Mitigating Stealthy False Data Injection Attacks Against State Estimation in Smart Grid

Jingyao Fan*, Youssef Khazbak*, Jue Tian†, Ting Liu† and Guohong Cao*
*Department of Computer Science and Engineering, The Pennsylvania State University, University Park, PA 16802
†School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, Shaanxi, China
Email: {jxf376, ymk111, gcao}@cse.psu.edu, {juetian,tliu}@sei.xjtu.edu.cn

***Abstract*—With the enhanced capabilities of the SCADA system, the power system can monitor its operating states in real-time. On the other hand, it also makes the power system more vulnerable to various kinds of attacks. One attack that has serious consequences is the False Data Injection (FDI) attack against the state estimation process. Although some techniques have been proposed to select meters to protect, none of them considers the cost of protecting meters, and thus will not perform well when only a limited number of meters can be protected due to budget limitation. In this paper, we consider a new problem: Given a limited budget, how to select the most critical meters to protect so that the probability of attackers launching successful stealthy FDI attack is minimized? We first formalize this problem which is NP-complete, and then propose heuristic based solutions. The idea is to rank and select meters based on a metric called vulnerability index, which considers two factors: how likely the meter will be targeted by the attacker to launch FDI attacks and how much damage will be caused by compromising the meter in case of a successful stealthy FDI attack. Evaluation results show that our algorithm can significantly reduce the probability of successful attacks, as well as the potential damage caused by FDI attacks.**

I. Introduction

Today's power system relies on Supervisory Control and Data Acquisition (SCADA) [1] to monitor and control the generation, transmission, and distribution of electricity. With its enhanced control and monitoring capabilities, SCADA can remotely monitor and control the power system to make sure it operates normally. In particular, there is a state estimation process where the control center estimates the state variables of the power system based on meter measurements [2]. These estimates will then be passed on to all system operators to control the physical components of the smart grid.

The evolution of the smart grid technology, especially the integration of the cyber-physical technology, has brought in many improvements to the electric power infrastructure, resulting in higher efficiency and reliability [3], [4]. However, it also brings a large amount of potential security threats to the power system [5], [6]. For example, it is possible that the attacker can compromise meter measurements and mislead the control center to make false estimates of the state variables. Such attacks may cause great damage to the power system and lead to serious consequences [7], [8]. Among them Liu *et al.* [7] were the first to demonstrate that a new FDI attack could circumvent bad data detection (BDD) techniques in today's SCADA system. They prove that with the knowledge of the power system configuration, the attacker can introduce arbitrary bias to estimated state values without being detected. Such an attack is referred to as an stealthy false data injection attack.

To protect the power system against such stealthy false data injection attacks, many researchers have proposed various solutions [9], [10], [11], [12]. In [12], the authors propose that by secretly changing the configuration of the bus system, the attacker will not be able to construct stealthy attacks since he only knows the previous configuration. However, it is possible for the attacker to learn and guess the new configuration. In [9], algorithms have been proposed to place PMUs (which can directly measure the bus voltage phasor with GPS timestamp) to directly verify the estimates of selected measurements independently, but these solutions are vulnerable to GPS spoofing attacks [13]. In [14], [10], [11], different algorithms have been proposed to select and protect meters to make sure that the stealthy FDI attacks will not succeed. However, all of them need to protect a relatively large number of meters (e.g., proportional to the number of bus in the system), which may not be practical for large systems with a limited budget.

In this paper, we consider a new problem: *Given a limited budget, how to select the most critical meters to protect so that the probability of attackers launching successful stealthy FDI attack is minimized?* We first formalize this problem which is NP-complete, and then propose heuristic based solutions. The idea is to rank and select meters based on a metric called *vulnerability index*, which considers two factors: (1) how likely the meter will be targeted by the attacker to launch FDI attacks; (2) how much damage will be caused by compromising the meter in case of a successful stealthy FDI attack. The major contributions of this paper are summarized as follows:

- We are the first to consider the cost constraint in selecting meters to protect against FDI attack, and we formalize the meter selection problem under a budget limitation.
- We propose a novel metric to rank the meters and propose a heuristic based algorithm to select meters based on the proposed metric.
- By launching false data injection attacks against IEEE 14 bus, 30 bus, 57 bus, 118 bus and 300 bus system, we demonstrate that the proposed algorithm can significantly reduce the probability of successful attacks, as well as the potential damage caused by FDI attacks.

The rest of the paper is organized as follows. Section II

overviews the related work. Section III presents preliminaries. Section IV formulates the problem and Section V presents our solution. Performance evaluations are presented in Section VI and Section VII concludes the paper.

II. Related Work

False data injection attacks have been studied in different fields, such as wireless sensor network [15], [16], control system [17], etc. Among them, false data injection attacks against the state estimation in smart grid have attracted considerable attention. In [7], [8], different attack scenarios were presented and the damage of the proposed attacks were demonstrated. Among them, Liu *et al.* [7] were the first to show that bad data detection (BDD) techniques could be bypassed if the attacker knew the configuration of the power system and demonstrated how to construct such attack vectors.

To mitigate the stealthy false data injection attacks, a large amount of research has been done. In [10], [11], [18], different algorithms have been proposed to select a set of meters to protect so that the attacker cannot launch false data injection attacks without being detected. However, none of the existing research considers the cost of protecting meters, and thus will not perform well when only a limited number of meters can be protected due to budget limitation.

III. Preliminaries

A. State Estimation

To maintain system reliability, the control center needs to monitor the running state of the power system. Some values can be observed directly from meters, such as line power flow, bus voltage magnitude, etc. However, there are some state variables that cannot be observed directly, such as bus voltage angles, etc. Thus, the control center needs to estimate these state variables using those values that are observable, and this is the state estimation process.

