This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3127353, IEEE Transactions on Power Systems

Detection of False Data Injection Attacks on Smart Grids: A Resilience-Enhanced Scheme

Beibei Li, *Member, IEEE,* Rongxing Lu, *Fellow, IEEE,* Gaoxi Xiao, *Senior Member, IEEE,* Tao Li, and Kim-Kwang Raymond Choo, *Senior Member, IEEE*

***Abstract*—The integration of phasor measurement units (PMUs) and phasor data concentrators (PDCs) in smart grids may be exploited by attackers to initiate new and sophisticated false data injection (FDI) attacks. Existing FDI attack mitigation approaches are generally less effective against sophisticated FDI attacks, such as collusive false data injection (CFDI) attacks launched by compromised PDCs (and PMUs) as we demonstrate in this paper. Thus, we propose a secure and resilience-enhanced scheme (SeCDM) to detect and mitigate such cyber threats in smart grids. Specifically, we design a decentralized homomorphic computation paradigm along with a hierarchical knowledge sharing algorithm to facilitate secure ciphertext calculation of state estimation residuals. Following this, a centralized FDI detector is implemented to detect FDI attacks. Findings from the security analysis demonstrate our approach achieves enhanced conventional FDI and CFDI attack resilience, and findings from our performance evaluations on the standard IEEE 14-, 24-, and 39-bus power systems also show that the communication overheads and computational complexity are reasonably "low".**

***Keywords*—Smart grids, state estimation, false data injection (FDI) attacks, collusion attacks, system resilience.**

TABLE I
SUMMARY OF NOTATIONS

Notation	Meaning
$\mathbf{z}$	The vector of measurement data in a power system
$\mathbf{x}$	The vector of real power system status data
$\mathbf{H}$	The measurement Jacobian matrix of a power system
$\boldsymbol{\gamma}$	The vector of measurement residuals
τ	The predefined threshold for bad data detection
$\boldsymbol{\Omega}$	The transformed matrix containing the secrets of $\mathbf{H}$
$\boldsymbol{\omega}_i^0$	The secret matrix shared by PDC V_i
$\boldsymbol{\omega}_i^1$	The secret matrix shared by the FDI detection module
H_0	The null hypothesis that $\mathbf{z}$ is valid with no FDI attack
H_1	The alternative hypothesis that $\mathbf{z}$ is under an FDI attack
$\tilde{\mathbf{z}}$	The non-negative integer vector by converting the measurement data vector $\mathbf{z}$
$\boldsymbol{z}'$	The vector of measurement data with false data injected
$E(\tilde{\mathbf{z}}_i)$	The encrypted measurement data of $\mathbf{z}$
$A_{i,j}$	The message authentication code (MAC) for $z_{i,j}$
l	The number of PMUs, as well as the number of buses
d	The dimension of measurement data $\mathbf{z}$
δ	The number of regions in a power grid

I. INTRODUCTION

There is an expectation that smart grids, benefiting from the wide-area measurement and control (WAMC) system, can help achieve accurate, efficient, and reliable bidirectional power flows (also explained in the IEEE Grid Vision 2050 [1]). However, the expanded interconnectivity of smart grids also implies a larger attack surface, with more potential for attacks and exploitations. For example, as shown in Fig. 1, the deployment of integrated intelligent equipment/devices, such as phasor measurement units (PMUs) and phasor data concentrators (PDCs), is increasingly common in smart grids. One relatively high profile incident is that involving Stuxnet, a malware reportedly designed to target Iran's nuclear power plant. In this particular example, over 20,000 network terminals were reportedly infected and an estimated number of 984 uranium enriching centrifuges were destroyed [2]. Other more recent high profile incidents include the distributed denial-of-service (DDoS) attacks on JEA, a major electric utility located in Jacksonville, Florida, U.S., in 2013 [3], the BlackEnergy3 & denial-of-service (DoS) attacks on Ukraine's power grids in 2015 [4], and the zero-day exploits targeting U.S. power grids in March 2019 [5]. Such incidents show that smart grids are much more likely to remain a major target of interest in the coming future, particularly by those state-sponsored or affiliated cyber threat actors. The importance of cyber security in smart grids is also reinforced by a recent report from the United States Government Accountability Office [6], which stated that '*threat actors are becoming increasingly capable of carrying out attacks on the grid. At the same time, the grid is becoming more vulnerable to attacks*'.

One commonly seen attack targeting smart grids is false data injection (FDI; also known as data integrity or data deception attacks in the literature). For example, Liu *et al.* demonstrated that the viability of circumventing conventional static state

The work of B. Li was supported in part by the National Key Research and Development Program of China under Grant No. 2020YFB1805400; the National Natural Science Foundation of China under Grants No. 62002248; the China Postdoctoral Science Foundation under Grants No. 2019TQ0217 and 2020M673277; the Provincial Key Research and Development Program of Sichuan under Grant No. 20ZDYF3145; the Fundamental Research Funds for the Central Universities (No. YJ201933); the China International Postdoctoral Exchange Fellowship Program (Talent-Introduction). The work of G. Xiao was partially supported by the Future Resilient Systems (FRS-II) Project at the Singapore-ETH Centre (SEC), which was funded by the National Research Foundation of Singapore (NRF) under its Campus for Research Excellence and Technological Enterprise (CREATE) program. The work of K.-K. R. Choo was supported only by the Cloud Technology Endowed Professorship. *(Corresponding author: Tao Li.)*

B. Li and T. Li are with the School of Cyber Science and Engineering, Sichuan University, Chengdu, China 610065 (email: libeibei@scu.edu.cn; litao@scu.edu.cn).

R. Lu is with the Faculty of Computer Science, University of New Brunswick, Fredericton, NB, Canada E3B 5A3 (e-mail: rlu1@unb.ca).

G. Xiao is with the School of Electrical and Electronic Engineering, Singapore 639798 (e-mail: egxxiao@ntu.edu.sg).

K.-K. R. Choo is with the Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249, USA (e-mail: raymond.choo@fulbrightmail.org).

0885-8950 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of New Brunswick. Downloaded on June 09,2022 at 00:08:30 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3127353, IEEE Transactions on Power Systems

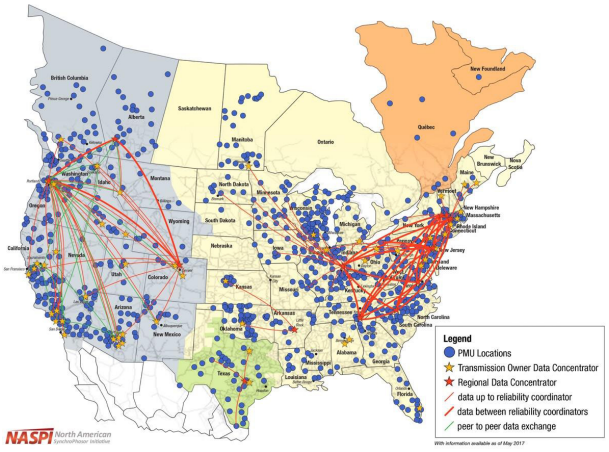


Fig. 1. A snapshot of PMU and PDC deployments in North America [7].

estimator and bad data detector, if the attackers are equipped with the knowledge of grid topology and configurations as well as a line of measurement data [8]. In such an attack, adversaries plan to inject fabricated measurement data via compromised metering devices, in purpose of blinding and misleading the power gird control center. Consequences of a successful FDI attack include system disturbance or downtime, power overloading, power outages, and potentially physical casualties. Thus, detecting and mitigating FDI attacks is a topic of ongoing research interest [9]–[18].

One can observe that there have also been attempts to utilize homomorphic encryption techniques for secure state estimation and/or FDI attack mitigation in power grids [9]–[12]. For example, Li *et al.* in 2018 proposed a PAMA scheme, where a hybrid Paillier cryptosystem is employed to allow FDI detection on ciphertexts, as well as minimizing the risk of information leakage [9]. In 2020, Zhang *et al.* [10] designed an encryption-based state estimation scheme by using both multiplicatively and additively homomorphic encryption approaches, in order to conceal the model parameters, measurement data, and state estimates. However, these studies generally assume weak adversarial settings, in the sense that participants (e.g., PDCs, and data aggregators [19], [20]) are fully trusted at all times. It is, now, an unrealistic assumption, because PDCs as well as their communication channels are suffering from a line of cyberattacks [21]–[24], particularly given that attackers (e.g., well-resourced attackers such as state-sponsored or advanced persistent threat (APT) actors) are capable of launching sophisticated large-scale attacks [25]. While there have been studies focusing on new categories of strong FDI attacks on smart grids, such as coordinated FDI-physical attacks [13], multiple-bus FDI attacks [14], and optimal FDI attacks [15], we observe that PDC- and/or PMU-empowered FDI attacks remain challenging to be addressed. The importance of securing PDCs and mitigating PDC-empowered FDI attacks should not be understated, as PDCs and PMUs are two key components in smart grids. In other words, compromised PDCs and PMUs can be abused to facilitate other damaging and sophisticated FDI attacks on smart grids [17], [18], with potentially fatal consequences.

Motivated by the above observations, we focus on the case where both PMUs and PDCs are not fully trusted participants, and they can collude to design new FDI attacks. Such new attacks are coined "collusive false data injection" (CFDI) attacks (see the adversarial model outlined in Section III-B), which can have a significant impact on smart grid operations resulting in devastating consequences. To defend against CDFI attacks, in this paper, we propose a **Se**cure **C**FDI **D**etection and **M**itigation scheme (SeCDM) for smart grid deployment. Specifically, we design a decentralized homomorphic computation paradigm, along with a hierarchical knowledge sharing algorithm, to enable secure calculation of measurement residuals in the ciphertext domain. Then, a centralized FDI detection is conducted to identify the existence of FDI attacks based on these measurement residuals. A summary of our main contributions is presented below:

- We demonstrate how several existing homomorphic encryption based FDI mitigation schemes (e.g., PAMA [9]) are vulnerable to CFDI attacks, a set of sophisticated FDI attacks initiated by a coalition of compromised PDCs (and PMUs). The importance of defending against such new attacks for smart grids is then discussed.
- We propose a novel secure and resilience-enhanced scheme (hereafter referred to as SeCDM) to detect and mitigate not only conventional FDI attacks, but also two new types of CFDI attacks on smart grids; thus, enabling smart grids to defend against a broader spectrum of FDI attacks.
- We design a new decentralized homomorphic computation paradigm, along with a hierarchical knowledge sharing algorithm for smart grids, which allows secure and efficient FDI detection (as demonstrated by our security analysis and extensive performance evaluations).

The remainder of this paper is organized as follows. In Section II, we review the state-of-the-art literature in terms of the FDI detection schemes and secure data transmission protocols for power grids. Section III presents our system model and adversarial model. In Section IV, we elaborate on our proposed SeCDM scheme, followed by the respective security analysis and performance evaluation in Sections V and VI. Finally, Section VII concludes this paper.

II. Related Literature

In this section, we will review the extant literature on FDI detection schemes and secure data transmission protocols for power grids.

A. FDI Detection in Power Grids

Studies focusing on FDI detection schemes for power grids have been widely reported in the literature, such as those using statistical and machine learning approaches [26]–[28]. For example, Bretas *et al.* in 2013 raised an innovation concept, i.e., the normalized composed measurement error (CME^N), in support of identifying bad data with gross errors in power systems [29]. In the same year, Esmalifalak *et al.* proposed two machine-learning-based techniques for

0885-8950 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of New Brunswick. Downloaded on June 09,2022 at 00:08:30 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3127353, IEEE Transactions on Power Systems

stealthy attack detection, one of which utilizes support vector machine (SVM) and the other requires no training data and detects deviation in measurements [30]. In 2015, Ozay *et al.* provided an attack detection framework by leveraging prior knowledge about the system, and using known batch and online learning algorithms [31]. However, these schemes usually incur significant computational overhead, for example due to the processing of raw measurements in power grids. Sparsity matrix optimization is another promising approach for FDI attack detection [32], [33]. For instance, Liu *et al.* in 2014 transformed the identification problem of FDI attacks into a low rank matrix recovery problem and the nuclear norm minimization problem [32]. Gao *et al.* in 2016 also proposed a convex-optimization-based method and theoretically demonstrated the data identification guarantee. Specifically, findings from their numerical experiments results suggested that the proposed approach achieves high detection rate [33].

