DDOA: A Dirichlet-based Detection Scheme for Opportunistic Attacks in Smart Grid Cyber-Physical System

Beibei Li, *Student Member, IEEE,* Rongxing Lu, *Senior Member, IEEE,* Wei Wang, *Student Member, IEEE,* and Kim-Kwang Raymond Choo, *Senior Member, IEEE*

***Abstract*—In the hierarchical control paradigm of a smart grid cyber-physical system, decentralized local agents (LAs) can potentially be compromised by opportunistic attackers to manipulate electricity prices for illicit financial gains. In this paper, to address such opportunistic attacks, we propose a Dirichlet-based detection scheme (DDOA), where a Dirichlet-based probabilistic model is built to assess the reputation levels of LAs. Initial reputation levels of the LAs are first trained using the proposed model, based on their historical operating observations. An adaptive detection algorithm with reputation incentive mechanism is then employed to detect opportunistic attackers. We demonstrate the utility of our proposed scheme using data collected from the IEEE 39-bus power system with the PowerWorld simulator.**

***Index Terms*—Cyber-physical system security, smart grid, opportunistic attack, intrusion detection, smart electricity market, Dirichlet-based reputation.**

I. Introduction

WITH the increasing connectivity of society and advancement of information and communications technologies (ICT), smart grid cyber-physical system is increasingly commonplace. Smart grid cyber-physical system is a large-scale interconnected power infrastructure spanning across one or more jurisdictions. To guarantee high reliability and robustness of the underlying critical infrastructure, real-time monitoring, data analytics, and control are highly critical. Empirically, data analytics is generally performed by the state estimator at the system control center (CC) [1]–[3]. However, with the increasing number of interconnections, nonlinearity, and dynamics, real-time data analytics will inevitably impose significant computational burden and complexity on CC [4]. If this is not well-managed, CC's operating efficiency will be adversely affected, resulting in cascading effects - e.g. affecting the reliability and the robustness of the power grid and eventually crippling the power grid. One of the potential solutions to address the exacting computational requirements on the CC identified in the literature is the hierarchical control framework. In such a framework, decentralized local agents (LAs) perform real-time data analytics activities in their local region [5], [6].

While hierarchical framework can effectively reduce the computational burden of the CC, it may result in unintended security consequences [4]. For example, in the current centralized power system, it is easier to devote efforts and resources to secure a central entity (i.e. CC); thus, CC is generally regarded as a fully trusted party. In a hierarchical framework, however, it is not realistic to expect that all decentralized LAs can be secured to the same level as the CC.

The upward trend in Internet-of-Things and integration of power grids with ICT have also resulted in an increased attack vector. For example, vulnerabilities in existing power system, or connected devices and/or entry points can be exploited by cybercriminals. According to the monitor newsletter of Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), in Fiscal Year 2015 (i.e. 1 October 2014 to 30 September 2015), ICS-CERT of the U.S. Department of Homeland Security has reportedly responded to 295 cybersecurity incidents involving critical infrastructures, and the energy sector is the second most targeted critical infrastructure sector [7]. The dangers of threats to cyber-physical systems are evidenced by recent attacks (e.g. on a German steel mill that destroyed a blast furnace [8]) and attempts (e.g. ISIS attempted to hack U.S. electric power utilities to steal confidential grid information and launch terrorist attacks [9]). Successful attacks could potentially overwhelm and paralyse the country's interconnected critical infrastructure sectors and, consequently, cause severe social unrest.

Unsurprisingly, security of smart electricity markets has attracted the attention of security researchers [10]–[12]. However, we observe existing efforts appear to focus on mitigating data integrity attacks (i.e. attackers falsify measurement data to "blind" the system in order to manipulate electricity prices [13]). Generally, it is assumed that attackers have access to the system configuration, and are able to simultaneously falsify a set of measurement data at several phasor measurement units (PMUs) at will.

In addition to criminally-, politically-, and ideologically-motivated attacks, cybercriminals may be interested in compromising smart grids by manipulating smart electricity markets for illicit financial gains [13]–[15]. Opportunistic attacks [1], [16] are one such example. Specifically, rather than seeking to falsify measurement data by compromising a set of PMUs, opportunistic attackers attempt to manipulate elec-

B. Li, R. Lu, and W. Wang are with the School of Electrical and Electronic Engineering, Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798. Email: bli012@e.ntu.edu.sg, rxlu@ntu.edu.sg, wei001@e.ntu.edu.sg.

K.K.-R. Choo is with (1) Department of Information Systems and Cyber Security, University of Texas at San Antonio, USA, (2) School of Information Technology & Mathematical Sciences, University of South Australia, Australia, and (3) School of Computer Science, China University of Geosciences, Wuhan, China. E-mail: raymond.choo@fulbrightmail.org.

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/TIFS.2016.2576898, IEEE Transactions on Information Forensics and Security

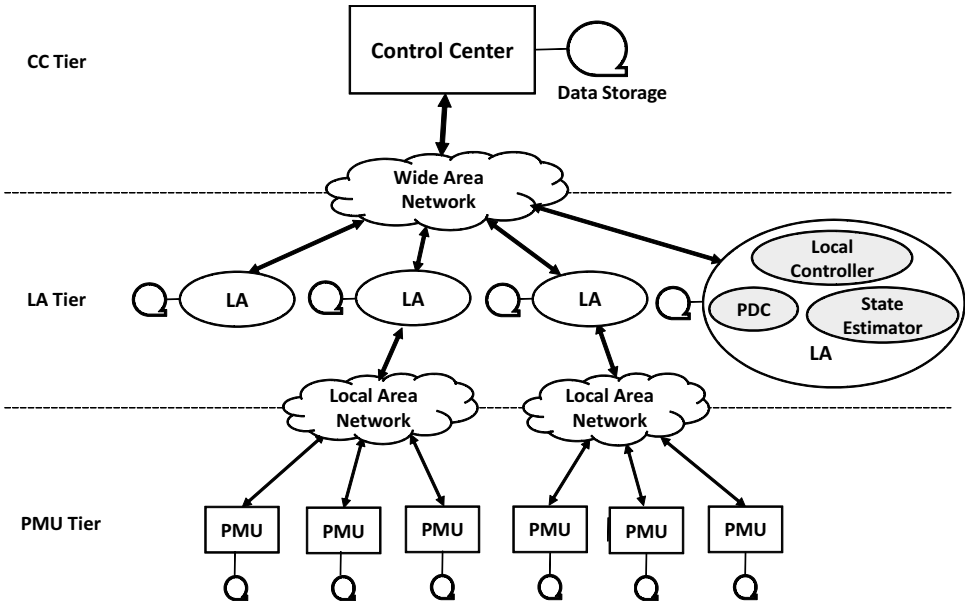

Fig. 1. Three-tier hierarchical flocking-based framework for future smart grids.

tricity prices by only compromising the intelligent electronic device which is responsible for determining the real-time electricity prices, say the LA. The compromised LA can issue fake commands to the local generators, distributors, and transformers to shift the normal demand-supply relations, which will further influence the electricity price at each local bus. If colluded with other participants in smart electricity markets (e.g. power suppliers and utilities), the attackers can make a great amount of illicit financial profits through the wide fluctuations of the electricity prices [14]. This is the focus of this paper.

