State Estimation for Energy Theft Detection in Microgrids

Sergio Salinas, Changqing Luo, Weixian Liao, and Pan Li
Department of Electrical and Computer Engineering
Mississippi State University, Mississippi State, MS 39762
Email: {sas573, cl1349, wl373, li@ece.}msstate.edu

***Abstract*—In traditional power networks, energy theft is a significant problem that causes severe financial losses to utility companies and legitimate users, jeopardizes system stability, and enables other illegal activities. Recently, governments and utility companies propose the Smart Grid as the next generation electric network to improve the current grid's efficiency, reliability, and security. In the Smart Grid, smart meters are deployed at users' premises to facilitate data collection, system control, etc. However, smart meters are vulnerable to cyber attacks, thus enabling easier energy pilfering. In this paper, we model the amount of energy stolen by a smart meter as a measurement bias, and propose an energy theft detection algorithm based on state estimation. In particular, our algorithm employs weighted least squares (WLS) state estimation, and can identify all the energy thieves in the system. We conduct extensive simulations in IEEE 13-bus and 123-bus test systems to validate our algorithm.**

I. Introduction

In traditional power networks, energy theft is a significant problem that causes financial losses to utility companies and legitimate users, jeopardizes system stability, and enables other illegal activities. Currently, utility companies in the U.S. and Canada estimate the revenue losses caused by energy theft to be more than $6 billion every year [1] [2], while in developing countries energy theft can amount to 50% of the total energy delivered [3]. Large revenue losses usually force utility companies to increase energy rates on legitimate users, which raise their energy costs. Besides, energy theft often leads to excessive energy consumption, which may cause equipment malfunction or damage [4], and enables other criminal activities, such as illegal production of controlled substances [2].

Recently, utility companies and governments propose the the Smart Grid to modernize the current electric gird and improve its efficiency, reliability, and security. In the smart grid, system operators are expected to replace traditional meters with cyber-physical devices, called smart meters. Smart meters are capable of taking power, current, and voltage phasor measurements, and reporting them to the system operator through a real-time, two-way communication network. This allows the implementation of novel energy-efficiency practices, for example demand response (DR) programs and microgrids. In DR programs, system operators can shape daily load demand curves, by using real-time pricing as an incentive for users to modify their consumption patterns. In the long run, DR programs reduce the required generation capacity to safely meet peak load demand, and defer investments in new power plants. Besides, a microgrid is a cluster of distributed generators, energy storage decvices, and energy loads within a distribution network that is able to operate either as part of the main grid (i.e., in grid-connected mode) or independently (i.e., in island mode). Microgrids reduce power losses at the transmission level by bringing generation closer to the loads, and allowing users to sell energy back to the grid. However, in microgrids, energy thieves can exploit smart meters' cyber vulnerabilities [5], and not only report fraudulent energy consumption, but also submit fake energy production reports to receive illegal payments. For example, in Virginia, Danville Utilities reports a growing problem with people tampering with smart meters [6]. Therefore, in microgrids, fraudulent users may be able to commit energy-theft more easily, and thus energy theft is a more serious problem in smart grids than in traditional power grids which demands careful consideration from the research community.

This work was partially supported by the U.S. National Science Foundation under grants CNS-1343220, CNS-1149786, ECCS-1128768.

In this paper, we propose an energy theft detection algorithm based on state estimation that can identify all the pirate users in the network. Specifically, we model the amount of energy stolen by a smart meter as a measurement bias. Then, we employ weighted least squares to optimally estimate all the measurement biases. A zero bias represents a truthful smart meter, while a non-zero bias indicates a fraudulent meter.