Another viable approach to FDI attack detection is to leverage moving target defenses (MTDs). However, existing MTD-based approaches generally focus on protecting the measurement variables, altering the grid topologies, or altering the line impedance. This can dynamically change the conditions that FDI attackers exploit [14], [34]–[36]. For example, in 2018, Tian *et al.* proposed an enhanced hidden MTD-based approach to maintain the power flows while ensuring stealthiness even when the attackers are capable of checking the activation of the distributed flexible AC transmission system (D-FACTS) devices [34]. More recently in 2020, we systematically explored the feasibility and limitations of perturbing D-FACTS devices, an MTD approach, to thwart FDI attacks on power grid state estimation [14]. In 2021, Higgins *et al.* presented an implementation of MTD, combined with physical watermarking, to facilitate the detection of traditional and intelligent FDI attacks, while remain hidden to the attackers and limiting the impact on system operation and stability [35].

B. Secure Data Transmission Protocols in Power Grids

Securing measurement variables, as well as the configuration and topology information of power grids, can be an effective way to resist FDI attacks, as demonstrated in studies such as those of [37]–[41]. For example, in 2013 Ruj *et al.* proposed a decentralized security framework for smart grids that supports data aggregation and access control [37]. Lu *et al.* also proposed a privacy protection aggregation scheme for smart grid communication, which can also help the control center to better monitor and control the smart grid [38]. In 2018, Abdallah *et al.* [39] proposed a lightweight privacy-preserving electricity consumption aggregation scheme that utilizes lightweight lattice-based homomorphic cryptosystem, and Wen *et al.* [40] proposed a lightweight number theory research unit (NTRU)-based scheme to achieve information privacy issues. In the same year, Guan *et al.* also proposed a privacy-preserving and efficient data aggregation scheme based on blockchain for power grids communications in smart communities [41]. In addition to these schemes preventing the measurement data from being stolen and tampered with by attackers, there have been attempts to utilize homomorphic encryption techniques for achieving secure state estimation and/or FDI attack mitigation in power grids. For example, Li *et al.* in 2018 proposed a hybrid Paillier based scheme to achieve FDI detection on ciphertexts, as well as minimizing the risk of information leakage [9]. Most recently in 2020, Zhang *et al.* designed an encryption-based state estimation scheme by using both multiplicatively and additively homomorphic encryption approaches, to conceal the model parameters, measurement data, and state estimates [18]. In this work, we aim to provide a privacy-preserving FDI detection and mitigation scheme, especially for those PDC-based sophisticated CFDI attacks.

III. System and Adversarial Models

In this section, we introduce the system model and formulate the types of FDI attacks that will be addressed in this work. The nomenclature is presented in Table I.

A. System Model

The system model considers the wide-area measurement and control (WAMC) system accompanied by an FDI detection module in smart grids, which allows time-synchronized phasor data collection in real-time and consequently facilitates wide-area monitoring, FDI detection, and control of smart grids.

1) Overview: Our system model (see Fig. 2) mainly comprises four entity types, namely: a control center, an FDI detection module, a set of PDCs $\mathcal{V} = \{V_1, V_2, \cdots, V_\delta\}$, and a line of PMUs $\mathcal{U} = \{U_1, U_2, \cdots, U_l\}$. Given that a smart grid is partitioned into δ regions $\mathcal{R} = \{R_1, R_2, \cdots, R_\delta\}$ in terms of their physical distributions, each region $R_k \in \mathcal{R}, k \in \mathcal{K} = \{1, 2, \cdots, \delta\}$ has one PDC V_k and l_k PMUs. The total numbers of PMUs and PDCs in a smart grid are respectively denoted by $l = \sum_{k\in\mathcal{K}} l_k$ and δ.

- PMUs $\mathcal{U} = \{U_1, \cdots, U_l\}$: Each PMU $U_i \in \mathcal{U}$ and its neighboring line meters jointly establish a PMU-centered measurement cluster. The PMU is responsible for measuring the current phasors and voltage phasors in real-time [42], as well as aligning the power flows and power injections measured by line meters. Then, all required measurement data, forming into a d-dimensional measurement vector (d is fixed for all PMUs), are periodically delivered to the regional PDC where PMU U_i is located.
- PDCs $\mathcal{V} = \{V_1, \cdots, V_\delta\}$: Upon receiving the measurement data reported by all l_k PMUs in region R_k, each PDC $V_k \in \mathcal{V}$ preprocesses these data (with reference to Section IV-B3), aggregates the processed data [43], and then relays them to the FDI detection module. Note that $V_k(U_i)$ denotes the PDC V_k located at the same region R_k with PMU U_i.
- FDI Detection Module: The module, located at the same premise as the control center, serves as a bad data detector responsible for FDI detection on ciphertexts. The detection results are then advised to the control center.
- Control center: The results from the FDI detection module will be utilized in the decision-makings, e.g., for determining what corresponding feedback operations are to be further performed to maintain normal grid operations.

0885-8950 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of New Brunswick. Downloaded on June 09,2022 at 00:08:30 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3127353, IEEE Transactions on Power Systems

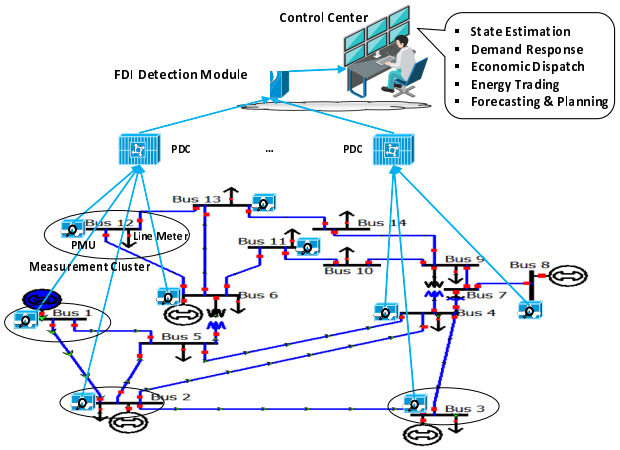


Fig. 2. The considered system model.

2) Hybrid State Estimation and Bad Data Detection: The focus of this work is on secure detection and mitigation of CFDI attacks based on a hybrid state estimation [44]–[47], which leverages measurement data (e.g., voltage magnitudes, power injections, power flows, and synchro phasors) from both PMUs, remote terminal units (RTUs), and line meters. In this work, we consider a DC power flow model for the hybrid state estimation, as the hybrid state estimation can be formulated to a linear problem [45], [46] and allows much faster and simpler calculations than AC based state estimation almost without sacrificing the accuracy of analysis [34], [48]. The state estimation algorithm, under the DC power flow model, is described by the following linear measurement model [46]:

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e}, \tag{1}$$

where $\mathbf{z} \in \mathbb{R}^{ld\times 1}$ is the measurement data vector including power flows and power injection measurements, $\mathbf{x} \in \mathbb{R}^{l\times 1}$ is the system state vector, and $\mathbf{e} \in \mathbb{R}^{ld\times 1}$ is the measurement noise vector with zero means [8], [49]. Importantly, $\mathbf{H} \in \mathbb{R}^{ld\times l}$ is the measurement Jacobian matrix, also the measurement function, containing the power grid topology and configuration information (see [44], [46] for more details). This problem can be resolved by a non-iterative procedure, which is given by

$$\hat{\mathbf{x}} = \left(\mathbf{H}^{\intercal}\mathbf{W}^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^{\intercal}\mathbf{W}^{-1}\mathbf{z}, \tag{2}$$

where $\mathbf{W} = \text{diag}(\sigma_1^2, \sigma_2^2, \cdots, \sigma_{ld}^2) \in \mathbb{R}^{ld\times ld}$ denotes the covariance matrix. Note that σ_i^2 is the non-zero noise variance for the i-th dimension of measurement data.

To perform classical bad data detection, the weighted measurement residuals are demanded [50]. With $\hat{\mathbf{x}}$ in hand, the estimated measurement data $\hat{\mathbf{z}}$ is computed by $\hat{\mathbf{z}} = \mathbf{H}\hat{\mathbf{x}}$. Then, the weighted measurement residual vector $\boldsymbol{\gamma} \in \mathbb{R}^{ld\times 1}$ is given by the weighted difference between the collected measurement data $\mathbf{z}$ and the estimated measurement data $\hat{\mathbf{z}}$, i.e.,

$$\boldsymbol{\gamma} = \sqrt{\mathbf{W}^{-1}}(\mathbf{z} - \hat{\mathbf{z}}) = \sqrt{\mathbf{W}^{-1}}(\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}). \tag{3}$$

In the last step, two hypotheses are considered [8], namely:

- H_0 is the null hypothesis, where the measurement data is valid with no FDI attack or bad data.
- H_1 is the alternative hypothesis, where the measurement data is under FDI attacks or contains bad data.

Since the main focus of this work is on secure detection and mitigation of FDI attacks, differentiating whether FDI attacks or bad measurement data trigger H_1 is not considered (see also [35], [36], [51]), as this has been the focus in other works such as those presented in [29], [52], [53].

The hypothesis test (decision rule) can then be made by the following equation:

$$\|\boldsymbol{\gamma}\|_2 \underset{H_0}{\overset{H_1}{\gtrless}} \tau, \tag{4}$$

where $\|\boldsymbol{\gamma}\|_2 = \sqrt{\sum_{\zeta\in\mathcal{M}} \gamma_\zeta^2}$ is the Euclidean norm of $\boldsymbol{\gamma}$, $\mathcal{M} = \{1, 2, \cdots, ld\}$, and τ is a predefined threshold. Since $\|\boldsymbol{\gamma}\|_2$ follows a chi-square distribution, τ can then be determined for the hypothesis test with a given significance level (see [8] for more details).

B. Adversary Model

In this paper, we assume that both the control center and the FDI detection module are fully trusted parties, and the PMUs and PDCs can be compromised by powerful attackers. This allows us to take conventional FDI attacks, P**D**C-P**M**U collusive FDI (DM-CFDI), and P**D**C-P**D**C collusive FDI (DD-CFDI) attacks on smart grids into consideration.

1) Conventional FDI Attacks: Conventional FDI attackers compromise the static DC state estimation by falsifying the normal measurement data in an attempt to blind the bad data detection. Holding the knowledge of the $\mathbf{H}$ matrix, attackers are able to forge an attack vector $\mathbf{a} \in \mathbb{R}^{d\times 1}$ by (see also [8]): $\mathbf{a} = \mathbf{H}\mathbf{c}$, where $\mathbf{c} \in \mathbb{R}^{l\times 1}$ is an arbitrary vector designed by the attackers, denoting the expected biases of the estimated power grid states which FDI attackers wish to cause. Upon having the capability of manipulating the measurement data, the attackers can forge a measurement data vector using the following equation: $\mathbf{z}' = \mathbf{z} + \mathbf{a}$. When $\mathbf{z}'$ is reported to the control center, the estimated system state vector $\hat{\mathbf{x}}$, referring to Eq. (2), can now be given by:

$$\hat{\mathbf{x}}' = \hat{\mathbf{x}} + \mathbf{c}. \tag{5}$$

The Euclidean norm of the weighted measurement residual vector $\boldsymbol{\gamma}'$ with injected false data is then given by:

$$\|\boldsymbol{\gamma}'\|_2 = \|\sqrt{\mathbf{W}^{-1}}(\mathbf{z}' - \mathbf{H}\hat{\mathbf{x}}')\|_2 = \|\sqrt{\mathbf{W}^{-1}}(\mathbf{z} - \mathbf{H}\hat{\mathbf{x}})\|_2 \leq \tau. \tag{6}$$

In this case, it is obvious that no anomaly can be detected; hence, a successful FDI attack has been carried out.

2) DM-CFDI Attacks: If FDI attackers are capable of manipulating both the PDC and at least two PMUs in a same region, the compromised PDC and PMUs can then collude to form a coalition. Note that by saying "compromise a device", we mean that the attackers are capable of obtaining the secret knowledge that the device holds and also intercepting with the communication sessions with other parties. It is possible for the coalition to orchestrate a set of falsified measurement data $\{\boldsymbol{z}_i' | i \in \mathcal{L}_k^c\}$ that satisfies the following:

$$\boldsymbol{\gamma}' = \sum_{i\in\mathcal{L}_k^c} \boldsymbol{\omega}_i \boldsymbol{z}_i' = \sum_{i\in\mathcal{L}_k^c} \boldsymbol{\omega}_i \boldsymbol{z}_i. \tag{7}$$

0885-8950 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of New Brunswick. Downloaded on June 09,2022 at 00:08:30 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3127353, IEEE Transactions on Power Systems

In the above equation, $\mathcal{L}_k^c$ denotes the index set of the compromised PMUs in region k, and $\{\boldsymbol{\omega}_i \in \mathbb{R}^{ld\times d} | i \in \mathcal{L}_k^c\}$ is the shared knowledge to the PDC used to calculate the partial measurement residuals on ciphertexts (see also Section IV-A). In this context, the orchestrated data will not be detected and consequently results in a successful DM-CFDI attack.