Since opportunistic attacks are unlikely to result in any physical damages to the power system, it is a challenging task for conventional intrusion detection system (IDS) to identify. Moreover, opportunistic attackers can flexibly adjust their attack strategies (e.g. probability to launch an attack when there is a chance) based on system noise level to evade detection or scrutiny [1]. Hence, to identify the abnormality of any possible compromised LA, an effective way is to observe and assess their behaviors (i.e. operations and corresponding variable states) over a long period of time. In this paper, we seek to mitigate opportunistic attacks by presenting a novel Dirichlet-based detection scheme (hereafter referred to as DDOA). The scheme allows CC to effectively identify compromised LAs by observing their operating behaviors. We regard the contributions of this paper to be three-fold:

- We first divide the smart grid infrastructure into a three-tier hierarchical framework, which is designed to effectively reduce the computational burden on the CC. This framework also makes it possible to guarantee high reliability and robustness of future smart grids.
- We pioneer to study the opportunistic attacks in smart electricity market, and build up a Dirichlet-based reputation model to monitor and assess the performance of the LAs by observing their behaviors over a long period of time.
- Lastly, we propose and evaluate an adaptive detection scheme with reputation incentive mechanism, which can effectively and accurately identify potential opportunistic attackers hidden in the smart electricity market and prevent them from manipulating electricity prices. In addition, two-level detection thresholds are also employed in our DDOA scheme, which can effectively differentiate malicious activities from common system faults in smart grids.

The remainder of this paper is organized as follows. In Section II, we present the system model, the threat model, and our design goals. Section III introduces the preliminaries required in the understanding of this paper. Our proposed Dirichlet-based reputation model and detection scheme is detailed in Section IV, and the performance evaluation is presented in Section V. Section VI reviews related work, and Section VII concludes the paper.

II. Models and Design Goals

In this section, we formalize both system and threat models, as well as describe the design goals.

A. System Model

As shown in Fig. 1, we consider a hierarchical flocking-based framework for future smart grids as our system model. This model comprises three tiers, namely: the lowermost tier of PMU, the intermediate tier of LA, and the uppermost tier of CC. Their roles and responsibilities are illustrated as follows:

- PMUs, deployed at each bus and generator across the whole power system, are geographically flocked, forming several flockings. They collect real-time measurement data of system status in each flocking area (e.g. power generations $\boldsymbol{G}$, power loads $\boldsymbol{L}$, and line power flows $\boldsymbol{F}$),

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/TIFS.2016.2576898, IEEE Transactions on Information Forensics and Security

and report collected data to the phasor data concentrator (PDC) located in the upper tier LA area.

- The LA (formed by PDC, state estimator, and local controller) in the flocking area analyzes the real-time system status of its monitored local area with the reported data, and transforms the data to the uppermost tier of CC as required. Specifically, the PDC collects reported measurement data from PMUs; the state estimator is utilized to estimate actual system status in the flocking area; and the local controller then analyzes the estimated data, determines the locational marginal price (LMP), and issues feedback commands to local generators, distributers, transformers, etc.
- The CC stores and analyzes the measurement data for various applications (e.g. state estimation, contingencies analysis, and event diagnostics). In addition, in our model, CC is also responsible for monitoring and assessing the reputation levels of the subordinate LAs to identify abnormal LA behavior.

In this work, we assume that both CC and LAs make use of state estimation to analyze the system status of either the entire region or local regions. Particularly, CC carries out state estimation with a low frequency to reduce computational requirements (see Section IV-C).

B. Threat Model

Unlike traditional power systems, future smart grids will delegate real-time monitoring, data analytics, and control tasks from CC to its subordinate LAs. As aforementioned, it is natural to assume that only CC is a fully trusted party, while LAs are more likely to be compromised by malicious attackers. In our model, PMUs are assumed to be honest (i.e. data reported by PMUs to PDC are assumed to be without falsification).

By successfully compromising an LA, attackers can issue fake control commands to local generators, distributers, and transformers to manipulate normal demand-supply relations in a specific flocking area. Such actions could result in changes of the LMP in the area. As this is a premeditated activity, attackers can exploit the price fluctuations/changes for financial gains. For example, attackers can collude with other players in the smart electricity markets and purchase a significant amount of electricity at a low price prior to the attacks. Once the price has been artificially jacked up, attackers will seek to sell the pre-purchased electricity to users in the grid.

Fig. 2 presents an example of the contouring map of the distribution of electricity prices under normal conditions on the IEEE 39-bus power system. Areas covered by various colors reflect different demand-supply relations. In case of occurrence of malicious attacks, these normal relations and consequently, electricity prices will be intentionally altered. These attacks can be broadly categorized into random attacks, reckless attacks, and opportunistic attacks.

1) Random attacks are conducted with a definite attack probability $P_a \in [0, 1]$. Since such attacks are carried out in a regular mode, it is easier to identify the attacks using traditional IDS or intrusion prevention systems (IPS).
2) Reckless attacks are launched on an ad-hoc basis. Specifically, once an opportunity appears, attackers will launch an attack without hesitation and planning. Consequently, reckless attackers are usually the easiest to be identified.
3) Opportunistic attacks are carried out based on the system noise with an attack probability $P_a = C \cdot {P_n}^{\varepsilon}$, where C is a constant coefficient, and ε denotes a scalar of the system noise P_n. Particularly, $\varepsilon > 1$ indicates conservative opportunistic attackers, while $\varepsilon < 1$ indicates aggressive ones. Therefore, the larger the system noise is, the higher the attack probability will be.

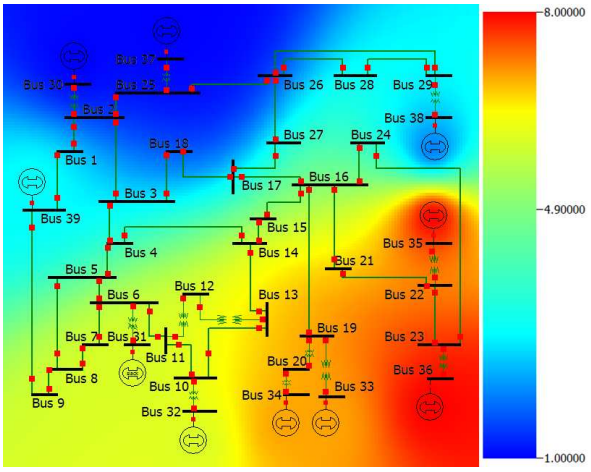

Fig. 2. The contouring map of electricity price distribution on IEEE 39-bus power system.

It is widely believed that opportunistic attackers are the most cunning attackers, as they adapt their attack probabilities according to the system noise. Therefore, it is significantly challenging to identify such attackers using traditional detection schemes (e.g. IDS and IPS). In this paper, we aim to propose an effective scheme to identify and detect opportunistic attackers.

C. Design Goals

The key objective of the proposed DDOA scheme is to provide an effective approach to accurately identify and detect opportunistic insider attacks in smart electricity markets. Our design goals are as follows:

1) Future smart grids are expected to be a hierarchical system, due to their capability to ensure efficiency, stability, and reliability of power system in situations with ever-increasing electricity demands, integration of renewable energy resources, and various data analytical applications. Thus, we employ a three-tier hierarchical control framework for future smart grids to support these critical requirements.
2) LAs play a prominent role in distributed flocking areas, and it is important to ensure their functionality. Since LAs cannot be fully trusted (unlike a CC), we need to be

able to efficiently and accurately monitor and assess their behaviors. Thus, we present a Dirichlet-based reputation model to assess LA's operating conditions.

