0 = \{N, 0, 0\}$ to $M_1 = \{N - 1, 1, 0\}$.
- *The second event*: In the second event, we consider a system operator issuing an incorrect control command after the first event. Performing a malicious act as R_{M1} describes leads to firing of transition T_BM. Then, a token from place P_BI is transferred to place P_MI. The current marking is updated from $M_1 = \{N - 1, 1, 0\}$ to $M_2 = \{N - 2, 1, 1\}$.
- *The third event*: In the third event, we consider the utility employee in place P_SI visiting an unsafe or prohibited website after the second event. In this case, transition T_SM is triggered, and one token from place P_SI is transferred to place P_MI. The current marking is updated from $M_2 = \{N - 2, 1, 1\}$ to $M_3 = \{N - 2, 0, 2\}$.
- *The fourth event*: In the fourth event, we consider that a detected malicious insider in place P_MI, e.g. the system operator in the second event, is fired by the company and a new operator is hired. In this case, 'resetting' an insider fires transition T_R, pulling one token from place P_MI to place P_BI. The current marking is updated from $M_3 = \{N - 2, 0, 2\}$ to $M_4 = \{N - 1, 0, 1\}$.
- *The fifth event*: In the fifth event, we consider that a suspicious insider in place P_SI is observed with long time benign behaviours. In this case, it is reasonable to conclude that this insider was considered being suspicious because of an unintentional suspicious act and now it can be cleared of suspicion. In this way, transition T_C is fired and a token from place P_SI is transferred to P_BI. Assume that the last time instant marking is $M_{t-1} = \{N - 3, 3, 0\}$, then the current marking is updated to $M_t = \{N - 2, 2, 0\}$.

As we can see, the proposed stochastic Petri net model can be used to model and analyse the insider behaviours, and detect suspicious or malicious insiders. Note that, a threshold T_{th} can be defined based on expert knowledge or history experience as the monitoring time window of suspicious insiders. If no more suspicious or malicious behaviours of these suspicious insiders are observed, they can be considered as benign insiders. In addition, insiders in place P_MI can be naturally regarded as being malicious. Close investigations or other further actions are recommended to clear such insider threats.

5.4 Steady-state analysis of system risk degree

As aforementioned, the stochastic Petri net is employed to achieve steady-state analysis.

5.4.1 Definition of risk degree.: In steady states of a discrete time Markov model transferred from the stochastic Petri net, the steady state probabilities for each state (i.e. marking here) can be obtained. In this way, the steady state numbers of tokens $N_{\mathrm{b}}, N_{\mathrm{s}}$, and N_{m} in place of P_BI, P_SI, and P_MI, respectively, can also be easily harvested. Based on these data, we define a metric *risk degree* to assess the overall operating status of the whole communication system, which is given by

$$R = 1 - \frac{w_{\mathrm{b}}N_{\mathrm{b}} + w_{\mathrm{s}}N_{\mathrm{s}} + w_{\mathrm{m}}N_{\mathrm{m}}}{N_{\mathrm{b}} + N_{\mathrm{s}} + N_{\mathrm{m}}}, \tag{6}$$

where $w_{\mathrm{b}}, w_{\mathrm{s}}$, and w_{m} are the impact factors denoting the contributions that each type of insiders (benign, suspicious, and malicious) can create on the overall system operating status, respectively.

To obtain the values of $N_{\mathrm{b}}, N_{\mathrm{s}}$, and N_{m}, we need to calculate the steady state probabilities of the underlying discrete time Markov model. Prior to that, we introduce the concept of firing rates first. The firing rate of a transition refers to the average number of tokens transferred through this transition in a unit time. We use $\boldsymbol{\lambda} = (\lambda_{\mathrm{bs}}, \lambda_{\mathrm{sb}}, \lambda_{\mathrm{mb}}, \lambda_{\mathrm{bm}}, \lambda_{\mathrm{sm}})$ to denote the firing rates for transitions T_BS, T_SB, T_MB, T_BM, and T_SM, respectively. Let $\boldsymbol{A}(\boldsymbol{\lambda})$ be the transition matrix of the Markov model obtained from the reachability graph and the firing rate vector $\boldsymbol{\lambda}$. Then, the steady-state probabilities $\boldsymbol{\pi} = (\pi_1, \pi_2, \ldots, \pi_K)$ can be solved by