3) DD-CFDI Attacks: If the adversaries are sufficiently powerful to manipulate at least two PDCs, these compromised PDCs can collude to form a coalition, as discussed earlier. Such a coalition can potentially access the measurement data reported by PMUs from various regions and manipulate these data to facilitate wider-range or more powerful FDI attacks, as well as circumventing bad data detector more easily. The technical details will be shown in Section V-D.

In this paper, we do not consider the case where multiple PMUs are compromised to construct coordinated FDI attacks, because these problems have been widely investigated in the existing literature (e.g., [14], [54]).

IV. The Proposed SeCDM Scheme

In this section, we elaborate our proposed SeCDM scheme and underpinning rationale.

A. Designing Rationale

1) Critical Information Hiding: To prevent the leakage of the $\mathbf{H}$ matrix, we design a two-layer protection mechanism. The first layer is to hide the $\mathbf{H}$ matrix in another transformed matrix. If we rewrite Eq. (3) by

$$\begin{aligned}\boldsymbol{\gamma} &= \sqrt{\mathbf{W}^{-1}}(\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}) \\ &= \sqrt{\mathbf{W}^{-1}}[\mathbf{I} - \mathbf{H}(\mathbf{H}^\intercal\mathbf{W}^{-1}\mathbf{H})^{-1}\mathbf{H}^\intercal\mathbf{W}^{-1}]\mathbf{z} \triangleq \boldsymbol{\Omega}\mathbf{z},\end{aligned} \tag{8}$$

where $\boldsymbol{\Omega}$ is defined by

$$\boldsymbol{\Omega} = \mathbf{W}^{-1}[\mathbf{I} - \mathbf{H}(\mathbf{H}^\intercal\mathbf{W}^{-1}\mathbf{H})^{-1}\mathbf{H}^\intercal\mathbf{W}^{-1}] \in \mathbb{R}^{ld\times ld}, \tag{9}$$

we observe that matrix $\boldsymbol{\Omega}$ is a useful alternative for $\mathbf{H}$. It can be used to calculate the weighted measurement residual vector $\boldsymbol{\gamma}$ and to further support bad data detection. In this way, only the knowledge of $\boldsymbol{\Omega}$, instead of $\mathbf{H}$, needs to be stored in the control center's database. Therefore, $\mathbf{H}$ matrix is protected.

2) Hierarchical Knowledge Sharing: To effectively reduce the computational costs of the control center, we decompose the computing task for bad data detection into various sub-tasks that are undertaken by PDCs as well as the FDI detection module. Prior to that, a key step is to share the sub-task undertakers with significant secrets used to perform the required computation (see Algorithm 1). As shown in Eqs. (10) and (11), both matrices $\boldsymbol{\Omega}$ and $\mathbf{z}$ can be separated into several submatrices, wherein $\boldsymbol{\omega}_i \in \mathbb{R}^{ld\times d}$ and $\mathbf{z}_i \in \mathbb{R}^{1\times d},\ \forall i \in \mathcal{L} = \{1, 2, \cdots, l\}$, are respectively given by

$$\boldsymbol{\omega}_i = \begin{bmatrix} \omega_{1,(i-1)d+1} & \cdots & \omega_{1,(i+1)d} \\ \omega_{2,(i-1)d+1} & \cdots & \omega_{2,(i+1)d} \\ \vdots & \ddots & \vdots \\ \omega_{ld,(i-1)d+1} & \cdots & \omega_{ld,(i+1)d} \end{bmatrix},\ \mathbf{z}_i = \begin{bmatrix} z_{i,1} \\ z_{i,2} \\ \cdots \\ z_{i,d} \end{bmatrix} \tag{12}$$

Then, with reference to Eq. (8), $\boldsymbol{\gamma}$ can be rewritten as

$$\boldsymbol{\gamma} = \boldsymbol{\Omega}\mathbf{z} = \sum_{i\in\mathcal{L}} \boldsymbol{\omega}_i\mathbf{z}_i = \boldsymbol{\omega}_1\mathbf{z}_1 + \boldsymbol{\omega}_2\mathbf{z}_2 + \cdots + \boldsymbol{\omega}_l\mathbf{z}_l. \tag{13}$$

Algorithm 1 Hierarchical knowledge sharing

1: **procedure**
2: The control center performs the following steps:
3: 1). Computes $\boldsymbol{\Omega}$ as per Eq. (9);
4: 2). Partitions $\boldsymbol{\Omega} = (\boldsymbol{\omega}_1, \boldsymbol{\omega}_2, \cdots, \boldsymbol{\omega}_l)$ as per Eq. (10);
5: 3). Partitions $\boldsymbol{\omega}_i = \boldsymbol{\omega}_i^0 + \boldsymbol{\omega}_i^1$, $\forall i \in \mathcal{L}$, as per Eq. (14);
6: 4). Distributes $\{\boldsymbol{\omega}_i^0 | i \in \mathcal{L}_k\}$ to PDC V_k, $k \in \mathcal{K}$, respectively; and
7: 5). Distributes $\{\boldsymbol{\omega}_i^1 | i \in \mathcal{L}\}$ to the FDI detection module.
8: **end procedure**

As we observe, the task for calculating $\boldsymbol{\gamma}$ can be completed by several sub-tasks. It is then natural to distribute these sub-tasks to PDCs. Since PDCs are not fully trusted participants, only partial tasks should be outsourced to them in order to avoid collusion attacks initiated by compromised PDCs and/or PMUs. In this case, our second layer protection for the $\mathbf{H}$ matrix is to distribute the knowledge of $\boldsymbol{\Omega}$ matrix to various parities including a trusted party. This can effectively prevent the attackers from obtaining the full knowledge of $\mathbf{H}$ matrix. Specifically, we divide $\boldsymbol{\omega}_i,\ \forall i \in \mathcal{L}$, into

$$\begin{cases} \boldsymbol{\omega}_1 = \boldsymbol{\omega}_1^0 + \boldsymbol{\omega}_1^1 \\ \boldsymbol{\omega}_2 = \boldsymbol{\omega}_2^0 + \boldsymbol{\omega}_2^1 \\ \quad\cdots \\ \boldsymbol{\omega}_l = \boldsymbol{\omega}_l^0 + \boldsymbol{\omega}_l^1, \end{cases} \tag{14}$$

where each entry $\omega_{i,j}^0$ of $\boldsymbol{\omega}_i^0$ is randomly selected and then each entry $\omega_{i,j}^1$ of $\boldsymbol{\omega}_i^1$ is calculated by $\omega_{i,j}^1 = \omega_{i,j} - \omega_{i,j}^0$, $\forall i, j \in \mathcal{M}$. Then, the total task for calculating $\boldsymbol{\gamma}$ is given by

$$\boldsymbol{\gamma} = \sum_{i\in\mathcal{L}} \boldsymbol{\omega}_i^0\mathbf{z}_i + \sum_{i\in\mathcal{L}} \boldsymbol{\omega}_i^1\mathbf{z}_i. \tag{15}$$

In this case, it is expected that

- **PDCs**: each PDC $V_k(U_i)$ computes $\sum_{i\in\mathcal{L}_k} \boldsymbol{\omega}_i^0\mathbf{z}_i$, where $\mathcal{L}_k \subseteq \mathcal{L}$ is the set of PMUs' indices in region R_k. Then, all the results are reported to the FDI detection module.
- **FDI Detection Module**: the module first computes one half part of measurement residuals by aggregating the received data from all PDCs, which is given by

$$\boldsymbol{\gamma}^0 = \sum_{k\in\mathcal{K}} \sum_{i\in\mathcal{L}_k} \boldsymbol{\omega}_i^0\mathbf{z}_i. \tag{16}$$

Then, with $\left\{\boldsymbol{\omega}_i^1 \mid i \in \mathcal{L}\right\}$ and $\left\{\boldsymbol{z}_i^1 \mid i \in \mathcal{L}\right\}$ in hand, the module computes the other half part of measurement residuals by

$$\boldsymbol{\gamma}^1 = \sum_{i\in\mathcal{L}} \boldsymbol{\omega}_i^1\mathbf{z}_i. \tag{17}$$

At last, the total measurement residuals can be calculated by $\boldsymbol{\gamma} = \boldsymbol{\gamma}^0 + \boldsymbol{\gamma}^1$.

B. Concrete Scheme Description

The proposed SeCDM scheme consists of the following five phases: the System Initialization, Measurement Data Encryption by PMUs, Encrypted Measurement Data Preprocessing by PDCs, Measurement Residuals Calculation by the Module, and Secure FDI Detection by the Module – see also Algorithm 2.

0885-8950 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of New Brunswick. Downloaded on June 09,2022 at 00:08:30 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3127353, IEEE Transactions on Power Systems

$$\mathbf{\Omega} = \left[\begin{array}{cccc|cccc|c|cccc} \omega_{1,1} & \omega_{1,2} & \cdots & \omega_{1,d} & \omega_{1,d+1} & \cdots & \omega_{1,2d} & \cdots & \omega_{1,(l-1)d+1} & \cdots & \omega_{1,ld} \\ \omega_{2,1} & \omega_{2,2} & \cdots & \omega_{2,d} & \omega_{2,d+1} & \cdots & \omega_{2,2d} & \cdots & \omega_{2,(l-1)d+1} & \cdots & \omega_{2,ld} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \cdots & \vdots & \ddots & \vdots \\ \omega_{ld,1} & \omega_{ld,2} & \cdots & \omega_{ld,d} & \omega_{ld,d+1} & \cdots & \omega_{ld,2d} & \cdots & \omega_{ld,(l-1)d+1} & \cdots & \omega_{ld,ld} \end{array}\right] = (\boldsymbol{\omega}_1, \boldsymbol{\omega}_2, \cdots, \boldsymbol{\omega}_l) \tag{10}$$

$$\mathbf{z} = \begin{array}{cccc|cccc|c|cccc} (z_{1,1} & z_{1,2} & \cdots & z_{1,d} & z_{2,1} & z_{2,2} & \cdots & z_{2,d} & \cdots & z_{l,1} & z_{l,2} & \cdots & z_{l,d})^\intercal \end{array} = (\mathbf{z}_1, \mathbf{z}_2, \cdots, \mathbf{z}_l)^\intercal \tag{11}$$

Algorithm 2 Decentralized homomorphic computation

1: **procedure**
2: **Phase-1**: System initialization;
3: **Phase-2**: Each PMU computes the ciphertexts of measurement data using the homomorphic hybrid Paillier cryptosystem – see Eq. (20);
4: **Phase-3**: Each PDC preprocesses the encrypted measurement data reported by PMUs in its own region using secrets $\{\boldsymbol{\omega}_i^0 | i \in \mathcal{L}_k\}$ – see Eqs. (24) and (25);
5: **Phase-4**: 1). The FDI detection module preprocesses the encrypted measurement data delivered by all the PDCs using secrets $\{\boldsymbol{\omega}_i^1 | i \in \mathcal{L}\}$ – see Eqs. (26) and (27);
6: 2). The FDI detection module aggregates all the preprocessed encrypted measurement data, including those reported by PDCs, with reference to Eq. (28), and calculates the ciphertexts of the measurement residuals – see Eq. (29);
7: **Phase-5**: The module decrypts the measurement residuals and checks the hypothesis test– see Eqs. (30) to (33);
8: **end procedure**

1) System Initialization: It is reasonable, for a single-authority smart grid, to assume that the trusted control center can bootstrap the entire system. This work exploits the hybrid Paillier cryptosystem [9], which allows faster homomorphic computation and more flexible message decryption methods than many existing homomorphic encryption methods (e.g., BGV [55], BFV [56], FHEW [57], etc.).