Let n denote the number of buses in the system and m denote the number of meters in the system. Let $\mathbf{x} = (x_1, x_2, ..., x_n)^T$ denote the state variables we want to estimate. Let $\mathbf{z} = (z_1, z_2, ..., z_m)^T$ denote the meter measurements. Based on the topology and configuration of the system as well as power laws such as power balance theory and Kirchhoff's Law, the state estimation problem can be formulated as follows:

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e},$$

$\mathbf{h}(\mathbf{x}) = (h_1(x_1, x_2, ..., x_n), ..., h_m(x_1, x_2, ..., x_n))^T$ and $h_i(x_1, x_2, ..., x_n)$ is a function of $(x_1, x_2, ..., x_n)$. $\mathbf{e} = (e_1, e_2, ..., e_m)^T$ are measurement errors, with $e_j \in R$, $j = 1, 2, ..., m$. The goal of state estimation process is to find an estimate $\hat{\mathbf{x}}$ of $\mathbf{x}$ that fits the measurement $\mathbf{z}$ and the above equation the best.

In this paper, we consider the DC power flow model, and the above state estimation problem can be simplified to the following model:

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

where $\mathbf{H} = (h_{i,j})_{m*n}$. $\mathbf{H}$ is usually called the measurement Jacobian matrix, and it is solely determined by the topology and configuration of the power system. Once the topology and configuration of the power system are fixed, it will not be changed by any real-time measurements such as voltage/current/power flow, etc.

B. Power System and Assumptions

In this paper, we consider the IEEE 14 bus, 30 bus, 57 bus, 118 bus and 300 bus system. Each bus in the grid is considered as a node, and power lines connecting buses are considered as edges between nodes. For each bus, there are meters connected to it measuring important data such as voltage and power.

With a limited budget, we need to decide which meters to protect so that the attackers' chance of launching successful attack is minimized. By "protection", we aim to prevent the meter readings against either form of manipulation: 1) tampering with the communication between meters and the control center; 2) tampering the meter physically. To secure the communications between meters and the control center, we can take advantage of proposed tamper-proof communication algorithms [19]. However, such algorithms require high computation capability and thus are not feasible with most previous smart meter models [20]. It is not possible to replace/upgrade millions of smart meters that have already been deployed. To protect smart meters against physical tampering, additional hardware such as tamper detection devices and video monitoring devices need to be installed. Such hardware and devices are costly to install and maintain, and thus it is not possible to secure every meter in the grid. Furthermore, the cost to protect different meters is different. For example, some meters have more complex hardware/software than others and may cost more to upgrade [21], [22]; some meters are located in the remote area and will cost more [23] (such as transportation, labor, etc.) to protect, etc.

C. Threat Model

The measurements used for state estimation may be inaccurate due to hardware malfunction, malicious behavior, etc., and this may cause the control center to have wrong estimates of state variables. Thus, it is very important for the power system to detect bad data. The most commonly used approach for bad data detection (BDD) is to use the L2-norm of measurement residual:

$$||\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}||$$

Here, $\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}$ is the measurement residual, which shows the difference between the vector of observed measurements and the vector of estimated measurements. $||\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}||$ is compared with a certain threshold τ. If $||\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}|| > \tau$, there is bad data and the state estimation results will be discarded by the control center. It can be proved mathematically that $||\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}||^2$ follows a χ^2 distribution with $v = m - n$ as the degree of freedom, assuming that all state variables are independent and meter errors follow a normal distribution [24]. τ can be

determined through a hypothesis test with a significance level α.

From the attacker's point of view, there is no point of launching a false data injection attack if the injected bad data will be detected by the aforementioned bad data detection process. Thus, we assume that the attacker only launches attacks that can bypass bad the data detection process. If the attacker chooses the attack vector wisely, it can pass the bad data detection.

Suppose the attacker chooses a non-zero arbitrary attack vector $\mathbf{a} = (a_1, a_2, ..., a_m)^T$, and then adds it to the original measurements to get the malicious measurements $\mathbf{z_a} = \mathbf{z} + \mathbf{a}$. Let $\hat{\mathbf{x}}_{\mathbf{bad}}$ and $\hat{\mathbf{x}}$ denote the estimates of $\mathbf{x}$ using the malicious measurements $\mathbf{z_a}$ and the original measurements $\mathbf{z}$, respectively. $\hat{\mathbf{x}}_{\mathbf{bad}}$ can be represented like this:

$$\hat{\mathbf{x}}_{\mathbf{bad}} = \hat{\mathbf{x}} + \mathbf{c}$$

Here $\mathbf{c}$ denotes the estimation error caused by the attack. As shown in [7], if the attacker chooses $\mathbf{Hc}$ to be the attack vector $\mathbf{a}$, then the L2-norm of the measurement residual of $\mathbf{z_a}$ is equal to that of $\mathbf{z}$. Thus, the malicious measurements can pass bad data detection as long as the original measurements $\mathbf{z}$ can pass the detection.

Theorem 1: If the attacker can compromise k specific meters, where $k \geq m - n + 1$, he/she can always construct an attack vector to bypass the detection.

Proof: As shown above, the attack vector that can pass bad data detection is $\mathbf{a} = \mathbf{Hc}$. Let $\mathbf{P} = \mathbf{H}\left(\mathbf{H^T H}\right)^{-1}\mathbf{H^T}$, and $\mathbf{B} = \mathbf{P} - \mathbf{I}$.

$$\begin{aligned}\mathbf{a} = \mathbf{Hc} &\Longleftrightarrow \mathbf{Pa} = \mathbf{PHc} \\ &\Longleftrightarrow \mathbf{Pa} = \mathbf{H}\left(\mathbf{H^T H}\right)^{-1}\mathbf{H^T Hc} \\ &\Longleftrightarrow \mathbf{Pa} = \mathbf{Hc} \Longleftrightarrow \mathbf{Pa} = \mathbf{a} \\ &\Longleftrightarrow \mathbf{Pa} - \mathbf{a} = \mathbf{0} \Longleftrightarrow \mathbf{Ba} = \mathbf{0}\end{aligned}$$

$\mathbf{H}$ is an $m * n$ full rank matrix. Assuming $m \geq n$, $rank(\mathbf{H}) = n$. Since $\mathbf{P} = \mathbf{H}\left(\mathbf{H^T H}\right)^{-1}\mathbf{H^T}$, $rank\left(\mathbf{P}\right) = rank\left(\mathbf{H}\right) = n$. Obviously, for $\mathbf{B} = \mathbf{P} - \mathbf{I}$, $rank\left(\mathbf{B}\right) = m - n$. Since the attacker can compromise k meters, then only k elements in $\mathbf{a}$ are non-zero. We get the k corresponding columns from $\mathbf{B}$ to get a new matrix $\mathbf{B'}$. Since $k \geq m - n + 1$, we have $rank\left(\mathbf{B'}\right) <= m - n < k$. Thus, $\mathbf{B}$ is a rank deficient matrix and there exist infinite number of non-zero solutions. □

We assume that the attacker can compromise k meters. He will try to construct the attack vectors that can pass the BDD process using the compromised measurements and launch attacks using all available attack vectors.