$$\boldsymbol{\pi}\boldsymbol{A}(\boldsymbol{\lambda}) = \boldsymbol{\pi} \tag{7a}$$

$$\sum_{i=1}^{K} \boldsymbol{\pi} = 1, \tag{7b}$$

where K is the total number of states in the Markov model, i.e. the total number of markings in the stochastic Petri net. With the steady-state probabilities, $N_{\mathrm{b}}, N_{\mathrm{s}}$, and N_{m} can be computed by

$$N_{\mathrm{b}} = \sum_{i=1}^{K} M_i(\mathrm{P\_BI}) \cdot \pi_i \tag{8a}$$

$$N_{\mathrm{s}} = \sum_{i=1}^{K} M_i(\mathrm{P\_SI}) \cdot \pi_i \tag{8b}$$

$$N_{\mathrm{m}} = \sum_{i=1}^{K} M_i(\mathrm{P\_MI}) \cdot \pi_i, \tag{8c}$$

where $M_i(\mathrm{P\_BI}), M_i(\mathrm{P\_SI})$, and $M_i(\mathrm{P\_MI})$ denote the number of tokens in places P_BI, P_SI, and P_MI in state M_i, respectively.

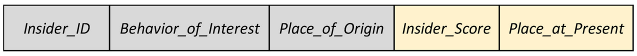
5.4.2 Learning of the transition matrix.: To achieve steady-state analysis and obtain the *risk degree*, system defenders need to know the transition matrix $\boldsymbol{A}(\boldsymbol{\lambda})$. An initial transition matrix $\boldsymbol{A}_0(\boldsymbol{\lambda})$ can be learned based on historical data by Algorithm 1 (see, Fig. 4). Then, given new observations of insiders' behaviours, the real-time transition matrix $\boldsymbol{A}(\boldsymbol{\lambda})$ can be obtained also by using Algorithm 1 with an updating strategy, such as periodically updating it in a fixed unit time T_0.

To help learn the transition matrix, each piece of an insider's behaviours of interest can be recorded in the following format in chronological order (see Fig. 5):