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

II. Related Works

Some research has been conducted to investigate the energy theft problem in smart grids. McLaughlin et al. [7] apply a data mining technique called Non-Intrusive Load Monitoring (NILM) to detect energy theft. They collect cyber-intrusion and physical-intrusion logs, and analyze users' load profiles. They generate a list of possible energy thieves with a minimum amount of false positives using an attack graph based fusion

978-1-4799-5970-9 © 2014 IEEE

algorithm. Cárdenas et al. [8] formulate a statistical anomaly detection scheme and then model the interactions between the utility company and the fraudulent users with a game. The utility company aims to maximize its profit and minimize the cost of detecting pirate users, while energy thieves's objective is to minimize the likelihood of being detected subject to a constraint related to the amount of stolen energy. Mashima and Cárdenas [9] evaluate the accuracy of anomaly detectors by using a novel threat model and several statistical metrics. Pereira et. al [10] find energy thieves by analyzing fine-grained load profiles from users' smart meters with a neural network classifier called charged system search. Huang et. al [11] propose an algorithm 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] can find energy thieves by modeling a distribution network as a linear equation, only if all the voltage measurements and some initial power measurements are authentic, i.e., not tampered by the energy thieves. Unfortunately, we find that all these techniques have low detection rates.

In our previous works [13], [14], we propose several energy theft detection algorithms utilizing distributed matrix decompositions. However, our previous works assume that typical power line losses are known by the system operator, which may be difficult to obtain in practice. In this paper, we propose a new state estimation based energy theft detection scheme that can successfully identify pirate users in a microgrid, while taking into account power losses. We model the amount of stolen energy by a smart meter as a measurement bias and employ weighted least squares (WLS) estimation to solve for all the meters' biases. Thus, a zero bias indicates a faithful meter, and a non-zero one identifies a pirate meter.

III. System Model

A. Microgrid Architecture

As shown in Fig. 1, we consider an electric power 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 [15] [16] and are able to communicate with each other by forming a multihop mesh communication network [17]. 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 microgrids.

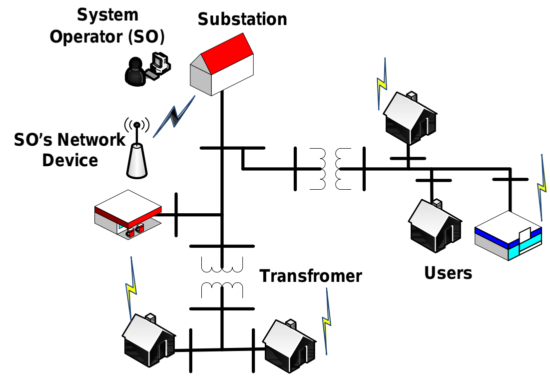

Fig. 1. The architecture for a radial microgrid.

B. A Power Network Model for Microgrids

In what follows, we model the steady-state currents and voltages in the MG. Specifically, suppose that user i 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 [18]:

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

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:

$$\mathbf{V}_i = \mathbf{A}_{i',i}\mathbf{V}_{i'} - \mathbf{Z}_{i',i}\mathbf{I}_i \tag{2}$$

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 and matrix $\mathbf{Z}_{i',i}$ is diagonal. For a transformer line segment (i', i), $\mathbf{A}_{i',i}$ can be calculated as

$$\mathbf{A}_{i',i} = \frac{1}{n_{i',i}} \begin{bmatrix} a_{i',i}^{1,1} & a_{i',i}^{1,2} & a_{i',i}^{1,3} \\ a_{i',i}^{2,1} & a_{i',i}^{2,2} & a_{i',i}^{2,3} \\ a_{i',i}^{3,1} & a_{i',i}^{3,2} & a_{i',i}^{3,3} \end{bmatrix} \tag{3}$$

where $n_{i',i}$ is the turns ratio of the transformer, and $a^{\phi,\phi'}_{i',i} \in \{0, 1, -1\}$ depending 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 in 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:

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

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, $\mathcal{P}$ contains the set of all the buses on the path from bus 0 to bus i (excluding bus 0), and $\mathcal{H}$ is empty. Note that we assume the voltage and current at the substation bus are constant and known to the MG operator. Besides, the parameters of the power lines and the transformer are known to the MG operator and the smart meters.

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:

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

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

In addition, the power consumed by the load at bus i is related to the load current 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 energy thieves are able to compromise all functions of their smart meters, including measurement taking and reporting, which makes energy theft detection a more challenging problem.