In this phase, given a security parameter $\kappa \in \mathbb{Z}^+$, the control center generate the public key $\mathcal{PK} = (n, g)$ and the corresponding private key $\mathcal{SK} = (\lambda, \mu)$. Specifically, $g = n + 1$, $\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n$, and function L is defined as $L(\alpha) = (\alpha - 1)/n$. Select a hash function $H : \{0,1\} \to \mathbb{Z}_n$, and publish both $\mathcal{PK}$ and H. Then, the control center distributes the relevant key materials to each PMU $U_i \in \mathcal{U}$, each PDC $V_k \in \mathcal{V}$, as well as the FDI detection module, which is described as follows:

- ***Step-1***: Let $\tilde{\alpha} = f(\alpha) = 1000 \cdot \alpha \bmod n$ and apply it over $\mathbf{\Omega}$, such that each element $\omega_{i,j} \in \mathbf{\Omega}$, $\forall i, j \in \mathcal{M}$, can be converted into a positive integer $\tilde{\omega}_{i,j} \in \tilde{\mathbf{\Omega}}$ in $\mathbb{Z}_n$. Note that each $\omega_{i,j}$ is set as a real number in either zero, positive or negative decimal (having up to three decimal places). Then, partition matrix $\mathbf{\Omega}$ into submatrices $\{\tilde{\boldsymbol{\omega}}_1, \tilde{\boldsymbol{\omega}}_2, \cdots, \tilde{\boldsymbol{\omega}}_l\}$ according to Eq. (10). For each submatrix $\tilde{\boldsymbol{\omega}}_i$ with $i \in \mathcal{L}$, further partition it by $\tilde{\boldsymbol{\omega}}_i = \tilde{\boldsymbol{\omega}}_i^0 + \tilde{\boldsymbol{\omega}}_i^1$, where each element $\tilde{\omega}_{i,j}^0$ in $\tilde{\boldsymbol{\omega}}_i^0$ with $j \in \mathcal{M}$ is a random number in $\mathbb{Z}_n$ and each element $\tilde{\omega}_{i,j}^1 = \tilde{\omega}_{i,j} - \tilde{\omega}_{i,j}^0 \mod n$ in $\tilde{\boldsymbol{\omega}}_i^1$ with $i, j \in \mathcal{M}$. Distribute each $\tilde{\boldsymbol{\omega}}_i^0$ to its corresponding PDC $V_k(U_i)$ for $i \in \mathcal{L}_k$ and $k \in \{1, 2, \cdots, \delta\}$, respectively.
- ***Step-2***: Let $\mathbf{s} = \{s_{i,j} \in \mathbb{Z}_n^* | i \in \mathcal{L}, j \in \mathcal{D}\}$ denote a set of secret keys, where $s_{i,j} \in \mathbf{s}$ is randomly selected. Then, distribute $\mathbf{s}_i = \{s_{i,1}, \cdots, s_{i,d}\} \subseteq \mathbf{s}$ to each PMU U_i.
- ***Step-3***: Finally, compute ld conjunctive secret keys:

$$sk_\zeta = n \cdot \sum_{i \in \mathcal{L}} \sum_{j \in \mathcal{D}} \tilde{\omega}_{\zeta,(i-1)d+j} \cdot s_{i,j} \bmod n^2, \tag{18}$$

for all $\zeta \in \mathcal{M}$, prior to distributing these ld secret keys $(sk_1, sk_2, \cdots, sk_{ld})$ to the FDI detection module.

2) Measurement Data Encryption by PMUs: At each epoch time t, PMU $U_i \in \mathcal{U}$ collects d-dimensional power grid status measurement data $\mathbf{z}_i = (z_{i,1}, z_{i,2}, \cdots, z_{i,d})^\intercal$ in either zeros, positive or negative decimals (having up to three decimal places). Next, PMU U_i computes each $\Upsilon_{i,j} = n \cdot s_{i,j} \bmod n^2$, $\forall j \in \mathcal{D}$, in an offline mode, and performs the following online steps:

- ***Step-1***: Compute $\tilde{\mathbf{z}}_i = f(\mathbf{z}_i)$ to guarantee that each element in $\tilde{\mathbf{z}}_i$ is a non-negative integer in $\mathbb{Z}_n$, i.e.,

$$\begin{aligned} \tilde{\mathbf{z}}_i = f(\mathbf{z}_i) &= 1000 \times \mathbf{z}_i \\ &= (\tilde{z}_{i,1}, \tilde{z}_{i,2}, \cdots, \tilde{z}_{i,d})^\intercal \bmod n. \end{aligned} \tag{19}$$

- ***Step-2***: Encrypt each dimensional data of $\tilde{\mathbf{z}}_i$, $\forall j \in \mathcal{D}$, using the secret keys $\mathbf{s}_i = \{s_{i,1}, s_{i,2}, \cdots, s_{i,d}\}$, by

$$\begin{aligned} E(\tilde{z}_{i,j}) &= Enc(\mathcal{PK}, \tilde{z}_{i,j}, s_{i,j}) \\ &= g^{\tilde{z}_{i,j}} \cdot H(t)^{n \cdot s_{i,j}} \bmod n^2. \end{aligned} \tag{20}$$

Given $g = n+1$, this equation is equivalent to calculating

$$\begin{aligned} E(\tilde{z}_{i,j}) &= (n+1)^{\tilde{z}_{i,j}} \cdot H(t)^{\Upsilon_{i,j}} \bmod n^2 \\ &= (n \cdot \tilde{z}_{i,j} + 1) \cdot H(t)^{\Upsilon_{i,j}} \bmod n^2, \end{aligned} \tag{21}$$

which significantly reduces the computational task by transforming exponential computations to multiplications. All the encrypted measurement data for PMU U_i are denoted by a vector $E(\tilde{\mathbf{z}}_i)$, which is given below:

$$E(\tilde{\mathbf{z}}_i) = \begin{pmatrix} (n \cdot \tilde{z}_{i,1} + 1) \cdot H(t)^{\Upsilon_{i,1}} \bmod n^2 \\ (n \cdot \tilde{z}_{i,2} + 1) \cdot H(t)^{\Upsilon_{i,2}} \bmod n^2 \\ \vdots \\ (n \cdot \tilde{z}_{i,d} + 1) \cdot H(t)^{\Upsilon_{i,d}} \bmod n^2 \end{pmatrix}. \tag{22}$$

- ***Step-3***: Using the standard Key-Hashed Message Authentication Code (HMAC) algorithm [58], PMU U_i calculates a message authentication code (MAC) for each piece of measurement data using the recommended SHA-256 hash function, i.e.,

$$A_{i,j} = HMAC_{SHA256}(s_{i,j}, \tilde{z}_{i,j}, t). \tag{23}$$

0885-8950 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of New Brunswick. Downloaded on June 09,2022 at 00:08:30 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3127353, IEEE Transactions on Power Systems

Then, $E(\tilde{\mathbf{z}}_i)$ along with the MACs $\mathbf{A}_{i,j} = (A_{i,1}, A_{i,2}, \cdots, A_{i,d})$ and the timestamp t are reported to PDC $V_k(U_i)$.

3) Encrypted Measurement Data Preprocessing by PDCs: In each region, PDC V_k conducts the following three subtasks:

- ***Step-1***: For each $E(\tilde{z}_{i,j})$ reported by PMU U_i in region R_k, PDC V_k computes each $\tilde{Z}^0_{i,\zeta}$ ($\zeta \in \mathcal{M}$) using $\tilde{\boldsymbol{\omega}}^0_i$, which is given by the following equation:

$$\tilde{Z}^0_{i,\zeta} = \prod_{j\in\mathcal{D}} E(\tilde{z}_{i,j})^{\tilde{\omega}^0_{\zeta,(i-1)d+j}} \bmod n^2 \tag{24}$$

- ***Step-2***: For all PMUs $\mathcal{U}_i, i \in \mathcal{L}_k$, $\tilde{Z}^0_{i,\zeta}$ can be further aggregated using the following equation:

$$\tilde{C}^0_{k,\zeta} = \prod_{i\in\mathcal{L}_k} \tilde{Z}^0_{i,\zeta} = g^{\sum_{i\in\mathcal{L}_k}\sum_{j\in\mathcal{D}}\tilde{\omega}^0_{\zeta,(i-1)d+j}\cdot\tilde{z}_{i,j}} \times H(t)^{\sum_{i\in\mathcal{L}_k}\sum_{j\in\mathcal{D}}\tilde{\omega}^0_{\zeta,(i-1)d+j}\cdot\Upsilon_{i,j}} \bmod n^2. \tag{25}$$

- ***Step-3***: Report the aggregated preprocessed measurement data $\tilde{\mathbf{C}}^0_k = (\tilde{C}^0_{k,1}, \tilde{C}^0_{k,2}, \cdots, \tilde{C}^0_{k,ld})^\intercal$, the encrypted measurement data $E(\tilde{\mathbf{z}}_i)$, and their MACs $\mathbf{A}_{i,j}, i \in \mathcal{L}_k$, along with t to the module.

4) Measurement Residuals Calculation by the Module: With the knowledge of $\tilde{\boldsymbol{\omega}}^1_1, \tilde{\boldsymbol{\omega}}^1_2, \cdots, \tilde{\boldsymbol{\omega}}^1_l$ and the received encrypted measurement data $E(\tilde{\mathbf{z}}_1), E(\tilde{\mathbf{z}}_2), \cdots, E(\tilde{\mathbf{z}}_l)$, the FDI detection module performs the following four subtasks:

- ***Step-1***: For each piece of encrypted measurements $E(\tilde{z}_{i,j}), i \in \mathcal{L}$, the module preprocesses it with $\tilde{\boldsymbol{\omega}}^1_i$ by computing each $\tilde{Z}^1_{i,\zeta}$, where $\zeta \in \mathcal{M}$, as

$$\tilde{Z}^1_{i,\zeta} = \prod_{j\in\mathcal{D}} E(\tilde{z}_{i,j})^{\tilde{\omega}^1_{\zeta,(i-1)d+j}} \bmod n^2. \tag{26}$$

- ***Step-2***: All $\tilde{Z}^1_{i,\zeta}, i \in \mathcal{L}, \zeta \in \mathcal{M}$, can jointly form into

$$\tilde{\Gamma}^1_\zeta = \prod_{i\in\mathcal{L}} \tilde{Z}^1_{i,\zeta} = g^{\sum_{i\in\mathcal{L}}\sum_{j\in\mathcal{D}}\tilde{\omega}^1_{\zeta,(i-1)d+j}\cdot\tilde{z}_{i,j}} \times H(t)^{\sum_{i\in\mathcal{L}}\sum_{j\in\mathcal{D}}\tilde{\omega}^1_{\zeta,(i-1)d+j}\cdot\Upsilon_{i,j}} \bmod n^2, \tag{27}$$

the half part of the encrypted measurement residuals.

- ***Step-3***: Similarly, having $\tilde{\mathbf{C}}^0_k$ collected from each region R_k ($k \in \mathcal{K}$), calculate $\tilde{\Gamma}^0_\zeta$ for $\zeta \in \mathcal{M}$, the remaining half part of the encrypted measurement residuals by

$$\tilde{\Gamma}^0_\zeta = \prod_{k=1}^{\delta} \tilde{C}^0_{k,\zeta} = g^{\sum_{i\in\mathcal{L}}\sum_{j\in\mathcal{D}}\tilde{\omega}^0_{\zeta,(i-1)d+j}\cdot\tilde{z}_{i,j}} \times H(t)^{\sum_{i\in\mathcal{L}}\sum_{j\in\mathcal{D}}\tilde{\omega}^0_{\zeta,(i-1)d+j}\cdot\Upsilon_{i,j}} \bmod n^2. \tag{28}$$

- ***Step-4***: Then, calculate each dimension of the encrypted measurement residuals $\tilde{\Gamma}_\zeta$ using the following equation:

$$\begin{aligned}\tilde{\Gamma}_\zeta &= \tilde{\Gamma}^0_\zeta \times \tilde{\Gamma}^1_\zeta \\ &= g^{\sum_{i\in\mathcal{L}}\sum_{j\in\mathcal{D}}\tilde{\omega}_{\zeta,(i-1)d+j}\cdot\tilde{z}_{i,j}} \times H(t)^{\sum_{i\in\mathcal{L}}\sum_{j\in\mathcal{D}}\tilde{\omega}_{\zeta,(i-1)d+j}\cdot\Upsilon_{i,j}} \bmod n^2 \\ &= \Big(n\cdot\sum_{i\in\mathcal{L}}\sum_{j\in\mathcal{D}}\tilde{\omega}_{\zeta,(i-1)d+j}\cdot\tilde{z}_{i,j} + 1\Big) \times H(t)^{\sum_{i\in\mathcal{L}}\sum_{j\in\mathcal{D}}\tilde{\omega}_{\zeta,(i-1)d+j}\cdot\Upsilon_{i,j}} \bmod n^2.\end{aligned} \tag{29}$$

5) Secure FDI Detection by the Module: The module performs the following steps to achieve secure FDI detection.