3) To continuously monitor all LAs' operating conditions, we propose an effective detection scheme based on our Dirichlet-based reputation model to identify LA compromised by an opportunistic attacker. In addition, we use collected real-time data in PowerWorld simulator to validate the effectiveness of our proposed DDOA scheme.

III. Preliminaries

In this section, we briefly introduce preliminaries required in the understanding of the remaining of this paper.

A. State Estimation

State estimation is usually used to estimate real-time operating status of power systems [17]. Assuming that $\boldsymbol{x} = [x_1, x_2, \ldots, x_n]^T$ denotes the vector of the real variable states of a power system, which consists of power generations $\boldsymbol{x_G}$, power loads $\boldsymbol{x_L}$, line power flows $\boldsymbol{x_F}$, etc. $\boldsymbol{z} = [z_1, z_2, \ldots, z_m]^T$ denotes the vector of the measurement data of these variable states collected from PMUs. n and m are positive integers, and $x_i, z_j \in \mathbb{R}$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, m$. In real-world applications, the state estimate usually involves a linearized DC power flow model, which can be expressed as

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

where $\mathbf{H}$ is an $m \times n$ Jacobian matrix determined by the system configurations, and $\boldsymbol{\eta} = [\eta_1, \eta_2, \ldots, \eta_m]^T \sim \mathcal{N}(0, \mathbf{R})$ is an independent measurement error vector with zero-mean and covariance $\mathbf{R}$, which is a diagonal matrix of $\boldsymbol{\eta}$ [17].

Given the observation of measurements $\boldsymbol{z}$, the maximum likelihood estimate of the state variables is given by [18]

$$\hat{\boldsymbol{x}} = [\mathbf{H}^T\mathbf{R}^{-1}\mathbf{H}]^{-1}\mathbf{H}^T\mathbf{R}^{-1}\boldsymbol{z}. \tag{2}$$

In particular, according to the invariance nature of maximum likelihood estimation, the maximum likelihood estimates of power generations $\boldsymbol{x_G}$, power loads $\boldsymbol{x_L}$, and line power flows $\boldsymbol{x_F}$ can be expressed as [13]

$$\begin{bmatrix} \hat{\boldsymbol{x}}_{\boldsymbol{G}} \\ \hat{\boldsymbol{x}}_{\boldsymbol{L}} \\ \hat{\boldsymbol{x}}_{\boldsymbol{F}} \end{bmatrix} = [\mathbf{H}^T\mathbf{R}^{-1}\mathbf{H}]^{-1}\mathbf{H}^T\mathbf{R}^{-1} \begin{bmatrix} \boldsymbol{z}_{\boldsymbol{G}} \\ \boldsymbol{z}_{\boldsymbol{L}} \\ \boldsymbol{z}_{\boldsymbol{F}} \end{bmatrix} \tag{3}$$

B. Real-time LMP

In smart electricity markets, the real-time LMP within an LA area is determined based on the estimated real-time system states. LMP is defined as the cost to serve the next unit increment of power load (say 1MWh) at each bus by comprehensively taking into account actual power generations, power loads, and line flows with respect to transmission line limits [19].

Such calculations can be formulated as an incremental linear optimization problem with state estimates as described in Eq. (4). The objective is to minimize the cost function subject to the power balance constraint, the generation megawatt bounds, the transaction megawatt bounds and any transmission constraints that currently exist on the system. This optimization problem can be formulated as follows:

$$\begin{aligned} \min \quad & \mathcal{J} = \sum C_i(\Delta G_i) - \sum C_j(\Delta L_j) \\ s.t. \quad & \sum \Delta G_i - \sum \Delta L_j = 0 \\ & \Delta G_i min \le \Delta G_i \le \Delta G_i max \\ & \Delta L_i min \le \Delta L_i \le \Delta L_i max \\ & A_{ik}\Delta G_i + D_{jk}\Delta L_j \le 0, \end{aligned} \tag{4}$$

where C_i and C_j are calculated real-time offer for generator i and real-time bid for load j, respectively [19]. A_{ik} is a matrix of shift factors for generation bus i (with respect to the reference bus) on the binding transmission constraints (k), and D_{jk} is a matrix of shift factors for load bus j (with respect to the reference bus) on the binding transmission constraints (k). The LMP values at each bus can be expressed as

$$LMP_i = \lambda - \sum A_{ik} * SP_k, \tag{5}$$

where λ is the marginal price of generation at the reference bus [17]. A_{ik} is a shift factor for bus i on binding constraint k, and SP_k is the shadow price of constraint k.

C. Dirichlet Distribution

Dirichlet distribution [20] is a family of continuous multivariate probability distributions, parameterized by a vector $\boldsymbol{\alpha}$ of positive reals. Let $X = \{x_1, x_2, \ldots, x_k\}$ be a discrete random variable, where $x_i > 0$ for $i = 1, 2, \ldots, k$ and $\sum_{i=1}^{k} x_i = 1$. Suppose that $\boldsymbol{\alpha} = [\alpha_1, \alpha_2, \ldots, \alpha_k]$ with $\alpha_i > 0$ for all i from 1 to k, and let $\alpha_0 = \sum_{i=1}^{k} \alpha_i$. Then, X is said to be a Dirichlet distribution with parameters $\boldsymbol{\alpha}$, which is denoted by $X \sim Dir(\boldsymbol{\alpha})$. Then, the probability density function is expressed as

$$f(X; \boldsymbol{\alpha}) = \frac{1}{B(\boldsymbol{\alpha})} \prod_{i=1}^{k} x_i^{\alpha_i - 1} = \frac{\Gamma(\alpha_0)}{\prod_{i=1}^{k} \Gamma(\alpha_i)} \prod_{i=1}^{k} x_i^{\alpha_i - 1}, \tag{6}$$

where $B(\cdot)$ is a Beta function, and $\Gamma(\cdot)$ is a Gamma function.

The expectation and variance of $X = x_i$ are respectively given by

$$E[x_i] = \frac{\alpha_i}{\alpha_0}, \mathrm{Var}[x_i] = \frac{\alpha_i(\alpha_0 - \alpha_i)}{\alpha_0^2(\alpha_0 + 1)}. \tag{7}$$

IV. Proposed DDOA Scheme

In this section, we elaborate our proposed DDOA scheme, which is composed of four parts: behavior rule specifications, Dirichlet-based reputation model, detailed description of D-DOA, and guarantee of data integrity with BLS short signature.

