Defending against Unidentifiable Attacks in Electric Power Grids

Zhengrui Qin, *Student Member*, *IEEE*, Qun Li, *Senior Member*, *IEEE*, and Mooi-Choo Chuah, *Senior Member*, *IEEE*

Abstract—The electric power grid is a crucial infrastructure in our society and is always a target of malicious users and attackers. In this paper, we first introduce the concept of unidentifiable attack, in which the control center cannot identify the attack even though it detects its presence. Thus, the control center cannot obtain deterministic state estimates, since there may have several feasible cases and the control center cannot simply favor one over the others. Given an unidentifiable attack, we present algorithms to enumerate all feasible cases, and propose an optimization strategy from the perspective of the control center to deal with an unidentifiable attack. Furthermore, we propose a heuristic algorithm from the view of an attacker to find good attack regions such that the number of meters required to compromise is as few as possible. We also formulate the problem that how to distinguish all feasible cases if the control center has some limited resources to verify some meters, and solve it with standard algorithms. Finally, we briefly evaluate and validate our enumerating algorithms and optimization strategy.

Index Terms—Power grid, unidentifiable attack, state estimates, false data injection, security, bad data identification

1 Introduction

The electric power grid is a distribution network that connects the electric power generators to customers through transmission lines, and its security and reliability are critical to society. To enable its safe and reliable operation, the power grid is monitored continuously by smart meters installed at important locations of the power grid. The meters take various measurements, including real and reactive power injections on buses and real and reactive power flows on transmission lines. Such data is then fed to the control center within the supervisory control and data acquisition system. Using the collected information, the control center estimates the state variables, which are the voltage amplitudes and phases on buses, and then makes corresponding adjustments to stabilize the power grid.

To obtain reliable state estimates, it is essential for the control center to be fed reliable and accurate meter measurements. However attackers may compromise meter measurements and send malicious data to the control center, thus misleading the control center to make bad decisions that may cause severe consequences to the power system. Researchers have developed various techniques to detect bad data measurements [1], [2], [3], [4], [5], most of which are based on measurement residuals.

However, Liu et al. [6] has presented an undetectable false data injection that can defeat all the detection techniques based on measurement residuals. Their simulation results indicate that for medium size power system (e.g., IEEE 30-bus system), the attackers may need to compromise 60 to 75 percent of all meters before they can succeed in launching a random false data injection attack. However, an attacker may either have limited attack resources or only limited access to some meters. Thus, we are interested in exploring if there are other types of attacks that require fewer meters.

In this paper, we focus on unidentifiable attacks, which are different from undetectable attacks discussed in [6]. *In unidentifiable attacks, the control center can detect that there are bad or malicious measurements, but it cannot identify which meters have been compromised*. As a result, the attacker does not need to manipulate as many meters for unidentifiable attacks as when he is launching undetectable attacks. Under an unidentifiable attack, the control center has no way to simply eliminate some "bad" data and thus get accurate state estimates. However, the control center has to make a decision how much power to generate, no matter good or bad, in response to the attack. We argue that a good decision during such an attack is one that minimizes the total cost which includes generation and penalty cost caused by damages of the attack.

Our main contributions in this paper are as follows:

1. We are the first to propose the unidentifiable attack in a power grid system. We demonstrate the feasibility of this type of attack. An adversary can launch an unidentifiable attack by compromising a smaller number of meters compared with the previously proposed attacks while at the same time confuse the control center on what really happens.
2. We propose a heuristic algorithm to enumerate all feasible cases under an unidentifiable attack. The previous classic "bad data detection" algorithms do not work for this attack scenario. Our algorithm is the first to resolve the problems of the previous

- *Z. Qin and Q. Li are with the Department of Computer Science, McGlothlin-Street Hall, The College of William and Mary, Williamsburg, VA 23187-8795. E-mail: {zhengrui, liqun}@cs.wm.edu.*
- *M.-C. Chuah is with the Department of Computer Science and Engineering, 19 Memorial Drive West, Lehigh University, Bethlehem, PA 18015. E-mail: chuah@cse.lehigh.edu.*

Manuscript received 11 Apr. 2012; revised 31 Aug. 2012; accepted 4 Sept. 2012; published online 17 Sept. 2012.
Recommended for acceptance by N. Kato.
For information on obtaining reprints of this article, please send e-mail to: tpds@computer.org, and reference IEEECS Log Number TPDS-2012-04-0374.
Digital Object Identifier no. 10.1109/TPDS.2012.273.

algorithms. It also significantly reduces the possible solution searching space compared with brute force approach. We show through empirical study that the algorithm can efficiently find all possible attacks.