Each insider is assigned with an *Insider_ID*. Behaviours of interest (denoted by *Behaviour_of_Interest*) includes proactive behaviours breaking suspicious or malicious rules and passive behaviours being cleared of suspicion or reset to benign. *Place_of_Origin* and *Place_at_Present* denotes the current place this insider should stay. *Insider_Score* evaluates the overall anomalous level of an insider, taking values from 0 to 2. Note that, based on an insider's *Behaviour_of_Interest* and *Place_of_Origin*, the values of *Insider_Score* as well as the *Place_at_Present* can be determined by Algorithm 1 (Fig. 4). Note that M is the number of insiders, K^{s} the number of suspicious rules, and K^{m} the number of malicious rules. $\mathscr{K}^{\mathrm{s}} = \{1, 2, \ldots, K^{\mathrm{s}}\}$ and $\mathscr{K}^{\mathrm{m}} = \{1, 2, \ldots, K^{\mathrm{m}}\}$ denote the set of indices for suspicious and malicious rules, respectively. T_i denotes the time duration since a suspicious insider i stays in place *P_SI* and $T_i = 0$ otherwise. Correspondingly, T_{th} is a safety threshold for duration of stay in place *P_SI*. If T_i exceeds T_{th}, insider i can be cleared of suspicion and considered as benign. Δ_{s} is defined as the increment of *Insider_Score* (e.g. 0.2) for insiders in place *P_SI* breaking suspicious rules.

```
input: $T_i, i = \{1, 2, \cdots, M\}, N_{bs}, N_{bm}, N_{sm}, N_{sb}, N_{mb}$
for $Insider\_ID = i, i \in \{1, 2, \cdots, M\}$ do
    switch $Place\_of\_Origin$ do
        case: $P\_BI$
            if $Behavior\_of\_Interest == R_{Sj}, j \in \mathcal{K}^s$ then
                $Insider\_Score_i \leftarrow 1$
                $Place\_at\_Present \leftarrow P\_SI$
                $N_{bs} = N_{bs} + 1$
            else ($Behavior\_of\_Interest == R_{Mj}, j \in \mathcal{K}^m$)
                $Insider\_Score_i \leftarrow 2$
                $Place\_at\_Present \leftarrow P\_MI$
                $N_{bm} = N_{bm} + 1$
            end if
        case: $P\_SI$
            if $T_i > T_{th}$ then
                $Insider\_Score_i \leftarrow 0$
                $Place\_at\_Present \leftarrow P\_BI$
                $N_{sb} = N_{sb} + 1$
            end if
            if $Behavior\_of\_Interest == R_{Sj}, j \in \mathcal{K}^s$ then
                $Insider\_Score_i \leftarrow Insider\_Score_i + \Delta_s$
                if $Insider\_Score_i > 1.5$ then
                    $Place\_at\_Present \leftarrow P\_MI$
                    $N_{bs} = N_{bs} + 1$
                else
                    $Place\_at\_Present \leftarrow P\_SI$
                end if
            else ($Behavior\_of\_Interest == R_{Mj}, j \in \mathcal{K}^m$)
                $Insider\_Score_i \leftarrow 2$
                $Place\_at\_Present \leftarrow P\_MI$
                $N_{bm} = N_{bm} + 1$
            end if
        case: $P\_MI$
            Reset is required
            $N_{mb} = N_{mb} + 1$
end for
output: $\lambda_s = N_{bs}/T_0$, $\lambda_{bm} = N_{bm}/T_0$, $\lambda_{sm} = N_{sm}/T_0$, $\lambda_c = N_{sb}/T_0$, $\lambda_r = N_{mb}/T_0$
```

Fig. 4 *Algorithm 1: transition rates learning algorithm*



Insider_ID	Behavior_of_Interest	Place_of_Origin	Insider_Score	Place_at_Present

Fig. 5 *Reference data format for each piece of an insider's behaviours of interest*

6 Numerical results

In this section, we conduct simulations to evaluate the effectiveness of the proposed framework using PIPE2 and MATLAB. Specifically, we conduct two groups of simulations, where the first group is to evaluate the relationship between the *risk degree R* and the firing rates (i.e. $\lambda_{\mathrm{s}}, \lambda_{\mathrm{bm}}, \lambda_{\mathrm{sm}}, \lambda_{\mathrm{c}}$, and λ_{r}) and the second is for the relationship between the *risk degree R* and the impact factors (i.e. $w_{\mathrm{b}}, w_{\mathrm{s}}$, and w_{m}).

In the first group of simulations, we fix $w_{\mathrm{b}} = 1.0, w_{\mathrm{s}} = 0.5$, and $w_{\mathrm{m}} = 0.1$ for the impact factors. Note that we would like to evaluate the relationship between *risk degree R* and the insiders behaviours using the proposed stochastic Petri net model, thus we also fix $\lambda_{\mathrm{r}} = 0.15$ and $\lambda_{\mathrm{c}} = 0.2$ which represent the risk handling capabilities of a system. As Fig. 6 shows, the numerical results of R versus λ_{s} with various values of λ_{bm} are plotted. It can be seen that, given $w_{\mathrm{b}} = 1.0, w_{\mathrm{s}} = 0.5, w_{\mathrm{m}} = 0.1, \lambda_{\mathrm{r}} = 0.15, \lambda_{\mathrm{c}} = 0.2,$ and $\lambda_{\mathrm{sm}} = 0.1$, the *risk degree R* of a communication system increases as λ_{s} grows. It means that, the more benign insiders conduct suspicious acts, the more tokens from place P_BI transferred to place P_SI, and as a result, the higher the system *risk degree*. In