IV. Problem Formulation

A. System Model

In our system, there are three major elements: buses, transmission lines, and meters. The attacker will try to compromise certain meters and launch stealthy FDI attacks against the power system. If the FDI attack can not be detected by the BDD of the power system, it is called a *successful attack*.

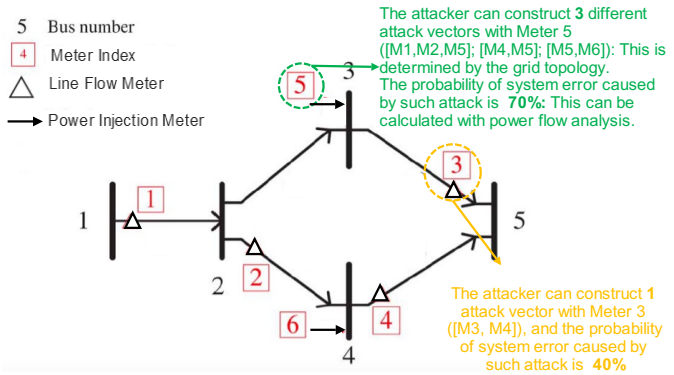

Fig. 1. Demo with 5 Bus System: Meter 5 should be protected before Meter 3.

There are many meters in the power grid, and the cost of protecting different types of meters may be different. For example, installing malware on different models of meters may cost differently, and installing physical protection for meters of different sizes may cost differently. Suppose we have a limited budget (denoted as C), and we have to select meters to protect among all meters. Our goal is to select the most important meters to protect. For example, as shown in Fig. 1, suppose we can only afford to protect one meter among meter 5 and meter 3, which one should we choose? Obviously, meter 5 is more vulnerable than meter 3 since it can be used to launch more attacks and then bring more damage to the system once the attack is successful. The techniques to identify such meters and to calculate the importance of these meters will be presented in the following sections.

B. Meter Selection Problem

Our goal is to select the most important meters to protect so that the probability of attachers launching successful stealthy FDI attack is minimized.

1) Original Problem: We want to select certain meters so that we can maximize our gain with a given cost. Suppose the chosen meters are $m_{k_1}, m_{k_2}, ..., m_{k_l}$, we first need to calculate the combined influence (denoted by matrix $\mathbf{I}$) of these l chosen meters on the grid. The meter selection problem can be formally defined as below:

$$\text{Maximize } Gain = \mathbf{I} \cdot \mathbf{m} \tag{1}$$

$$\text{ST } \sum c_i \leq C \tag{2}$$

$$\text{ST } i = k_1, k_2, ..., k_l, \mathbf{m} = (m_{k_1}, m_{k_2}, ..., m_{k_l})^T \tag{3}$$

Here, c_i denotes the cost of protecting m_i. It is clear that this problem is an integer programming problem, which is NP-complete. The following is a reduction from the minimum vertex cover to the integer programming that can be served as the proof of NP-completeness. Let $G = (V, E)$ be an undirected graph. Define a linear program as follows:

$$\begin{aligned}&\min \sum_{v \in V} y_v \\ &y_v + y_u \geq 1 \ \forall u, v \in E \\ &y_v \in \mathbb{Z}?_{\geq 0} \ \forall v \in V\end{aligned} \tag{4}$$

Given that the constraints limit y_v to either 0 or 1, any feasible solution to the integer program is a subset of vertices. The first constraint implies that at least one end point of every edge is included in this subset. Therefore, the solution describes a vertex cover. Additionally given some vertex cover C, y_v can be set to 1 for any $v \in C$ and to 0 for any $v \notin C$ thus giving us a feasible solution to the integer program. Thus we can conclude that if we minimize the sum of y_v we have also found the minimum vertex cover.

2) Approximated Problem: In this section, we will introduce our Approximated Meter Selection Problem. In the original problem, for each possible combination of meters, we need to calculate the joint gain by protecting all meters in the combination. However, it is difficult to actually quantify this joint gain, since it is difficult to quantify the inter-influence between meters in a group. Thus, we define an approximated problem that treat each meter independently, and simply assume that the joint gain of protecting a group of meters is simply the sum of the gain of protecting each meter in the group. Let m_i denote meter i and c_i denote the cost of protecting m_i. Let $critical_i$ denote the critical degree of m_i. Our approximated meter selection problem can be expressed more formally as below:

$$\text{Maximize } Gain = \sum critical_i * x_i \tag{5}$$

$$\text{ST } \sum c_i * x_i \leq C; \tag{6}$$

$$\text{ST } x_i \in \{0,1\}, i = 0,1,2,...,n; \tag{7}$$

In the above model, x_i is the indicator variable to be determined. $x_i = 1$ if m_i is selected; $x_i = 0$ otherwise. The purpose of the optimization is to determine the variables x_i to maximize the gain subject to the constraints 6 and 7. Constraint 6 states that the total cost of protecting selected meters should not exceed the given budget.

Theorem 2: The Approximated Meter Selection Problem is NP-complete.

Proof: The problem of Meter Selection can be proved to be NP-complete via a reduction from the Knapsack problem, which can be stated as follows. Given a set of n items numbered from 1 up to n, each with a weight w_i and a value v_i, along with a maximum weight capacity W,

$$\text{maximize } \sum_{i=1}^{n} v_i x_i$$

$$\text{subject to } \sum_{i=1}^{n} w_i x_i \leq W \text{ and } x_i \in \{0,1\}.$$

Here x_i represents the number of instances of item i to include in the knapsack. Informally, the problem is to maximize the sum of the values of the items in the knapsack so that the sum of the weights is less than or equal to the knapsack's capacity. It is quite obvious to see the reduction: let C be the weight capacity of the knapsack, c_i be the weight of each item and $critical_i$ be the value of each item. Our meter selection problem the becomes a knapsack problem. □

V. The Proposed Meter Selection Algorithm

In this Section, we explain our solution in details. First, we will introduce an important concept, *target set*, and our algorithms to search for target sets. Then we will introduce our novel metrics: *Attack Centrality, Damage Index and Vulnerability Index*. In the end, we will demonstrate how we use target sets and our novel metrics to select meters to protect.