- ***Step-1***: With the hash function H, timestamp t, and secret keys $(sk_1, sk_2, \cdots, sk_{ld})$ in hand, compute $H(t)^{sk_\zeta} \bmod n^2$, $\forall \zeta \in \mathcal{M}$. Next, each $\tilde{\Gamma}_\zeta$ is decrypted:

$$\begin{aligned}\tilde{\gamma}_\zeta &= \textit{Dec-II}(sk_\zeta, \tilde{\Gamma}_\zeta, t) \\ &= L(\frac{\tilde{\Gamma}_\zeta}{H(t)^{sk_\zeta}} \bmod n^2) \\ &= \sum_{i\in\mathcal{L}}\sum_{j\in\mathcal{D}} \tilde{\omega}_{\zeta,(i-1)d+j}\cdot\tilde{z}_{i,j} \bmod n.\end{aligned} \tag{30}$$

The decrypted $\tilde{\boldsymbol{\gamma}} = (\tilde{\gamma}_1, \tilde{\gamma}_2, \cdots, \tilde{\gamma}_{ld})^\intercal$ is the plaintext vector of weighted measurement residuals in $\mathbb{Z}_n$. Considering that weighted measurement residuals can either be zero, positive, or negative, we recover the weighted measurement residuals to the original scale by

$$\begin{cases}\gamma_\zeta = f^{-1}(\tilde{\gamma}_\zeta), & \text{if } \tilde{\gamma}_\zeta < \frac{n}{2} \\ \gamma_\zeta = f^{-1}(\tilde{\gamma}_\zeta - n), & \text{otherwise.}\end{cases} \tag{31}$$

- ***Step-2***: Compute the summed squares of γ_ζ modulo n, for $\zeta \in \mathcal{M}$, by

$$\phi = \sum_{\zeta\in\mathcal{M}} \gamma^2_\zeta \bmod n. \tag{32}$$

- ***Step-3***: As per Eq. (4), check the hypothesis test by

$$\phi \underset{H_1}{\overset{H_0}{\gtrless}} \tau^2. \tag{33}$$

- **Step-4**: If no FDI attack or bad data is detected, the encrypted measurement data $E(\tilde{\mathbf{z}}_i)$ along with the MACs $\mathbf{A}_{i,j} = (A_{i,1}, A_{i,2}, \cdots, A_{i,d})$ will be sent to the control center. The control center will verify the value of MACs.

V. Security Analysis and Proof

In this section, the vulnerability of existing homomorphic encryption based FDI mitigation schemes, taking the PAMA scheme as an example, to CFDI attacks is demonstrated, and the security of our proposed SeCDM scheme is analyzed. Specifically, we will show that SeCDM can effectively mitigate FDI attacks by preserving both the measurement data vector $\mathbf{z}$ and the Jacobian matrix $\mathbf{H}$. More importantly, the SeCDM scheme can also achieve enhanced resilience against DM-CFDI and DD-CFDI attacks.

A. Preservation of Vector $\mathbf{z}$

In the proposed scheme, the secrecy of vector $\mathbf{z}$ is preserved mainly on the communication links by using the secure hybrid Paillier cryptosystem. The vector $\mathbf{z}_i$ for any $i \in \mathcal{L}$ is encrypted at each PMU side, before being transmitted to the PDC, the module, and all the way to the control center. In this case, any eavesdropper along the communication links, such as PMU-to-PDC link and PDC-to-the-module link, cannot recover the plaintexts of vector $\mathbf{z}$ without the secret keys $s_{i,j} \in \mathbf{s}$ or the private key $\mathcal{SK}$. Note that, if PMUs serving as the measurement data generators are compromised, it is

0885-8950 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of New Brunswick. Downloaded on June 09,2022 at 00:08:30 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3127353, IEEE Transactions on Power Systems

nearly impossible to prevent them from leaking the original measurement data. Also, since PMUs are equipped with the secret keys $s_{i,j} \in \mathbf{s}$, if they are compromised and collude with the PDC, the coalition formed by these PMUs and the PDC are endowed with the capability of decrypting the measurement data; therefore, they can also cause data leakage. As we can see, the original measurement data $\mathbf{z}$ is well preserved along the entire communication links in our scheme, although no one can guarantee that PMUs may not commit data leakages.

B. Preservation of Matrix $\mathbf{H}$

In the proposed SeCDM scheme, we provide two layers of protection for the $\mathbf{H}$ matrix. In the first layer, rather than delivering the real $\mathbf{H}$ matrix to the FDI detection module for bad data detection, the control center first computes an $\mathbf{\Omega}$ matrix with reference to Eq. (9), where $\mathbf{H}$ is encapsulated, and distributes its partitions to the FDI detection module and the PDCs, respectively, as introduced in Section IV-B. In such a way, the knowledge of $\mathbf{H}$ matrix is hidden from all the entities except for the control center. In the second layer protection, each PDC V_k is only armed with the knowledge of $\{\boldsymbol{\omega}_i^0 | i \in \mathcal{L}_k\}$ (see Section IV-B). Even if the adversaries are capable of compromising all PDCs (also a strong assumption), they only have access to half the knowledge of $\mathbf{\Omega}$, i.e., $\{\boldsymbol{\omega}_i^0 | i \in \mathcal{L}\}$. Since the FDI detection module is fully trusted, the adversary is not able to access $\{\boldsymbol{\omega}_i^1 | i \in \mathcal{L}\}$, construct $\mathbf{\Omega}$, or recover $\mathbf{H}$. Therefore, in our proposed SeCDM scheme, matrix $\mathbf{H}$ that contains the knowledge of power grid topology and configurations is well protected against unauthorized access.

While it may be claimed that partial knowledge of $\mathbf{H}$ matrix can possibly be determined if attackers can get access to sufficient number of plaintexts for a power system historical measurement data. However, this is a strong assumption and generally implies an advanced persistent attacker with dedicated and significant resources (e.g., nation state). Moreover, the $\mathbf{H}$ matrix (containing the information of system topology and configurations) adapts from time to time in the highly complex, dynamic, and geographically-dispersed power system, particularly given that distributed flexible AC transmission system (D-FACTS) or FACTS devices are increasingly deployed over the smart grids [14]. Furthermore, in the proposed scheme, all the measurement data are protected by our proposed decentralized homomorphic computation algorithm (see Algorithm 2). It is, therefore, hard for attackers to eavesdrop on or intercept the communication links for harvesting the measurement data.

C. Resilience Against DM-CFDI Attacks

As introduced in Section III-B, if the PDC and at least two PMUs in the same region collude, say in PAMA [9], the coalition can design a DM-CFDI attack. In this case, with reference to Eqs. (4) and (13), we have

$$\|\boldsymbol{\gamma}'\|_2 = \| \sum_{i \in \mathcal{L}_k^c} \boldsymbol{\omega}_i \boldsymbol{z}_i' + \sum_{i \in \mathcal{L}/\mathcal{L}_k^c} \boldsymbol{\omega}_i \boldsymbol{z}_i \|_2 = \|\mathbf{\Omega}\mathbf{z}\| < \tau. \tag{34}$$

As we see, no bad data can be detected by using the given bad data detector. However, in our proposed scheme, PDCs hold less knowledge for help calculating the measurement residuals; even though they collude with PMUs, no effective DM-CFDI attacks can be successfully constructed. We summarized our finding in Theorem 1.

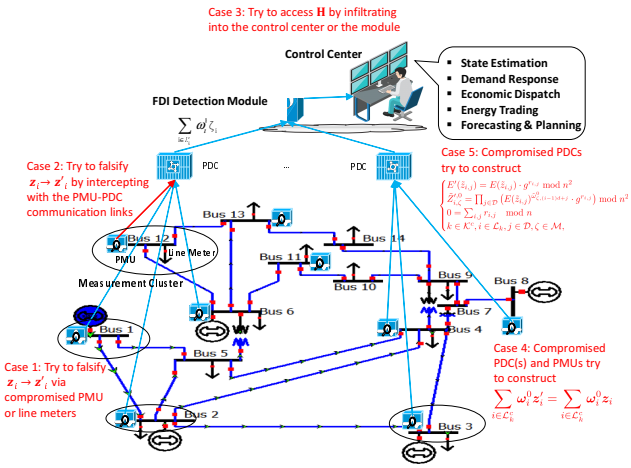


Fig. 3. Five test cases to demonstrate the security of the proposed scheme.

Theorem 1. *The proposed scheme can achieve effective resilience of DM-CFDI attacks.*

Proof. Given that in a region k, the PDC and PMUs indexed by $\mathcal{L}_k^c$ are compromised by FDI attackers, the PDC is equipped with the knowledge of $\boldsymbol{\omega}_i^0, i \in \mathcal{L}_k$, and PMUs can access the plaintexts of measurement data $\boldsymbol{z}_i, i \in \mathcal{L}_k^c$. The coalition formed by this PDC and PMUs can only construct

$$\sum_{i \in \mathcal{L}_k^c} \boldsymbol{\omega}_i^0 \boldsymbol{z}_i' = \sum_{i \in \mathcal{L}_k^c} \boldsymbol{\omega}_i^0 \boldsymbol{z}_i. \tag{35}$$

Since $\boldsymbol{\omega}_i^1, i \in \mathcal{L}_k^c$ are owned by the FDI detection module, they cannot falsify a set of measurement data $\{\boldsymbol{z}_i' | i \in \mathcal{L}_k^c\}$ that satisfies

$$\sum_{i \in \mathcal{L}_k^c} \boldsymbol{\omega}_i^0 \boldsymbol{z}_i' + \sum_{i \in \mathcal{L}_k^c} \boldsymbol{\omega}_i^1 \boldsymbol{z}_i' = \sum_{i \in \mathcal{L}_k^c} \boldsymbol{\omega}_i^0 \boldsymbol{z}_i + \sum_{i \in \mathcal{L}_k^c} \boldsymbol{\omega}_i^1 \boldsymbol{z}_i. \tag{36}$$

Following this, it is by no means for FDI attackers to achieve

$$\|\boldsymbol{\gamma}\|_2 = \| \sum_{i \in \mathcal{L}_k^c} (\boldsymbol{\omega}_i^0 + \boldsymbol{\omega}_i^1) \boldsymbol{z}_i' + \sum_{i \in \mathcal{L}/\mathcal{L}_k^c} (\boldsymbol{\omega}_i^0 + \boldsymbol{\omega}_i^1) \boldsymbol{z}_i \|_2 = \|\mathbf{\Omega}\mathbf{z}\|_2. \tag{37}$$

Although it is possible that attackers can inject any false data that leads to $\|\boldsymbol{\gamma}\|_2 \neq \|\mathbf{\Omega}\mathbf{z}\|_2 < \tau$ in this case, such false data are regarded as measurement noises, which is proved to be trivial and can be surely tolerated for the state estimation [8], [14], [49]. Hence, $\|\boldsymbol{\gamma}\|_2 \neq \|\mathbf{\Omega}\mathbf{z}\|_2 > \tau$ holds all the time, as long as attackers aim to launch an effective FDI attack (see [14] for more detailed discussions on the effective FDI attacks). The hypothesis H_0 is therefore false, and DM-CFDI attacks cannot be a success by using our proposed scheme. □

D. Resilience Against DD-CFDI Attacks

In PAMA, if compromised PDCs in different regions (having the knowledge of $\boldsymbol{\omega}_i$ and $E(\boldsymbol{z}_i), i \in \mathcal{L}_k, k \in \mathcal{K}^c$) collude

