Defending against Energy Dispatching Data Integrity Attacks in Smart Grid

Xiaofei He*, Xinyu Yang*, Jie Lin*, Linqiang Ge†, Wei Yu† and Qingyu Yang‡
* School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China
Emails: hexiaofei@stu.xjtu.edu.cn, {yxyphd, jielin}@mail.xjtu.edu.cn
† Department of Computer and Information Sciences, Towson University, Towson, MD, USA
Emails: lge2@students.towson.edu, wyu@towson.edu
‡ SKLMSE Lab, Xi'an Jiaotong University, Xi'an, China
Email: yangqingyu@mail.xjtu.edu.cn

***Abstract*—The smart grid is a new type of energy-based cyber-physical system (CPS), which enables interactions between the utility provider and customers through smart meters and advanced metering infrastructures (AMI). Nonetheless, an adversary can inject misleading energy usage information to the utility provider through compromised smart meters and disrupt the grid and electricity market operations. To address this issue, in this paper, we propose an *Energy Dispatching False Data Defense (EDF2D)* approach, which can effectively detect the forged interactive information between customers and the utility provider with a great accuracy and mitigate the damage raised by attacks on grid operations. Particularly, EDF2D uses the historical interactive information of normal users to determine the conditional probabilities of data anomalies. Based on these conditional probabilities, a Bayesian network designed for detecting false data can be established by EDF2D, and this network is then used to confirm the authenticity of interactive information received by the utility provider originally transmitted from customers. Through a combination of theoretical analysis and performance evaluation, our experimental data shows that EDF2D can effectively detect harmful false interactive data forged by the adversary and mitigate false data injection attacks on smart grid operations.**

***Keywords*—Smart measurement devices, Data integrity attacks, Smart grid.**

I. Introduction

With the development of modern communication and computing technologies, the smart grid, also denoted as an energy-based cyber-physical system (CPS), has been developed to make the power grid efficient, reliable, and secure [7]. One critical service in the smart grid is to enable the two-way information interactions between customers and the utility provider through smart meters and advanced metering infrastructure (AMI). As a crucial component that enables interactions between customers and the utility provider, demand response has been developed and attracted growing attention [1]. In demand response, smart meters deployed at customers can be used to measure the energy usage information associated with consumers and send measured information to the utility provider through wireless communication in an AMI [4]. Then, the utility provider optimizes grid operations based on the received information and makes the power dispatching process effectively and efficiently. The utility provider can send the real-time electricity price and other operational status to customers. In this way, customers can actively participate in grid operations [19].

In the smart grid, smart meters can not only measure and transmit local energy usage information to the utility provider, but also serve as relay nodes to forward the energy usage information of other customers to the utility provider through wireless communications. Nonetheless, the use of wireless communication can increase the probability of smart meters being compromised by the adversary. As a negative consequence, the adversary can inject false interactive information (e.g., energy usage data, etc.) associated with demand response process to the utility provider through compromised meters. The injected false interactive information can not only disrupt grid operations [15], but also pose a negative impact on electricity markets operations [10], [12].

There have been considerable efforts devoted on understanding the impact of false data injection attacks and developing countermeasures to mitigate these attacks [3], [5], [6], [6], [8], [9], [13], [14], [16], [17], [17], [18], [20]–[25]. For example, Liu *et al.* investigated the impact of the false data injection attacks on the state estimation in the power grid [14]. Yang *et al.* formalized the least effort false data injection attacks and developed countermeasures [25]. Yang *et al.* investigated various attack strategies against Kalman filters, which have been widely used by dynamic state estimation [24]. Xie *et al.* investigated a false data injection attack against the electric market [22]. Yi *et al.* analyzed the attack and defense mechanisms on the bad data injection [8]. Manandhar *et al.* proposed a Kalman Filter based scheme against the false data injection [16]. Li *et al.* presented a state summation scheme to detect false data injection attacks [11]. Nonetheless, the impact of false data injection attacks against energy dispatching process and the development of effective detection and response mechanisms remain opening issues.

To this end, in this paper, we developed an effective approach to defend against false data injection attacks on energy dispatching process. To be specific, we proposed an *Energy Dispatching False Data Defense approach* (also called EDF2D), which can not only effectively detect the false interactive information with a great accuracy, but also mitigate the damage of false data injection attacks on grid operations. Particularly, EDFDD developed a Bayesian network based mechanism to determine conditional probabilities of false data

978-1-4673-8590-9/15/$31.00 ©2015 IEEE

and limits its impacts on grid operations. In our developed approach, random factors, which are correlated to the authenticity of users' energy usage information (e.g., current time, the previous demand data, etc.), are used to establish a Bayesian network to accurately detect false data.

After receiving the energy demand information from users, the utility provider obtains the conditional probability on the authenticity of the received users' energy usages information through the established Bayesian network. If the obtained conditional probability is larger than a pre-defined confidence threshold, the received users' energy usage information is considered as valid. Otherwise, the received information is considered as a forged energy usage information. Because the conditional probability of the interactive information is based on the historical data and the information of neighbors, EDF2D can effectively detect the false information with a great accuracy. In addition, as the false energy usage information is detected before the power dispatching process, EDF2D can effectively mitigate the negative impact of false data injection attacks on grid operations.