Denote by $\mathbf{b}_i$ 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

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

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 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 equation (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

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

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

IV. Optimal State Estimation for Energy Theft Detection

State estimation finds the most likely state of a process by minimizing the sum of the squares of the differences between observed values and the calculated state [19]. In this section, we propose an state estimation algorithm to find line segment currents and measurement biases, which can be used to identify energy thieves as explained in Section III-C, using voltage and current observations. Our algorithm employs the technique of weighted least squares (WLS) [20] to solve our estimation problem.

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

$$\mathbf{x} = [\mathbf{V}_0\ \mathbf{I}_1\ \mathbf{I}_2\ \dots\ \mathbf{I}_n\ \mathbf{b_1}\ \mathbf{b_2}\ \dots\ \mathbf{b_n}]^\top$$

. Then, the vector of load current and voltage measurements, denoted by

$$\mathbf{y} = [\mathbf{V'}_0\ \mathbf{I'}_1\mathbf{L'}_1\mathbf{L'}_2\ \dots\ \mathbf{V'}_1\mathbf{V'}_2\ \dots\ \mathbf{V'}_n]^\top,$$

can be expressed as follows:

$$\mathbf{y} = \mathbf{h}(\mathbf{x}) + \mathbf{e}. \quad (9)$$

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 equations (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. Specifically, the measurements in $\mathbf{y}$ are:

$$\begin{aligned}
\mathbf{V'}_0 &= \mathbf{V}_0 + e_{\mathbf{V}_0} \\
\mathbf{I'}_1 &= \mathbf{I}_1 + e_{\mathbf{I}_1} \\
\mathbf{L'}_i &= \mathbf{I}_i - \mathbf{b}_i - \sum_{r\in\mathcal{R}_i} \mathbf{I}_r - \sum_{q\in\mathcal{Q}_i} \mathbf{B}_{i,q}\mathbf{I}_q + e_{\mathbf{L}_i} \ \forall i \in [1,n] \\
\mathbf{V'}_i &= \mathbf{A}_{p,h}(\mathbf{V}_0 - \sum_{j\in\mathcal{P}_i} \mathbf{Z}_{j',j}\mathbf{I}_j) \\
&\quad - \sum_{k\in\mathcal{H}_i} \mathbf{Z}_{k',k}\mathbf{I}_k + \mathbf{Z}_i\mathbf{b}_i + e_{\mathbf{V}_i} \ \forall i \in [1,n]
\end{aligned} \tag{10}$$

We can see from (10) that (9) 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 $\partial\mathbf{h}(\mathbf{x})/\partial\mathbf{x} = \partial\mathbf{y}/\partial\mathbf{x}$)

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

The first two rows are related to $\mathbf{V}_0$ and $\mathbf{I}_1$, where the partial derivatives $\frac{\partial \mathbf{V}_0}{\partial \mathbf{V}_0}$ and $\frac{\partial \mathbf{I}_1}{\partial \mathbf{I}_1}$ are equal to $\mathbf{1}$ (a 3×3 identity matrix) and the rest elements are equal to zero. 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 b_j, i.e.,

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

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

where $\mathbf{1}$ 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 $\mathbf{b_j}$ as follows:

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

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

According to WLS, the system operator intends to minimize the weighted sum of the squares of the differences between measurements and calculated values [19], i.e.,

$$J(\mathbf{x}) = \frac{1}{2}[\mathbf{y} - \mathbf{H}_{aug}(\mathbf{x})]^\top \mathbf{R}^{-1}[\mathbf{y} - \mathbf{H}_{aug}(\mathbf{x})] \tag{16}$$

where $\mathbf{R}$ is the covariance matrix of the measurement error vector, i.e., $\mathbf{R} = \mathbb{E}[\mathbf{e}\mathbf{e}^\top]$.