0885-8950 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of New Brunswick. Downloaded on June 09,2022 at 00:08:30 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3127353, IEEE Transactions on Power Systems

together, this coalition is able to design

$$\begin{cases} \tilde{Z}'_{i,\zeta} = \prod_j \left(E(\tilde{z}_{i,j})^{\tilde{\omega}_{\zeta,(i-1)d+j}} \cdot g^{r_{i,j}} \right) \bmod n^2, \\ 0 = \sum_{i,j} r_{i,j} \mod n, \\ k \in \mathcal{K}^c, i \in \mathcal{L}_k, j \in \mathcal{D}, \zeta \in \mathcal{M}, \end{cases} \tag{38}$$

where $\tilde{Z}'_{i,\zeta}$ is the desired falsified data, $\mathcal{K}^c$ denotes the indices set of compromised PDCs, and $r_{i,j} \in \mathbb{Z}_n^*$ is a random positive integer less than n. In this case, with reference to Eqs. (4) and (13), when DD-CFDI attacks are launched, we have

$$\begin{aligned} \|\boldsymbol{\gamma}\|_2 &= \Big\| \sum_{i \in \mathcal{L}_k, k \in \mathcal{K}^c} \boldsymbol{\omega}_i \boldsymbol{z}_i + \begin{pmatrix} \sum_{i \in \mathcal{L}_k, j \in \mathcal{D}} r_{i,j} \mod n \\ \cdots \\ \sum_{i \in \mathcal{L}_k, j \in \mathcal{D}} r_{i,j} \mod n \end{pmatrix}_{ld \times 1} \\ &\quad + \sum_{i \in \mathcal{L}_k, k \in \mathcal{K}/\mathcal{K}^c} \boldsymbol{\omega}_i \boldsymbol{z}_i \Big\|_2 \\ &= \| \sum_{i \in \mathcal{L}_k, k \in \mathcal{K}^c} \boldsymbol{\omega}_i \boldsymbol{z}_i + \mathbf{0} + \sum_{i \in \mathcal{L}_k, k \in \mathcal{K}/\mathcal{K}^c} \boldsymbol{\omega}_i \boldsymbol{z}_i \|_2 \\ &= \|\boldsymbol{\Omega} \mathbf{z}\|_2 < \tau, \end{aligned} \tag{39}$$

where $k \in \mathcal{K}^c$ and $\mathbf{0}$ is an $ld \times 1$ column vector with its all entries equalling 0. In this case, no bad data can be detected by using the given bad data detector.

Nevertheless, in our proposed scheme, each PDC holds relatively less knowledge for help calculating the measurement residuals (partial knowledge of $\boldsymbol{\omega}_i, i \in \mathcal{L}_k$) and MACs are exploited to verify the integrity of the encrypted measurement data. In this way, even though PDCs collude together, no effective DD-CFDI attacks can be successfully constructed. We summarized this finding in Theorem 2.

Theorem 2. *The proposed scheme can achieve effective resilience of DD-CFDI attacks.*

Proof. Given that a line of PDCs $V_k,\ k \in \mathcal{K}^c$, in a power grid are compromised by FDI attackers, they know $\boldsymbol{\omega}_i^0, i \in \mathcal{L}$ and can access the ciphertexts of measurement data $E(\mathbf{z}_i), i \in \mathcal{L}$ delivered by all the PMUs. The coalition formed by these compromised PDCs may design

$$\begin{cases} E'(\tilde{z}_{i,j}) = E(\tilde{z}_{i,j}) \cdot g^{r_{i,j}} \bmod n^2 \\ \tilde{Z}'^{,0}_{i,\zeta} = \prod_{j \in \mathcal{D}} \left(E(\tilde{z}_{i,j})^{\tilde{\omega}^0_{\zeta,(i-1)d+j}} \cdot g^{r_{i,j}} \right) \bmod n^2 \\ 0 = \sum_{i,j} r_{i,j} \mod n \\ k \in \mathcal{K}^c, i \in \mathcal{L}_k, j \in \mathcal{D}, \zeta \in \mathcal{M}, \end{cases} \tag{40}$$

which can lead to

$$\begin{aligned} &\prod_{i \in \mathcal{L}_k, k \in \mathcal{K}^c} \tilde{Z}'^{,0}_{i,\zeta} \\ &= \prod_{i \in \mathcal{L}_k, k \in \mathcal{K}^c} \prod_{j \in \mathcal{D}} \left(E(\tilde{z}_{i,j})^{\tilde{\omega}^0_{\zeta,(i-1)d+j}} \cdot g^{r_{i,j}} \right) \bmod n^2 \\ &= g^{\sum_{i \in \mathcal{L}_k, k \in \mathcal{K}^c} \sum_{j \in \mathcal{D}} \tilde{\omega}^0_{\zeta,(i-1)d+j} \cdot \tilde{z}_{i,j}} \times \\ &\quad H(t)^{\sum_{i \in \mathcal{L}_k, k \in \mathcal{K}^c} \sum_{j \in \mathcal{D}} \tilde{\omega}^0_{\zeta,(i-1)d+j} \cdot \Upsilon_{i,j}} \bmod n^2. \end{aligned} \tag{41}$$

at the FDI detection module. It is equivalent to constructing

$$\sum_{i \in \mathcal{L}_k, k \in \mathcal{K}^c} \boldsymbol{\omega}_i^0 \boldsymbol{z}'_i = \sum_{i \in \mathcal{L}_k, k \in \mathcal{K}^c} \boldsymbol{\omega}_i^0 \boldsymbol{z}_i \tag{42}$$

in plaintexts. If $E(\mathbf{z}_i), i \in \mathcal{L}_k, k \in \mathcal{K}^c$, are reported to the module without falsifications, the coalition can cause

$$\begin{aligned} \|\boldsymbol{\gamma}\|_2 &= \Big\| \sum_{i \in \mathcal{L}_k, k \in \mathcal{K}^c} \boldsymbol{\omega}_i^0 \boldsymbol{z}'_i + \sum_{i \in \mathcal{L}_k, k \in \mathcal{K} \setminus \mathcal{K}^c} \boldsymbol{\omega}_i^0 \boldsymbol{z}_i + \sum_{i \in \mathcal{L}} \boldsymbol{\omega}_i^1 \boldsymbol{z}_i \Big\|_2 \\ &= \Big\| \sum_{i \in \mathcal{L}} (\boldsymbol{\omega}_i^0 + \boldsymbol{\omega}_i^1) \boldsymbol{z}_i \Big\|_2 \\ &= \|\boldsymbol{\Omega} \mathbf{z}\|_2 < \tau, \end{aligned} \tag{43}$$

which will trigger hypothesis H_0 (no false data can be detected) in this case. It is seemingly a fancy result. However, it is meaningless if only falsifying $\tilde{Z}^0_{i,\zeta}$ by the desired $\tilde{Z}'^{,0}_{i,\zeta}$, but not the $E(\mathbf{z}_i), i \in \mathcal{L}_k, k \in \mathcal{K}^c$, concurrently. The reason is that, if $E(\mathbf{z}_i), i \in \mathcal{L}_k, k \in \mathcal{K}^c$, are replaced by $E'(\tilde{z}_{i,j}) = E(\tilde{z}_{i,j}) \cdot g^{r_{i,j}} \bmod n^2, i \in \mathcal{L}_k, k \in \mathcal{K}^c, j \in \mathcal{D}$, MAC validation will certainly be failed at the control center. Hence, we can see that no DD-CFDI attack can be a success by implementing our proposed SeCDM scheme.

□

VI. Performance Evaluation

In this section, we will explain our evaluation setup and the findings of the evaluations, in terms of the effectiveness of SeCDM in detecting both conventional FDI and CFDI attacks, the computational complexity of the PMU, PDC, and FDI detection module, and the communication overheads of PMU-to-PDC and PDC-to-Module communication links. The simulations are carried out on an Intel(R) Core(TM) i7-9700 CPU @3.00GHz with 8GB RAM Windows platform in Java, and the key parameter settings are summarized in Table II.

TABLE II
Parameter Settings

Parameter	Setting
$\kappa, \lvert p \rvert, \lvert q \rvert$	512
$\lvert n \rvert$	1024
Hash function for $H(t)$	SHA-256
Simulation rounds	1000
Test bus systems	IEEE 14-, 24-, and 39-bus systems

A. Effectiveness in Detecting FDI Attacks

In this part, we conduct three groups of simulation experiments using the PowerWorld[1] simulator on the standard IEEE 14-bus test power system[2], for verifying the effectiveness of the proposed SeCDM scheme in detecting conventional FDI, DM-CFDI, and DD-CFDI attacks, respectively.

In the first group, we simulate a conventional FDI attack targeting Bus 2 (where $1MW$ is added to the measurement data of Load 2 as the falsified measurement data) and a conventional FDI attack targeting Bus 6 (where $-1MW$ is added to the measurement data of Load 6 as the falsified measurement data). As Figs. 4 and 5 show, the estimated power system states, i.e., the bus voltage angles, suffer significant disturbances if no proper defense is in place. Importantly,

[1]PowerWorld (https://www.powerworld.com/)
[2]ICSEG Power Cases (https://icseg.iti.illinois.edu/power-cases/)

0885-8950 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of New Brunswick. Downloaded on June 09,2022 at 00:08:30 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3127353, IEEE Transactions on Power Systems

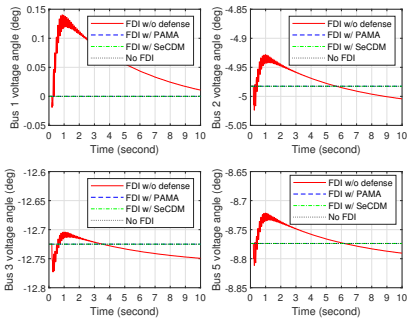


Fig. 4. The voltage angle values when a conventional FDI attack is launched at Bus 2.

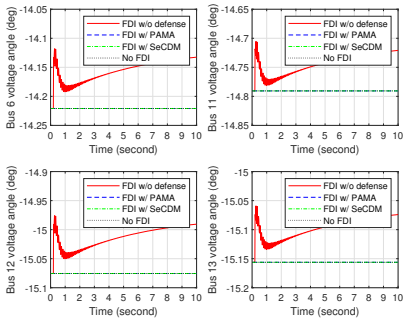


Fig. 5. The voltage angle values when a conventional FDI attack is launched at Bus 6.

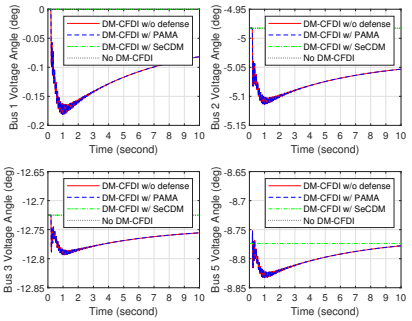


Fig. 6. The voltage angle values of Bus 2's neighboring buses, when a DM-CFDI attack is launched at Buses 2 and 6.

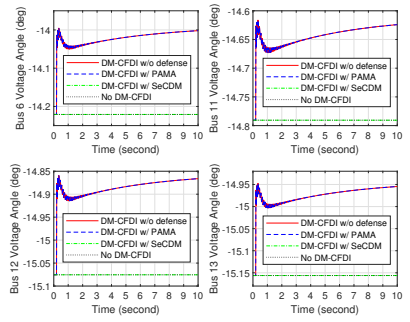


Fig. 7. The voltage angle values of Bus 6's neighboring buses, when a DM-CFDI attack is launched at Buses 2 and 6.

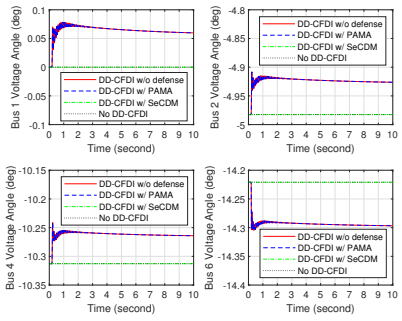


Fig. 8. The voltage angle values of Bus 5's neighboring buses, when a DD-CFDI attack is launched at Buses 4, 5, 6, and 9.

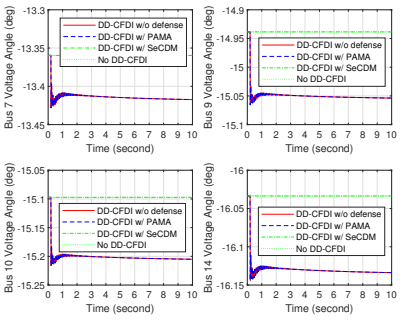


Fig. 9. The voltage angle values of Bus 9's neighboring buses, when a DD-CFDI attack is launched at Buses 4, 5, 6, and 9.

both SeCDM and the PAMA scheme can identify conventional FDI attacks. Note that, in Figs. 4 to 9, only 10 seconds of bus voltage angle values are presented, in purpose of simply showing the variation trends after an FDI attack.