Through a combination of extensive theoretical analysis and simulation experiments, we evaluated the accuracy and efficiency of our proposed approach in terms of false negative rate and detection rate of false data. We also evaluated the effectiveness of our developed approach to mitigate the attack on grid operations. We used the energy loss as an example to demonstrate the effectiveness of mitigating attacks. Our experimental data shows that EDF2D can detect almost all the harmful false energy usage data injected by the adversary. For example, if the manipulated energy usage data is increased by 40% of the original value, the false negative rate of BNF2D approach around 98%. In addition, EDF2D can reduce almost half of errors between the amount of predicted energy demand and the amount of the actual consumed energy. Therefore, the utility provider can reduce the unnecessary energy from the bulk generator and increase the efficiency of energy usage.

The remainder of the paper is organized as follows: We introduce system and threat models in Section II. We present our proposed approach in Section III. In Section IV, we show experimental results to validate our findings. Finally, we conclude the paper in Section V.

II. System and Threat Models

In the smart grid, the AMI provides an infrastructure to enable two-way information interactions between the utility provider and consumers. Smart measurement devices (e.g., smart meters) in an AMI deployed at consumers can measure and collect information (e.g., the power usage of consumers, the amount of predicted energy generations from distributed renewable energy resources, the state of energy storage devices, etc.) and transmit the collected information to the utility provider through wireless communications. The utility provider can also transmit the operation status and real-time electricity price to customers. Through two-way information interactions, customers can effectively participate in grid operations and improve the efficiency of power dispatching process.

In our paper, we use nodes to represent customers and plants. We also use smart meters to represent smart measurement devices. In our approach, two types of nodes are considered: bulk generators and user nodes. As shown in Fig. 1, user nodes can be categorized as either demand-nodes or supply-nodes. Bulk generators, as same as that in the traditional power grid, generate the majority amount of power with fuel resources. Supply-nodes represent customers if the predicted amount of generated power is larger than the amount of power that they need to use. Demand-nodes represent customers if the predicted amount of generated power is smaller than the amount of power that they need to consume. Notice that, in the smart grid, either supply-nodes or demand-nodes, can generate power by transforming distributed energy resources (e.g., wind, solar, etc.). In addition, supply-nodes can provide extra power to the grid and some demand-nodes. With the extra power provided by supply-nodes, the power generated by bulk generator can be dynamically dispatched so that the power can be effectively utilized in the grid.

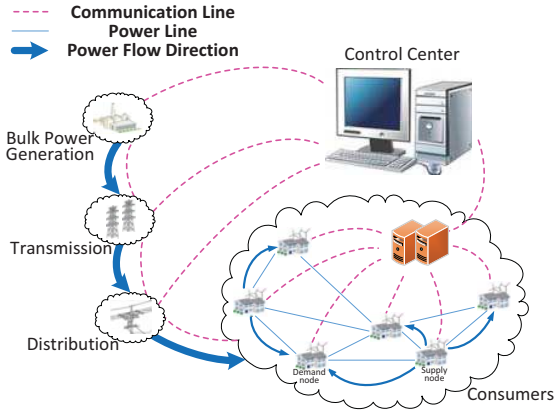

Fig. 1. An Example of AMI Network

As smart meters are interconnected through wireless communications, we assume that the adversary can compromise smart meters and launch false data injection attacks through compromised meters. Once meters are compromised, the adversary can take full access to the memory of devices remotely. The adversary can also modify the secret measurement data stored in the memory and report the false information to the utility provider through compromised meters. Therefore, the attack can pose economic or physical damage to grid operations by disrupting the demand response process, etc. We assume that the adversary can obtain and analyze the usage information from compromised meters and can manipulate the information of users' energy usage data to avoid being detected. According to the common security practice, we consider the adversary has limited capacity and can only compromise a limited number of smart meters, i.e., most of meters in the system work normally.

III. Our Approach

In this section, we first present the design rationale of our approach. We then describe three key components: energy demand generation, false data detection, and energy dispatching process.

A. Basic Idea

Recall that, the impact of false data injection attacks against energy dispatching process and the development of effective

detection and response mechanisms remain opening issues. To deal with this issue, we proposed an approach to effectively detect the injected false interactive information with a great accuracy and mitigate the damage of false data injection attacks on grid operations.

The main idea of our approach is described as follows: EDF2D uses the historical data of usage demand information to confirm the injected false data. The historical measurement data will be formed into discrete values. Depending on these values, EDF2D can establish a Bayesian network, which provides the conditional probability of the authenticity of the predicted energy demand information. The conditional probability is related to random events (e.g., current time, current consumed energy, etc.). The utility provider can use the established Bayesian network to detect the false injected data from the reported usage information based on a properly configured confidence threshold. A higher confidence threshold will lead to a higher detection, while a higher false negative rate and a lower confidence threshold will reduce false negative rate, but increase false positive rate.

