Privacy-Preserving Energy Theft Detection in Microgrids: A State Estimation Approach

Sergio A. Salinas, *Student Member, IEEE*, and Pan Li, *Member, IEEE*

***Abstract*—Energy theft is a notorious problem in electric power systems, which causes great economic losses and threatens the reliability of the power grid. Recently, the Smart Grid has been proposed as the next-generation power system to modernize the current grid and improve its efficiency, sustainability, and security. Key technologies of the Smart Grid include smart meters, which allow system operators to collect real-time power consumption data from users, and microgrids, which allow users to own and control renewable resources. However, the Smart Grid is vulnerable to cyber attacks, thus making stealing energy much easier in it. Most existing energy theft detection schemes require the collection of real-time power consumption data from users, i.e., users' load profiles, which violates their privacy. In this paper, we first propose a centralized energy theft detection algorithm utilizing the Kalman filter, called SEK. It can efficiently identify the energy thieves but cannot protect users' privacy. Then, based on SEK, we develop a privacy-preserving energy theft detection algorithm called PPBE, which privately finds the energy thieves by decomposing the Kalman filter into two parallel and loosely coupled filters. Finally, we conduct thorough privacy analysis and extensive simulations to validate our proposed algorithms.**

***Index Terms*—Energy theft, microgrid, privacy, state estimation.**

I. Introduction

ENERGY theft is a notorious problem in electric power systems and has serious implications for both utility companies and legitimate users. Particularly, in the U.S. and Canada, it is estimated that utility companies loose billions of dollars in revenue every year [1], [2], while in developing countries energy theft can amount to 50% of the total energy delivered [3]. Energy theft also leads to excessive energy consumption which may cause equipment malfunction or damage [4], and often enables other criminal activities, such as illegal production of controlled substances [2]. Besides, utility companies usually amortize energy theft losses by increasing energy rates on legitimate users.

Recently, the Smart Grid has been proposed as the next-generation power gird to modernize the current electric gird and improve its efficiency, reliability, and security. Especially, in the smart grid, traditional mechanical meters are replaced with cyber-physical devices, usually called "smart meters". Another important feature of the Smart Grid is microgrids, where distributed generators, energy storage devices, and energy loads, typically within a distribution network, are capable of operating independently (i.e., in island mode) and also as part of the macrogrid (i.e., in grid-connected mode). Microgrids reduce transmission power losses and alleviate network congestion by bringing generation closer to the load and allowing users to sell energy back to the grid. However, in the Smart Grid, particularly in microgrids, energy thieves can easily launch cyber attacks against smart meters [5]. They can not only lie about their energy consumption, but also demand illegitimate payments by submitting fraudulent energy production reports. For example, in Virginia, Danville Utilities reports a growing problem with people tampering with smart meters [6]. It is noticeable that energy theft is much easier to commit in microgrids, and thus a much more serious problem in smart grids than in traditional power grids which needs to be carefully addressed.

Some research has been conducted to investigate the energy theft problem in smart grids. McLaughlin *et al.* [7] collect cyber-intrusion and physical-intrusion logs, and analyze users' load profiles using a data mining technique called non-intrusive load monitoring (NILM). The idea is to fuse the information using an attack graph based fusion algorithm and identify the possible energy thieves with a minimum number of false positives. Cárdenas *et al.* [8] propose a statistical anomaly detection scheme by modeling a game between a utility company and the fraudulent users. The objective of the utility company is to maximize its profit and minimize the cost of detecting pirate users, while the objective of the energy thieves is to minimize the likelihood of being detected subject to a constraint related to the amount of stolen energy. Mashima and Cárdenas [9] develop a threat model and several metrics to evaluate the accuracy of anomaly detectors. Pereira *et al.* [10] collect fine-grained load profiles from users' smart meters and apply a neural network classifier using a technique called charged system search. Huang *et al.* [11] propose a scheme that first finds out a fraudulent user's transformer, and then tries to identify the particular fraudulent user by analyzing the energy consumption variance of all the users connected to the transformer. Weckx *et al.* [12] develop a linear model for a distribution network, and can find energy thieves only if all the voltage measurements and some initial power measurements can be trusted, i.e., not tampered by the energy thieves. Unfortunately, all these techniques have low detection rates and need to manage large amounts of energy consumption data from users.

Manuscript received March 11, 2014; revised August 19, 2014 and December 29, 2014; accepted February 10, 2015. Date of publication April 16, 2015; date of current version February 17, 2016. This work was supported in part by the U.S. National Science Foundation under grants CNS-1343220, CNS-1149786, and ECCS-1128768, and in part by the Pacific Northwest National Laboratory under U.S. Department of Energy Contract DE-AC05-76RL01830. Paper no. TPWRS-00346-2014.

The authors are with the Department of Electrical and Computer Engineering, Mississippi State University, Mississippi State, MS 39762 USA (e-mail: sas573@msstate.edu; li@ece.msstate.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TPWRS.2015.2406311

More importantly, notice that all the above works [7]–[13] require the system operators to collect private information from their users, i.e., fine-grained load-profiles. However, the release of such data to system operators poses a serious risk to users' privacy [14]. In particular, residential users' load profiles can reveal their daily routines, electronic appliances, and medical devices used in their houses, and even whether any alarm system is present. This information is valuable to some third parties. For instance, burglars can use daily routine and alarm information to select the most vulnerable targets. Insurance companies may adjust users' premiums based on information extracted from load-profiles [15]. Marketing companies may conduct unsolicited directed advertising based on users' appliances, daily routines, etc. On the other hand, industrial users' load profiles contain proprietary information about equipments and logistics [16]. This information represents a competitive advantage to other companies that may want to mimic the industrial processes or gain insight into the operations. For example, similarly to that in a house, the amount, type and operation time of machinery used in a production plant can be revealed through its load-profiles, which can help competitors reproduce proprietary processes and products.

Although there exist some works studying privacy in smart grids such as [17]–[19], they cannot address the privacy issues in energy theft detection. In our previous works [20], [21], we propose several privacy-preserving energy theft detection algorithms utilizing distributed matrix decomposition. However, these approaches assume that power line losses are known, which in practice may be difficult to obtain. In this paper, we relax this assumption and propose a new state estimation based energy theft detection scheme that can successfully identify pirate users in a microgrid while preserving users' privacy. Our main idea is to model the amount of stolen energy by a smart meter as a measurement bias and use optimal state estimation techniques to solve for all the meters' biases. Thus, a zero bias indicates a faithful meter, and a non-zero one identifies a pirate meter.

Specifically, we first design a centralized state estimation algorithm based on the Kalman filter, called SEK. This algorithm is capable of identifying energy thieves by employing a centralized Kalman filter, but requires smart meters to reveal users' real-time measurements to the system operator. Then, based on the SEK algorithm, we develop a privacy-preserving bias estimation algorithm, called PPBE, that works in a distributed manner. In particular, this algorithm privately estimates the biases by decomposing the previous Kalman filter into two parallel and loosely-coupled filters. One filter, oblivious to the biases, estimates the state variable vector which consists of power line currents, while the other filter estimates the bias vector. We call them the bias-ignorant filter and the bias filter, respectively. The smart meter network computes the bias-ignorant filter in a private and distributed manner, while the microgrid operator, based on the bias-ignorant filter's residuals, carries out the bias filter. The separation of the bias-ignorant state estimation from the bias estimation hides users' measurements from the system operator and allows for a distributed algorithm, thus protecting users' private energy consumption information. Moreover, such a decomposed filter design also makes PPBE converge faster and have better numerical stability than SEK since it involves the computations of matrices of smaller sizes.

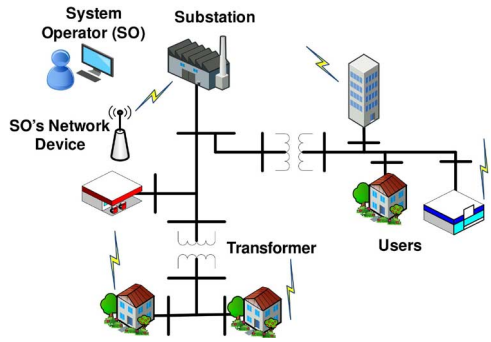


Fig. 1. Architecture for a radial microgrid.

In addition, we formally analyze the privacy of the proposed algorithm, and show that each users' privacy can be well protected from the microgrid operator, other users, and eavesdroppers as well. We also conduct extensive simulations to evaluate the performance of our algorithms and investigate the impact of system parameter uncertainty, i.e., uncertain power line parameters, on our algorithms.

The rest of the paper is organized as follows. Section II introduces the considered microgrid architecture, our mathematical models for power distribution and energy theft, and the threat model. In Section III we describe in detail our energy theft detection algorithms. We conduct privacy analysis in Section IV and simulations in Section V, respectively, to evaluate the performance of our algorithms. We finally conclude this paper in Section VI.

II. System Model

A. Microgrid Architecture

As shown in Fig. 1, we consider an electric microgrid (MG) consisting of a set of buses $\mathcal{I} = \{0, 1, 2 \ldots, n\}$ equipped with distributed generations (DGs), and a set of line segments $\mathcal{J} = \{1, 2, \ldots, m\}$ which connect the buses together and are used to model the power lines and transformers in the network. We assume a radial system denoted by graph $\mathcal{G} = \{\mathcal{I}, \mathcal{J}\}$, where buses are the vertices with bus 0 being the root, and line segments are the edges (note that in this case $m = n$). Particularly, bus 0 represents the substation which serves as the interconnection between the macrogrid and the MG. It is operated by a third-party, called the MG operator (e.g., a utility company, or a community manager).

Besides, smart meters are installed on user buses to take power, current, and voltage measurements [22], [23] and are able to communicate with each other by forming a multihop communication network [24]. The MG operator controls a network device to engage in two-way communications with the smart meter network, and performs monitoring and control actions such as state estimation, billing, and demand response. In this paper, we leverage the measurements and communication capabilities of smart meters to detect energy thieves in a privacy-preserving manner.

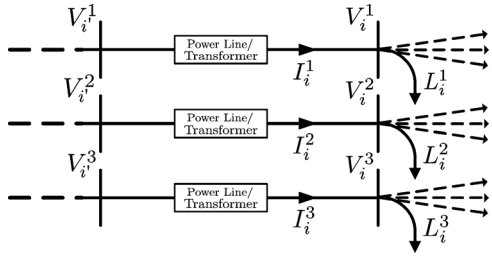


Fig. 2. Three-phase line model.