A. Behavior Rule Specifications

Smart grid is a large-scale interconnected cyber-physical system. The behaviors (i.e. operations and variable status) of the physical devices are an accurate reflection of their responses to the feedback commands from the control unit. Thus, assessing the behaviors of physical devices will be an

TABLE I
RULE SPECIFICATIONS

Index	Rule	Description
$R1$	$\lvert G_i^t - \hat{G}_i^t \rvert \leq \tau_G$	The absolute difference of G between measured and expected values should be below a safe threshold τ_G
$R2$	$\lvert L_i^t - \hat{L}_i^t \rvert \leq \tau_L$	The absolute difference of L between measured and expected values should be below a safe threshold τ_L
$R3$	$\lvert F_i^t - \hat{F}_i^t \rvert \leq \tau_F$	The absolute difference of F between measured and expected values should be below a safe threshold τ_F
$R4$	$\tau_{Pmin} \leq G_i^t \leq \tau_{Gmax}$	The value of G itself should be limited within a specified safe range $[\tau_{Gmin}, \tau_{Gmax}]$
$R5$	$\tau_{Lmin} \leq L_i^t \leq \tau_{Lmax}$	The value of L itself should be limited within a specified safe range $[\tau_{Lmin}, \tau_{Lmax}]$
$R6$	$\tau_{Fmin} \leq F_i^t \leq \tau_{Fmax}$	The value of F itself should be limited within a specified safe range $[\tau_{Fmin}, \tau_{Fmax}]$

efficient and reliable way to detect abnormalities in the control units. The complex interconnections within a smart grid result in multiple inter-constraints between the state variables, which can be utilized to specify a set of rule specifications for the control units' behaviors. Therefore, in this work, we define several behavior rule specifications that LAs must follow under normal operating conditions (see Table I). This will allow us to identify any operating abnormality.

Let us take the first rule $R1$ as an example, G_i^t denotes the measurement value of power generation at generator i at time instant t, while $\hat{G}_i^t$ denotes the corresponding expected value. $R1$ describes that the absolute difference between the measured value and the expected value should be limited to a specified safe threshold τ_G. In our scheme, the expected values are defined by the values estimated by the CC (other than by LAs) using state estimation, since CC is the fully trusted party. Apart from $R1$, in real-world applications, the value of G_i^t should also be constrained within a safe range, say $[\tau_{Gmin}, \tau_{Gmax}]$ as described in $R4$. Similarly, parallel rules can also be specified for power loads $\boldsymbol{L}$, power line flows $\boldsymbol{F}$ as described in other rules.

Measurement values of the state variables are revealing of the LA's behavior. Thus, it is logical to infer that deviation of these rule specifications imply abnormality. A single deviation may not sufficiently indicate that an LA is compromised, as the deviation may be due to system noise. Therefore, a conjunctive form of these rules and long-term observation of these conjunctive rules are employed in this work to effectively and accurately assess LAs' behaviors (and reduce false positive rate).

$$\boldsymbol{\mathcal{R}} = R1 \cup R2 \cup R3 \cup R4 \cup R5 \cup R6 \tag{8}$$

The conjunctive rule $\boldsymbol{\mathcal{R}}$ is the combination of all specified rules as shown in Eq. (8). To simply represent whether a rule is compliant, we use "1" to denote non-compliance of a rule, while "0" to denote compliance. As such, $\boldsymbol{\mathcal{R}}$ can be represented as a binary sequence. For example, "100010" indicates that $R1$ and $R5$ are non-compliant while the remaining rules are compliant. Particularly, full compliance of the conjunctive six rules is expressed as "000000", which is our reference sequence, seq_{ref}.

We now define the *compliance level* of each binary sequence as follows:

$$\rho = 1 - dist(seq, seq_{ref}) \tag{9}$$

where seq_{ref} is the binary sequence extracted from each piece of measurement data, and $dist$ function denotes the normalized distance between each binary sequence and the seq_{ref}. Many distance-based algorithms can be utilized in our scheme, like Hamming distance, Euclidean distance, etc. In this work, we use Euclidean distance to conduct our simulation experiments.

In real-word applications, multi-level systems (e.g. quaternary, octonary) can be employed instead of binary system, which will yield a more accurate compliance level of these rules. In addition, different rules may have various significance levels to the power system. Hence, distinguished weights can be assigned to each rule to enhance the accuracy of the compliance levels. However, either multi-level systems or weighted rules can impose considerable computational burden on CC and require a significant amount of storage for real-time detection applications. Therefore, if multi-level systems and/or weighted rules are to be integrated into our DDOA scheme, efficient optimization algorithms or balancing mechanisms will be required prior to deploying this enhanced scheme.

B. Dirichlet-based Reputation Model

In our system model, CC is responsible for monitoring and assessing the behaviors of LAs, and determining whether any LA has been compromised based on a series of historical observations. As known to us, Bayesian statistics can be used to measure the uncertainty of a decision and provide future knowledge of such decision based on a set of historical observations. In this way, a Bayesian statistics methodology is employed in our work to assist CC in making correct decisions of whether or not an LA has been compromised, and provide CC with knowledge of LAs' most possible behaviors in the future. Specifically, of the statistical techniques, Beta distribution is a viable method to determine whether a decision is correct, while a Dirichlet distribution can determine at what level a decision is correct [20]. In this paper, to obtain a more accurate assessment of LAs' behaviors and hence, a more accurate decision, we consider a Dirichlet-based probabilistic model.

Dirichlet distribution is grounded on initial beliefs regarding an unknown event represented by a prior distribution. The initial beliefs combined with a series of historical observations can be represented by a posterior distribution. The posterior distribution is best suited for our reputation model, as the reputations are required to be updated based on historical observations. Let X be a discrete random variable denoting

the compliance level ρ of the measurement data for an LA. X takes values in the set $X = \{x_1, x_2, \ldots, x_k\}$, where $x_i \in [0, 1]$ and $x_{i+1} > x_i$ $(i = 1, \ldots, k)$. Usually, we have $x_1 = 0$, and $x_k = 1$. Let $\boldsymbol{p} = [p_1, p_2, \ldots, p_k]$ with $\sum_{i=1}^{k} p_i = 1$ be the probability distribution of X, i.e. $p\{X = x_i\} = p_i$. In addition, let $\boldsymbol{\zeta} = [\zeta_1, \zeta_2, \ldots, \zeta_k]$ denote the cumulative historical observations and initial beliefs of X. Then, we can model $\boldsymbol{p}$ with a posterior Dirichlet distribution as follows:

$$f(\boldsymbol{p}|\boldsymbol{\zeta}) = Dir(\boldsymbol{p}|\boldsymbol{\zeta}) = \frac{1}{B(\boldsymbol{\zeta})} \prod_{i=1}^{k} p_i^{\zeta_i - 1} = \frac{\Gamma(\zeta_0)}{\prod_{i=1}^{k} \Gamma(\zeta_i)} \prod_{i=1}^{k} p_i^{\zeta_i - 1}, \tag{10}$$

where $B(\cdot)$ is a Beta function, and $\Gamma(\cdot)$ is a Gamma function. $\zeta_0 = \sum_{i=1}^{k} \zeta_i$.