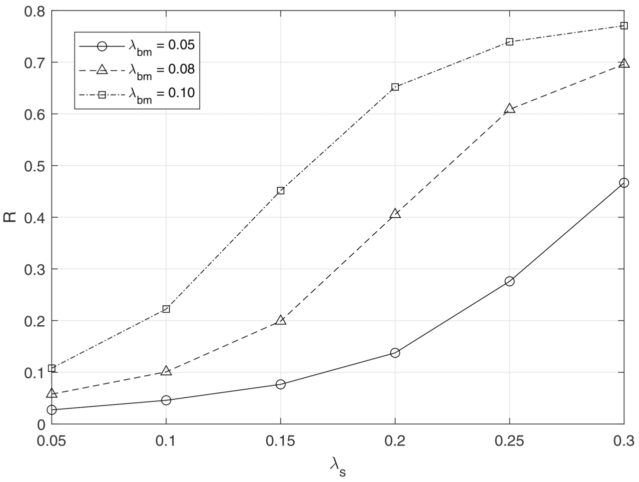


Fig. 6 *Risk degree versus various λ_s with various values of λ_{bm} ($w_b = 1.0, w_s = 0.5, w_m = 0.1, \lambda_r = 0.15, \lambda_c = 0.2$, and $\lambda_{sm} = 0.1$)*

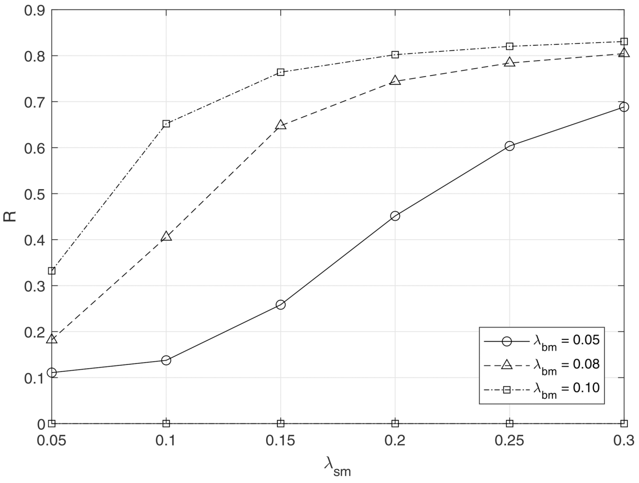


Fig. 7 *Risk degree versus λ_{sm} with various values of λ_{bm} ($w_b = 1.0, w_s = 0.5, w_m = 0.1, \lambda_r = 0.15, \lambda_c = 0.2$, and $\lambda_s = 0.2$)*

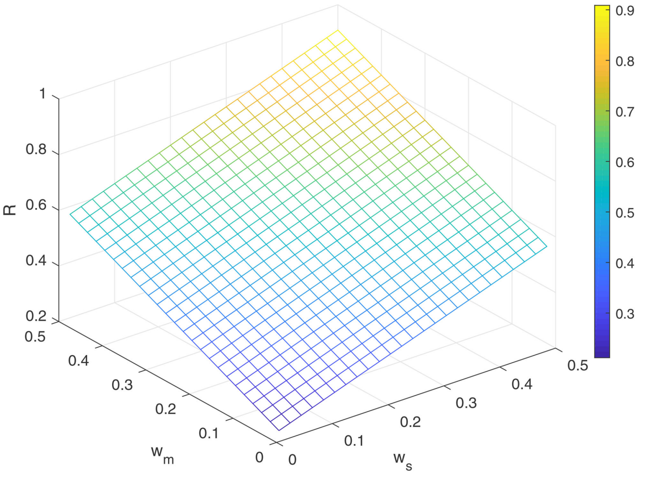


Fig. 8 *Risk degree versus w_s and w_m ($\lambda_s = 0.2, \lambda_{sm} = 0.1, \lambda_{bm} = 0.05, \lambda_r = 0.15$, and $\lambda_c = 0.2$)*

addition, we see that given a fixed value of λ_s, a larger λ_{bm} leads to a higher *risk degree*. It is natural that, the more benign insiders conduct malicious acts, the higher the system *risk degree*.