B. Power Network Model for Microgrids

In what follows, we model the currents and voltages in the MG. Specifically, as shown in Fig. 2, suppose that user i ($i \in [1, n]$) is connected to the power grid through a three-phase, bi-directional connection at bus i, which it employs to serve its load demand and supply the MG with energy generated by its DG. Thus, we can calculate the three-phase voltage at bus i with respect to the upstream node, bus i', using Kirchoff's voltage law [25]:

$$\begin{bmatrix} V_i^1 \\ V_i^2 \\ V_i^3 \end{bmatrix} = \begin{bmatrix} a_{i',i}^{1,1} & a_{i',i}^{1,2} & a_{i',i}^{1,3} \\ a_{i',i}^{2,1} & a_{i',i}^{2,2} & a_{i',i}^{2,3} \\ a_{i',i}^{3,1} & a_{i',i}^{3,2} & a_{i',i}^{3,3} \end{bmatrix} \begin{bmatrix} V_{i'}^1 \\ V_{i'}^2 \\ V_{i'}^3 \end{bmatrix} - \begin{bmatrix} z_{i',i}^{1,1} & z_{i',i}^{1,2} & z_{i',i}^{1,3} \\ z_{i',i}^{2,1} & z_{i',i}^{2,2} & z_{i',i}^{2,3} \\ z_{i',i}^{3,1} & z_{i',i}^{3,2} & z_{i',i}^{3,3} \end{bmatrix} \begin{bmatrix} I_i^1 \\ I_i^2 \\ I_i^3 \end{bmatrix} \quad (1)$$

where $a_{i',i}^{\phi,\phi'}$ ($\phi, \phi' \in \{1, 2, 3\}$ denote the phases) models the impact of $V_{i'}^{\phi'}$ on V_i^{ϕ} due to the impedance of the line segment between bus i' and bus i (denoted by (i', i)), $z_{i',i}^{\phi,\phi'}$'s are the elements of the line segment's impedance matrix, $\mathbf{V}_i = [V_i^1\ V_i^2\ V_i^3]^\top$ is the three-phase voltage vector at bus i, and $\mathbf{I}_i = [I_i^1\ I_i^2\ I_i^3]^\top$ is the three-phase current vector arriving at bus i, respectively. We assume that power lines are less than one mile long, and thus shunt admittance can be neglected. (1) can also be rewritten in matrix form as follows:

$$\mathbf{V}_i = \mathbf{A}_{i',i}\mathbf{V}_{i'} - \mathbf{Z}_{i',i}\mathbf{I}_i. \quad (2)$$

Recall that line segments represent power lines and transformers. For a power line segment (i', i), matrix $\mathbf{A}_{i',i}$ is equal to the identity matrix. For a transformer line segment (i', i), $\mathbf{A}_{i',i}$ can be calculated as

$$\mathbf{A}_{i',i} = \frac{1}{n_{i',i}} \begin{bmatrix} \bar{a}_{i',i}^{1,1} & \bar{a}_{i',i}^{1,2} & \bar{a}_{i',i}^{1,3} \\ \bar{a}_{i',i}^{2,1} & \bar{a}_{i',i}^{2,2} & \bar{a}_{i',i}^{2,3} \\ \bar{a}_{i',i}^{3,1} & \bar{a}_{i',i}^{3,2} & \bar{a}_{i',i}^{3,3} \end{bmatrix} \quad (3)$$

where $n_{i',i}$ is the turns ratio of the transformer, and $\bar{a}_{i',i}^{\phi,\phi'} \in \{0, 1, -1\}$ depends on the transformer's connection type (e.g., delta-grounded wye, wye-delta).

In practice, there is rarely more than one transformer between substations and meters. When there is one transformer on the path between bus 0 and bus i, say in the line segment between bus p (closer to bus 0) and bus h (closer to bus i), (2) can be further rewritten in the following:

$$\mathbf{V}_i = \mathbf{A}_{p,h}\left(\mathbf{V}_0 - \sum_{j \in \mathcal{P}_i} \mathbf{Z}_{j',j}\mathbf{I}_j\right) - \sum_{k \in \mathcal{H}_i} \mathbf{Z}_{k',k}\mathbf{I}_k \quad (4)$$

where $\mathcal{P}_i$ is the set of all the buses on the path from bus 0 to bus p (excluding bus 0), $\mathcal{H}_i$ is the set of all the buses on the path from bus h to bus i, j' is the upstream node of j, and k' is the upstream node of k, respectively. In the case that there is no transformer between bus 0 and bus i, then $\mathbf{A}_{p,h}$ is equal to the identity matrix, $\mathcal{P}_i$ contains the set of all the buses on the path from bus 0 to bus i (excluding bus 0), and $\mathcal{H}_i$ is empty. Note that we assume the voltage and current at the substation bus are constant. Besides, the MG operator is able to obtain very accurate power line parameters using signal injection techniques [26], or by collecting power measurements from the smart meters [27]. Previous works like [11] on state estimation in power systems make similar assumptions that the impedance parameters are accurate. In addition, the MG operator also makes the power line parameters available to the smart meters [28].

Moreover, the three-phase load current consumed or produced at bus i can be calculated according to Kirchoff's current law as follows:

$$\mathbf{L}_i = \mathbf{I}_i - \sum_{r \in \mathcal{R}_i} \mathbf{I}_r - \sum_{q \in \mathcal{Q}_i} \mathbf{B}_{i,q}\mathbf{I}_q \quad (5)$$

where $\mathbf{I}_i$ is the current arriving to bus i, $\mathcal{R}_i$ and $\mathcal{Q}_i$ are the set of downstream buses of bus i connected by power lines and that connected by transformer line segments, respectively. In addition, matrix $\mathbf{B}_{i,q}$ is as follows:

$$\mathbf{B}_{i,q} = \frac{1}{n_{i,q}} \begin{bmatrix} b_{i,q}^{1,1} & b_{i,q}^{1,2} & b_{i,q}^{1,3} \\ b_{i,q}^{2,1} & b_{i,q}^{2,2} & b_{i,q}^{2,3} \\ b_{i,q}^{3,1} & b_{i,q}^{3,2} & b_{i,q}^{3,3} \end{bmatrix}$$

where $b_j^{\phi,\phi'} \in \{0, 1, -1\}$ depends on the transformer's connection type.

In addition, the power consumed by the load at bus i is related to the load current $\mathbf{L}_i$ as follows:

$$\mathbf{L}_i = \frac{(\mathbf{P}_i + j\mathbf{Q}_i)^*}{\mathbf{V}_i} \quad (6)$$

where $\mathbf{P}_i$ and $\mathbf{Q}_i$ are the three-phase real and reactive power consumption vectors at bus i, respectively. The * operator denotes the complex conjugate operation.

C. Compromised Measurement Model

The MG operator instructs smart meters to take and report synchronized measurements at specified time instances to facilitate energy theft detection. The objective of a dishonest user is to steal energy but not get caught. To that end, it needs to manipulate its measurements in such a way that its power, current, and voltage reports are consistent with each other. In this paper, we assume that energy thieves are very powerful, i.e., they know all the system parameters [28] and are able to compromise all functions of their smart meters, including measurement taking

and reporting, which makes energy theft detection a very challenging problem.

Denote by $\mathbf{b}_i$ $(i \geq 1)$ the current that an energy thief at bus i intends to steal, which we call "the current measurement bias" controlled by the energy thief. Then, the load measurement at bus i, denoted by $\mathbf{L}'_i$, is

$$\mathbf{L}'_i = \mathbf{I}_i - \mathbf{b}_i - \sum_{r \in \mathcal{R}_i} \mathbf{I}_r - \sum_{q \in \mathcal{Q}_i} \mathbf{B}_{i,q} \mathbf{I}_q. \tag{7}$$

Note that an honest user j's load measurement is given by $\mathbf{L}'_j = \mathbf{L}_j$, since $\mathbf{b}_j = 0$ for an honest user.

Besides, the energy thief i $(i \geq 1)$ has to tamper its voltage measurement as well in order not to be easily detected. The reason is that if the energy thief i does not, all true currents can be computed based on (2) and compared to the reported ones, making itself very easy to be detected. Thus, by pretending that the incoming current is $\mathbf{I}'_i = \mathbf{I}_i - \mathbf{b}_i$ instead of $\mathbf{I}_i$, according to (2) the energy thief i can set its voltage measurement to be

$$\mathbf{V}'_i = \mathbf{A}_{p,h} \left(\mathbf{V}_0 - \sum_{j \in \mathcal{P}_i} \mathbf{Z}_{j',j} \mathbf{I}_j \right) - \sum_{k \in \mathcal{H}_i} \mathbf{Z}_{k',k} \mathbf{I}_k + \mathbf{Z}_{i',i} \mathbf{b}_i. \tag{8}$$

Clearly, an honest user's voltage measurement is $\mathbf{V}'_i = \mathbf{V}_i$.

D. Threat Model

Users' real-time power consumption data, including voltage and current measurements, can reveal their private information. In this study, we consider that there are three kinds of entities who may attempt to obtain a user's (or a smart meter's) private data: the MG operator, other users (or other smart meters), and eavesdroppers. Besides, we consider that the MG operator and smart meters work in the semi-honest mode, i.e., they faithfully and correctly execute the system protocol, but are curious about other users' privacy.

E. Paillier Cryptosystem

Paillier designed an efficient asymmetric cryptosystem, called Paillier cryptosystem [29], based on decisional composite residuosity assumption. In particular, letting $E(\cdot)$ denote the encryption function of the Paillier scheme, we have $E(m_1) \cdot E(m_2) = E(m_1 + m_2)$. The Paillier cryptosystem is semantically secure for sufficiently large public keys, which means that it is infeasible for a computationally bounded adversary to derive significant information about a message (plaintext) when given only its ciphertext and the corresponding public key.

III. Optimal State Estimation for Energy Theft Detection

In this section, we propose state estimation algorithms to find measurement biases, which can be used to identify energy thieves as explained in Section II-C, based on voltage and current observations.