Given the historical statistics ζ, the expected value of the probability of $\boldsymbol{X}$ to be x_i is given by

$$E(p_i|\boldsymbol{\zeta}) = \frac{\zeta_i}{\zeta_0}. \tag{11}$$

Let $p_i^j(t)$ denotes the probability that LA_j behaves with an compliance level x_i at time instant t, where $\sum_{i=1}^{k} p_i^j(t) = 1$. We model $p_i^j(t)$ using a posterior Dirichlet distribution as shown in Eq. (10). We define a random variable $Y^j(t)$ denoting the sum of the products of the grade and probability of each compliance level in $\boldsymbol{p}^j(t) = [p_1^j(t), p_2^j(t), \ldots, p_k^j(t)]$ for LA_j, which is given by

$$Y^j(t) = \boldsymbol{\omega} \boldsymbol{p}^j(t) = \sum_{i=1}^{k} \omega_i p_i^j(t), \tag{12}$$

where $\boldsymbol{\omega} = [\omega_1, \omega_2, \ldots, \omega_k]$ is the grade assignment for each compliance level, measuring the different impacts on LA_j's overall operating performance. This design will significantly improve the accuracy of CC's decisions.

To assess the overall status of an LA's behaviors, we leverage the *reputation level* in our scheme. Specifically, the LA's behaviors can be described using various compliance levels. Thus, the reputation level of an LA can be defined by the graded mean value of each compliance level at time instant t as shown below:

$$R^j(t) = E[Y^j(t)] = \sum_{i=1}^{k} \omega_i E[p_i^j(t)] = \frac{1}{\zeta_0^j(t)} \sum_{i=1}^{k} \omega_i \zeta_i^j(t), \tag{13}$$

where $\zeta_i^j(t)$ is the cumulative historical observations of LA_j at time instant t with compliance level x_i. The variance of $Y^j(t)$ is then given by

$$\sigma^2[Y^j(t)] = \sum_{i=1}^{k} \sum_{l=1}^{k} \omega_i \omega_l cov[p_i^j(t), p_l^j(t)]. \tag{14}$$

Notice that the covariance of $p_i^j(t)$ and $p_l^j(t)$ is given by

$$cov[p_i^j(t), p_l^j(t)] = \frac{-\zeta_i^j(t)\zeta_l^j(t)}{\left(\zeta_0^j(t)\right)^2 \left(\zeta_0^j(t) + 1\right)}. \tag{15}$$

C. Description of DDOA

In DDOA, CC first trains the initial reputation levels of the LAs based on the collected historical observations, as shown in Algorithm 1.

Algorithm 1 Reputation Level Training Algorithm

procedure DIRICHLET-BASED REPUTATION TRAINING
  for $j = 1$ to M, CC **do** ▷ M is the number of LAs
    1). Extracts N pieces of reported data from LA_j;
    2). Computes the compliance level of each piece of data $\rho^j(t)$, $t \in [1, N]$ with Eq. (9);
    for $t = 1$ to N **do**
      for $i = 1$ to k **do**
        if $\rho^j(t) = x_i$ **then**
          $\zeta_i^j(t) \leftarrow \zeta_i^j(t-1) + 1$;
          break;
        else
          $\zeta_i^j(t) \leftarrow \zeta_i^j(t-1)$;
        end if
      end for
      a). $\zeta_0^j(t) = \sum_{i=1}^{k} \zeta_i^j(t)$;
      b). Determines the reputation level of LA_j by $R^j(t) = \frac{1}{\zeta_0^j(t)} \sum_{i=1}^{k} \omega_i \zeta_i^j(t)$.
    end for
  end for
end procedure

After the training phase, CC obtains the initial reputation level of each LA. While, these initial reputation levels only represent their historical performance. Recall that a smart grid needs to provide near real-time monitoring and control of the whole power system. As such, persistent observation and assessment of LAs' behaviors is always required to detect whether any LA may have been compromised. In the detection phase, we propose an adaptive algorithm with a *reputation incentive mechanism* to update LAs' reputation levels, whose functionality is described in Algorithm 2.

Based on historical experiences, CC first specifies two thresholds H_s and H_m for the reputation level as the detection criteria, where H_s indicates suspicious threshold while H_m indicates malicious threshold. In a real-world scenario, occasional occurrence of system faults in smart grids is unavoidable and consequently, causes wide fluctuations of state variables. Such incidents impact (and reduce) both compliance and reputation levels. If a single detection threshold is utilized, we could possibly have a high false positive rate. However, two levels of threshold can successfully tolerate these system faults; thus, it can considerably reduce the false positive rate and further improve the detection rate.

By comparing the current reputation levels with the two specified thresholds, LAs can be classified into one of the three distinct groups, namely: normal, suspicious, and malicious group.

- *normal group* ($\mathbb{N}$): for those who reside in the normal group, we consider them as benign LAs. Thus, no further actions will be taken.
- *suspicious group* ($\mathbb{S}$): for those who fall into the suspicious group, reputation incentive mechanism will be triggered to adjust the monitor frequency and grades for different compliance levels.
- *malicious group* ($\mathbb{M}$): for those who belong to the malicious group, we consider them as malicious LAs that

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/TIFS.2016.2576898, IEEE Transactions on Information Forensics and Security

Algorithm 2 DDOA Algorithm

procedure REPUTATION UPDATING AND INTRUSION DETECTION
  Initialization:
  $T_{max},\ T_{min},\ T_S,\ T_W,\ H_s > H_m,\ N_{count} = 0,$
  $\mu_1 > \mu_2 > \cdots > \mu_k,\ T_1 = T_2 = \cdots = T_M = T_{max},$
  $\omega_1 = \overline{\omega}_1,\ \omega_2 = \overline{\omega}_2,\ \ldots,\ \omega_k = \overline{\omega_k}$
  for $j = 1$ to M, CC **do** with a frequency of $1/T_j$
    1). Input: $\rho^j(t), R^j(t-1), \omega_1^j, \omega_2^j, \ldots, \omega_k^j$
    2). Classification:

$$LA_j \in \begin{cases} \mathbb{N}, & \text{if } R^j(t-1) > H_s \\ \mathbb{S}, & \text{if } H_s \geq R^j(t-1) \geq H_m \\ \mathbb{M}, & \text{if } R^j(t-1) < H_m \end{cases}$$

    3). Judgement:
    switch LA_j **do**
      case: $LA_j \in \mathbb{N}$
        a). LA_j is benign;
        b). $\omega_k^j \leftarrow \min\{\omega_k^j e^{\mu_k}, 1\}$;
        c). $\omega_i^j \leftarrow \overline{\omega}_i, \forall\ i = 1, 2, \ldots, k-1$;
        d). $T_j \leftarrow T_{max}$;
      case: $LA_j \in \mathbb{S}$
        $T_j \leftarrow \max\{T_j/2, T_{min}\}$;
        if $\rho^j(t) = x_k$ **then** ▷ $x_k = 1$
          $\omega_k^j \leftarrow \min\{\omega_k^j e^{\mu_k}, 1\}$;
          $T_{count} \leftarrow T_{count} + 1$;
          if $T_{count} > T_S$ **then**
            $T_j \leftarrow \min\{T_j * 2, T_{max}\}$;
            $T_{count} \leftarrow 0$;
          end if
        else
          $\omega_k^j \leftarrow \omega_k^j e^{-\mu_k}$;
          if $\rho^j(t) = x_i\ (i \neq k)$ **then**
            $\omega_i^j \leftarrow \omega_i^j e^{-\mu_i}$;
          end if
          $T_{count} \leftarrow 0$;
        end if
      case: $LA_j \in \mathbb{M}$
        LA_j is compromised.
    4). Updates ζ_i^j for $i = 1, 2, \ldots, k$ with reference to Algorithm 1.
    5). Determines $R^j(t)$ using Eq. (13) with observation window T_W.
  end for
end procedure

have been compromised by opportunistic attackers.