In the second group, we show an example of DM-CFDI attack launched by compromised PMUs located at Buses 2, 5, 6, and 12, and collusively by the compromised PDC in this region. Figures 6 and 7 describe the estimated voltage angle values of buses neighboring Buses 2 and 6, respectively, after the DM-CFDI attack is launched. As observed from the figures, the power system suffers significant disturbances if no proper defense against DM-CFDI attacks is in place. We also observe that the PAMA scheme fails to identify the DM-CFDI attack, unlike our proposed SeCDM scheme.

Likewise, in the third group, we show an example of DD-CFDI attack launched by two compromised PDCs in different regions, each of which resides with compromised PMUs at Buses 2, 5, 6, and 12, as well as those at Buses 3, 4, 7, and 9, respectively. In Figs. 8 and 9, we show the estimated voltage angle values of buses neighboring Buses 5 and 9, respectively, after a DD-CFDI attack. Similarly, the power system experiences disturbances if no protection is implemented. Moreover, only the proposed SeCDM scheme is able to successfully identify such a DD-CFDI attack.

B. Computational Complexity

We conducted $1,000$ times of the entire scheme over the standard IEEE 14-, 24-, and 39-bus test systems, respectively, for each case wherein the settings of the total number of PMUs l, total number of PDCs δ, and dimension of measurement data d vary. The numerical results of the communication overheads are summarized in Table III and the computational costs are respectively plotted in Figs. 10, 11, and 12.

As per the proposed SeCDM scheme, each PMU requires d exponentiation operations in $\mathbb{Z}^*_{n^2}$ and a line of multiplication operations in $\mathbb{Z}^*_{n^2}$, etc., to encrypt d pieces of the measurement data. We observe that, the computational cost of each PMU grows almost linearly proportionally to the dimension of the measurement data d. In Fig. 10, the computational costs of each PMU on average to generate the report of encrypted measurement data versus d, under IEEE 14-bus, 24-bus, 39-bus test systems for both PAMA and SeCDM schemes are respectively plotted. It can be seen in this figure that, given a same d, the average computational cost for each PMU is almost the same for different test systems. Compared to PAMA, the proposed SeCDM scheme requires less computational capability.

The PDC needs to conduct $\nu \times l \times d^2$ exponentiation operations and a series of multiplication operations in $\mathbb{Z}^*_{n^2}$ on average, where ν denotes the average number of PMUs deployed in a given region. Figure 11 shows the computational cost of each PDC versus l under different ds for various test power systems, respectively. As observed in this figure, the computational cost for each PDC increases nearly linearly proportionally to l and also increases almost quadratically to d. Additionally, we observe that PAMA and SeCDM require a similar level of computational capability for PDCs, in that

0885-8950 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of New Brunswick. Downloaded on June 09,2022 at 00:08:30 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3127353, IEEE Transactions on Power Systems

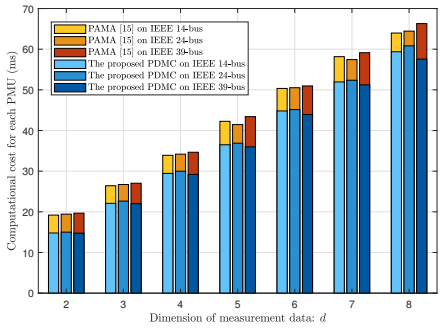


Fig. 10. The computational cost of each PMU versus d for both PAMA and SeCDM schemes under various test power systems ($\delta = 5$).

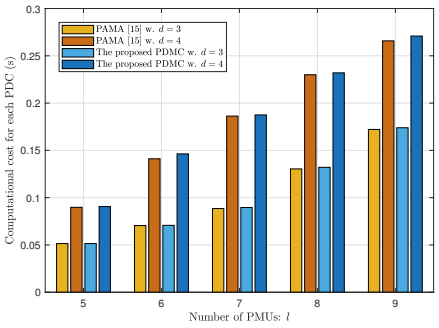


Fig. 11. The computational cost of each PDC versus l for both PAMA and SeCDM schemes ($\delta = 5$).

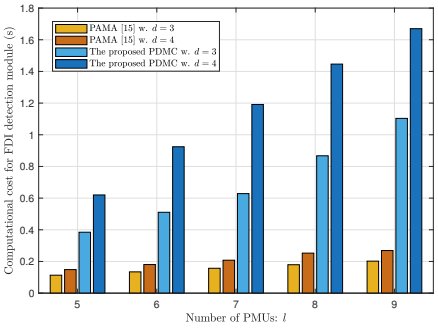


Fig. 12. The computational cost of the FDI detection module versus l for both PAMA and SeCDM schemes under the IEEE 14-bus test power system ($\delta = 5$).

TABLE III
SUMMARY OF COMMUNICATION OVERHEADS

Scheme	PMU to PDC	PDC to Module
PAMA [9]	$d \times 2\|n\|$ bits	$l_k \times d \times 4\|n\|$ bits
The proposed SeCDM	$d\times(2\|n\|+256)$ bits	$l_k \times d\times(4\|n\|+256)$ bits

similar operations are demanded for both schemes. For the FDI detection module, it needs to perform $l^2 \times d^2 + l \times d$ exponentiation operations and a series of multiplication operations. Figure 12 plots the computational cost of the FDI detection module versus l and d for both PAMA and SeCDM schemes. This figure shows that the proposed SeCDM incurs relatively heavier (but acceptable) computational costs than the original PAMA for the FDI detection module. The reason is that in the proposed SeCDM scheme the module shares almost half of the entire data preprocessing tasks (same as PDCs), which is the key for SeCDM to achieve CFDI attack resilience.

C. Communication Overheads

In our scheme, we mainly consider two communication links, the PMU-to-PDC link and the PDC-to-Module link. In relation to the PMU-to-PDC communication link, where PMUs convey the collected measurements to the regional PDC, each report comprises d encrypted data in $\mathbb{Z}^*_{n^2}$ as well as d pieces of MAC values. Hence, the communication overhead from each PMU-to-PDC link is $d\times(2|n|+256)$ bits. As for the PDC-to-Module communication link, where PDCs deliver the preprocessed measurement data to the FDI detection module, each report comprises $l_k \times d$ preprocessed data in $\mathbb{Z}^*_{n^2}$, $l_k \times d$ encrypted data in $\mathbb{Z}^*_{n^2}$, and $l_k \times d$ pieces of MAC values. In this way, the communication overhead for each PDC-to-Module link is $l_k \times d \times (4|n| + 256)$ bits. The communication overheads of the existing PAMA scheme and the proposed SeCDM scheme are summarized in Table III. We remark that in the PAMA scheme, data integrity verification is not well considered, while the MAC (requiring an extra 256 bits for each piece of measurement data) is employed in the proposed SeCDM scheme to achieve this goal.

VII. CONCLUSIONS

In this paper, we demonstrated how several existing homomorphic encryption based FDI mitigation schemes are vulnerable to CFDI attacks on smart grids, and introduced our proposed resilience-enhanced SeCDM scheme. The scheme is designed to detect and mitigate both conventional FDI and two types of CFDI attacks (i.e., DM-CFDI and DD-CFDI) on smart grids. A decentralized homomorphic computation paradigm along with a hierarchical knowledge sharing algorithm for securely executing the FDI detection was also designed to help achieve our aims. Both security analysis and performance evaluations demonstrated the enhanced resilience of SeCDM in defending against FDI, DM-CFDI, and DD-CFDI attacks. This is the first work, to the best of our knowledge, that focuses on CFDI attacks in smart grids. In addition, experiments on the standard IEEE 14-, 24-, and 39-bus test power systems show that the communication overheads and computational complexity are reasonably low.

Future research directions include 1) extending our proposed scheme to detecting and mitigating CFDI attacks on AC model based state estimation and 2) enhancing the scheme by differentiating the normal bad data and hacked bad data.

REFERENCES

[1] G. Simard, "IEEE grid vision 2050," Apr. 2013, DOI:10.1109/IEEESTD.2013.6577603.
[2] N. Falliere, L. O. Murchu, and etc., "W32. Stuxnet dossier," *White paper, Symantec Corp., Security Response*, vol. 5, no. 6, p. 29, Feb. 2011.
[3] J. Goldman, "In cyberattack on Saudi firm, U.S. sees Iran firing back," *eSecurity Planet*, Feb. 2013. [Online]. Available: https://www.esecurityplanet.com/network-security/florida-utility-company-hit-by-cyber-attack.html
[4] K. Zetter, "Inside the cunning, unprecedented hack of Ukraine's power grid," *Wired*, Mar. 2016. [Online]. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
[5] C. Cimpanu, "Cyber-security incident at US power grid entity linked to unpatched firewalls," *ZDNet Zero Day*, Sep. 2019. [Online]. Available: https://www.zdnet.com/article/cyber/security-incident-at-us-power-grid-entity-linked-to-unpatched-firewalls/
[6] U. S. G. A. Office, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*. United States Government Accountability Office, Aug. 2019, vol. GAO-19-332. [Online]. Available: https://www.gao.gov/assets/710/701079.pdf
[7] N. A. S. P. Initiative, *Synchrophasor Technology Fact Sheet*. North American SynchroPhasor Initiative, Oct. 2014. [Online]. Available: https://www.naspi.org/sites/default/files/reference_documents/33.pdf

0885-8950 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of New Brunswick. Downloaded on June 09,2022 at 00:08:30 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3127353, IEEE Transactions on Power Systems

[8] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, p. 13, May 2011.

[9] B. Li, R. Lu, G. Xiao, Z. Su, and A. Ghorbani, "PAMA: A proactive approach to mitigate false data injection attacks in smart grids," in *Proc. 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, UAE, Dec. 9-13*, 2018, pp. 1–6.

[10] Z. Zhang, P. Cheng, J. Wu, and J. Chen, "Secure state estimation using hybrid homomorphic encryption scheme," *IEEE Trans. Control Syst. Technol.*, vol. 29, no. 4, pp. 1704–1720, Jul. 2021.

[11] Y. Lu and M. Zhu, "Privacy preserving distributed optimization using homomorphic encryption," *Automatica*, vol. 96, pp. 314–325, Oct. 2018.

[12] Y. Shoukry, K. Gatsis, A. Alanwar, G. J. Pappas, S. A. Seshia, and etc., "Privacy-aware quadratic optimization using partially homomorphic encryption," in *Proc. 2016 IEEE Conference on Decision and Control (CDC)*, Las Vegas, NV, USA, Dec. 12-14, 2016, pp. 5053–5058.

[13] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2420–2430, May 2017.

[14] B. Li, G. Xiao, R. Lu, R. Deng, and H. Bao, "On feasibility and limitations of detecting false data injection attacks on power grid state estimation using D-FACTS devices," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 854–864, Jun. 2019.

[15] L. Che, X. Liu, Z. Li, and Y. Wen, "False data injection attacks induced sequential outages in power systems," *IEEE Trans. Power Syst.*, vol. 34, no. 2, pp. 1513–1523, Mar. 2019.

[16] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, "Cyber risk analysis of combined data attacks against power system state estimation," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3044–3056, Mar. 2018.

[17] S. D'Antonio, L. Coppolino, I. A. Elia, and V. Formicola, "Security issues of a phasor data concentrator for smart grid infrastructure," in *Proc. European Workshop on Dependable Computing (EWDC), Pisa, Italy, May 11-12*, 2011, pp. 3–8.

[18] B. Moussa, A. Al-Barakati, M. Kassouf, M. Debbabi, and C. Assi, "Exploiting the vulnerability of relative data alignment in phasor data concentrators to time synchronization attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2541–2551, Dec. 2019.

[19] S. Sarkar, T. Sharma, A. Baral, B. Chatterjee, D. Dey, and S. Chakravorti, "An expert system approach for transformer insulation diagnosis combining conventional diagnostic tests and PDC, RVM data," *IEEE Trans. Dielectr. Electr. Insul.*, vol. 21, no. 2, pp. 882–891, Apr. 2014.

[20] S. Nabavi, J. Zhang, and A. Chakrabortty, "Distributed optimization algorithms for wide-area oscillation monitoring in power systems using interregional PMU-PDC architectures," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2529–2538, Sep. 2015.

[21] S. Tan, D. De, W.-Z. Song, J. Yang, and S. K. Das, "Survey of security advances in smart grid: A data driven approach," *IEEE Commun. Surv. Tutor.*, vol. 19, no. 1, pp. 397–422, Firstquarter 2017.

[22] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 4, pp. 3453–3495, Fourthquarter 2018.