Notice that according to security requirements of the smart grid, the utility provider can choose the proper confidence threshold, which leads to a high detection accuracy. After false data is confirmed, the utility provider can response to the attack via replacing the detected false usage information by the predicted energy demand based on historical data. Finally, the utility provider will dispatch energy to consumers according to their energy demand information after excluding false data. To balance energy demand and supply in the gird, EDF2D can not only ensure that most of nodes works regularly, but also limit the damage of the attack in a cost-effective manner.

Our approach consists the following three key components:

- (i) *Demanded energy determination* is used to predict the user's demand information, according to the historical information of users' energy consumption and generation;
- (ii) *False data detection and response* is used to confirm the authenticity of the predicted energy demand information on each node (i.e., interactive energy usage information associated with customers) and response to it correspondingly;
- (iii) *Energy dispatching* is used to allocate the energy to each node based on the predicted energy demand. All these components will be detailed in following subsections. All notations in this paper is shown in Table I.

TABLE I. NOTATION

N	Number of all nodes in the network
U	The set of all nodes in the network
v_i	The i^{th} node in set U
t	The index of time duration
$c_i(t)$	The energy consumed by node i in the time duration t
$\varepsilon_i(t)$	The extra energy demanded by node i in the time duration t
$BG(t)$	The energy of bulk generation in the time duration t
$p_i(t)$	The predicted energy demanded by node i in the time duration t
$Pr_i(t)$	The conditional probability of $p_i(t)$
φ	The confidence threshold
$a_i(t)$	The confirmed result of the energy demand at node i in the time duration t
$Gap(t)$	The gap of the total demand and the total supply in the network
$d_i(t)$	The energy demanded by node i in the time duration t after exclusion of the false data
$l_i(t)$	The load of node i in the time duration t
U_l	The set of nodes that consume less than the predicted amount of energy
U_g	The set of nodes that consume more than the predicted amount of energy
U_c	The set of compromised nodes
φ	The confidence threshold of Bayesian Network

B. Demanded Energy Determination

In the smart grid, consumers can not only use the power generated by bulk generators, but also access the power provided by wind energy and solar energy resources, which are deployed locally near to consumers. To maximize the efficiency of energy usage, smart measurement devices deployed at consumers will measure and send the energy usage information (e.g., the predicted energy demand information) of the next time duration to the utility provider via wireless communications. Based on the received energy usage information, the utility provider can dispatch the power correspondingly. In this way, the power generation cost can be reduced and the power utilization can be improved in the grid.

In our approach, customers are divided into two types: power supply-nodes and demand-nodes. The former can supply the extra power to the grid, while the latter needs to receive the demanded power from the grid. The power supply-nodes can also be considered as nodes whose demanded power is negative. The demanded energy of users in the next time duration is predicted by the smart meter through the historical energy usage associated with consumers, the energy generated by distributed energy generation resources, and the status of energy storage devices.

Then, we have

$$p_i(t+1) = Pred(H_i, c_i(t), DG_i(t), S_i(t)), \tag{1}$$

where H_i is the historical energy usage information on node i, $c_i(t)$ is the actual energy consumed on node i, $DG_i(t)$ is the amount of energy generated by distributed generation resources in the time duration t, $S_i(t)$ is the amount of energy stored in the energy storage device in the time duration t, and $Pred(\cdot)$ is the prediction function of the energy demand. To simplify the problem, we use the expectancy of the historical data as the predicted energy demand information in the next time duration. As we can see that if $p_i(t+1)$ is positive, node i needs the amount of extra energy $p_i(t+1)$ in the next time duration $t+1$, while if $p_i(t+1)$ is negative, node i can provide the amount of energy $|p_i(t+1)|$ to the grid in the next time duration $t+1$.

C. False Data Detection and Response

The false data detection in EDF2D consists of the following three steps: (i) *Measurement Discretization*: The smart meters transform continuous measurement values to discrete values; (ii) *Bayesian Network Establishment*: The control center establishes a Bayesian network using the previous discrete values in step (i); (iii) *Authenticity Confirmation and Response*: The control center compares the conditional probability with the

given confidence threshold, detects the false data from the user's predicted energy demand information, and responds to the attack to protect grid operations.

1) Measurement Discretization: As the measurement values in the grid are continuous, we need to discretize them in order to be used as the states of nodes in the Bayesian network. To ensure that each state is significantly different from the other, we use the k-means method [2] to discretize the measurement data.

The continuous data that needs to be discretized is listed as follows: (i) the set of next predicted energy demand information $S^{(p)}$, (ii) the set of the amount of consumed energy $S^{(c)}$ on node i, (iii) the set of total consumed energy in the grid $S^{(C)}$, and (iv) the set of error between the actual and the predicted value $S^{(\varepsilon)}$.