The first order optimal condition can be obtained by taking the first-order partial derivative of (16) with respect to the augmented state vector$\mathbf{x}$, that is

$$\frac{\partial J(\mathbf{x})}{\partial \mathbf{x}} = -\mathbf{H}_{aug}^\top \mathbf{R}^{-1}[\mathbf{y} - \mathbf{H}_{aug}(\mathbf{x})] = \mathbf{0} \tag{17}$$

The second order optimal condition is given by the second order partial derivative of (17) with respect to $\mathbf{x}$, i.e.,

$$\frac{\partial^2 J(\mathbf{x})}{\partial \mathbf{x}^2} = \mathbf{H}_{aug}^\top \mathbf{R}^{-1}\mathbf{H}_{aug} \tag{18}$$

which is positive semi-definite. Hence, (17) is an optimal condition to find the minimum value of (16).

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 best unbiased linear estimator to solve for $\mathbf{x}$ in equation (17), i.e.,

$$\begin{aligned}\hat{\mathbf{x}} &= (\mathbf{H}_{aug}^\top \mathbf{R}^{-1}\mathbf{H}_{aug})^{-1}\mathbf{H}_{aug}^\top \mathbf{R}^{-1}\mathbf{y} \\ &= \mathbf{N}_{aug}\mathbf{y}\end{aligned} \tag{19}$$

where $\hat{}$ denotes estimated values, and $\mathbf{N}_{aug}$ is a constant in the estimator.

Third, the system operator examines bias estimates $\hat{b}_i^\phi$ ($\forall i, \phi$) and determines that users with $\hat{b}_i^\phi$ greater than a predefined parameter ϵ are energy thieves. This parameter is a multiple of the standard deviation of the largest bias estimate error, i.e.,

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

where k is a positive integer. Particularly, we can find the estimates' error variance as follows:

$$\begin{aligned}
\mathbf{Var}[\mathbf{x} - \hat{\mathbf{x}}] &= \mathbb{E}[(\mathbf{x} - \hat{\mathbf{x}})(\mathbf{x} - \hat{\mathbf{x}})^\top] \\
&= \mathbb{E}[\mathbf{x}\mathbf{x}^\top] - \mathbb{E}[\mathbf{x}\hat{\mathbf{x}}^\top] - \mathbb{E}[\hat{\mathbf{x}}\mathbf{x}^\top] + \mathbb{E}[\hat{\mathbf{x}}\hat{\mathbf{x}}^\top]. \\
&= \mathbf{N}_{aug}\mathbb{E}[\mathbf{e}\mathbf{e}^\top]\mathbf{N}_{aug}^\top
\end{aligned}$$

The final step is due to the fact that $\mathbf{N}_{aug}\mathbf{H}_{aug}$ is equal to the identity matrix. Thus, since $\mathbb{E}[\mathbf{e}\mathbf{e}^\top] = \mathbf{R}$, we have $\mathbf{Var}[b_i^\phi - \hat{b}_i^\phi] = \mathbf{n}_i^\phi \mathbf{R} \mathbf{n}_i^{\phi\top}$ where $\mathbf{n}_i^\phi$ is the row vector of $\mathbf{N}_{aug}$ corresponding to the ith bias on phase ϕ.

V. Simulation Results

In this section, we employ our proposed algorithm to find energy thieves in the IEEE 13-bus and IEEE 123-bus distribution test systems shown in Fig. 2 and Fig. 3, respectively. We use the line segment and bus load information of both systems contained in [21]. Besides, in the IEEE 13-bus system, we ignore the voltage regulator between buses 632 and 650, consider the switch between buses 671 and 692 to be closed, and use the load demand presented in Table I. In the IEEE 123-bus system, we also ignore the voltage regulators and consider closed switches between buses $150-149, 13-152, 54-94, 18-135$, and generate random loads for all buses that we omit for brevity. Both systems are radial networks with unbalanced loads, which makes them realistic scenarios for a microgrid.