A. Target Set

The attackers will only launch stealthy FDI attacks, and only certain meters can be used to construct valid attack vectors. Thus, we only need to protect the meters that are likely to be chosen by the attackers. In other words, we need to find out the meters that will be in the attack vectors to be candidates for protection.

A target set is a set of meters that satisfy the following two conditions: 1) The attacker can launch a successful false data injection attack with the meters in the target set without being detected; 2) Attacking any subset of meters in this target set will be detected.

Theorem 3: rank($\mathbf{H} - \mathbf{S}$) = rank($\mathbf{H}$) - 1. $\mathbf{S}$ denotes all the rows corresponding to the target set.

Algorithm 1 Target Sets Search Algorithm

```
Input: measurement Jacobian matrix H, size of target sets is k (initialized to 1), K that contains all the possible sets whose size is k
output: Set of all target sets S
Initialize: k = 1, K = {{a_1}, {a_2}, ..., {a_m}} , where a_i is the i^th row of matrix H
while k ≤ m and K is not empty do
    for each set E in K do
        if rank(H − E) == n − 1 then
            if no strict subsets of E is in S then
                put E in S
            end if
        end if
        if rank(H − E) == n then
            put all E + 1 in K
        end if
        k = k + 1
    end for
end while
```

Proof: Since the rows of S can form an attack vector for stealthy FDI attack, we have $rank(\mathbf{H} - \mathbf{S}) < rank(\mathbf{H})$. Since the rows of any subset of $\mathbf{S}$ cannot form a stealthy FDI attack, $\forall\ \mathbf{P} \subset \mathbf{S}$, we have $rank(\mathbf{H} - \mathbf{P}) = rank(\mathbf{H})$.

Suppose there exists a target subset $\mathbf{S}'$ that satisfies the following condition: $rank(\mathbf{H} - \mathbf{S}') < rank(\mathbf{H}) - 1$. We can keep removing rows from $\mathbf{S}'$ until the new set $\mathbf{S}''$ satisfies: $rank(\mathbf{H} - \mathbf{S}'') = rank(\mathbf{H}) - 1$. Then, we have $\mathbf{S}''$, which is also a target set. Since $\mathbf{S}'' \subset \mathbf{S}'$, according to the condition 2) of the definition of target set, $\mathbf{S}'$ cannot be a target set. There

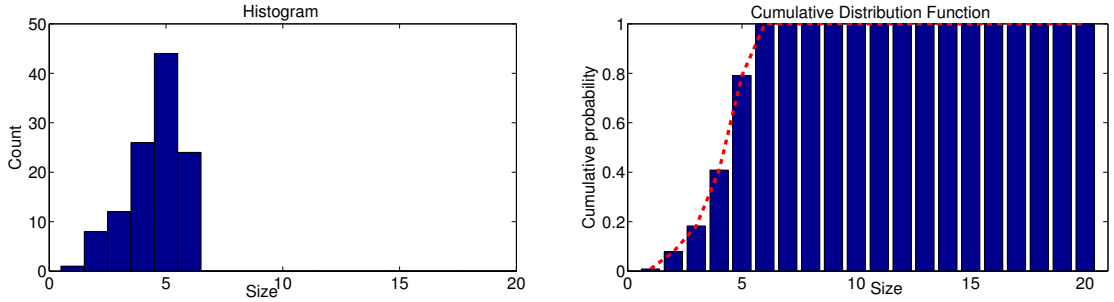

Fig. 2. IEEE 14-Bus System: histogram and CDF of the size of target sets

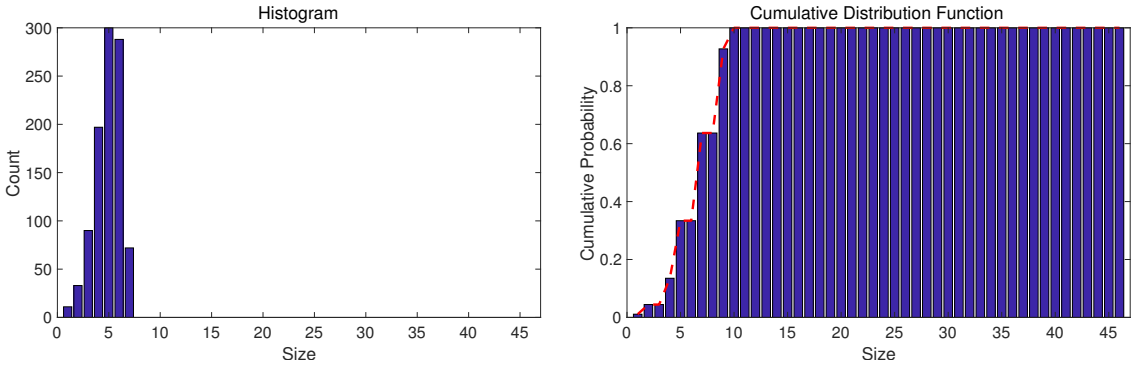

Fig. 3. IEEE 39-Bus System: histogram and CDF of the size of target sets

is a controdiction. Thus, $rank(\mathbf{H}-\mathbf{S}) = rank(\mathbf{H}) - 1 \ \forall \ \mathbf{S}$ that is a target set. □

We need to consider meters in the union of all target sets, and thus we need to find all the target sets before selecting crucial meters. Our target sets search algorithm is shown in Algorithm 1.

Here, $\mathbf{E}+1$ means all sets that have $\mathbf{E}$ as its strict subset and whose size is larger than $\mathbf{E}$ by 1. Since the search with different k is independent, we can use multi-threads to run the algorithm, where each thread is responsible for finding potential target sets (sets with rank $rank(\mathbf{H})-1$) of different size. The parrellel search algorithm is shown in Algorithm 2.

Algorithm 2 Parrellel Search Algorithm

```
Input: Thread number i, measurement Jacobian matrix H,
    all possible sets with current size K_i
output: Set of all potential target sets S_i
for each set E in K_i do
    if rank(H − E) == n − 1 then
        put E in S_i
    end if
end for
```

After all potential sets are found, we check from $k=1$ to $k=m$ to find out the true target sets (sets with no subsets as target sets).