To obtain the discrete value, the above data should be divided into subsets $S_1^{(p)}, S_2^{(p)}, \ldots, S_{k_p}^{(p)}$, $S_1^{(c)}, S_2^{(c)}, \ldots, S_{k_c}^{(c)}$, $S_1^{(C)}, S_2^{(C)}, \ldots, S_{k_C}^{(C)}$, $S_1^{(\varepsilon)}, S_2^{(\varepsilon)}, \ldots, S_{k_\varepsilon}^{(\varepsilon)}$. To minimize the error of k-means method, the objectives are to find:

$$\arg\min_{S^{(p)}} \sum_{j=1}^{k_p} \sum_{p_i \in S_j^{(p)}} \left\| p_i - \mu_j^{(p)} \right\|^2, \tag{2}$$

$$\arg\min_{S^{(c)}} \sum_{j=1}^{k_c} \sum_{c_i \in S_j^{(c)}} \left\| c_i - \mu_j^{(c)} \right\|^2, \tag{3}$$

$$\arg\min_{S^{(C)}} \sum_{j=1}^{k_C} \sum_{C \in S_j^{(C)}} \left\| C_i - \mu_j^{(C)} \right\|^2, \tag{4}$$

$$\arg\min_{S^{(\varepsilon)}} \sum_{j=1}^{k_\varepsilon} \sum_{\varepsilon_i \in S_j^{(\varepsilon)}} \left\| \varepsilon_i - \mu_j^{(\varepsilon)} \right\|^2, \tag{5}$$

where k_p, k_c, k_C, k_e are the number of elements in sets $S^{(p)}, S^{(c)}, S^{(C)}, S^{(\varepsilon)}$, μ_i is the mean of all elements in the set S_i. In this paper, we choose $\mu_j^{(p)}, \mu_j^{(c)}, \mu_j^{(C)}, \mu_j^{(\varepsilon)}$ as the discrete values of all nodes in the set $S_j^{(p)}, S_j^{(c)}, S_j^{(C)}, S_j^{(\varepsilon)}$, respectively.

2) Bayesian Network Establishment: In this paper, we developed a Bayesian network based scheme to confirm the authenticity of the predicted energy demand information on each node. The model of the established Bayesian network is illustrated in Fig. 2. Notice that nodes are used to present states of random events, while directed arcs are used to represent the relationship between random events. Node T represents the current time t, node K_i represents the type of node i, node C represents the sum of the current consumed energy in the grid $C(t)$, node ε_i represents the error between the predicted energy demand and the actual consumed energy $\varepsilon_i(t)$, node r_i represents the authenticity of the predicted energy demand $r_i(t+1)$, and node P_i represents the predicted energy demand $p_i(t+1)$.

In the Bayesian network model, we consider the authenticity $r_i(t+1)$ of the predicted energy demand in the next time duration as unobservable nodes, and others as observable nodes, including the current time t, the total consumed energy $C(t)$ in the grid at the time duration t, the consumed energy

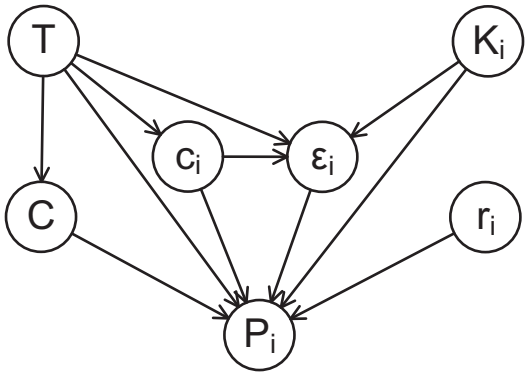

Fig. 2. A Model of Bayesian Network

$c_i(t)$ on node i at the time duration t, the predicted energy demand $p_i(t+1)$ on node i at the next time duration $t+1$, and the error between the amount of actual consumed energy and the amount of predicted energy $\varepsilon_i(t)$. The aforementioned measurement values discretized by k-means method will be considered as the marginal probability of each node in the Bayesian network.

To obtain the conditional probability of the authenticity of the user's predicted energy demand information, EDF2D needs the following inference steps:

- All observable random variables are instantiated as observable values and unobservable nodes are instantiated as random values.
- In the traversal of directed acyclic graph (DAG), for an unobservable node y, the conditional probability of y can be presented by

$$Pr(y|w_i) = \alpha Pr(y|Parents(y)) \prod_j Parents(s_j), \tag{6}$$

  where w_i is the node except node y, α is the normalization factor, and s_j is the j^{th} child node of node y.
- We use node y to instantiate the new values of unknown nodes and repeat the second step until results fully converge.
- The converged results will be considered as the inferential value, i.e., the conditional probability $Pr_i(t)$ that the amount of predicted energy demand $d_i(t)$ sent by node i is forged.

3) Authenticity Confirmation and Response: The utility provider will determine whether the user's predicted energy demand information on node i is false or not by using both the conditional probability $Pr_i(t)$ obtained through the established Bayesian network with the configured confidence threshold φ. We consider: (i) If the conditional probability $Pr_i(t)$ is greater than the confidence threshold φ, the energy demand is considered as true. Then, the control center can adjust the energy supply in the grid according to the energy demand from nodes. (ii) If the conditional probability $Pr_i(t)$ is less than the confidence threshold φ, the energy demand is considered as

false. Then, the control center can predict the energy demand based on the historical energy usage information.