A. State Estimation With the Kalman Filter

The Kalman filter [30] recursively estimates the state of a process in a way that minimizes the mean square estimation error. In the following, we present a centralized state estimation algorithm using the Kalman filter, called SEK, to find line current and bias estimates simultaneously without considering users' privacy.

Recall that we denote the voltage at the substation by $\mathbf{V}_0$. We define an augmented state vector of line segment currents and biases as $\mathbf{x} = [\mathbf{V}_0\ \mathbf{I}_1\ \mathbf{I}_2\ \ldots\ \mathbf{I}_n\ \mathbf{b}_1\ \mathbf{b}_2\ \ldots\ \mathbf{b}_n]^\top$. Then, the state equation of vector $\mathbf{x}$ can be modeled as follows:

$$\mathbf{x}^k = \mathbf{x}^{k-1} + \mathbf{w}^{k-1} \tag{9}$$

where k is the time slot index, and $\mathbf{w}^k$ is zero-mean white process noise with covariance matrix $\mathbf{Q}$.

Besides, the vector of current and voltage measurements, denoted by $\mathbf{y} = [\mathbf{V'}_0\ \mathbf{I'}_1\ \mathbf{L'}_1\ \ldots\ \mathbf{L'}_n\ \mathbf{V'}_1\ \ldots\ \mathbf{V'}_n]^\top$, can be expressed as follows:

$$\mathbf{y} = \mathbf{h}(\mathbf{x}) + \mathbf{e} \tag{10}$$

where $\mathbf{h}(\mathbf{x})$ is a function that determines the measurement vector $\mathbf{y}$ given the system state variable vector $\mathbf{x}$ according to (7) and (8), and $\mathbf{e}$ is a measurement error vector, the elements of which are three-phase measurement error vectors that are independent of each other. We assume that $\mathbf{e}$ is zero-mean white measurement noise with covariance matrix $\mathbf{R}$, i.e., $\mathbf{R} = \mathbb{E}[\mathbf{e}\mathbf{e}^\top]$. We denote the diagonal elements in $\mathbf{R}$ by σ_l^2 for $l = 0, 1, \ldots, 6n+5$.

We can see from (7) and (8) that (10) is linear and can be expressed as

$$\mathbf{y} = \mathbf{H}_{aug}\mathbf{x} + \mathbf{e} \tag{11}$$

where matrix $\mathbf{H}_{aug}$ is the Jacobian matrix of $\mathbf{h}(\mathbf{x})$ with respect to $\mathbf{x}$ and can be calculated as follows (note that $\partial \mathbf{h}(\mathbf{x})/\partial \mathbf{x} = \partial \mathbf{y}/\partial \mathbf{x}$):

$$\mathbf{H}_{aug} = \left(\begin{array}{cccc|ccc} \frac{\partial \mathbf{V}'_0}{\partial \mathbf{V}_0} & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \frac{\partial \mathbf{I}'_1}{\partial \mathbf{I}_1} & 0 & \cdots & \cdots & \cdots & 0 \\ \hline \frac{\partial \mathbf{L}'_1}{\partial \mathbf{V}_0} & \frac{\partial \mathbf{L}'_1}{\partial \mathbf{I}_1} & \frac{\partial \mathbf{L}'_1}{\partial \mathbf{I}_2} & \frac{\partial \mathbf{L}'_1}{\partial \mathbf{I}_n} & \frac{\partial \mathbf{L}'_1}{\partial \mathbf{b}_1} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{\partial \mathbf{L}'_n}{\partial \mathbf{V}_0} & \cdots & \cdots & \frac{\partial \mathbf{L}'_n}{\partial \mathbf{I}_m} & 0 & \cdots & \frac{\partial \mathbf{L}'_n}{\partial \mathbf{b}_n} \\ \hline \frac{\partial \mathbf{V}'_1}{\partial \mathbf{V}_0} & \frac{\partial \mathbf{V}'_1}{\partial \mathbf{I}_1} & \cdots & 0 & \frac{\partial \mathbf{V'}_1}{\partial \mathbf{b}_1} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{\partial \mathbf{V}'_n}{\partial \mathbf{V}_0} & \frac{\partial \mathbf{V}'_n}{\partial \mathbf{I}_1} & \frac{\partial \mathbf{V}'_n}{\partial \mathbf{I}_2} & \frac{\partial \mathbf{V}'_n}{\partial \mathbf{I}_n} & 0 & \cdots & \frac{\partial \mathbf{V}'_n}{\partial \mathbf{b}_n} \end{array} \right).$$

The first two rows are related to $\mathbf{V}_0$ and $\mathbf{I}_1$, where the partial derivatives $\partial \mathbf{V}'_0/\partial \mathbf{V}_0$ and $\partial \mathbf{I}'_1/\partial \mathbf{I}_1$ are equal to $\mathbf{1}$ (a 3×3 identity matrix) and the rest elements are equal to zero, since $\mathbf{V}'_0$ and $\mathbf{I}'_1$ are directly measured by the MG operator.

The rows in the middle section of $\mathbf{H_{aug}}$ correspond to load current measurements, where the elements are calculated by taking the first order partial derivative of $\mathbf{L}'_i$ with respect to $\mathbf{I}_j$ or $\mathbf{b}_j$, i.e.,

$$\frac{\partial \mathbf{L}'_i}{\partial \mathbf{I}_j} = \begin{cases} \mathbf{1}, & \text{if } i = j \\ -\mathbf{1}, & \text{if } j \in \mathcal{R}_i \\ -\mathbf{B}_{i,j} & \text{if } j \in \mathcal{Q}_i \\ \mathbf{0}, & \text{otherwise} \end{cases} \tag{12}$$

$$\frac{\partial \mathbf{L}'_i}{\partial \mathbf{b}_j} = \begin{cases} -\mathbf{1}, & \text{if } i = j \\ \mathbf{0}, & \text{otherwise.} \end{cases} \tag{13}$$

Here, $\mathbf{1}$ is a 3×3 identity matrix, and $\mathbf{0}$ is a 3×3 zero matrix.

The entries in the bottom section of $\mathbf{H_{aug}}$ are obtained by taking the first-order partial derivative of voltage measurements with respect to state variables $\mathbf{I}_j$ and $\mathbf{b}_j$, i.e.,

$$\frac{\partial \mathbf{V'}_i}{\partial \mathbf{I}_j} = \begin{cases} -\mathbf{A}_{p,h}\mathbf{Z}_{j',j}, & \text{if } j \in \mathcal{P}_i \\ -\mathbf{Z}_{j',j}, & \text{if } j \in \mathcal{H}_i \\ \mathbf{0}, & \text{otherwise} \end{cases} \tag{14}$$

$$\frac{\partial \mathbf{V'}_i}{\partial \mathbf{b}_j} = \begin{cases} \mathbf{Z}_{j',j}, & \text{if } i = j \\ \mathbf{0}, & \text{otherwise.} \end{cases} \tag{15}$$

Consequently, the MG operator can find the energy thieves as follows.

First, the MG operator collects smart meters' measurement vector $\mathbf{y}$.

Second, it applies the Kalman filter to find the state estimate $\hat{\mathbf{x}}^k$ at time k ($k \geq 1$). Particularly, the Kalman filter has two parts: time (or *a priori*) update and measurement (or *a posteriori*) update. In the time update part, the MG operator predicts the state at time k, i.e.,

$$\hat{\mathbf{x}}^{k-} = \hat{\mathbf{x}}^{k-1} \tag{16}$$

where $\hat{\mathbf{x}}^{k-1}$ is the state estimate at time $k-1$, and $\hat{\mathbf{x}}^0$ is set to the expected value of $\mathbf{x}$, i.e., $\mathbb{E}[\mathbf{x}]$, for example, based on the average historical power consumption data. It also finds the *a priori* estimation error covariance matrix $\mathbf{P}^{k-} = \mathbf{P}^{k-1} + \mathbf{Q}$, where $\mathbf{P}^{k-1}$ is the *a posteriori* estimation error covariance matrix at time $k-1$. Note that the initial estimation error covariance matrix $\mathbf{P}^0$ can be calculated as $\mathbf{P}^0 = \mathbb{E}[(\mathbf{x}^0 - \hat{\mathbf{x}}^0)(\mathbf{x}^0 - \hat{\mathbf{x}}^0)^\top]$, where $\mathbf{x}^0$ can be randomly selected.

In its measurement update part, the MG operator employs the available measurements at time k to correct the time update estimate, i.e.,

$$\hat{\mathbf{x}}^k = \hat{\mathbf{x}}^{k-} + \mathbf{K}^k \left(\mathbf{y}^k - \mathbf{H}_{aug}\hat{\mathbf{x}}^{k-}\right) \tag{17}$$

where the gain matrix $\mathbf{K}^k$ is updated as $\mathbf{K}^k = \mathbf{P}^{k-}\mathbf{H}_{aug}^\top(\mathbf{H}_{aug}\mathbf{P}^{k-}\mathbf{H}_{aug}^\top\mathbf{R})^{-1}$. Such a $\mathbf{K}^k$ can minimize the *a posteriori* estimation error covariance $\mathbf{P}^k = \mathbb{E}[(\mathbf{x}^k - \hat{\mathbf{x}}^k)(\mathbf{x}^k - \hat{\mathbf{x}}^k)^\top]$ [31], which can be updated as $\mathbf{P}^k = (I - \mathbf{K}^k\mathbf{H}_{aug})\mathbf{P}^{k-}$. Note that I is the identity matrix. The iteration continues until the mean of the diagonal values in $\mathbf{P}^k$, i.e., the estimate error variances, is less than a convergence parameter ν.

Third, the system operator examines bias estimates $\hat{b}_i^\phi$ (for any $i \in [1, n], \phi \in [1, 3]$) and determines that users with $\hat{b}_i^\phi$ greater than a parameter ϵ are energy thieves. This parameter ϵ is set to a multiple of the standard deviation of the largest bias estimate error, i.e.,

$$\epsilon = s \times \max_{i,\phi} \mathbf{Var}\left[b_i^\phi - \hat{b}_i^\phi\right]^{1/2} \tag{18}$$

where s is a positive integer, and $\max_{i,\phi}\mathbf{Var}[b_i^\phi - \hat{b}_i^\phi]$ is the maximum of the values in the diagonal of $\mathbf{P}^k$ that correspond to bias estimates.