1) Upper bound of the size of the target sets: In the search algorithms we have introduced, we need to search for all possible subsets of the meters and check if each one is a target set. However, if the number of meters is large, this search space will be exponentially increased, and hence we need to reduce the search space. One possible solution is to set an upper bound to the size of target sets being searched, since most target sets are of relatively small size (e.g., 6). This assumption is reasonable due to the following:

(1) In our experiments, we found that the size of the target set is usually small. As shown on the left side of Fig. 2, for the IEEE 14-Bus system, no target set has size larger than 6. As shown on the left side of Fig. 3, for the IEEE 39-Bus System, no target set has size larger than 7. The target set size does not grow too much even when the number of buses significantly increases. We can also see from the right figures in both Fig. 2 and Fig. 3, the cumulative distribution function of target set size for the two bus systems are quite similar.

(2) From the attacker point of view, if the number of meters that need to be compromised is large, it is less likely for him to launch the attack. In other words, when different attack vectors are available, the attacker will choose the one with fewer meters to compromise.

Next, we rely on a probability-based model to calculate the proper cut-off size of the target sets. First, we obtain the cumulative distribution functions of the target set size for IEEE 14 bus system, 30 bus system and 39 bus system. Then, we obtain a fitting curve $F(k,m)$ from the above functions using exponential regression analysis:

$$F(k,m) = B(m) * P(k)$$

where k denotes the size of target sets, and m denotes the number of buses in the system. To determine the cut-off size, we first find $CoverRate$ (how many target sets among all target sets to cover). In our experiments, we choose 80% as our $CoverRate$. With the chosen $CoverRate$ and the above

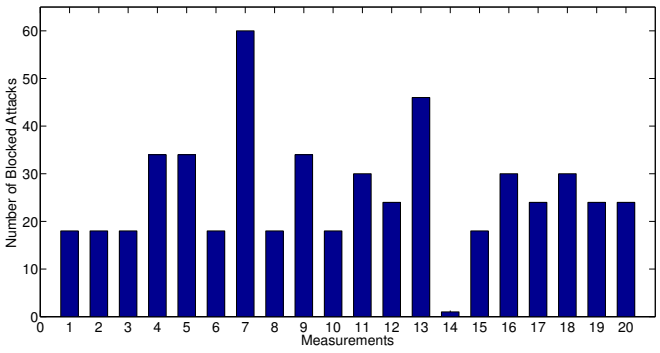

Fig. 4. 14 bus System: the number of attack vectors blocked by protecting each meter

fitting curve, we are able to obtain the cut-off size C_s for any given bus system from the equation below:

$$F(C_s, m) = CoverRate$$

where m is the number of meters in the target bus system.

B. Metrics

Even though all meters in the target sets are likely to be used by the attacker to launch stealthy FDI attacks, they are not equally vulnerable. The more attack vectors a meter can form, the more vulnerable it is. For example, suppose there are 3 different attack vectors that can bypass BDD: $\{m_1, m_2, m_5\}$, $\{m_1, m_3, m_4\}$, $\{m_1, m_5, m_6\}$. Then, m_1 is the most vulnerable meter, and by protecting this meter, we will be able to block all three potential attacks. m_5 is the second vulnerable, and two potential FDI attacks will be blocked if it is protected. Protecting the other four meters (m_2, m_3, m_4, m_6) can only block one potential attack, and hence less important.

Different FDI attacks may affect different buses and power lines in the grid and thus cause different problems to the power system. For example, the attack that causes power outage on a major power line connecting to New York City is certainly more dangerous than a secondary power line connecting to a small town, since it will affect more people and cause more damage to the power system. Thus, we also consider this important factor - the damage of the potential attack, when determining how crucial each meter is. The more damage the attacks constructed with the meter can cause, the more critical this meter is. To quantify the effects of these two factors, we define two metrics: *Attack Centrality* and *Damage Index*.

1) Attack Centrality: Even though all meters are likely to be compromised by the attacker, and protecting any meter is helpful, the benefits of protecting different meters are different.

As shown in Fig. 4, for the IEEE 14-Bus system, by protecting each meter, the number of attack vectors that can be blocked is different. For example, by protecting meter 7, 60 attack vectors become invalid. However, by protecting meter 14, only 1 attack vector is disabled. Thus, protecting meter 7 can provide more benefits than protecting meter 14. To prioritize the vulnerable meters (meters in the union of the target sets), "Attack centrality" is used to quantify the importance of a meter.

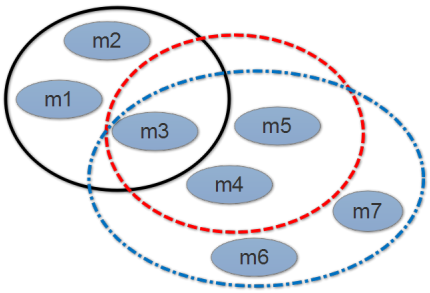

Fig. 5. Demonstration of Attack Centrality

$$AC_i = \sum_{j=1,2,\ldots,N} \mathbf{I}_{TS_j}(m_i)$$

Where N demotes the number of target sets, TS_j denotes the j^{th} target set, and m_i denotes the i^{th} meter. $\mathbf{I}()$ is an indicator function:

$$\mathbf{I}_{TS_j}(m_i) = \begin{cases} 1 & \text{if } m_i \in TS_j, \\ 0 & \text{if } m_i \notin TS_j. \end{cases}$$

Fig. 5 is a simple demonstration of how the Attack Centrality metric is used. As shown in the figure, the attack centrality of m_1, m_2, m_6, m_7 is 1, the attack centrality of m_4, m_5 is 2, and the attack centrality of m_3 is 3. Thus, m_3 is the most important mode, and should be the first to be protected.