In other words, we have

$$d_i(t+1) = \begin{cases} p_i(t+1), & Pr_i(t+1) \geq \varphi \\ a_i(t) + \sum\limits_{j=1} \frac{a_i(t-j)-a_i(t)}{j+2}, & Pr_i(t+1) < \varphi \end{cases}, \tag{7}$$

where $a_i(t)$ is the amount of actual energy consumed by node i in the time duration t. Notice that $d_i(t+1)$ is the amount of confirmed energy demand in the next time duration $t+1$ on node i after excluding the false data by our proposed approach. It is worth noting that, as the false energy usage information is detected before the power dispatching process, our defense approach can effectively mitigate the negative impact of false data injection attacks on grid operations.

D. Energy Dispatching

To balance the energy demand and supply in the grid and achieve a better energy utilization efficiency, the control center will limit the users' energy consumption according to the amount of energy provided by bulk generators. We assume that the error between the amount of actual consumed energy and the amount of predicted demand ($\varepsilon_i(t) = l_i(t) - d_i(t)$) is a random event and follows a normal distribution [26][1]. Then, we have

$$\varepsilon_i(t) \sim N(0, \sigma^2), \tag{8}$$

where the σ^2 is the variance of $\varepsilon_i(t)$, and the mean of $\varepsilon_i(t)$ is 0.

To maximize the efficiency of energy usage, the utility provider will control the supply of the bulk generation based on the predicted energy demand information sent by smart meters deployed at consumers locally. According to the property of the normal distribution of metering data [26], we have

$$Pr(-3\sigma \leq \varepsilon_i(t) \leq 3\sigma) = 99.7\%. \tag{9}$$

Therefore, the utility provider can set the electricity energy production as,

$$BG(t) \geq \sum_{v_i \in U} [d_i(t) + 3\sigma] = \sum_{v_i \in U} d_i(t) + 3N\sigma. \tag{10}$$

In this paper, we define that the set $U_g = \{v_i | \varepsilon_i > 0, v_i \in U\}$ is composed of nodes, where the amount of actual consumed energy is greater than the amount of predicted energy demand. On the other hand, the set $U_l = \{v_i | \varepsilon_i < 0, v_i \in U\}$ is composed of nodes, where the amount of actual consumed energy is less than the amount of predicted energy demand.

Because of the error ε_i in the energy dispatching process, the produced energy of bulk generation does not always match the sum of user's actual consumed energy. Then, the gap amount of energy in the grid is

$$\begin{aligned} Gap(t) &= \sum_{v_i \in U} l_i(t) - BG(t) \\ &\leq \sum_{v_i \in U} l_i(t) - \sum_{v_i \in U} d_i(t) - 3N\sigma \\ &= E(t) - 3N\sigma, \end{aligned} \tag{11}$$

where $E(t) = \sum\limits_{v_i \in U} \varepsilon_i(t)$ is the sum of the error between the amount of actual consumed energy $l_i(t)$ and the amount of predicted energy demand $d_i(t)$.

When the amount of energy gap, $Gap(t)$, is positive, a shortage of energy in the grid exists. On the contrary, when the amount of energy gap $Gap(t)$ is negative, there is extra energy remained in the grid. Obviously, the objective of the utility provider is to make sure that $Gap(t) < 0$, and to minimize the $|Gap(t)|$ as follows:

$$\begin{aligned} \min \quad & |Gap(t)| \\ s.t. \quad & \begin{cases} Gap(t) \leq 0 \\ E(t) \geq 0 \\ \sigma \geq 0 \end{cases} \end{aligned}. \tag{12}$$

In the energy dispatching process, there are the following two cases: (i) the amount of energy supply is greater than the amount of predicted energy demand, and (ii) the amount of energy supply is less than the amount predicted energy demand. Therefore, the control center will make decisions based on the amount of energy gap $Gap(t)$. In the following, we describe these two cases in detail:

Case 1: Energy Supply is Larger Than Energy Demand

When the amount of energy demand is less than the amount of energy supply, $Gap(t) < 0$ exists. Then, the utility provider will require nodes, where the amount of predicted energy demand is more than the amount of actually consumed energy, store the extra energy according to the ratio of the error between the amount of actually consumed energy and the amount of predicted energy demand. If the extra energy is greater than the sum of errors between the amount of energy demand and the amount of actually consumed energy, the utility provider will allocate the residual energy to energy storage devices, which are deployed near to nodes. This means that if $\sum\limits_{v_i \in U_l} \varepsilon_i(t) \leq Gap(t)$, the amount of actual energy consumed by node i in the time duration t becomes

$$a_i(t) = \begin{cases} l_i(t), & v_i \in U_g \\ l_i(t) - \frac{\varepsilon_i(t)}{E_l(t)} \cdot Gap(t), & v_i \in U_l \end{cases}. \tag{13}$$