B. Privacy-Preserving Bias Estimation

Although we can find energy users' biases ($\mathbf{b}_i$'s) and identify energy thieves using the previous SEK algorithm, the system operator needs to obtain energy users' load current and voltage measurements as shown in (17), which is a serious breach to their privacy. In the following, we develop a privacy-preserving bias estimation algorithm called PPBE, that can find energy thieves while preserving users' privacy. In particular, the proposed algorithm protects users' measurements and state estimates from the system operator and other users in the MG. Our main idea is to privately estimate $\mathbf{b}^k$ ($\forall k$) by decomposing the previous Kalman filter into two parallel and loosely coupled filters. One filter, oblivious to the biases, estimates the state variable vector, while the other filter estimates the bias vector. We call them the bias-ignorant filter and the bias filter, respectively. The smart meter network computes the bias-ignorant filter in a private and distributed manner, while the MG operator, based on the bias-ignorant filter's residuals, carries out the bias filter.

Denote by $\mathbf{z}^k$ the state variable vector of the substation's voltage and line segment currents at time k, i.e., $\mathbf{z}^k = [\mathbf{V}_0^k\ \mathbf{I}_1^k\ \mathbf{I}_2^k\ \ldots\ \mathbf{I}_n^k]^\top$, and by $\mathbf{b}^k$ the measurement bias vector at time k, i.e., $\mathbf{b}^k = [\mathbf{b}_1^k\ \mathbf{b}_2^k\ \ldots\ \mathbf{b}_n^k]^\top$. Similar to that in our SEK algorithm, the state $\mathbf{z}^k$ has the following dynamics:

$$\mathbf{z}^k = \mathbf{z}^{k-1} + \mathbf{v}^{k-1} \tag{19}$$

where $\mathbf{v}^k$ is zero-mean white process noise with constant covariance matrix $\tilde{\mathbf{Q}}$. Besides, we assume that the bias vector is independent of the state vector and a constant,[1] i.e., $\mathbf{b}^k = \mathbf{b}^{k-1}$.

Thus, the measurement vector can be modeled as

$$\mathbf{y}^k = \mathbf{H}^k\mathbf{z}^k + \mathbf{C}^k\mathbf{b}^k + \mathbf{e}^k \tag{20}$$

where $\mathbf{e}^k$ is zero-mean white measurement noise with constant covariance matrix $\tilde{\mathbf{R}}$. Note that the first component is bias-ignorant while the second component is only related to

[1]Note that we can sample the measurements at a high frequency. Thus, the sampled data in a short period can be used for conducting the proposed algorithm, during which the bias vector remains a constant.

biases. Besides, $\mathbf{H}^k$ is the Jacobian matrix of $\mathbf{y}^k$ regarding $\mathbf{z}^k$, i.e.,

$$\mathbf{H}^k = \begin{pmatrix} \frac{\partial \mathbf{V'}_0}{\partial \mathbf{V}_0} & 0 & \cdots & \cdots & 0 \\ 0 & \frac{\partial \mathbf{I'}_1}{\partial \mathbf{I}_1} & \cdots & \cdots & 0 \\ \hline \frac{\partial \mathbf{L'}_1}{\partial \mathbf{V}_0} & \frac{\partial \mathbf{L'}_1}{\partial \mathbf{I}_1} & \frac{\partial \mathbf{L'}_1}{\partial \mathbf{I}_2} & \cdots & \frac{\partial \mathbf{L'}_1}{\partial \mathbf{I}_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{\partial \mathbf{L'}_n}{\partial \mathbf{V}_0} & \frac{\partial \mathbf{L'}_n}{\partial \mathbf{I}_1} & \cdots & \cdots & \frac{\partial \mathbf{L'}_n}{\partial \mathbf{I}_n} \\ \hline \frac{\partial \mathbf{V'}_1}{\partial \mathbf{V}_0} & \frac{\partial \mathbf{V'}_1}{\partial \mathbf{I}_1} & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{\partial \mathbf{V'}_n}{\partial \mathbf{V}_0} & \frac{\partial \mathbf{V'}_n}{\partial \mathbf{I}_1} & \frac{\partial \mathbf{V'}_n}{\partial \mathbf{I}_2} & \cdots & \frac{\partial \mathbf{V'}_n}{\partial \mathbf{I}_n} \end{pmatrix}.$$

The first two rows correspond to $\mathbf{I}_0$ and $\mathbf{V}_0$, while the rest of the elements are that same as those defined in (12) and (14). In addition, $\mathbf{C}^k$ is as follows:

$$\mathbf{C}^k = \begin{bmatrix} 0 & \cdots & 0 \\ 0 & \cdots & 0 \\ \frac{\partial \mathbf{L'}_1}{\partial \mathbf{b}_1} & \cdots & 0 \\ \vdots & \vdots & \vdots \\ 0 & \cdots & \frac{\partial \mathbf{L'}_n}{\partial \mathbf{b}_n} \\ \frac{\partial \mathbf{V'}_1}{\partial \mathbf{b}_1} & \cdots & 0 \\ \vdots & \vdots & \vdots \\ 0 & \cdots & \frac{\partial \mathbf{V'}_n}{\partial \mathbf{b}_n} \end{bmatrix}$$

whose elements are defined in (13) and (15). In the following, we drop the time index from $\mathbf{H}^k$ and $\mathbf{C}^k$ because they are constant.

1) Bias-Ignorant Filter: The bias-ignorant filter is based on the Kalman filter. In particular, the bias-ignorant filter estimates line segment currents $\mathbf{z}^k$ that evolve according to the stochastic difference equation (19) and assumes measurements (20) are bias-free, i.e., $\mathbf{C} = \mathbf{0}$. The noise processes $\mathbf{v}^k$ and $\mathbf{e}^k$ are assumed to be independent of each other.

Specifically, the bias-ignorant filter first initializes by randomly selecting $\mathbf{z}^0$, setting $\hat{\mathbf{z}}^0 = \mathbb{E}[\mathbf{z}^0]$, and the initial estimate error covariance matrix $\tilde{\mathbf{P}}^0$ to a large symmetric matrix.

Then, the bias-ignorant filter recursively computes the time updates and measurement updates. In particular, the filter predicts the state at time k, i.e., $\hat{\mathbf{z}}^{k-} = \hat{\mathbf{z}}^{k-1}$, and then adjusts the prediction using the measurements at time k as follows:

$$\hat{\mathbf{z}}^k = \hat{\mathbf{z}}^{k-} + \tilde{\mathbf{K}}^k \mathbf{r}^k \tag{21}$$

where $\mathbf{r}^k = \mathbf{y}^k - \mathbf{H}\hat{\mathbf{z}}^{k-1}$ is the measurement residual vector, and the bias-ignorant gain matrix $\tilde{\mathbf{K}}^k$ is

$$\tilde{\mathbf{K}}^k = \tilde{\mathbf{P}}^{k-}\mathbf{H}^\top(\mathbf{H}\tilde{\mathbf{P}}^{k-}\mathbf{H}^\top\mathbf{R})^{-1}. \tag{22}$$

Besides, the bias-ignorant error covariance matrix $\tilde{\mathbf{P}}^k$ is updated as follows:

$$\tilde{\mathbf{P}}^k = (\boldsymbol{I} - \tilde{\mathbf{K}}^k\mathbf{H})\tilde{\mathbf{P}}^{k-} \tag{23}$$

where $\tilde{\mathbf{P}}^{k-} = \tilde{\mathbf{P}}^{k-1} + \tilde{\mathbf{Q}}$. The bias-ignorant filter ends when the mean of the diagonal values of $\tilde{\mathbf{P}}^k$ is less than the convergence parameter ν.

Note that according to the above, each smart meter i would need to obtain estimates $\hat{z}_j^{k-1}$'s from all the other smart meters to calculate residuals r_i^k. Directly sharing such data in plaintext with other smart meters could compromise users' privacy. In particular, recall that all the smart meters know the measurement matrix $\mathbf{H}$, and as we will explain in the following section, the system operator receives $\mathbf{r}^k$ to find bias estimates. Thus, a threatening entity may obtain users' private power consumption by first solving for $\mathbf{y}^k$ in the residual, i.e., $\mathbf{y}^k = \mathbf{r}^k + \mathbf{H}\hat{\mathbf{z}}^{k-1}$, and then using the result to calculate $\mathbf{P}_i + j\mathbf{Q}_i$ in (6). Therefore, in the following we design a private vector multiplication scheme, which encrypts and aggregates privacy-sensitive data and allows each smart meter i to compute or update $\hat{z}_i^k$, r_i^k, and r_{i+n}^k by itself without knowing other smart meters' private data.

Specifically, notice that smart meter i needs to compute the residuals shown as follows:

$$r_q^k = y_q^k - \sum_{j\in\mathcal{I}} h_{q,j}\hat{z}_j^{k-1} \quad \text{for } q = i, i+n \tag{24}$$

where $q = i, i+n$ indicates that smart meter i computes the residuals for its current and voltage measurements, respectively. In the second term of (24), we can see that smart meter i needs to aggregate the weighted elements of $\hat{\mathbf{z}}_{k-1}$. In order to protect users' privacy, we need to keep each bias-ignorant estimate $\hat{z}_i^k$ known to smart meter i only.

Denote the second term in (24) by $t_q^k = \sum_{j\in\mathcal{I}} h_{q,j}\hat{z}_j^{k-1}$ for $q = i, i+n$. To prevent smart meter i from knowing smart meter j's private data $\hat{z}_j^k$, we let smart meter j locally compute $f_j^k = h_{i,j}\hat{z}_j^k$, and encrypt it for transmissions, i.e., $E_i(f_j^k) = E_i(h_{i,j}\hat{z}_j)$, where $E_i(\cdot)$ denotes Paillier encryption with smart meter i's public key. However, transmitting $E_i(f_j)$ directly to smart meter i would still reveal $\hat{z}_j^k$ because $\mathbf{H}$ is known to all smart meters. Thus, we conduct an in-network aggregation as in [19].