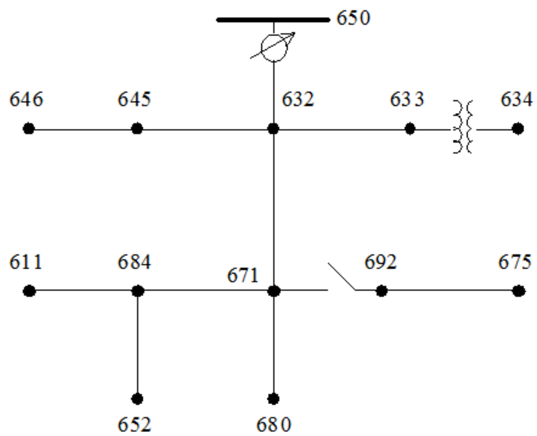

Fig. 2. The IEEE 13-bus test system

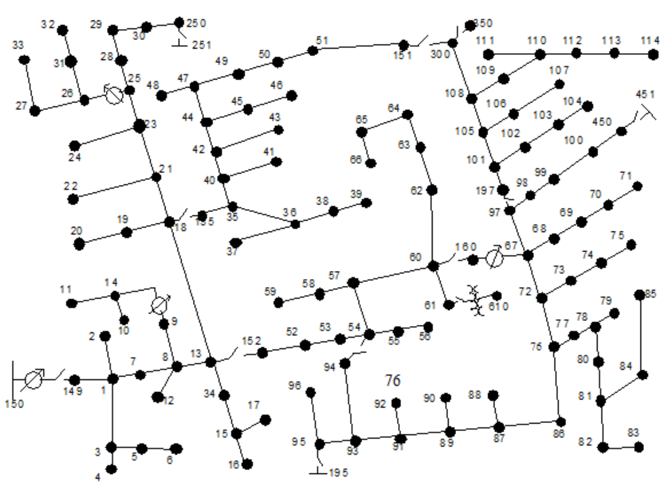

Fig. 3. The IEEE 123-bus test system

First, to generate the true state of the system, we calculate load currents, line currents, and bus voltages using the ladder iterative technique in [18]. We then generate, for each bus, three-phase load current and three-phase voltage measurements, with biases and normally distributed errors.

TABLE I
IEEE 13-bus loads

Phase Bus	$\phi=1$ (kW)	$\phi=1$ (kVar)	$\phi=2$ (kW)	$\phi=2$ (kVar)	$\phi=3$ (kW)	$\phi=3$ (kVar)
634	160	110	120	90	120	90
645	0	0	170	125	0	0
646	0	0	230	132	0	0
652	128	86	0	0	0	0
671	385	220	385	220	385	220
675	485	190	68	60	290	212
692	0	0	0	0	170	151
611	0	0	0	0	170	80

TABLE II
The bias threshold ϵ

Parameter	13-bus	123-bus
Measurement Variance	0.0023	0.0023
ϵ	0.45	4.23
Probability a user steals energy	0.3	0.3
Bias magnitude interval	[3,10]	[3,10]

The current and voltage measurements' errors have zero mean and variances equal to 0.0023. 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 $[3, 10]A$ 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 who are connected to less than three phases.

Moreover, we set the bias threshold

$$\epsilon = k \times \max_{i,\phi} (\mathbf{n}_i^{\phi} \mathbf{R} \mathbf{n}_i^{\phi\top})^{1/2}$$

by choosing $k = 4$, which makes it 0.43 and 4.23 for the 13-bus system and 123-bus system, respectively. Note that since the measurement error follows a Gaussian distribution, choosing $k > 3$ sets a threshold that is larger than any honest user's bias estimation error with a very high probability. In contrast, since energy thieves' true biases are usually much larger than ϵ, their bias estimates are larger than ϵ with a very high probability as well. Table II summarizes our simulation parameters.

A. IEEE 13-bus Test System

Fig. 4 compares bias estimates obtained by the proposed algorithm to their true values, for all users and all phases. 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 and the bias estimates for energy thieves are larger than ϵ.