If $\sum\limits_{v_i \in U_l} \varepsilon_i(t) > Gap(t)$, the amount of actual energy consumed by node i in the time duration t is:

$$a_i(t) = \begin{cases} l_i(t) - \frac{Gap(t) - E_l(t)}{N}, & v_i \in U_g \\ d_i(t) - \frac{Gap(t) - E_l(t)}{N}, & v_i \in U_l \end{cases}. \tag{14}$$

Case 2: Energy Supply is Less Than Energy Demand

When the amount of energy demand is greater than the amount of energy supply, $Gap(t) > 0$ remains. The control

[1]In our preliminary study using real-world Google meters collected from houses over 200 days, we found that amount of energy usage can be approximated by normal distribution.

center will choose nodes that claim a higher amount of predicted energy demand and reduce the amount of energy to ensure the energy supply to other nodes. The objective of choosing outage nodes is to find:

$$\min \quad \|U_{outage}\| \qquad s.t. \quad \begin{cases} \sum_{v_i \in U_{outage}} d_i(t) \geq Gap(t), \\ \forall v_i \in U_{outage}, v_j \in U_g - U_{outage}, \varepsilon_i(t) \geq \varepsilon_j(t) \end{cases} \tag{15}$$

where the set U_{outage} is composed of outage nodes, and $\|U_{outage}\|$ is the number of elements in the set U_{outage}.

To the exclusion of outage nodes, the amount of energy gap in the grid is $Gap'(t) = Gap(t) - \sum_{v_i \in U_{outage}} l_i(t) \geq 0$. Then, the situation is similar to Case 1. Therefore, the amount of energy is dispatched to nodes as follows: If $\sum_{v_i \in U_l - U_c} \varepsilon_i \leq Gap'(t)$, the amount of actual energy consumed by node i in the time duration t is:

$$a_i(t) = \begin{cases} l_i(t), & v_i \in U_g - U_c \\ l_i(t) - \frac{\varepsilon_i(t)}{\sum_{v_i \in U_l - U_c} \varepsilon_i} \cdot Gap'(t), & v_i \in U_l \\ 0. & v_i \in U_c \end{cases} \tag{16}$$

If $\sum_{v_i \in U_l - U_c} \varepsilon_i > Gap'(t)$, the amount of actual energy consumed by node i in the time duration t is:

$$a_i(t) = \begin{cases} l_i(t) - \frac{Gap'(t) - \sum_{v_i \in U_l - U_c} \varepsilon_i}{N - \|U_{outage}\|}, & v_i \in U_g - U_c \\ d_i(t) - \frac{Gap'(t) - \sum_{v_i \in U_l - U_c} \varepsilon_i}{N - \|U_{outage}\|}, & v_i \in U_l \\ 0. & v_i \in U_c \end{cases} \tag{17}$$

In conclusion, the utility provider can dispatch the energy to node i according to $a_i(t)$.

IV. Performance Evaluation

In this section, we show the evaluation results of our approach in terms of detect accuracy and the effectiveness of attack mitigation on grid operations. In the following, we first present the evaluation setup and then detail the evaluation results.

A. Evaluation Setup

In our experiment, we consider a grid that consists of 50 nodes. There are two types of nodes in the system: bulk generation (BG) nodes and user nodes. BG nodes are referred to as power plants, which provide most of power to the grid. User nodes are referred to as users with renewable energy resources, which can request energy from the grid or supply extra energy to the grid. To distinguish nodes, we divide user nodes into four types: residential nodes, heavy industry nodes, light industry nodes, and tertiary industry nodes.

To present a realistic scenario, we used the historical electricity usage data in some provinces in Central China in August 2009. The historical data consists of hourly average consumed energy associated with different users. We divided data into two parts: one is used as the training set for the Bayesian network and the other is used as the test data. We assume that all smart meters report the amount of the predicted energy demand every half hour. To avoid outage, the utility provider needs to make sure that the amount of bulk generation is 10% more than the sum of user's demanded energy. We also assume that the capacity of the adversary is limited and can attack $1-4$ nodes in each time duration. To confirm the false data, with the conditional probability provided by our proposed approach, we consider the confidence threshold as the $[0, 0.93, 0.94, 0.95, 0.96]$. All our simulations are implemented in MATLAB.

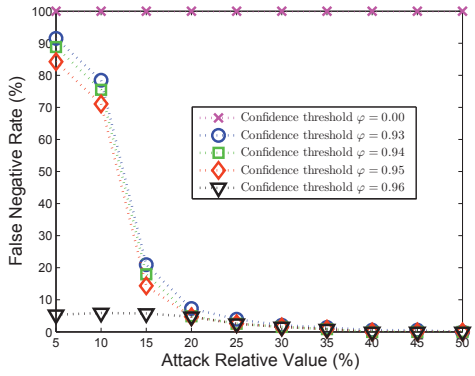

Fig. 3. False Negative Rate

Notice that in the simulation, we assume that there exists an adversary in the system, who has an objective of maximizing the damage of false data without being identified. We also compare our proposed approach with a baseline detection approach, which only performs the detection based on the amount of energy consumption without taking other correlated random factors into consideration. To verify the effectiveness of our proposed approach, we consider the following metrics: (i) The accuracy of detecting the false data injected by the adversary, and (ii) the energy damage loss raised by the error between the amount of the predicted energy demand and the amount of the actual consumed energy. To verify the accuracy of our proposed approach, we consider the following metrics: (i) *False Negative Rate* defined as the probability of that the false data that is confirmed as the true data, (ii) *Detection Accuracy* defined as the probability of that the false data are detected accurately.