In particular, the MG operator's network device, i.e., smart meter 0, acts as the aggregator and computes t_q^k $(q = i, i+n)$ for each smart meter i. It works as follows. Smart meter 0 first builds a logical binary tree of smart meters as shown in Fig. 3, with itself being the root. Then, it instructs each smart meter j to collect its children nodes' (say, smart meters j^a and j^b) aggregated data, say $E_i(c_{j^a}^k)$ and $E_i(c_{j^b}^k)$, and multiply them with its own $E_i(f_j^k)$. Particularly, smart meter j's aggregated data encrypted with smart meter i's public key, denoted by $E_i(c_j^k)$, can be obtained according to the properties of Paillier encryption, i.e.,

$$\begin{aligned} E_i\left(c_j^k\right) &= E_i\left(f_j^k\right) \cdot E_i\left(c_{j^a}^k\right) \cdot E_i\left(c_{j^b}^k\right) \\ &= E_i\left(f_j^k + c_{j^a}^k + c_{j^b}^k\right). \end{aligned}$$

Notice that if smart meters j^a and j^b are leaf nodes, then we have $c_{j^a}^k = f_{j^a}^k$ and $c_{j^b}^k = f_{j^b}^k$. To prevent smart meter i from knowing its children nodes' private data when any of them is a leaf node in the binary tree, we always let one of smart meter i's children nodes send its data, say $E_i(c_{i^a}^k)$, to the other, who computes $E_i(c_{i^a}^k)\cdot E_i(c_{i^b}^k)$ and sends it to smart meter i. Smart meter i simply forwards its children's aggregated data to its parent

node without incorporating its own data. The last aggregation is done by smart meter 0, which then transmits $E_i(c_0^k)$ to smart meter i, who decrypts $E_i(c_0^k)$ and computes $t_q = h_{q,i}\hat{z}_i^{k-1} + c_0^k$.

Finally, after obtaining t_q, smart meter i can compute the residuals r_q^k for $q = i, i+n$ locally, i.e., $r_q^k = y_q^k - t_q^k$, and update $\hat{z}^k$. It also transmits r_q^k to the MG operator so that it can estimate the bias vector through a bias filter, which will be introduced next.

2) Bias Filter: Friedland [32] showed that the bias estimate can be conducted separately from the bias-ignorant state estimate by employing a Kalman-like filter and using bias-ignorant measurement residuals $\mathbf{r}^k$ as follows:

$$\mathbf{V}^k = [\mathbf{I} - \tilde{\mathbf{K}}^k\mathbf{H}]\mathbf{V}^{k-1}$$
$$\hat{\mathbf{b}}^k = [\mathbf{I} - \bar{\mathbf{K}}^k\mathbf{S}^k]\hat{\mathbf{b}}^{k-1} + \bar{\mathbf{K}}^k\mathbf{r}^k$$

where $\mathbf{V}^0$ is set to a zero matrix, $\mathbf{S}^k = \mathbf{H}\mathbf{V}^k + \mathbf{C}$, the bias filter's gain matrix is $\bar{\mathbf{K}}^k = \mathbf{M}^k[(\mathbf{V}^k)^\top(\mathbf{H})^\top + \mathbf{C}]\mathbf{R}^{-1}$, and matrix $\mathbf{M}^k$ is

$$\mathbf{M}^k = \mathbf{M}^{k-1} - \mathbf{M}^{k-1}(\mathbf{S}^{k-1})^\top \cdot \left[\mathbf{H}\mathbf{P}^k\mathbf{H}^\top + \mathbf{R} + \mathbf{S}^k\mathbf{M}^{k-1}(\mathbf{S}^k)^\top\right]^{-1}\mathbf{S}^k\mathbf{M}^{k-1}$$

where $\mathbf{M}^0$ is set to a large symmetric matrix, analogously to $\tilde{\mathbf{P}}^0$.

The MG operator may compute the bias-ignorant filter's gain matrix $\tilde{\mathbf{K}}^k$ as shown in (22). Besides, the MG operator can compute $\mathbf{P}^k$ in the same way as for SEK in Section III-A and set the same threshold ϵ as in (18).

To summarize, the PPBE algorithm is carried out by the network of smart meters and the MG operator as follows. First, smart meters take voltage and load current measurements to form the vector $\mathbf{y}^0$, and initialize their local state estimates $\hat{z}_i^0$'s. The MG operator initializes the matrices $\tilde{\mathbf{P}}^0$ and transmits the ith row of $\tilde{\mathbf{K}}^1$ to smart meter i. Then, the smart meters find the residuals $\mathbf{r}^1$ and the bias-ignorant current estimates $\hat{\mathbf{z}}^1$, and transmit the residuals to the MG operator. After that, the MG operator finds the bias estimates $\mathbf{b}^1$, and updates the gain matrix $\tilde{\mathbf{P}}^{1-}$. The iteration continues until the mean of the diagonal values of $\tilde{\mathbf{P}}^k$ is less than a convergence parameter ν.

C. Convergence of SEK and PPBE

Notice that in the proposed SEK and PPBE algorithms, the state vector, i.e., the voltage at the substation, line segment currents, and biases, are assumed to remain constant before the algorithms finish. We contend that this is reasonable. In particular, as will be shown in the simulations, the PPBE (SEK) algorithm converges in as few as 5 ($<$200) iterations in IEEE 13-bus and IEEE 123-bus test systems, which only needs the measurements in 5 ($<$200) s given that the smart meters can take measurements once per second as shown in [33], [34]. It is fair to assume that the state vector is constant during this period, since real-world data collected from individual users in [33] and [34] shows that power demand remains constant for up to 2 min, and some works like [35] assume that the voltages and currents remain constants for up to 10 min. Moreover, although we exploit the capabilities of smart meters to take real-time measurements, the proposed algorithms are not required to be carried out in real-time. To be more prominent, if the communication network is congested, the MG operator may instruct the smart meters to take measurements and defer the computation of the proposed algorithms to a later time with less data traffic.

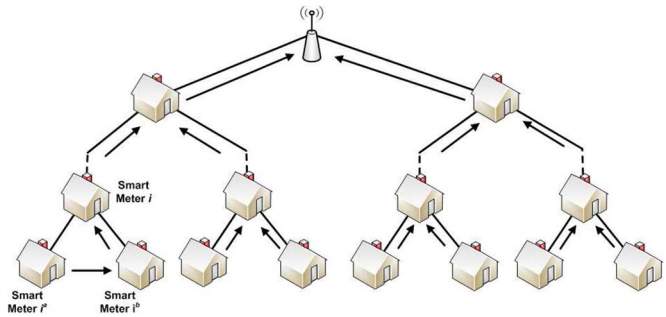


Fig. 3. Example of a logical binary tree for residual update.

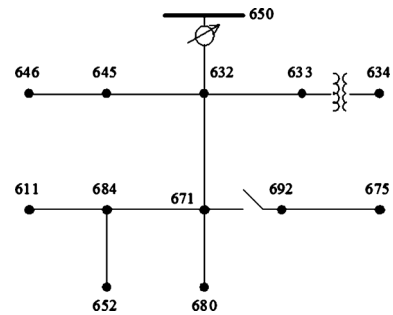


Fig. 4. IEEE 13-bus test system.

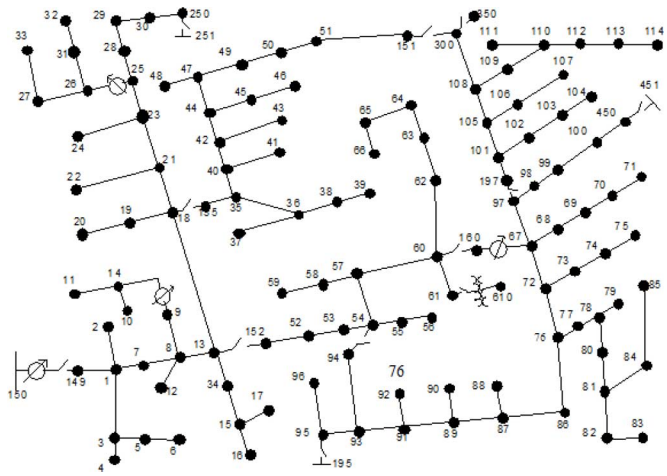


Fig. 5. IEEE 123-bus test system.

IV. Privacy Analysis

As described in the threat model, there could be three entities which may compromise users' privacy: the MG operator, compromised smart meters, and eavesdroppers. In this section, we analyze how each of the threatening entities may attempt to obtain users' private information, including their load current and voltage measurements, and how our privacy-preserving energy theft algorithm prevents such attacks.

The MG Operator: according to our privacy-preserving energy theft detection algorithm in Section III-B, the MG operator receives the residual vector $\mathbf{r}^k$ from the smart meters. Recall that it can try to recover users' measurements by calculating

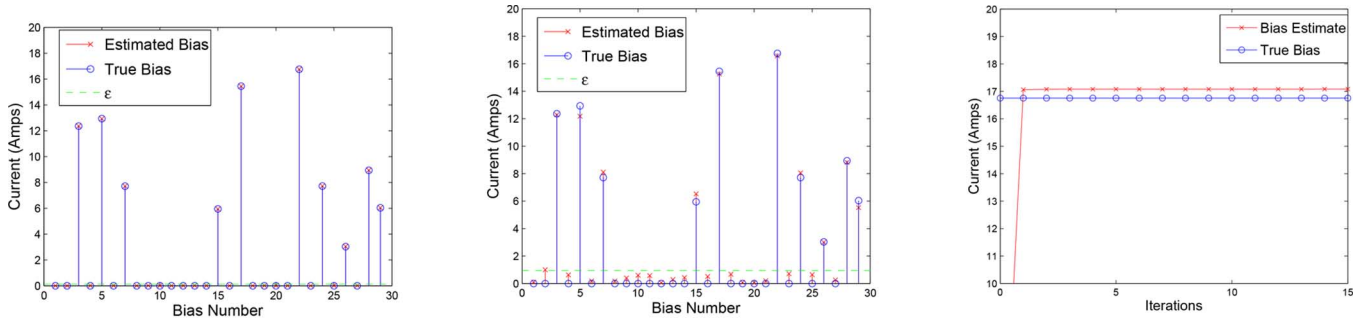


Fig. 6. Energy theft detection in the IEEE 13-bus system using SEK. (a) Bias estimation using SEK under $\sigma_l = 10^{-4}$. (b) Bias estimation using SEK under $\sigma_l = 10^{-2}$. (c) Estimate of bias 22 ($n = 8$, $\phi = 1$) using SEK under $\sigma_l = 10^{-2}$.