2) Damage Index: With Attack Centrality, we have considered the "importance" of each meter in terms of how likely the attacker will target on it. However, for different successful attacks, the damage they bring to the power system are different. Thus, when choosing meters to protect, we should also consider the potential damage to the power system once the meter is compromised and try to protect the meters that might bring more damage. To analyze the potential damage associated with each meter, we adapt the sensitivity analysis of power system. There are two popular sensitivity analysis: $n-1$ and $n-k$. Since here we want to study the damage caused by each meter independently, we choose the $n-1$ analysis. To quantify how much damage a meter might bring if it is compromised during a successful FDI attacks, we define a metric *Damage Index* as:

$$DI_i = \sum_{j \neq i} \gamma \cdot P_{j,i} \cdot Sensitivity_{j,i}$$

Here, j, i denotes power line that connects meter j and meter i. $P_{j,i}$ is the current power flow (in MW) in power line j, i. It can be observed from meter readings directly. $Sensitivity_{j,i}$ denotes the influence of line j, i on the other lines in the power system. It can be obtained through power system contingency analysis [25].

$$Sensitivity_{j,i} = \sum_{(j,i) \neq (l,k)} \frac{1}{2} \left(\frac{P_{l,k}}{{P_{l,k}}^{lim}} \right)^2$$

${P_{l,k}}^{lim}$ is the power capacity (in MW) of transimission line l, k. It solely depends on the power grid topology and configuration. Power capacity values of widely used power systems

TABLE I
NUMBER OF COMPUTATIONS NEEDED TO SEARCH TARGET SETS

Bus System	Number of Computations
24-Bus System	$5 * e^{10}$
30-Bus System	$3 * e^{10}$
39-Bus System	$1 * e^{9}$

TABLE II
NUMBER OF COMPUTATIONS NEEDED TO SEARCH TARGET SETS W. UPPER BOUND (UBOUND)

Number of Meters	UBound = 5	UBound = 6	UBound = 7
80(57-Bus System)	$2 * e^{7}$	$3 * e^{8}$	$3 * e^{9}$
186(118-Bus System)	$2 * e^{9}$	$5 * e^{10}$	$1 * e^{12}$

are available to the public and can be loaded from MATLAB power models.

3) Vulnerability Index: Both *Attack Centrality* and Damage Index affect how crucial each meter is. Thus, when selecting the most crucial meters to protect, we need to consider both factors at the same time. To quantify the joint effect of the two metrics, we define the *Vulnerability Index* of a meter i (VI_i) as:

$$VI_i = \alpha \cdot AC_i + (1 - \alpha) \cdot DI_i$$

where $0 < \alpha < 1$. We will rank all the meters that might be targeted by the attacker according to their $VulnerabilityIndex_i/cost_i$ and select the top k meters, where k is determined by the given cost.

C. Meter Selection

The meters are selected according to Algorithm 3.

Algorithm 3 Greedy Algorithm

```
Input: budget C, for each meter m_i, its vulnerability index VI_i and cost to protect it c_i
output: Selected meter set S
Rank the meters based on VI_i/c_i from high to low. Let L denote the ranked list.
while C > 0 do
    for each m_i ∈ L do
        if C > c_i then
            S = S ∪ {m_i}
            L = L \ {m_i}
            C = C − c_i
            break
        end if
    end for
end while
```

The greedy algorithm is executed in iterations. During each iteration, it picks the meter with the high vulnerability and low protecting cost. The whole process is then repeated, until we have used up all the budget.

Theorem 4: The greedy algorithm has an approximation ratio of $1/2$.

Proof: Let k be the index of the first item that is not accepted by greedy algorithm. Consider the following claim:

Claim 1: $VI_1 + VI_2 + ... + VI_k \geq OPT$. In fact, $VI_1 + VI_2 + ... + \alpha VI_k \geq OPT$. where $\alpha = (C - (c_1 + c_2 + + c_{k-1}))/c_k$, is the fraction of item k that can still fit in the knapsack after packing the first $k-1$ items.

The proof of Theorem 4 follows immediately from the claim. In particular, either $VI_1 + VI_2 + ... + VI_{k-1}$ or VI_k must be at least $OPT/2$. We now only have to prove Claim 1. Now set $x_1 = x_2 = ... = x_{k-1} = 1, x_k = \alpha$, and $x_i = 0$ for all $i > k$. This is a feasible solution to our problem that cannot be improved by changing any one tight constraint, as we sorted the items. $VI_1 + VI_2 + ... + \alpha VI_k \geq OPT$. The first statement of the lemma follows from the second as $alpha \leq 1$. □

VI. PERFORMANCE EVALUATIONS

In this section, we evaluate the performance of our meter selection algorithm. Since there is no existing work on meter selection, we compare it to RandomSelect, which randomly selects the same number of meters as ours based on the cost requirement.

A. Computation Cost

In this section, we evaluate the computation cost of our proposed meter selection algorithm. It is easy to see that most of the computation cost is on searching target sets. The runtime of our search algorithm on IEEE 14 bus system is shown in Fig. 6, and the total search time is around 20 seconds. For larger systems, the computation overhead grows exponentially in theory. The number of computations needed for IEEE 14-Bus, 30-Bus and 39-Bus Systems are shown in Table I. In our experiments, our algorithm can run 20,000 computations per second. Then, 39-Bus System will take around 12 hours to search all sets.

As discussed in the previous section, we can reduce the cost by setting an upper bound for the target size. The number of computations needed for different systems with different upper bound is shown in Table II. We can see that with an upper bound, larger systems will become solvable. Since our search algorithm only needs to run once for each grid topology, the computation cost is acceptable.

B. Successful Rates of Stealthy FDI Attacks

To show the effectiveness of our defense technique against stealthy FDI attacks, we evaluate the attack successful rate after deploying our technique, and compare it to that of RandomSelect. We assume the attacker can compromise l meters (in our experiments, these meters are generated randomly). He then tries to construct attack vectors that can bypass the BDD process and then launches attacks with all available attack vectors. If he is able to construct such attack vectors (in other words, there exists at least one target set in the compromised meters), he will launch FDI attacks. For our defense algorithm, we first get the list of all vulnerable meters and rank them based on our proposed algorithm. Then k meters (k is determined by the cost limit) are selected from the top of the list. If the selected k meters overlap with the attack vector, the attack fails. Otherwise, the attack is successful.