B. Evaluation Results

In the following, we show evaluation results.

1) Accuracy of the Proposed Approach: **False Negative Rate:** Fig. 3 depicts the false negative rate of our proposed detection approach, which reflects the ratio of false data is confirmed as true. The results show that our approach can detect almost all the harmful false data injected by the adversary. Even though the adversary only manipulates the amount of predicted energy demand with a very small attack value, our approach can still detect most of them. For example, if the attack value approaches 40% of the original value, the false negative rate of our approach can approach almost 98%. Even though the attack value is 20% of the original value,

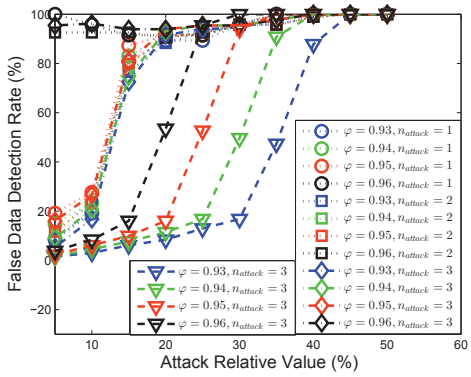

Fig. 4. Detection Rate

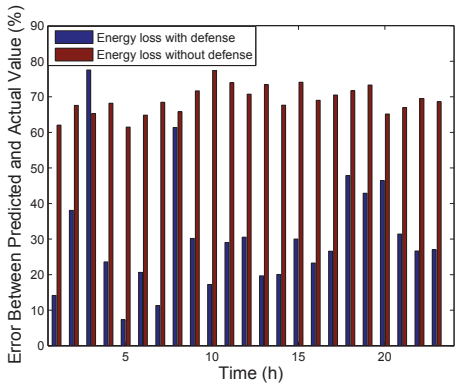

Fig. 5. Impact of False Data Injection Attacks

our approach can achieve a low false negative rate of 10%. Further, experimental results show that the greater confidence threshold φ can achieve a lower false negative rate. Therefore, the adversary who wants to launch false data injection attacks successfully has to inject a small attack strength in order to avoid being detected. Nonetheless, the damage caused by a small attack strength can be limited in a small range.

Accuracy on False Data Detection: As shown in Fig. 4, with the Bayesian conditional probability, our proposed approach can detect most of false data injection attacks. We compare our scheme with others under the different confidence threshold φ and different attack number n_{attack}. The results show that our proposed approach can detect most harmful false data injection attacks with varying confidence thresholds and attack strengths. For example, if the attack strength is more than 15% of the original predicted value, the detection rate approaches $70 - 90\%$ with various confidence thresholds. In addition, we compared our approach with a baseline approach, which is represented by curves with triangle in Fig. 4. Since the baseline approach does not consider factors captured by the conditional probability, it cannot achieve a high detection rate when the attack strength is relatively low.

2) Energy Loss: As shown in Fig. 5, the results show the error between the amount of predicted energy demand and the amount of actual consumed energy. We compare the amount of energy loss when our proposed approach in place with the energy loss injected by the adversary when our proposed approach is not in place. The false data injected by the adversary will increase the error between the amount of predicted energy demand and the amount of actual consumed energy, leading to wasted energy. As our proposed approach can accurately detect the injected false data (especially harmful ones), the amount of predicted energy demand will be much closer to the amount of actually consumed energy. Therefore, it is easier to maintain the balance between the energy demand and supply when the proposed approach is in place.

V. Conclusion

In this paper, we proposed an energy dispatching false data defense approach, also called EDF2D, to defend against false data injection attacks in smart grid. Our proposed approach can accurately detect the harmful false data injection from the user's energy demand information. Based on the historical data of user's energy usage, EDF2D establishes a Bayesian network, which derives from the Bayesian conditional probability, reflecting the authenticity of the user's energy demand information. With a properly configured confidence threshold, the proposed approach can accurately confirm whether the data is false or not. Through a combination of both theoretical analysis and performance evaluation, our results show that the proposed approach can accurately detect false data and effectively reduce the damage raised by attacks.

Acknowledgments

The work was supported in part by the National Science Foundation of China (NSFC) under Grant 61373115 and Grant 61402356. This work was supported by Fundamental Research Funds for the Project Funded by China Post doctoral Science Foundation (2015M572565) and the Fundamental Research Funds for the Central Universities (xkjc2015010). This work was also supported in part by the U.S. National Science Foundation (NSF) under the following grant: CNS 1350145. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding agencies.

References

[1] C. O. Adika and L. Wang. Demand-side bidding strategy for residential energy management in a smart grid environment. *IEEE Transactions on Smart Grid*, 5(4):1724–1733, 2014.