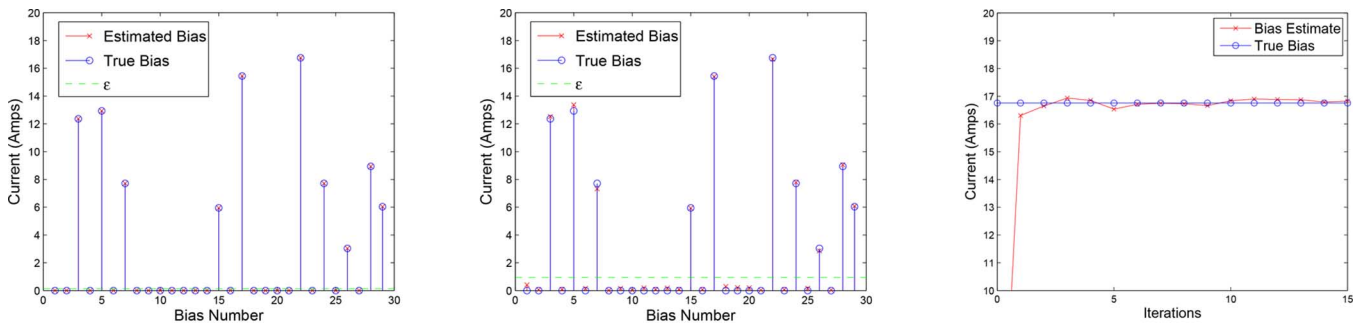


Fig. 7. Energy theft detection in the IEEE 13-bus system using PPBE. (a) Bias estimation using PPBE under $\sigma_l = 10^{-4}$. (b) Bias estimation using PPBE under $\sigma_l = 10^{-2}$. (c) Estimate of bias 22 ($n = 8$, $\phi = 1$) using PPBE under $\sigma_l = 10^{-2}$.

$\mathbf{y}^k = \mathbf{H}\hat{\mathbf{z}}^{k-1} + \mathbf{r}^k$. However, although the MG operator knows $\mathbf{H}$ and $\mathbf{r}^k$, it does not know $\hat{\mathbf{z}}^{k-1}$ and hence cannot obtain $\mathbf{y}^k$. Besides, although the MG operator employs the bias filter to get the bias estimate $\mathbf{b}^k$, it can only learn whether a user is honest or not. It cannot infer any users' private energy consumption data $\mathbf{y}^k$ or $\mathbf{z}^k$ from $\mathbf{b}^k$.

Smart Meters: notice that in the bias ignorant filter, smart meter j needs to transmit its bias-ignorant state estimate multiplied by the corresponding elements of the system matrix, i.e., $h_{q,j}\hat{z}_j^{k-1}$ for $q = i, i+n$, to the MG operator's network device for smart meter i's aggregation. Since such data is encrypted by smart meter i's public key and aggregated in the network, any other smart meter cannot know $\sum_{j\in\mathcal{I}} h_{q,j}\hat{z}_j^{k-1}$ in (24). Thus, even if any other smart meter knows r_q^k, it cannot figure out y_q^k $(q = i, i+n)$ using (24).

Eavesdroppers: similarly, even if some eavesdroppers can overhear all the communications in the system, they would only know $\mathbf{H}$ and $\mathbf{r}^k$, and thus cannot obtain users' private data $\mathbf{y}^k$ or $\mathbf{z}^k$.

V. Simulation Results

In this section, we evaluate the performances of our proposed SEK and PPBE algorithms. We analyze their success rates, which we define as the ratio of the number of users correctly identified as thieves or honest users to the total number of users in the system, and the convergence performances under different measurement error standard deviations. We also study the impact of line impedance uncertainty on the success rates of our proposed PPBE algorithm.

In our simulations, we employ our algorithms to find energy thieves in the IEEE 13-bus and the IEEE 123-bus distribution test systems shown in Figs. 4 and 5, respectively [36]. In the IEEE 13-bus system, we ignore the voltage regulator between buses 632 and 650, and consider the switch between buses 671 and 692 to be closed. In the IEEE 123-bus system, we also ignore the voltage regulators and consider closed switches between buses 150–149, 13–152, 54–94, and 18–135. Both systems are radial networks with unbalanced loads, which makes them realistic scenarios for a microgrid. To generate the true state of the system, we calculate load currents, line currents, and bus voltages using the ladder iterative technique in [25]. We then generate for each bus the three-phase load current and three-phase voltage measurements, with biases and random errors. Note that modern smart meters, such as the one in [22], take very accurate measurements, whose errors are usually modeled by white uncorrelated noise with zero mean and standard deviation on the order of 10^{-4} [11], [37], [38]. However, to further validate our algorithms, we test them with current and voltage measurement error standard deviations ranging from $\sigma_l = 10^{-4}$ to $\sigma_l = 10^{-2}$ for $l = 0, \ldots, 6n+5$, which have units of Amperes and Volts, respectively.

Besides, the probability of a user bus having a non-zero measurement bias on any of its phases, i.e., the probability of a user deciding to steal energy, is set to 0.3. Each energy thief's measurement bias magnitude is uniformly chosen from the interval $[3, 20]A$ and has the same angle as its corresponding phase. The substation measurements have zero biases with probability 1. Finally, we omit certain bias estimates of users

TABLE I
PERFORMANCE OF SEK AND PPBE IN THE IEEE 13-BUS SYSTEM

	IEEE 13-bus test system			
	Iterations		Success Rate	
σ_l	SEK	PPBE	SEK	PPBE
10^{-4}	2	2	1.00	1.00
10^{-3}	5	2	1.00	1.00
10^{-2}	35	4	0.99	0.99

who are connected to less than three phases. Moreover, we set the bias threshold $\epsilon = s \times \max_{i,\phi} \mathbf{Var}[b_i^\phi - \hat{b}_i^\phi]^{1/2}$ by choosing $s = 4$, set the convergence parameter $\nu = 0.05$, and initialize some matrices like $\mathbf{P}^0 = \tilde{\mathbf{P}}^0 = 1 \times 10^3 I$ and $\mathbf{M}^0 = 2 \times 10^6 I$ for both systems.

A. IEEE 13-Bus Test System

SEK: Fig. 6(a) and (b) compares bias estimates obtained by one run of the SEK algorithm to their true values, for all users and all phases when the measurement error standard deviation is equal to 10^{-4} and 10^{-2}, respectively. When $\sigma_l = 10^{-4}$, it is clear that the estimated biases closely correspond to the true values. Moreover, the threshold ϵ correctly differentiates energy thieves from honest users, i.e., the bias estimates for honest users are smaller than ϵ while the bias estimates for energy thieves are larger than ϵ. In the case of $\sigma_l = 10^{-2}$, we observe that the threshold ϵ is larger due to the increased error estimation variance and that estimates start to deviate from their true values. We also show in Fig. 6(c) the convergence of the bias estimate for user 8, phase 1 under a measurement error standard deviation of 10^{-2}. In this case, we can see that the bias estimate converges to a different value.

Besides, as shown in Table I, we find that the SEK has a high success rate under all measurement error standard deviation values. Note that the results in Table I are obtained by averaging the results of 100 runs. In particular, SEK has a success rate of 1.00 when σ_l equals 10^{-4} and 10^{-3}, and 0.99 when $\sigma_l = 10^{-2}$. Table I also presents the average number of iterations that it takes SEK to converge. As expected, SEK converges faster under lower standard deviation values.

PPBE: In Fig. 7(a) and (b), we show the bias estimates of one run of the PPBE algorithm along with the true bias values, when the measurement error standard deviation is equal to 10^{-4} and 10^{-2}, respectively. In the case of $\sigma_l = 10^{-4}$, we observe that the PPBE algorithm can identify the energy thieves successfully and its estimates are very accurate. In the case of $\sigma_l = 10^{-2}$, in contrast to the SEK algorithm, we can see that the bias estimates of PPBE are still very close to their true values. In fact, from Table I we can see that the PPBE algorithm has a success rate of 1.0 under 10^{-4} and 10^{-3} standard deviation values, and 0.99 under a standard deviation of 10^{-2}.

Moreover, we present the convergence of the bias estimate for user 8, phase 1 in Fig. 7(c) under a measurement error standard deviation of 10^{-2}, which is more accurate than that in Fig. 6(c). In addition, Table I shows that the PPBE algorithm is capable of converging in 4 iterations when $\sigma_l = 10^{-2}$, which is much faster than SEK. We also find that PPBE can converge in as few as 2 iterations when the measurement error standard deviation is low, i.e., 10^{-4}.

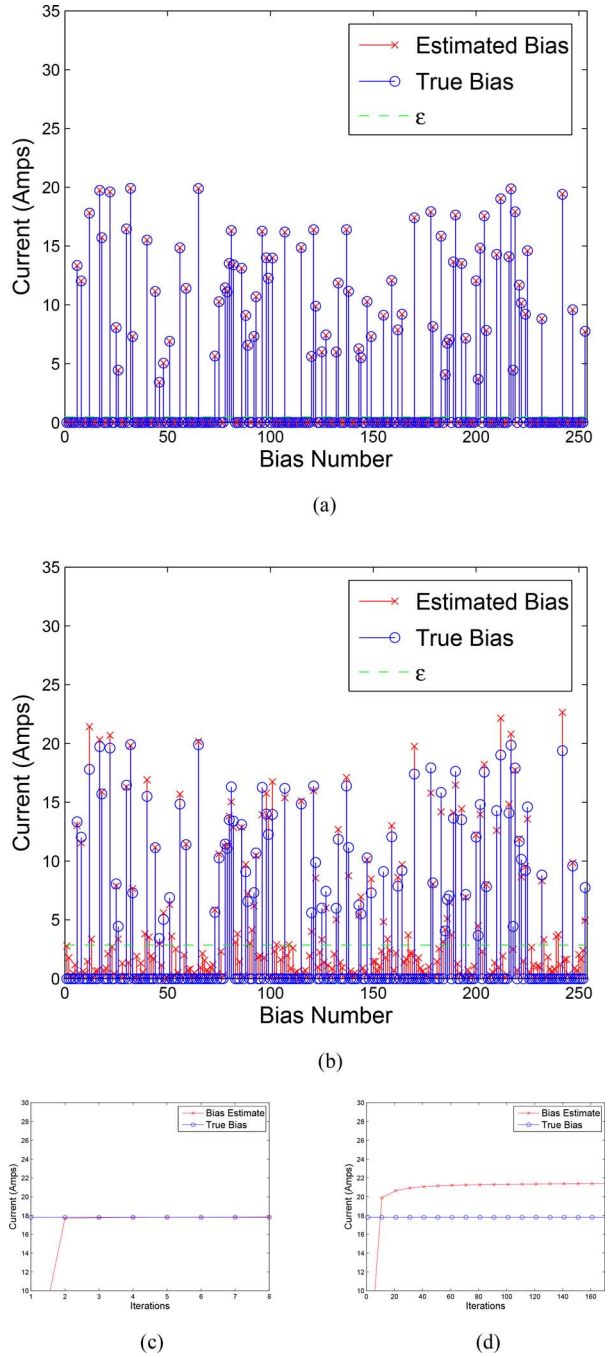


Fig. 8. Energy theft detection in the IEEE 123-bus system using SEK. (a) Bias estimation using SEK under $\sigma_l = 10^{-4}$. (b) Bias estimation using SEK under $\sigma_l = 10^{-2}$. (c) Estimate of bias 12 ($n = 4$, $\phi = 3$) using SEK under $\sigma_l = 10^{-4}$, (d) Estimate of bias 12 ($n = 4$, $\phi = 3$) using SEK under $\sigma_l = 10^{-2}$.