From a social perspective, one needs to spend a considerable amount of time performing good behaviors consistently in order to build up a good reputation, and only a few instances of bad behaviors will cause doubt on the individual's personality and result in a rapid fall in social reputation [21]. Similarly, for LAs in the suspicious group, we employ a reputation incentive mechanism to achieve adaptive assessment of their behaviors. In this mechanism, we increase the grade ω_k in response to an input of $x^j(t) = x_k$ (the full compliance level), and decrease both ω_k and ω_i responding to an input of $x^j(t) = x_i, i \neq k$. In addition, when LA_j falls in the suspicious group $\mathbb{S}$, CC will increase the monitor frequency of LA_j twofold (i.e. $T_j \leftarrow T_j/2$) to pay closer attention to it. Under normal circumstances, CC monitors LA_j with a constant period T_{max}. If CC observes that LA_j behaves perfectly with all full compliance levels within a safe observation time period T_S, the monitor frequency will be reduced by half (say $T_j \leftarrow T_j * 2$). Particularly, in the case that any LA returns from group $\mathbb{S}$ to the normal group $\mathbb{N}$, the monitor frequency and all the grades, with the exception of ω_k, will be recovered to the initial values.

In this work, we observe LA's behavior over a long period of time, rather than their entire operating history, as the latter will reduce the response speed of the reputation levels and consequently reduce the detection accuracy. Hence, we employ a relatively long observation window T_W as our reference observation period. In other words, CC only needs to assess LA's behavior within a time period of $[t - T_W, t]$.

This incentive mechanism is designed to encourage non-malicious LAs, who reside in the normal group or may fall into suspicious group due to system noise, to keep up with their good behaviors in order to increase their reputation levels, as well as rapidly decrease a suspicious LA's reputation level due to non-compliance behaviors.

D. Guarantee of Data Integrity with BLS Signature

We need to ensure that the measurement data received by CC have not been falsified, in order to carry out genuine state estimation. Thus, in DDOA, we employ BLS short signature [22] to ensure data integrity during transmission as well as improve the efficacy of our proposed scheme. The choice of BLS short signature is due to its length (i.e. short) and capability to efficiently support data aggregation.

V. PERFORMANCE EVALUATION

We conducted a set of experiments to evaluate the effectiveness of our proposed scheme. First, we carried out Time Step Simulation experiments using the PowerWorld simulator to collect extensive real-time data from the IEEE 39-bus power testing system [23]. Then, a series of simulations were conducted in MATLAB 2014b to analyze the collected data.

A. Data Collection in PowerWorld

The IEEE 39-bus power system, used as our testing system (see Fig. 3), is geographically partitioned into m areas (in our simulations, $m = 6$), which we referred to as LAs. In PowerWorld, we make use of Time Step Simulation to collect

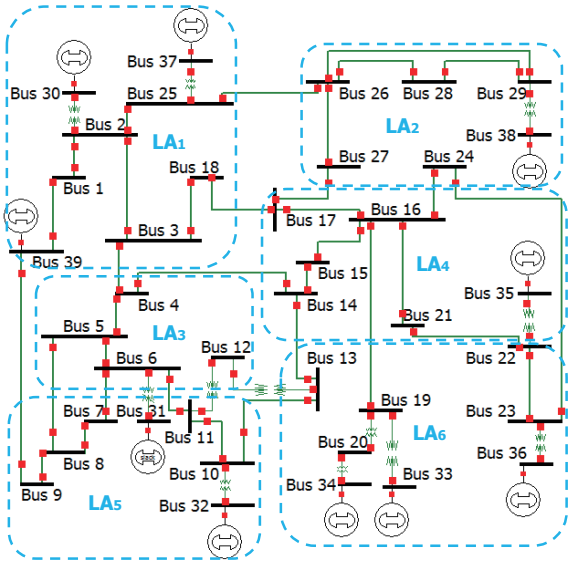

Fig. 3. IEEE 39-bus power system.

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/TIFS.2016.2576898, IEEE Transactions on Information Forensics and Security

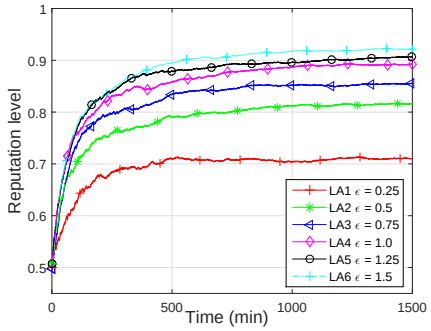

Fig. 4. Reputation level versus different ϵ during training phase with $P_n = 0.1$.

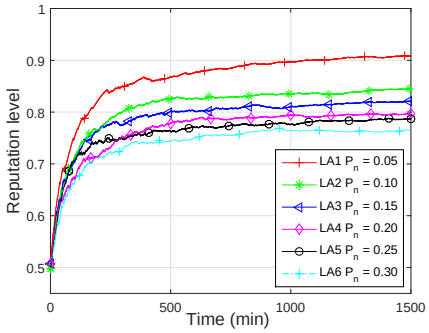

Fig. 5. Reputation level versus different P_n during training phase with $\epsilon = 0.75$.

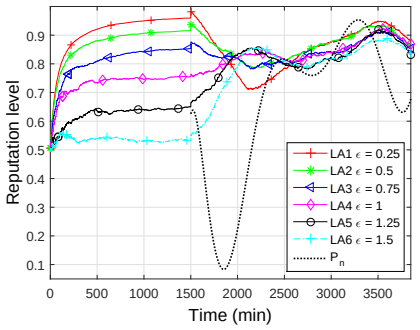

Fig. 6. Reputation level versus different ϵ during training phase with daily dynamic P_n.

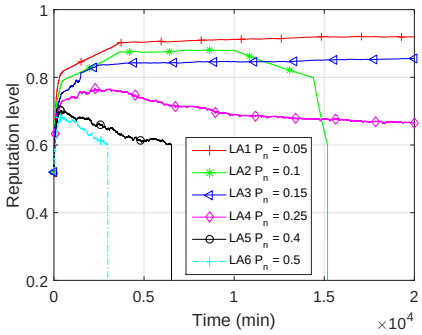

Fig. 7. Reputation level with an aggregative attacker during detection phase with $\epsilon = 0.75$.

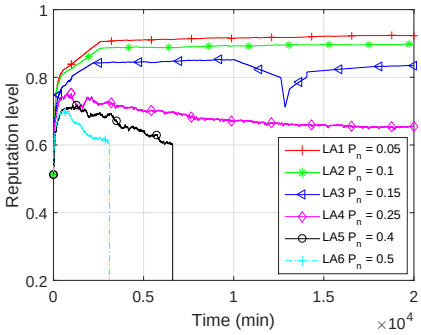

Fig. 8. Reputation level with an inserted temporal system fault during detection phase with $\epsilon = 0.75$.