[2] K. Alsabti, S. Ranka, and V. Singh. An efficient k-means clustering algorithm. 1997.

[3] A. Anwar and A. N. Mahmood. Vulnerabilities of smart grid state estimation against false data injection attack. In *Renewable Energy Integration*, pages 411–428. Springer, 2014.

[4] J. Byun, I. Hong, B. Kang, and S. Park. A smart energy distribution and management system for renewable energy distribution and context-aware services based on user patterns and load forecasting. *IEEE Transactions on Consumer Electronics*, 57(2):436–444, 2011.

[5] M. Esmalifalak, N. T. Nguyen, R. Zheng, and Z. Han. Detecting stealthy false data injection using machine learning in smart grid. In *Proceedings of IEEE 2013 Global Communications Conference (GLOBECOM)*, pages 808–813, 2013.

[6] M. Esmalifalak, G. Shi, Z. Han, and L. Song. Bad data injection attack and defense in electricity market using game theory study. *arXiv preprint arXiv:1210.3252*, 2012.

[7] X. Fang, S. Misra, G. Xue, and D. Yang. Smart grid the new and improved power grid: A survey. *IEEE Communications Surveys & Tutorials*, 14(4):944–980, 2012.

[8] Y. Huang, M. Esmalifalak, H. Nguyen, R. Zheng, Z. Han, H. Li, and L. Song. Bad data injection in smart grid: attack and defense mechanisms. *IEEE Communications Magazine*, 51(1):27–33, 2013.

[9] L. Jia, R. J. Thomas, and L. Tong. Malicious data attack on real-time electricity market. In *Proceedings of 2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 5952–5955, 2011.

[10] F. Li, W. Qiao, H. Sun, H. Wan, J. Wang, Y. Xia, Z. Xu, and P. Zhang. Smart transmission grid: vision and framework. *IEEE Transactions on Smart Grid*, 1(2):168–177, 2010.

[11] Y. Li and Y. Wang. State summation for detecting false data attack on smart grid. *International Journal of Electrical Power & Energy Systems*, 57:156–163, 2014.

[12] J. Lin, W. Yu, and X. Yang. On false data injection attack against multistep electricity price in electricity market in smart grid. In *Proceedings of IEEE 2013 Global Communications Conference (GLOBECOM)*, pages 760–765, 2013.

[13] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao. On false data injection attacks against distributed energy routing in smart grid. In *Proceedings of 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems (ICCPS)*, pages 183–192, 2012.

[14] Y. Liu, P. Ning, and M. K. Reiter. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security (TISSEC)*, 14(1):13, 2011.

[15] Z. Lu, X. Lu, W. Wang, and C. Wang. Review and evaluation of security threats on the communication networks in the smart grid. In *Proceedings of IEEE Military Comminication Conference (MILCOM)*, pages 1830–1835, 2010.

[16] K. Manandhar, X. Cao, F. Hu, and Y. Liu. Combating false data injection attacks in smart grid using kalman filter. In *Proceeding of IEEE 2014 International Conference on Computing, Networking and Communications (ICNC)*, pages 16–20, 2014.

[17] P. Moulema, W. Yu, D. Griffith, and N. Golmie. Performance evaluation of smart grid applications using co-simulation. In *Proceedings of IEEE International Conference on Computer Communication and Networks (ICCCN)*, pages 1–8, 2015.

[18] H. Sedghi and E. Jonckheere. Statistical structure learning of smart grid for detection of false data injection. In *Proceedings of IEEE 2013 Power and Energy Society General Meeting (PES)*, pages 1–5, 2013.

[19] P. Siano. Demand response and smart gridsa survey. *Renewable and Sustainable Energy Reviews*, 30:461–478, 2014.

[20] D. Wang, X. Guan, T. Liu, Y. Gu, C. Shen, and Z. Xu. Extended distributed state estimation: A detection method against tolerable false data injection attacks in smart grids. *Energies*, 7(3):1517–1538, 2014.

[21] S. Wang and W. Ren. Stealthy false data injection attacks against state estimation in power systems: Switching network topologies. In *Proceedings of 2014 IEEE American Control Conference (ACC)*, pages 1572–1577, 2014.

[22] L. Xie, Y. Mo, and B. Sinopoli. False data injection attacks in electricity markets. In *Proceedings of 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 226–231, 2010.

[23] L. Xie, Y. Mo, and B. Sinopoli. Integrity data attacks in power market operations. *IEEE Transactions on Smart Grid*, 2(4):659–666, 2011.

[24] Q. Yang, L. Chang, and W. Yu. On false data injection attacks against kalman filtering in power system dynamic state estimation. *Journal of Security and Communication Networks (SCN)*, 2013.

[25] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao. On false data-injection attacks against power system state estimation: Modeling and countermeasures. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 25(3):717–729, 2014.

[26] W. Yu, D. An, D. Griffith, Q. Yang, and G. Xu. On statistical modeling and forecasting of energy usage in smart grid. In *Proceedings of ACM International Conference on Reliable and Convergent Systems (RACS)*, pages 12–17, 2014.