B. IEEE 123-Bus Test System

SEK: Fig. 8(a) and (b) compares the bias estimates of the SEK algorithm to their true values, when the measurement error standard deviation is equal to 10^{-4} and 10^{-2}, respectively. We observe that the SEK algorithm offers high success rates, but its performance degrades when the measurement error standard deviation is 10^{-2}. In Fig. 8(c) and (d), we find that the estimated bias converges quickly and very close to its true value when $\sigma_l = 10^{-4}$, but converges slowly to a different value than its value when $\sigma_l = 10^{-2}$.

TABLE II
PERFORMANCE OF SEK AND PPBE IN THE IEEE 123-BUS SYSTEM

	IEEE 123-bus test system			
	Iterations		Success Rate	
σ_l	SEK	PPBE	SEK	PPBE
10^{-4}	3	2	1.00	1.00
10^{-3}	20	2	1.00	1.00
10^{-2}	184	5	0.94	0.99

Besides, from Table II, we can see that the SEK algorithm converges in 3 iterations when $\sigma_l = 10^{-4}$ and 184 iterations when $\sigma_l = 10^{-2}$, respectively.

PPBE: In Fig. 9(a) and (b), we show the bias estimates obtained by PPBE and compare them to their true values under measurement error standard deviations of 10^{-4} and 10^{-2}, respectively. We can see that in both cases the success rates are high. Fig. 9(c) and (d) show the bias estimate for user 4, phase 3 when the measurement error standard deviation is equal to 10^{-4} and 10^{-2}, respectively. We observe that the bias estimate quickly converges closely to its true value in both cases.

Besides, from Table II, we can see that the PPBE algorithm has very high success rates and converges quickly in all the cases, which demonstrates its efficiency and practicality.

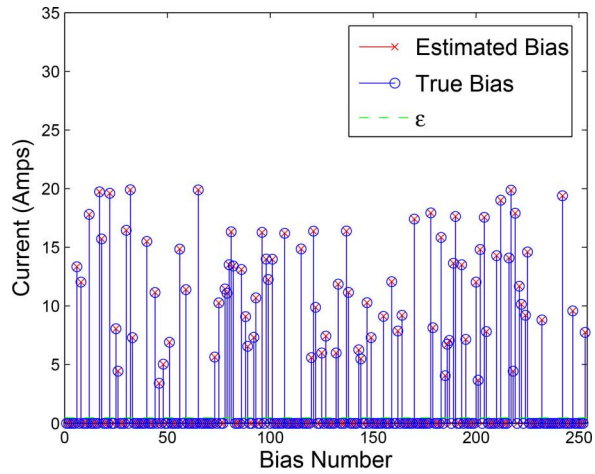
In addition, we note that PPBE is capable of finding bias estimates more accurately and more efficiently due to the fact that it involves matrices of smaller sizes in its computations than SEK, which reduces the number of round-off errors and increases numerical stability.

C. Impact of System Parameter Uncertainty

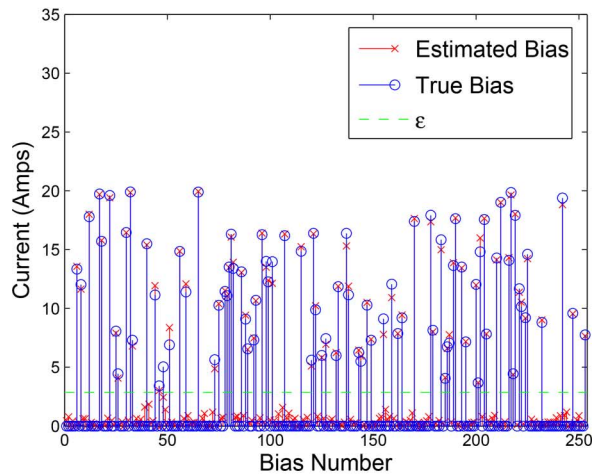
Although very accurate system parameters can be obtained [26], [27], temperature changes in the environment and other inaccuracies may lead to uncertainty in our distribution system parameters, e.g., power line impedances. To investigate the performance of our algorithms under system parameter uncertainty, we add white uncorrelated noise, which has zero mean and standard deviation proportional to an error bound, to the nominal power line impedances. Specifically, for a given error bound $0 \leq \rho \leq 1$, we set the standard deviations for resistance and reactance values to $\sigma_p^R = (1/3) \times \rho \times \mathcal{R}e(\mathbf{Z}_{p',p})$, $\sigma_p^X = (1/3) \times \rho \times \mathcal{I}m(\mathbf{Z}_{p',p})$ for $p = 1, \ldots n$, respectively. These choices of σ_p^R and σ_p^X result in random errors that are at most ρ percent of the nominal impedance values with a high probability of 99.7% according to the 68-95-99.7 rule. We notice that a typical error bound for line parameter uncertainty in power systems is $\rho = 2\%$ [39]. Furthermore, considering that temperature changes may cause deviations greater than 2% of the nominal resistance values, we test our algorithms with σ_p^R accounting for temperature changes of up to 30°C, as summarized in Table III, and setting $\rho = 2\%$ for σ_p^X. In particular, the resistance of a conductor as a function of temperature can be approximated with the following formula [40]:

$$R = R_0(1 + \beta \cdot \Delta T)$$

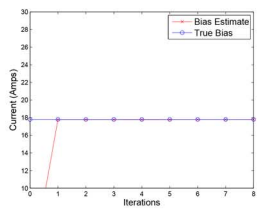
where R_0 is the nominal impedance, $\Delta T = T_0 - T$ is the change in temperature, and β is the thermal coefficient. Usually, the nominal temperature, T_0, is set to 20°C. Assuming copper conductors, we have $\beta = 3.9 \times 10^{-3}$ and hence set $\rho = \Delta R = \beta \Delta T$.



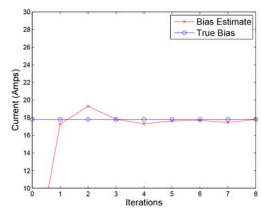
(a)



(b)



(c)



(d)

Fig. 9. Energy theft detection in the IEEE 123-bus system using PPBE. (a) Bias estimation using PPBE under $\sigma_l = 10^{-4}$. (b) Bias estimation using PPBE under $\sigma_l = 10^{-2}$. (c) Estimate of bias 12 ($n = 4$, $\phi = 3$) using PPBE under $\sigma_l = 10^{-4}$. (d) Estimate of bias 12 ($n = 4$, $\phi = 3$) using PPBE under $\sigma_l = 10^{-2}$.

TABLE III
CHANGES IN THE RESISTANCE OF COPPER DUE TO TEMPERATURE CHANGES

$\mathbf{\Delta T}$ $(^\circ C)$	$\mathbf{\Delta R}(\%)$	$\sigma_{\mathbf{p}}^{\mathbf{R}}$
5	2.0	$6.7 \times 10^{-3} \times \mathcal{R}e(\mathbf{Z}_{p',p})$
10	3.9	$13 \times 10^{-3} \times \mathcal{R}e(\mathbf{Z}_{p',p})$
20	7.8	$26 \times 10^{-3} \times \mathcal{R}e(\mathbf{Z}_{p',p})$
25	9.7	$32 \times 10^{-3} \times \mathcal{R}e(\mathbf{Z}_{p',p})$
30	11.7	$39 \times 10^{-3} \times \mathcal{R}e(\mathbf{Z}_{p',p})$

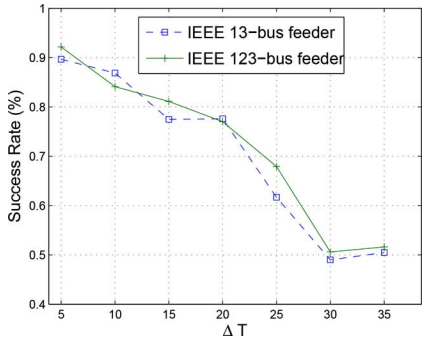


Fig. 10. Success rate of PPBE under system parameter uncertainty.

To study the impact of system parameter uncertainty on the success rate of the PPBE algorithm, we run the algorithm for different values of σ_p^R when $\sigma_l = 10^{-2}$, and measure its success rate. We set $s = 10$ to account for temperature changes that were not considered in the original computation of threshold ϵ. The results are plotted in Fig. 10. Specifically, we observe that the PPBE algorithm can identify energy thieves with a success rate of about 0.9 when the uncertainty bound is 2%. Therefore, the PPBE algorithm is very robust to typical line impedance uncertainties due to temperature changes ($\Delta T = 5°$C). Besides, the success rate of PPBE remains above 0.75 when the uncertainty bound of the resistance is 7.8% ($\Delta T = 20°$C), and drops to 0.5 when the uncertainty bound of the resistance is 11.7% ($\Delta T = 30°$C).