[23] S. N. Islam, Z. Baig, and S. Zeadally, "Physical layer security for the smart grid: vulnerabilities, threats, and countermeasures," *IEEE Trans. Ind. Inform.*, vol. 15, no. 12, pp. 6522–6530, Dec. 2019.

[24] M. Qiu, W. Gao, M. Chen, J.-W. Niu, and L. Zhang, "Energy efficient security algorithm for power grid wide area monitoring system," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 715–723, Dec. 2011.

[25] F. Justin, "Cyber trends defenders can expect to see in 2018," *SecurityWeek*, Dec. 2017. [Online]. Available: https://www.securityweek.com/cyber-trends-defenders-can-expect-see-2018

[26] H. Sedghi and E. Jonckheere, "Statistical structure learning of smart grid for detection of false data injection," in *Proc. 2013 IEEE Power Energy Society General Meeting*, Vancouver, BC, Canada, Jul. 21-25, 2013, pp. 1–5.

[27] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476–2483, Sep. 2015.

[28] B. Li, R. Lu, and G. Xiao, "HMM-based fast detection of false data injections in advanced metering infrastructure," in *Proc. 2017 IEEE Global Communications Conference (GLOBECOM)*, Singapore, Dec. 4-8, 2017, pp. 1–6.

[29] N. G. Bretas, A. S. Bretas, and A. C. P. Martins, "Convergence property of the measurement gross error correction in power system state estimation, using geometrical background," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 3729–3736, Nov. 2013.

[30] M. Esmalifalak, N. T. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," in *Proc. 2013 IEEE Global Communications Conference (GLOBECOM)*, Atlanta, GA, USA, Dec. 9-13, 2013, pp. 808–813.

[31] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8, pp. 1773–1786, Mar. 2015.

[32] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, Mar. 2014.

[33] P. Gao, M. Wang, J. H. Chow, S. G. Ghiocel, B. Fardanesh, G. Stefopoulos, and M. P. Razanousky, "Identification of successive 'unobservable' cyber data attacks in power systems through matrix decomposition," *IEEE Trans. Signal Process.*, vol. 64, no. 21, pp. 5557–5570, Nov. 2016.

[34] J. Tian, R. Tan, X. Guan, and T. Liu, "Enhanced hidden moving target defense in smart grids," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2208–2223, Oct. 2018.

[35] M. Higgins, F. Teng, and T. Parisini, "Stealthy MTD against unsupervised learning-based blind FDI attacks in power systems," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1275–1287, Aug. 2021.

[36] J. Zhao, L. Mili, and M. Wang, "A generalized false data injection attacks against power system nonlinear state estimator and countermeasures," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4868–4877, Sep. 2018.

[37] S. Ruj and A. Nayak, "A decentralized security framework for data aggregation and access control in smart grids," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 196–205, Mar. 2013.

[38] R. Lu, K. Alharbi, X. Lin, and C. Huang, "A novel privacy-preserving set aggregation scheme for smart grid communications," in *Proc. 2015 IEEE Global Communications Conference (GLOBECOM)*, San Diego, CA, USA, Dec. 6-10, 2015, pp. 1–6.

[39] A. Abdallah and X. S. Shen, "A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 396–405, Jan. 2018.

[40] M. Wen, D. Yao, B. Li, and R. Lu, "State estimation based energy theft detection scheme with privacy preservation in smart grid," in *Proc. 2018 IEEE International Conference on Communications (ICC)*, Kansas City, MO, USA, May 20-24, 2018, pp. 1–6.

[41] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 82–88, Jul. 2018.

[42] W. Li, *Risk assessment of power systems: models, methods, and applications*. John Wiley & Sons, Feb. 2014.

[43] IEEE Power & Energy Society, "IEEE standard for synchrophasor data transfer for power systems," *IEEE Std C37.118.2-2011 (Revision of IEEE Std C37.118-2005)*, pp. 1–53, Dec. 2011.

[44] A. Jovicic, N. Codoni, and G. Hug, "Computationally efficient robust state estimation for power transmission systems with RTU and PMU measurements," in *Proc. 2020 52nd North American Power Symposium (NAPS)*, Tempe, AZ, USA, Apr. 11-13, 2021, pp. 1–6.

[45] A. Jovicic and G. Hug, "Linear state estimation and bad data detection for power systems with RTU and PMU measurements," *IET Gener. Transm. Distrib.*, vol. 14, no. 23, pp. 5675–5684, Dec. 2020.

[46] A. Jovicic, B. Bilgic, and G. Hug, "Linear state estimation considering refresh rates of RTU and PMU measurements," in *Proc. 2021 IEEE Madrid PowerTech*, Madrid, Spain, Jun. 28- Jul. 2, 2021, pp. 1–6.

[47] J. James and S. Bindu, "Hybrid state estimation including PMU measurements," in *Proc. 2015 International Conference on Control Communication & Computing India (ICCC)*, Trivandrum, India, Nov. 19-21, 2015, pp. 309–313.

[48] K. Purchala, L. Meeus, D. Van Dommelen, and R. Belmans, "Usefulness of DC power flow for active power flow analysis," in *Proc. 2005 IEEE Power Engineering Society General Meeting*, San Francisco, CA, USA, 2005, pp. 454–459.

[49] A. Abur and A. Gomez-Exposito, *Power System State Estimation: Theory and Implementation*, Mar. 2004.

[50] B. Arturo, G. Newton, J. Bretas, and B. Carvalho, "Cyber-physical power systems state estimation," May 2021.

[51] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 198–207, Feb. 2017.

[52] H. d. N. Alves, N. G. Bretas, A. S. Bretas, and B.-H. Matthews, "Smart grids false data injection identification: A deep learning approach," in *Proc. 2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, Bucharest, Romania, Sep. 29-Oct. 2, 2019, pp. 1–5.

0885-8950 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of New Brunswick. Downloaded on June 09,2022 at 00:08:30 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2021.3127353, IEEE Transactions on Power Systems

[53] K. Nagaraj, N. Aljohani, S. Zou, C. Ruben, A. Bretas, A. Zare, and J. McNair, "State estimator and machine learning analysis of residual differences to detect and identify FDI and parameter errors in smart grids," in *Proc. 2020 52nd North American Power Symposium (NAPS)*. IEEE, Tempe, AZ, USA, Apr. 11-13, 2021, pp. 1–6.
[54] R. Deng and H. Liang, "False data injection attacks with limited susceptance information and new countermeasures in smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 3, pp. 1619–1628, Aug. 2018.
[55] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) fully homomorphic encryption without bootstrapping," *ACM Trans. Comput. Theory*, vol. 6, no. 3, pp. 1–36, Jul. 2014.
[56] J. Fan and F. Vercauteren, "Somewhat practical fully homomorphic encryption," *IACR Cryptol. ePrint Arch.*, vol. 2012, p. 144, Mar. 2012.
[57] L. Ducas and D. Micciancio, "FHEW: bootstrapping homomorphic encryption in less than a second," in *2015 Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, Sofia, Bulgaria, Apr. 26-30, 2015, pp. 617–640.
[58] N. Information Technology Laboratory, "The keyed-hash message authentication code (HMAC)," *Federal Information Processing Standards Publications (FIPSP)*, Jul. 2008. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf

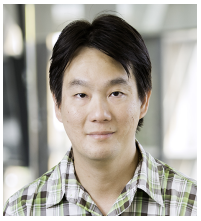
Beibei Li (S'15-M'19) received his B.E. degree (awarded Outstanding Graduate) in communication engineering from Beijing University of Posts and Telecommunications, China, in 2014 and his Ph.D. degree (awarded Full Research Scholarship) from the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, in 2019. He was invited as a visiting researcher at the Faculty of Computer Science, University of New Brunswick, Canada, from March to August 2018 and also the research group of NEtworked Sensing and Control (NESC), College of Control Science and Engineering, Zhejiang University, China, from February to April 2019.

Dr. Li joined the School of Cyber Science and Engineering, Sichuan University, China, in April 2019, where he has been working as an associate professor (doctoral advisor). His research interests span several areas in cyber-physical system security, with a focus on intrusion detection techniques, applied cryptography, and big data privacy, e.g., smart grids and industrial control systems, etc. He served as a TPC member for several international conferences, including AAAI, IEEE ICC, and IEEE GLOBECOM, etc. His research studies have been published in IEEE Trans. on Information Forensics and Security, IEEE Trans. on Industrial Informatics, ACM Trans. on Cyber-Physical Systems, IEEE Internet of Things J., Information Sciences, IEEE ICC 2021, and IEEE ISCC 2021 (Best Paper Award), etc.

Rongxing Lu (S'09-M'11-SM'15-F'21) is a University Research Scholar, an associate professor at the Faculty of Computer Science (FCS), University of New Brunswick (UNB), Canada. Before that, he worked as an assistant professor at the School of Electrical and Electronic Engineering, Nanyang Technological University (NTU), Singapore from April 2013 to August 2016. Rongxing Lu worked as a Postdoctoral Fellow at the University of Waterloo from May 2012 to April 2013. He was awarded the most prestigious "Governor General's Gold Medal", when he received his PhD degree from the Department of Electrical & Computer Engineering, University of Waterloo, Canada, in 2012; and won the 8th IEEE Communications Society (ComSoc) Asia Pacific (AP) Outstanding Young Researcher Award, in 2013. Dr. Lu is an IEEE Fellow. His research interests include applied cryptography, privacy enhancing technologies, and IoT-Big Data security and privacy.

Gaoxi Xiao (M'99-SM'18) received the B.S. and M.S. degrees in applied mathematics from Xidian University, Xi'an, China, in 1991 and 1994 respectively. He was an Assistant Lecturer in Xidian University in 1994-1995. In 1998, he received the Ph.D. degree in computing from the Hong Kong Polytechnic University. He was a Postdoctoral Research Fellow in Polytechnic University, Brooklyn, New York in 1999; and a Visiting Scientist in the University of Texas at Dallas in 1999-2001. He joined the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, in 2001, where he is now an Associate Professor. His research interests include complex systems and complex networks, communication networks, smart grids, and system resilience and risk management. Dr. Xiao serves/served as an Editor or Guest Editor for IEEE Transactions on Network Science and Engineering, PLOS ONE and Advances in Complex Systems etc., and a TPC member for numerous conferences including IEEE ICC and IEEE GLOBECOM etc.

Tao Li received his Ph.D. degree in computer science from the University of Electronic Science and Technology of China, in 1994. He is currently a Professor with the School of Cyber Science and Engineering, Sichuan University, China. He is the Chief Scientist of the National Key Research and Development Plan for Cyberspace Security. He is also an editorial board member of Immune Computation and several other international academic journals. His main research interests include network security, artificial immune systems, cloud computing, and cloud storage.



Kim-Kwang Raymond Choo (SM'15) received the Ph.D. in Information Security in 2006 from Queensland University of Technology, Australia. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA). He is the founding co-Editor-in-Chief of ACM Distributed Ledger Technologies: Research & Practice, and founding Chair of IEEE TEMS Technical Committee on Blockchain and Distributed Ledger Technologies. He currently serves as the Department Editor of IEEE Transactions on Engineering Management, and the Associate Editor of IEEE Transactions on Dependable and Secure Computing, and IEEE Transactions on Big Data. He is an ACM Distinguished Speaker and IEEE Computer Society Distinguished Visitor (2021 - 2023), a Web of Science's Highly Cited Researcher in the field of Cross-Field – 2020, and the recipient of the 2019 IEEE Technical Committee on Scalable Computing Award for Excellence in Scalable Computing (Middle Career Researcher). His other awards include the British Computer Society's 2019 Wilkes Award Runner-up, the Fulbright Scholarship in 2009, the 2008 Australia Day Achievement Medallion, and the British Computer Society's Wilkes Award in 2008. He has also received best paper awards from IEEE Systems Journal in 2021, 2021 IEEE Conference on Dependable and Secure Computing (DSC 2021), IEEE Consumer Electronics Magazine for 2020, Journal of Network and Computer Applications for 2020, EURASIP Journal on Wireless Communications and Networking in 2019, IEEE TrustCom 2018, and ESORICS 2015; the IEEE Blockchain 2019 Outstanding Paper Award; and Best Student Paper Awards from Inscrypt 2019 and ACISP 2005.

0885-8950 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: University of New Brunswick. Downloaded on June 09,2022 at 00:08:30 UTC from IEEE Xplore. Restrictions apply.