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
GetCriticalSet	1	12.004 s	1.936 s	
rank	263949	8.402 s	8.402 s	
findrow	81664	1.156 s	1.156 s	
combnk	5814	0.488 s	0.488 s	
loadcase	1	0.010 s	0.006 s	
makeBdc	1	0.007 s	0.005 s	
nchoosek	24	0.006 s	0.006 s	
fileparts	1	0.003 s	0.003 s	
idx_bus	1	0.001 s	0.001 s	
idx_brch	1	0.001 s	0.001 s	
case14	1	0.000 s	0.000 s	
ispc	1	0.000 s	0.000 s	

Fig. 6. Running time of our algorithm on IEEE 14 bus system

In our experiments, we choose $l = m * 30\%$, $k = m * 10\%$. m is the number of meters in the system. The results are shown in Table III.

C. Damage of FDI Attacks

In this section, we evaluate the damage caused by FDI attacks and compare the performance of our defense technique with RandomSelect. In our experiments, the attacker randomly chooses n meters and increases their readings by 50%. RandomSelect randomly chooses k meters to protect, and our scheme chooses the top k meters based on our ranking. The protected meters can not be compromised, i.e., the readings can not be changed.

We calculate the percentage error of state estimation using the estimated states after the attack (denoted as z_i') and the estimated states without attack (denoted as z_i) as follows:

$$percentage\ error = \frac{|z_i' - z_i|}{z_i} * 100\%$$

Table IV shows the results (with percentage error for each bus) of the IEEE 14 bus system. As can be seen, with our selection algorithm, the power grid is much less affected by the attacks compared to RandomSelect. Here, the phase error for Bus 1 is not available since during state estimation, bus 1 is used as the reference bus, and its phase is considered to be 0. We also did experiments with IEEE 30 bus, 57 bus, 118 bus and 300 bus system. To save space, we only show the max percentage error and average percentage error among all buses in Table V. As can be seen, our meter selection algorithm has much better performance compared to RandomSelect. Furthermore, as the bus system increases, the performance gain of using our meter selection algorithm also increases. Thus, for power grid with a larger number of meters, our algorithm performs better.

D. Failures

When the state estimation error is larger than the power system can tolerate (we use 10% in our experiments), there may be failures of components (lines, buses, etc.) in the bus system. In this section, we show the number of possible failures caused by the attack with/without using our meter selection algorithm and compare it with RandomSelect. The results are shown in Fig. 7, where θ is the percentage of compromised nodes. As we can see, our selection algorithm reduces the number of outage lines significantly compared with RandomSelect. Also, as the number of protected nodes increases, the benefits of our algorithm also increases.

TABLE III
SUCCESSFUL RATES OF STEALTHY FDI ATTACKS WITH OUR DEFENSE VS. RANDOM SELECTION

	No Defense	OurDefense	RandomSelect
IEEE 14-Bus System	100%	28%	72%
IEEE 30-Bus System	100%	18%	82%
IEEE 39-Bus System	100%	24%	76%
IEEE 57-Bus System	100%	12.2%	85%
IEEE 118-Bus System	100%	8.1%	91%
IEEE 300-Bus System	100%	5.4%	95%

TABLE IV
IEEE 14-BUS: THE PERFORMANCE OF OUR DEFENSE VS. RANDOMSELECT WITH L = 5, K = 2

Bus	OurDefense		RandomSelction	
	Volt Error	Phase Error	Volt Error	Phase Error
1	1.88%	NaN	10.31%	NaN
2	1.94%	3.68%	10.53 %	15.30%
3	2.07%	3.80%	11.21%	16.72%
4	2.03%	3.78%	10.68%	11.83%
5	2.01%	3.73%	10.63%	11.25
6	1.68%	3.17%	9.47%	12.36%
7	1.77 %	2.82 %	11.04 %	5.21%
8	2.00 %	5.64 %	10.91 %	5.38%
9	1.25 %	0.97 %	10.93 %	2.63%
10	1.38%	0.12 %	10.75 %	5.22%
11	1.60 %	2.11%	10.08%	9.89%
12	1.74%	3.18%	9.79%	12.61%
13	1.76%	1.8 %	9.92 %	12.62%
14	1.54 %	1.03 %	10.88%	7.80%

E. Influence of UpperBound of Target Set Size

As introduced in Section V-A1, we set an upper bound for target set size and only search for target sets that are smaller than this upper bound. As shown in Section VI-A, the computation cost can be reduced significantly by this upper bound. In this section, we evaluate the influence of this upper bound on the performance. The successful rates of FDI attacks with different UpperBound are shown in Table VI. We can see that with upper bound, the successful rates of FDI attacks increase, but only very slightly. We can also see that the upper bound has a larger influence on larger bus system.

VII. CONCLUSIONS

In this paper, we studied the problem of how to select the most critical meters to protect to minimize the probability of attackers launching successful stealthy FDI attacks given a limited budget. We first formalized this problem which is NP-complete, and then proposed heuristic based solutions. The idea is to rank and select meters based on the vulnerability index, which considers how likely the meter will be targeted by the attacker to launch FDI attacks and how much damage will be caused by compromising the meter. Evaluations based on IEEE 14 bus, 30 bus, 57 bus, 118 bus and 300 bus system demonstrate that the proposed algorithm can significantly reduce the probability of successful FDI attacks, as well as the potential damage caused by FDI attacks.

TABLE V
AVERAGE ESTIMATION ERROR CAUSED BY FDI ATTACKS FOR IEEE 30-BUS, IEEE 57-BUS, IEEE 118-BUS AND IEEE 300-BUS: OUR DEFENSE VS. RANDOMSELECT

	IEEE 30-Bus		IEEE 57-Bus		IEEE 118-Bus		IEEE 300-Bus	
Max Voltage Error	OurDefense	1.4%	OurDefense	1.0%	OurDefense	0.9%	OurDefense	0.6%
	RandomSelect	14.57%	RandomSelect	23.16%	RandomSelect	27.79%	RandomSelect	33.62%
Average Voltage Error	OurDefense	0.6%	OurDefense	0.4%	OurDefense	0.4%	OurDefense	0.2%
	RandomSelect	14.13%	RandomSelect	20.03%	RandomSelect	24.30%	RandomSelect	30.31%
Max Phase Error	OurDefense	6.7%	OurDefense	5.1%	OurDefense	4.7%	OurDefense	3.0%
	RandomSelect	22.77%	RandomSelect	31.24%	RandomSelect	35.69%	RandomSelect	43.15%
Average Phase Error	OurDefense	0.7%	OurDefense	0.4%	OurDefense	0.3%	OurDefense	0.1%
	RandomSelect	16.20%	RandomSelect	25.78%	RandomSelect	29.46%	RandomSelect	37.24%