VI. Conclusion

In this paper, we have investigated energy theft detection in microgrids, considering a realistic model for the microgrid's power system and the protection of users' privacy. We have proposed two energy theft detection algorithms capable of successfully identifying energy thieves. One algorithm called SEK employs a centralized Kalman filter but cannot protect users' privacy and does not have very good numerical stability in large systems with high measurement errors. The other one called PPBE is based on two loosely coupled filters, and can preserve users' privacy by hiding their energy measurements from the system operator, other users, and eavesdroppers. We have finally validated the proposed algorithms through privacy analysis and extensive simulations. Noticeably, PPBE can converge much faster and have much better numerical stability than SEK. We also find that the PPBE algorithm has good performance under system parameter uncertainty. We leave for future work the design of a robust algorithm that can provide theoretical performance guarantee under line impedance uncertainty.

References

[1] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77, May–Jun. 2009.

[2] G. Bellett, "Pot growers stealing $100 m worth of power: B.C. Hydro," *Edmonton J.* 2010 [Online]. Available: http://www2.canada.com/edmontonjournal/news/story.html?id=0d0332f0-b8c8-42f1-a9a2-696728dbae57

[3] J. Smith, Smart Meters Take Bite Out of Electricity Theft, 2011 [Online]. Available: http://news.nationalgeographic.com/news/energy/2011/09/110913-smart-meters-for-electricity-theft/

[4] P. Kelly-Detwiler, Electricity Theft: A Bigger Issue Than You Think, 2013 [Online]. Available: http://www.forbes.com/sites/peterdetwiler/2013/04/23/electricity-theft-a-bigger-issue-than-you-think/

[5] B. Krebs, FBI: Smart Meter Hacks Likely to Spread, 2012 [Online]. Available: http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/

[6] H. Rosenbaum, Danville Utilities Sees Increase in Meter Tampering, 2012 [Online]. Available: http://www.wset.com/story/20442252/danville-utilities-sees-increase-in-meter-tampering

[7] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, "A multi-sensor energy theft detection framework for advanced metering infrastructures," *IEEE J. Select. Areas Commun.*, vol. 31, no. 7, pp. 1319–1330, Jul. 2013.

[8] A. Cárdenas, S. Amin, G. Schwartz, R. Dong, and S. Sastry, "A game theory model for electricity theft detection and privacy-aware control in AMI systems," in *Proc. 15th Annu. Conf. Communication, Control, and Computing*, Allerton, IL, USA, 2012, pp. 1830–1837.

[9] D. Mashima and A. A. Cárdenas, "Evaluating electricity theft detectors in smart grid networks," in *Proc. 15th Int. Conf. Research in Attacks, Intrusions, and Defenses*, Amsterdam, The Netherlands, 2012.

[10] L. Pereira, L. Afonso, J. Papa, Z. Vale, C. Ramos, D. Gastaldello, and A. Souza, "Multilayer perceptron neural networks training through charged system search and its application for non-technical losses detection," in *Proc. IEEE Conf. Innovative Smart Grid Technologies Latin America (ISGT LA)*, Apr. 2013, pp. 1–6.

[11] S.-C. Huang, Y.-L. Lo, and C.-N. Lu, "Non-technical loss detection using state estimation and analysis of variance," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 2959–2966, Aug. 2013.

[12] S. Weckx, C. Gonzalez, J. Tant, T. De Rybel, and J. Driesen, "Parameter identification of unknown radial grids for theft detection," in *Proc. Innovative Smart Grid Technologies (ISGT Europe)*, Berlin, Germany, 2012.

[13] S. Salinas, W. Liao, C. Luo, and P. Li, "State estimation for energy theft detection in microgrids," in *Proc. Int. ICST Conf. Communications and Networking in China (CHINACOM)*, Maoming, China, Aug. 2014.

[14] N. I. of Standards and Technology, "Privacy and the smart grid," NIST Guidelines for Smart Grid Cyber Security, Aug. 2010, vol. 2 [Online]. Available: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

[15] E. L. Quinn, "Privacy and the new energy infrastructure," pp. 1995–2008, 2009 [Online]. Available: http://ssrn.com/paper=1370731

[16] U. D. of Energy, Data Access and Privacy Issues Related too Smart Grid Technologies, 2010 [Online]. Available: http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf

[17] Y. Kim, E. Ngai, and M. Srivastava, "Cooperative state estimation for preserving privacy of user behaviors in smart grid," in *Proc. IEEE Int. Conf. Smart Grid Communications (SmartGridComm)*, Brussels, Belgium, 2011, pp. 178–183.

[18] F. Li and B. Luo, "Preserving data integrity for smart grid data aggregation," in *Proc. IEEE Int. Conf. Smart Grid Communications (SmartGridComm)*, Tainan City, Taiwan, 2012, pp. 366–371.

[19] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Proc. 1st IEEE Int. Conf. Smart Grid Communications (SmartGridComm)*, Oct. 2010, pp. 327–332.

[20] S. Salinas, M. Li, and P. Li, "Privacy-preserving energy theft detection in smart grids," in *Proc. IEEE Communications Society Conf. Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, Seoul, Korea, Jun. 2012, pp. 605–613.

[21] S. Salinas, M. Li, and P. Li, "Privacy-preserving energy theft detection in smart grids: A p2p computing approach," *IEEE J. Select. Areas Commun.*, vol. 31, no. 9, pp. 1–11, Sep. 2013.

[22] Itron [Online]. Available: https://www.itron.com/PublishedContent/OpenWay%20Centron%20Meter.pdf

[23] F. Briese, C. Fouquet, C. Hyder, C. Lowe, and J. Schlarb, "Electronic revenue meter with automatic service sensing " USA Patent US20080068004 A1, 2008 [Online]. Available: http://www.google.com/patents/US20080068004

[24] S. Depuru, L. Wang, V. Devabhaktuni, and N. Gudi, "Smart meters for power grid; challenges, issues, advantages and status," in *Proc. IEEE/PES Power Systems Conf. Expo. (PSCE)*, Phoenix, AZ, USA, Mar. 2011, pp. 1–7.

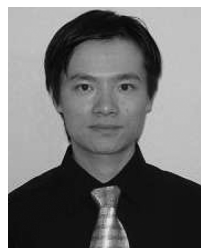
[25] W. H. Kersting, *Distribution System Modeling and Analysis*. Boca Raton, FL, USA: CRC, 2001.

[26] M. Sumner, B. Palethorpe, D. Thomas, P. Zanchetta, and M. Di Piazza, "A technique for power supply harmonic impedance estimation using a controlled voltage disturbance," *IEEE Trans. Power Electron.*, vol. 17, no. 2, pp. 207–215, Mar. 2002.

[27] T. Short, "Advanced metering for phase identification, transformer identification, and secondary modeling," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 651–658, Jun. 2013.
[28] O. Kosut, L. Jia, R. 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] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Conf. Advances in Cryptology (EUROCRYPT)*, Santa Barbara, CA, USA, Aug. 1999, pp. 223–238.
[30] R. E. Kalman, "A new approach to linear filtering and prediction problems," *J. Basic Eng.*, vol. 82, pp. 35–45, 1960.
[31] D. Simon, *Optimal State Estimation*. New York, NY, USA: Wiley, 2006.
[32] B. Friedland, "Treatment of bias in recursive filtering," *IEEE Trans. Autom. Control*, vol. 14, no. 4, pp. 359–367, Aug. 1969.
[33] S. Barker, A. Mishra, D. Irwin, E. Cecchet, P. Shenoy, and J. Albrecht, "Smart*: An open data set and tools for enabling research in sustainable homes," in *Proc. ACM SustKDD*, Beijing, China, Aug. 2012.
[34] W. Kleiminger, C. Beckel, T. Staake, and S. Santini, "Occupancy detection from electricity consumption data," in *Proc. 5th ACM Workshop Embedded Systems for Energy-Efficient Buildings*, Rome, Italy, Nov. 2013.
[35] S. Deshmukh, B. Natarajan, and A. Pahwa, "State estimation and voltage/var control in distribution network with intermittent measurements," *IEEE Trans. Smart Grid*, vol. 5, no. 1, pp. 200–209, Jan. 2014.
[36] IEEE Power and Energy Society, Distribution Test Feeders, 2010 [Online]. Available: http://ewh.ieee.org/soc/pes/dsacom/testfeeders/
[37] P. Yang, Z. Tan, A. Wiesel, and A. Nehora, "Power system state estimation using PMUs with imperfect synchronization," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 4162–4172, Nov. 2013.
[38] E. Ghahremani and I. Kamwa, "Dynamic state estimation in power system by applying the extended Kalman filter with unknown inputs to phasor measurements," *IEEE Trans. Power Syst.*, vol. 26, no. 4, pp. 2556–2566, Nov. 2011.
[39] A. Al-Othmana and M. Irving, "Analysis of confidence bounds in power system state estimation with uncertainty in both measurements and parameters," *Elect. Power Syst. Res.*, vol. 76, no. 12, pp. 1011–1018, Aug. 2006.
[40] V. Callcut, "Coppers for electrical purposes," *IEE Proc.*, vol. 133, no. 4, pp. 174–201, Jun. 1986.

Sergio A. Salinas (S'06) received the B.S. degree in telecommunications engineering from Jackson State University, Jackson, MS, USA, in 2010. He is currently pursuing the Ph.D. degree in electrical and computer engineering at Mississippi State University, Mississippi State, MS, USA.

His research interests include security, privacy, and optimization in power systems, wireless networks, cloud computing, and big data applications.



Pan Li (S'06–M'09) received the B.E. degree in electrical engineering from Huazhong University of Science and Technology, Wuhan, China, in 2005, and the Ph.D. degree in electrical and computer engineering from University of Florida, Gainesville, FL, USA, in 2009.

He is currently an Assistant Professor in the Department of Electrical and Computer Engineering, Mississippi State University, Mississippi State, MS, USA. His research interests include network science and economics, energy systems, security and privacy, and big data.

Dr. Li has been serving as an Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS—COGNITIVE RADIO SERIES and IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, a Feature Editor for IEEE WIRELESS COMMUNICATIONS, a Guest Editor for the IEEE WIRELESS COMMUNICATIONS SI on User Cooperation in Wireless Networks, and a Technical Program Committee (TPC) Co-Chair for Ad-hoc, Mesh, Machine-to-Machine and Sensor Networks Track, IEE VTC 2014, Physical Layer Track, Wireless Communications Symposium, WTS 2014, and Wireless Networking Symposium, IEEE ICC 2013. He received the NSF CAREER Award in 2012.