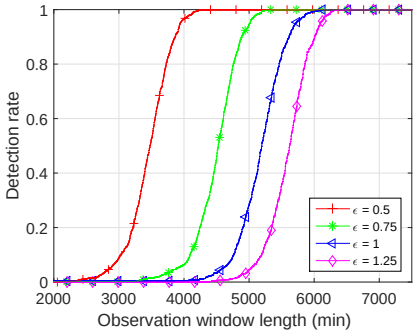

Fig. 9. Detection rate versus different length of observation window with $P_n = 0.1$.

massive real-time data for around 20,000 minutes, including power generations of each generator $\boldsymbol{G}$, power loads of each bus $\boldsymbol{L}$, and line power flows of each transmission line $\boldsymbol{F}$, etc. The first 1,500 minutes of data is used for the training phase, and the remaining data is used for the detection phase.

We randomly inserted fictitious data into the collected data to simulate the behaviors of LAs under different scalar ϵ and system noise P_n.

B. Data Analytics in MATLAB

With our proposed reputation level training algorithm, we analyze the reputation levels using the collected data. In the training phase, the effects of different ϵ and system noise P_n are first evaluated. Fig. 4 plots the reputation levels with respect to ϵ along the training period. It can be observed that the reputation level converges to a constant value as time progresses, and the higher the ϵ, the higher the reputation. This is because, as explained in Section II-B, a higher ϵ indicates a lower attack probability, hence leading to a higher reputation level. The reputation levels under different system noise P_n along the training period are plotted in Fig. 5. Similar to the effect of ϵ, the reputation level asymptotically converges to a constant value, while the lower the system noise, the higher reputation level (recall lower system noise results in lower attack probability).

In addition, to demonstrate how opportunistic attackers can adapt their attack probabilities according to the system noise, we profile the daily system noise level based on real-time daily load pattern in Fig. 6. Chertkov *et al.* have demonstrated a significant correlation between system noise and load pattern in [24]. Under such circumstances, the reputation level versus system noise level under different ϵ is also presented. From this figure, we observe that the reputation level fluctuates conversely with the system noise, due to the same reason (i.e. system noise has inverse impacts on the reputation level).

In the detection phase, we study two scenarios to demonstrate the effectiveness of our proposed scheme. In the first scenario (see Fig. 7), we assume that at time instant 10,000 minutes, LA_2 is compromised by a malicious attacker. Since LA_2 belongs to the normal group in the beginning, we observe that after it is compromised, the reputation level decreases slightly to the suspicious group threshold H_S. With our reputation incentive mechanism, once the reputation level drops below H_S, it is regarded as suspicious and the reputation level decreases rapidly to the malicious group threshold H_M with respect to continuous non-compliance behaviors. Thus, the compromised LA_2 has been identified. By contrast, LA_5 and LA_6 are designed to be compromised from the very beginning. A notable difference is that LA_6 suffers from a higher system noise than LA_5, and the reputation level of LA_6 decreases faster than LA_5.

Modelling a different opportunistic attacker, we insert a temporal system fault to LA_3 at time instant 10,000 minutes in scenario two to highlight the different performance between attackers and system faults, and the corresponding reputation

level variation is shown in Fig. 8. We observe that due to the system fault, the reputation level of LA_3 first decreases from the normal group to the suspicious group with a low decrease rate in normal group and a high decrease rate in suspicious group. This is because the proposed reputation incentive mechanism adaptively changes the decrease rate accordingly. After that, the reputation level gradually recovers and, finally, converges to a steady level. It is clear that the system fault will not change the behavior of the LA, and although the reputation decreases within a short period of time, our scheme is able to recover the reputation.

Finally, the detection rate versus the length of the observation window T_W is presented in Fig. 9. We observe that within a specific period (say [2000, 4000]), the detection rate increases with the growth of the observation window length, as a longer observation window can provide additional evidence to identify the hidden attackers. Compared with conservative attackers (with $\epsilon > 1$), it is quicker to identify the aggressive attackers (with $\epsilon < 1$) using our proposed scheme.

In summary, we have demonstrated that a potential class of opportunistic attackers in smart grids can adapt their attack probabilities according to the dynamic system noise level P_n, and our proposed DDOA scheme can effectively detect and identify these opportunistic attackers (e.g. state-sponsored actors). In addition, our scheme has been shown to accommodate occasional system faults due to the two specified thresholds H_s and H_m. We have also shown that our scheme achieves a high detection rate with long observation windows. Therefore, our proposal is an effective and promising solution to detect opportunistic attackers in smart grid cyber-physical systems.

VI. Related Work

In the increasing Internet-connected society (e.g. Internet-of-Things), ensuring the security of smart grids and other cyber-physical systems is crucial to the stability of a society [1], [3], [25], [26]. One current line of research is detecting and mitigating insider attacks in smart grids (see [1], [3], [11], [27]–[29]). Liu [29] is, probably, the first to study a new class of insider attacks, the false data injection (FDI) attacks. In FDI attacks, attackers seek to circumvent conventional IDS or IPS without triggering alarms in power grids. Kosut investigated the various attack strategies and their countermeasures for malicious data integrity attackers in smart grids [28]. Xie and Esmalifalak *et al.* also examined FDI attacks in deregulated electricity markets, which could be used to manipulate nodal electricity prices [11], [14], [30].

These studies focused on the centralized power system model. With the increasing demands on interconnectivity between systems in future smart grids, recent research focus have shifted to security in hierarchical smart grids (see [4], [21], [31], [32]). For example, Li [32] proposed a distributed quick detection scheme for FDI attacks in smart grids. Vukovic [4] analyzed the security issues in distributed power system and proposed a methodology to detect and mitigate data integrity attacks.

Unfortunately, most existing efforts were directed to the insider data integrity attacks. There appears to be a lack of attention to other types of insider attacks, which can have devastating consequences on smart grids. One such example of an understudied insider attacks is opportunistic attacks. Opportunistic attackers were first introduced by Mitchell [16] in a medical cyber-physical system context.

In this work, we have studied the problem of opportunistic attacks in future hierarchical smart grids, where attackers seek to profit from hierarchical electricity markets via compromised LAs, rather falsifying measurement data. Existing mitigation strategies are generally ineffective against such attackers. For example, [33], [34] noted that inside attackers can evade detection by hiding behind a typical system operation for a long time, making observations on how the system works, etc; thus, monitoring schemes are more effective and reliable in addressing inside attackers. This observation is also supported by findings from this paper, where we demonstrated that our novel Dirichlet-based reputation scheme can reliably and effectively identify and detect opportunistic attackers.

VII. Conclusion

In this work, we have presented a three-tier hierarchical framework for future smart grids, and highlighted the importance of resilience against financially-motivated opportunistic attackers (seeking to manipulate smart electricity prices). To defend against opportunistic attacks, we have proposed a Dirichlet-based detection scheme (DDOA) to identify and detect potential attackers. Using simulations of extensive real-time data collected from the IEEE 39-bus power testing system, we demonstrated the practicality of DDOA simulations.

Future work includes deploying DDOA in a real-world environment, with the aims of refining the scheme and improving the efficiency and accuracy.

References

[1] H. Bao, R. Lu, B. Li, and R. Deng, "BLITHE: Behavior rule based insider threat detection for smart grid," *IEEE Internet Things J.*, vol. 3, no. 2, pp. 190–205, Apr. 2016.

[2] Y. L. Yuan, Z. Y. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, June 2011.