B. IEEE 123-bus Test System

Fig. 5 compares bias estimates of the proposed algorithm to their true values. We find that estimated biases are very close to their true values, thus correctly identifying the energy thieves. We also observe that the value for ϵ correctly differentiates

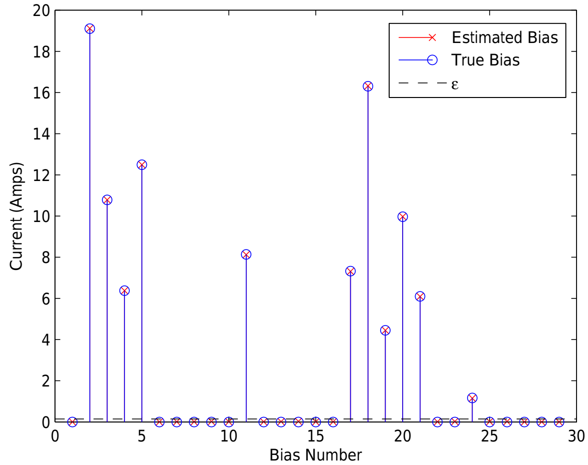

Fig. 4. Energy theft detection in the 13-bus system.

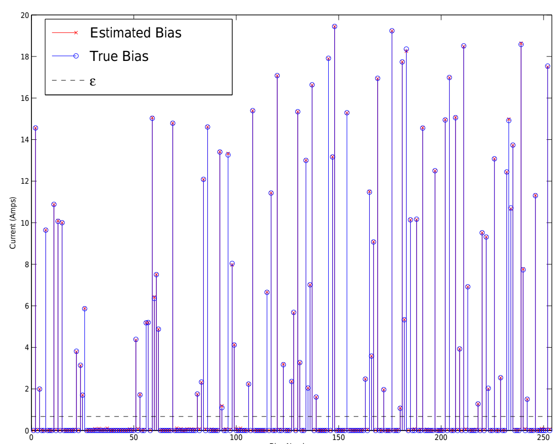

Fig. 5. Energy theft detection in the 123-bus system.

between fraudulent and legitimate measurements, as in the 13-bus case.

VI. Conclusions

In this paper, we have investigated energy theft detection in microgrids by employing a realistic model for the power system. A key characteristic of microgrids is the use of cyber-physical devices for energy metering, called smart meters. We model the amount of stolen energy by a smart meter as a measurement bias, and propose an algorithm that optimally estimates all the smart meters' biases. A zero bias indicates a faithful meter, and a non-zero one identifies a pirate meter. Our proposed energy theft detection algorithm utilizes weighted least squares and can find all the energy thieves in the network. We have validated our algorithm through extensive simulations.

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-June 2009.

[2] E. Journal, Pot growers stealing $100M worth of power: B.C. Hydro, 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," *Selected Areas in Communications, IEEE Journal on*, vol. 31, no. 7, pp. 1319–1330, July 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 *Fiftieth Annual Conference on 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 *Proceedings of the 15th international conference on Research in Attacks, Intrusions, and Defenses*, Amsterdam, 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 *IEEE Conference on Innovative Smart Grid Technologies Latin America (ISGT LA)*, April 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 Transactions on Power Systems*, vol. 28, no. 3, pp. 2959–2966, July 2013.

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

[13] S. Salinas, M. Li, and P. Li, "Privacy-preserving energy theft detection in smart grids," in *IEEE Communications Society Conference o nSensor, Mesh and Ad Hoc Communications and Networks (SECON)*, Seoul, Republic of Korea, June 2012, pp. 605–613.

[14] ——, "Privacy-preserving energy theft detection in smart grids: A p2p computing approach," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1–11, September 2013.

[15] Itron, Online. [Online]. Available: https://www.itron.com/na/PublishedContent/OpenWay\%20Centron\%20Meter.pdf

[16] F. Briese, C. Fouquet, C. Hyder, C. Lowe, and J. Schlarb, Patent US20080068004 A1, 2008. [Online]. Available: http://www.google.com/patents/US20080068004

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

[18] W. H. Kersting, *Distribution System Modeling and Analysis*. CRC Press, 2001.

[19] A. Monticelli, *State Estimation In Electric Power Systems: A Generalized Approach*. Kluwer Academic Publishers Group, 1999.

[20] M. E. Baran and A. W. Kelley, "A branch-current based state estimation method for distribuition systems," *IEEE Transactions on Power Systems*, vol. 10, no. 1, pp. 483–491, February 1995.

[21] I. power and E. Society, Distribution Test Feeders, 2010. [Online]. Available: http://ewh.ieee.org/soc/pes/dsacom/testfeeders/