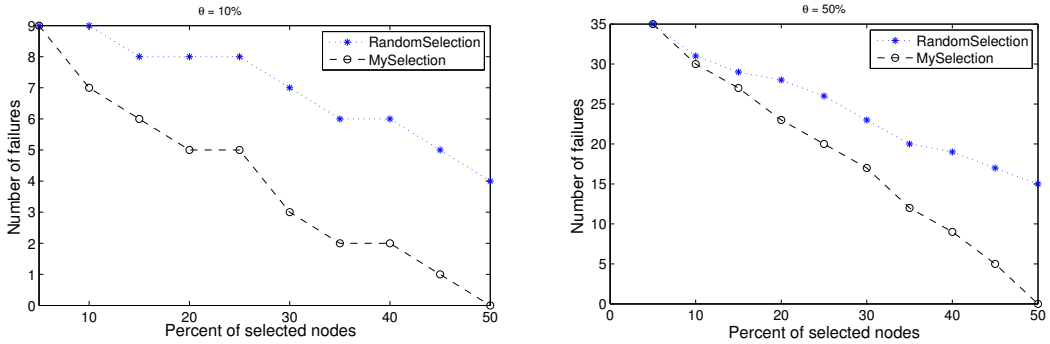

Fig. 7. Number of potential failures with different θ in IEEE 57-bus system

TABLE VI
SUCCESSFUL RATES OF FDI ATTACKS W. DIFFERENT TARGET SET SIZE UPPERBOUND (UB)

Bus System	No UB	UB = 20	UB = 10	UB = 5
30-Bus System	18%	18%	18.7%	19.6%
39-Bus System	24%	24%	24%	25.1%
57-Bus System	12.2%	12.7%	13.5%	14.7%

REFERENCES

[1] F. F. Wu, K. Moslehi, and A. Bose, "Power System Control Centers: Past, Present, and Future," *Proceedings of the IEEE*, vol. 93, no. 11, pp. 1890–1908, 2005.

[2] A. Monticelli, "Electric Power System State Estimation," *Proceedings of the IEEE*, vol. 88, no. 2, pp. 262–282, 2000.

[3] M. Hossain, N. Madlool, N. Rahim, J. Selvaraj, A. Pandey, and A. F. Khan, "Role of Smart Grid in Renewable Energy: An Overview," *Renewable and Sustainable Energy Reviews*, vol. 60, 2016.

[4] X. Dong, H. Lin, R. Tan, R. K. Iyer, and Z. Kalbarczyk, "Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges," in *ACM Workshop on Cyber-Physical System Security*, 2015.

[5] H. Sandberg, A. Teixeira, and K. H. Johansson, "On Security Indices for State Estimators in Power Networks," in *CPSWEEK Workshop on Secure Control Systems*, 2010.

[6] J. Fan, Q. Li, and G. Cao, "Privacy Disclosure Through Smart Meters: Reactive Power Based Attack and Defense," in *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2017.

[7] Y. Liu, P. Ning, and M. K. Reiter, "False Data Injection Attacks Against State Estimation in Electric Power Grids," in *ACM CCS*, 2009.

[8] J. Kim, L. Tong, and R. J. Thomas, "Dynamic Attacks on Power Systems Economic Dispatch," in *IEEE Asilomar Conference on Signals, Systems and Computers (ACSSC)*, 2014.

[9] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart Grid Data Integrity Attacks," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1244–1253, 2013.

[10] J. Kim and L. Tong, "On Topology Attack of A Smart Grid: Undetectable Attacks and Countermeasures," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1294–1305, 2013.

[11] S. Bi and Y. J. Zhang, "Graphical Methods for Defense Against False-Data Injection Attacks on Power System State Estimation," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1216–1227, 2014.

[12] J. Tian, R. Tan, X. Guan, and T. Liu, "Hidden Moving Target Defense in Smart Grids," in *2nd ACM Workshop on Cyber-Physical Security and Resilience in Smart Grids*, 2017.

[13] S. Barreto, A. Suresh, and J.-Y. Le Boudec, "Cyber-Attack on Packet-Based Time Synchronization Protocols: The Undetectable Delay Box," in *IEEE International Conference on Instrumentation and Measurement Technology*, 2016.

[14] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting False Data Injection Attacks on DC State Estimation," in *CPSWEEK Workshop on Secure Control Systems*, 2010.

[15] W. Zhang and G. Cao, "Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-Based Approach," in *IEEE INFOCOM*, 2005.

[16] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False Data Injection Attacks Against State Estimation in Wireless Sensor Networks," in *IEEE Conference on Decision and Control*, 2010.

[17] Q. D. Vu, R. Tan, and D. K. Yau, "On Applying Fault Detectors Against False Data Injection Attacks in Cyber-Physical Control Systems," in *IEEE INFOCOM*, 2016.

[18] J. Kim, L. Tong, and R. J. Thomas, "Data Framing Attack on State Estimation," *IEEE Journal on Selected Areas in Communications*, 2014.

[19] R. Lu, X. Liang, X. Li, X. Lin, and X. S. Shen, "EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, 2012.

[20] "PACE Smart Meters," http://pacepowersystems.com/smart-meters/.

[21] "GE I-210 meters," http://www.gedigitalenergy.com/SmartMetering/catalog/i210_family.htm.

[22] "Landis Gyr Meters," http://www.landisgyr.com/products/.

[23] M. P. McHenry, "Technical and Governance Considerations for Advanced Metering Infrastructure/Smart Meters: Technology, Security, Uncertainty, Costs, Benefits, and Risks," *Energy Policy*, 2013.

[24] A. J. Wood and B. F. Wollenberg, *Power Generation, Operation, and Control*. John Wiley & Sons, 2012.

[25] Y. C. Chen, A. D. Domínguez-García, and P. W. Sauer, "Online Computation of Power System Linear Sensitivity Distribution Factors," in *IEEE IREP Symposium on Bulk Power Systems Dynamics and Control*, 2013.