In Fig. 7, the numerical results of the *risk degree R* versus λ_{sm} with various values of λ_{bm} are plotted. Given $w_b = 1.0, w_s = 0.5, w_m = 0.1, \lambda_r = 0.15, \lambda_c = 0.2$, and $\lambda_{sm} = 0.1$, the *risk degree R* of a communication system increases as λ_{sm} grows. This indicates that, when the number of suspicious insiders conducting malicious acts are increasing, there will be more insiders transferring from P_SI to P_MI, leading to an increased system *risk degree*. Also, we can see that given a fixed values of λ_{sm}, the larger the λ_{bm}, the higher the system *risk degree*. Intuitively, if the number of benign insiders conducting malicious acts are increasing, there will be more insiders transferring from P_BI to P_MI, leading to an increased system *risk degree*.

When it comes to the second group, we carry out simulations to evaluate the relationship between the *risk degree R* and the impact factors. In this group, we set $\lambda_s = 0.2, \lambda_{sm} = 0.1, \lambda_{bm} = 0.05, \lambda_r = 0.15$, and $\lambda_c = 0.2$. Hence we have $N_b = 24.52743, N_s = 3.47627$, and $N_m = 1.99631$ in steady states. Limit the values of w_s and w_m to the range of $[0, 0.5]$. The numerical results of the *risk degree R* versus w_s and w_m are plotted in Fig. 8. It can be easily seen that large values of w_s and w_m always result in high *risk degrees*. This is because that, according to (7b), large values of w_s and w_m lead to small values of w_b, contributing to high *risk degrees* with given parameter settings. Particularly, if $w_s = w_m = 0$, then $w_b = 1$. It means that in this case, the *risk degree* is only determined by N_b, and consequently $R = 0.182$, the lowest *risk degree* with given parameter settings. In addition, if $w_s = w_m = 0.5$, then $w_b = 0$. It means that in this case, the *risk degree* is only determined by N_s and N_m, and $R = 0.909$, the highest *risk degree* with given parameter settings.

7 Conclusion

In this paper, we investigated the insider threats in smart grid communication systems. The architecture of a smart grid and its specific security requirements were first introduced. Then, we developed a taxonomy of existing insider threats, and investigated the corresponding attack prototypes. In addition, a summary and the comparison of existing insider threat detection approaches for smart grid communication systems were presented. Most importantly, a novel hybrid insider threats modelling, analysis, and detection framework, which is based on stochastic Petri net and behaviour rule specifications, was proposed for smart grid communication systems. In future work, we aim to conduct research studies on fine-grained access control and granular data auditing to help prevent and mitigate insider threats in smart grid communication systems.

Q4

8 References

[1] Gungor, V.C., Sahin, D., Kocak, T., *et al.*: 'Smart grid technologies: communication technologies and standards', *IEEE Trans. Ind. Inf.*, 2011, **7**, (4), pp. 529–539

[2] Wolf, W.H.: 'Cyber-physical systems', *IEEE Comput.*, 2009, **42**, (3), pp. 88–89

[3] Khurana, H., Hadley, M., Lu, N., *et al.*: ''Smart-grid security issues'', *IEEE Security Privacy*, 2010, **8**, (1)

Q5 [4] Li, B., Lu, R., Wang, W., *et al.*: 'DDOA: a dirichlet-based detection scheme for opportunistic attacks in smart grid cyber-physical system', *IEEE Trans. Inf. Forensics Secur.*, 2016, **11**, (11), pp. 2415–2425

[5] Metke, A.R., Ekl, R.L.: 'Security technology for smart grid networks', *IEEE Trans. Smart Grid*, 2010, **1**, (1), pp. 99–107

[6] Li, B., Lu, R., Wang, W., *et al.*: 'Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system', *J. Parallel. Distrib. Comput.*, 2017

Q6 [7] Li, B., Lu, R., Xiao, G.: 'HMM-based fast detection of false data injections in advanced metering infrastructure'. Proc. GLOBECOM 2017, Singapore, December 2017

[8] Bao, H., Lu, R., Li, B., *et al.*: 'BLITHE: behavior rule-based insider threat detection for smart grid', *IEEE Internet Things J.*, 2016, **3**, (2), pp. 190–205