[3] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Inf.*, no. 99, Aug. 2015.

[4] O. Vukovic and G. Dan, "Security of fully distributed power system state estimation: Detection and mitigation of data integrity attacks," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 7, pp. 1500–1508, July 2014.

[5] V. Kekatos and G. B. Giannakis, "Distributed robust power system state estimation," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1617–1626, May 2013.

[6] S. Iwamoto, M. Kusano, and V. H. Quintana, "Hierarchical state estimation using a fast rectangular-coordinate method," *IEEE Trans. Power Syst.*, vol. 4, no. 3, pp. 870–880, Aug. 1989.

[7] ICS-CERT. (2016) NCCIC/ICS-CERT monitor november-december 2015. Accessed on 20 Jan. 2016. [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT%20Monitor_Nov-Dec2015_S508C.pdf

[8] K. Zetter, "A cyberattack has caused confirmed physical damage for the second time ever," *Wired Magazine*, 2015.

[9] CNNMoney. (2015) ISIS is attacking the U.S. energy grid. Accessed on 8 Jan. 2016. [Online]. Available: http://money.cnn.com/2015/10/15/technology/isis-energy-grid/

[10] S. Z. Bi and Y. J. Zhang, "False-data injection attack to control real-time price in electricity market," *Proc. IEEE Glob. Telecomm. Conf. (GLOBECOM)*, pp. 772–777, Dec. 2013.

[11] L. Xie, Y. L. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," *Proc. IEEE 1st International Conference on Smart Grid Communications (SmartGridComm)*, pp. 226–231, Oct. 2010.
[12] R. Tan, V. B. Krishna, D. K. Yau, and Z. Kalbarczyk, "Integrity attacks on real-time pricing in electric power grids," *ACM T. Inform. Syst. Se. (TISSEC)*, vol. 18, no. 2, p. 5, Dec. 2015.
[13] L. Jia, R. J. Thomas, and L. Tong, "Impacts of malicious data on real-time price of electricity market operations," in *Proc. 45th Hawaii International Conference on System Sciences*, Jan. 2012, pp. 1907–1914.
[14] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 160–169, Mar. 2013.
[15] J. Ma, Y. Liu, L. Song, and Z. Han, "Multiact dynamic game strategy for jamming attack in electricity market," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2273–2282, Sep. 2015.
[16] R. Mitchell and I.-R. Chen, "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 1, pp. 16–30, Jan. 2015.
[17] F. C. Schweppe, J. Wildes, and D. B. Rom, "Power system static-state estimation, parts I, II, and III," *IEEE Trans. Power App. Syst.*, vol. 89, no. 1, pp. 120–135, Jan. 1970.
[18] P. Paolino, "Maximum likelihood estimation of models with beta-distributed dependent variables," *Political Analysis*, vol. 9, no. 4, pp. 325–346, Jan. 2001.
[19] A. L. Ott, "Experience with PJM market operation, system design, and implementation," *IEEE Trans. Power Syst.*, vol. 18, no. 2, pp. 528–534, May 2003.
[20] N. L. Johnson, S. Kotz, and N. Balakrishnan, *Continuous Multivariate Distributions, volume 1, Models and Applications*. New York: John Wiley & Sons, Apr. 2002, vol. 59.
[21] Y. L. Sun, Z. Han, W. Yu, and K. J. R. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," *Proc. IEEE INFOCOM*, vol. 6, pp. 1–13, Apr. 2006.
[22] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, Sep. 2004.
[23] P. Corporation. Powerworld. Accessed on 8 Jan. 2016. [Online]. Available: http://www.powerworld.com/
[24] M. Chertkov, F. Pan, and M. G. Stepanov, "Predicting failures in power grids: The case of static overloads," *IEEE Trans. Smart Grid*, vol. 2, no. 1, pp. 162–172, Mar. 2011.
[25] J. Wu, M. Dong, K. Ota, Z. Zhou, and B. Duan, "Towards fault-tolerant fine-grained data access control for smart grid," *Wireless Personal Communications*, vol. 75, no. 3, pp. 1787–1808, Apr. 2014.
[26] M. Dong, K. Ota, L. T. Yang, A. Liu, and M. Guo, "LSCD: A low storage clone detecting protocol for cyber-physical systems," *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, vol. 35, no. 5, pp. 712–723, May 2016.
[27] T. Lin, Y. Gu, D. Wang, Y. H. Gui, and X. H. Guan, "A novel method to detect bad data injection attack in smart grid," *Proc. IEEE INFOCOM*, pp. 3423–3428, Apr. 2013.
[28] O. Kosut, L. Y. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.
[29] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM T. Inform. Syst. Se. (TISSEC)*, vol. 14, no. 1, May 2011.
[30] M. Esmalifalak, Z. Han, and L. Y. Song, "Effect of stealthy bad data injection on network congestion in market based power system," *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, Apr. 2012.
[31] R. X. Lu, X. H. Liang, X. Li, X. D. Lin, and X. M. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621–1631, Sep. 2012.
[32] S. Li, Y. Yilmaz, and X. D. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2725–2735, Nov. 2015.
[33] P. A. Legg, O. Buckley, M. Goldsmith, and S. Creese, "Automated insider threat detection system using user and role-based profile assessment," *IEEE Syst. J.*, June 2015.
[34] N. Kanaskar, J. Bian, R. Seker, M. Nijim, and N. Yilmazer, "Dynamical system approach to insider threat detection," in *Proc. IEEE International Systems Conference (SysCon)*, Apr. 2011, pp. 232–238.

Beibei Li (S'15) received the B.E. degree in communication engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 2014. He is currently a Ph.D. candidate with the INFINITUS Laboratory, School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. His research interests include smart grid security, cyber-physical system security, and applied cryptography.

Rongxing Lu (S'09-M'11-SM'15) received the Ph.D. degree in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2006, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2012. From May 2012 to April 2013, he was a Postdoctoral Fellow with the University of Waterloo. Since May 2013, he has been an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. His research interests include computer network security, mobile and wireless communication security, and applied cryptography. Dr. Lu was the recipient of the Canada Governor General Gold Metal.

Wei Wang (S'14) received the B.Eng. degree in Information Countermeasure Technology and the M.S. degree in Signal and Information Processing from Xidian University in 2011 and 2014, respectively. He is currently pursuing the Ph.D. degree in Electrical and Electronic Engineering at Nanyang Technological University, Singapore. His research interests include cooperative communications, cognitive radios and physical layer security.

Kim-Kwang Raymond Choo (SM'15) received the Ph.D. in Information Security in 2006 from Queensland University of Technology, Australia. He is currently a cloud technology endowed associate professor at University of Texas at San Antonio, an associate professor at the University of South Australia, and a guest professor at China University of Geosciences, Wuhan. He was named one of 10 Emerging Leaders in the Innovation category of The Weekend Australian Magazine / Microsofts Next 100 series in 2009, and is the recipient of ESORICS 2015 Best Research Paper Award, 2015 Winning Team of Germanys University of Erlangen-Nuremberg Digital Forensics Research Challenge, 2014 Australia New Zealand Policing Advisory Agencys Highly Commended Award, 2010 Australian Capital Territory Pearcey Award, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Societys Wilkes Award.