[9] 'IBM X-Force Threat Intelligence Index 2017', Available at https://www.leadersinsecurity.org/component/phocadownload/category/11-2017-cybersecurity-publications.html?download=185:2017-cybersecurity-publications, accessed 10 July, 2018

[10] 'IBM X-Force Threat Intelligence Index 2018', Available at https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=77014377USEN, accessed 10 July, 2018

[11] Saxena, N., Choi, B.J., Lu, R.: 'Authentication and authorization scheme for various user roles and devices in smart grid', *IEEE Trans. Inf. Forensics Secur.*, 2016, **11**, (5), pp. 907–921

[12] Dingle, N.J., Knottenbelt, W.J., Suto, T.: 'PIPE2: a tool for the performance evaluation of generalised stochastic Petri nets (PDF format)', *ACM SIGMETRICS Perform. Eval. Rev.*, 2009, **36**, (4), pp. 34–39

[13] 'NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0', Available at https://www.nist.gov/sites/default/files/documents/smartgrid/NIST-SP-1108r3.pdf, accessed 10 July, 2018

[14] Liu, Y., Ning, P., Reiter, M.K.: 'False data injection attacks against state estimation in electric power grids', *ACM Trans Inf. Syst. Secur.*, 2011, **14**, (1), p. 13

[15] Gao, W., Morris, T.H., Reaves, B., *et al.*: 'On SCADA control system command and response injection and intrusion detection'. Proc. eCrime 2010, Dallas, USA, October 2010, pp. 1–9

[16] Pindoriya, N.M., Dasgupta, D., Srinivasan, D., *et al.*: 'Infrastructure security for smart power grids: a survey', in Pappu, V., Carvalho, M., Pardalos, P (Eds.): '*Optimization and security challenges in smart power grids*' (Springer, New York, 2013), pp. 161–180

[17] '2018 Data Breach Investigations Report', Available at: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf, accessed on 10 July, 2018

[18] Yang, Y., McLaughlin, K., Littler, T., *et al.*: 'Intrusion detection system for IEC 60870-5-104 based SCADA networks'. Proc. Power and Energy Society General Meeting (PES), Vancouver, British Columbia, Canada, July 2013, pp. 1–5

[19] Faisal, M.A., Aung, Z., Williams, J.R., *et al.*: 'Securing advanced metering infrastructure using intrusion detection system with data stream mining'. Proc. Pacific-Asia Workshop on Intelligence and Security Informatics 2012, Kuala Lumpur, Malaysia, May 2012, pp. 96–111

[20] Molloy, M.K.: 'Performance analysis using stochastic Petri nets', *IEEE Trans. Comput.*, 1982, **31**, (9), pp. 913–917

Q7 [21] Schweppe, F.C., Wildes, J.: 'Power system static-state estimation, part I: exact model', *IEEE Trans. Power Appl. Syst.*, 1970, (1), pp. 120–125

Q8

IET-COM20185736

Author Queries

Q Please make sure the supplied images are correct for both online (colour) and print (black and white). If changes are required please supply corrected source files along with any other corrections needed for the paper.

Q All equations too long to fit within a single column are automatically floated to the bottom of the page and a '(see equation below)' or '(see (equation number) and (equation number)' left in their place. This is done automatically by our new XML transform, so please specify in your corrections very clearly where they should be broken as your paper is edited by non-experts.

Q1 Please check the edits made to the sentence 'Customers with ...'.

Q2 Please confirm the edits made in the sentence.

Q3 We have changed the algorithm 1 to figure 4 and figures have been renumbered accordingly as per style. Please check and approve.

Q4 As per journal style references are renumbered in the text and reference list. Please confirm.

Q5 Please provide page range in Ref. [3].

Q6 Please provide volume number and page range in Ref. [6].

Q7 Please confirm the inserted volume number in Ref. [21].

Q8 Please provide the volume number for Ref. [21] and is listed in the reference list but not cited in the text. Please cite in the text, else delete from the list.