3. Enumerating possible attacks is not equivalent to locating the exact attack. To defend against all possible attack scenarios, we also propose a strategy to minimize the average damage to the system. We formulate the problem as a nonlinear programming problem and solve it through a standard optimization package.
4. We improve on [7] by considering from the view of an attacker. As an attacker, he is interested in finding good attack regions to attack such that the number of meters he needs to compromise to launch an unidentifiable attack is minimized. To find such regions, we propose a heuristic algorithm that can reveal good attack regions by performing column transformations on the Jacobian matrix of a power system.
5. As another improvement on [7], we propose an algorithm that a control center with limited resource can use to identify the meters they should verify during an unidentifiable attack.
6. We analyze our system in AC model, which is nonlinear and doubles the number of variables compared to the DC model. The recent security investigations of the power system, such as [6], [8], [9], [10], are all based on DC model. Although DC model can be representative of the power system, AC model can capture more subtleties and is more complicated and realistic to describe a power system. We believe this is the first piece of work to carefully examine the attacks and solutions in realistic AC model. The formulation and optimization can be used as a basis for future work.

A preliminary version of this paper was presented in [7]. Herein, we add one algorithm from the view of an attacker to find good attack regions for unidentifiable attacks and another algorithm from the view of the control center to identify the meters they should verify under an unidentifiable attack. Furthermore, one more case study is conducted in simulation. The nomenclatures used in the paper are listed below Section 8.

2 Related Work

To ensure the power system operates correctly, the control center needs to collect measurements to estimate the state variables, and then takes control actions against any contingency. For a system with n buses and m meters, the state estimates are determined through the model of $\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e}$, where $\mathbf{x} = (V_1, \ldots, V_n, \theta_1, \ldots, \theta_n)$ is the state variable vector, $\mathbf{z} = (z_1, \ldots, z_m)$ is the measurement vector, and $\mathbf{e}$ is the measurement error vector.

Bad measurements, however, may exist due to faulty meters, transmission errors, or alterations by malicious attackers. Researchers have developed lots of approaches on bad data detection and identification since 1970s, such as identification by elimination (IBE) [1], nonquadratic criteria (NQC) [2], hypothesis testing identification (HTI) [3], combinatorial optimization identification (COI) [4], [5]. An early comparative study of the first three approaches can be found in [11].

Another way to deter malicious users is securing communications and ensuring data integrity [12], [13], [14]. Besides, public-key schemes, such as [15], [16], [17], can also be implemented to prevent malicious users from manipulating meter measurements.

Liu et al. [6] have shown that, given the topology and line impedance of a power system in DC model, an attacker can inject malicious data without being detected by the control center, since the injected malicious data does not change the residual. Since then, the undetectable attack has drawn a lot of attention, such as in [8], [9], and [18]. In [8] and [18], a specific undetectable attack called the load redistribution attack is analyzed. In [9], minimum residue energy attack is discussed as well.

The unidentifiable attack considered in this paper is different from the undetectable attack in that the control center can detect the presence of an attack but cannot identify which meters have been compromised. This is in fact the concept of *nondeducibility* [19] but with an inverse form, in which the attacker maintains the property of nondeducibility. Our unidentifiable attacks aim to confuse the control center to the extent that it does not know what the exact demand scenario is and hence needs to rely on a strategy to deal with such attacks. Compared with undetectable attack, an attacker only needs to manipulate at most half as many meters to launch an unidentifiable attack as those he needs for an undetectable attack. The concept of unidentifiable attacks is hence of great value and more practical, especially for an attacker with limited attack resources. Consequently, this paper complements the research in cyber-physical systems [20], [21], [22], [23], [24], [25].

3 Unidentifiable Attack

The unidentifiable attack in this paper is a new type of attack in the power system. Before we present the formal definition of the unidentifiable attack, we define *feasible case* for a power system and make an assumption regarding to the capability of an attacker.

Feasible case. A feasible case for a power system is a vector of all m meter readings that 1) is consistent with negligible error; and 2) hence can produce a distinct set of state variables.

We denote the collection of feasible cases by set $\mathbf{F}$. And we assume that an attacker can at most compromise r meters. Suppose the meter reading vector under an attack is $\mathbf{z}_a$. Then the formal definition is:

Unidentifiable attack. An attack is unidentifiable if the following two conditions are satisfied: 1) $d(\mathbf{z}_a, \mathbf{z}) \neq 0$, $\forall \mathbf{z} \in \mathbf{F}$, where d is a function that returns the number of mismatch elements between two vectors; 2) there exists a set $\mathbf{F}' \subseteq \mathbf{F}$ such that $d(\mathbf{z}_a, \mathbf{z}') \leq r$, $\forall \mathbf{z}' \in \mathbf{F}'$, and $|\mathbf{F}'| \geq 2$, where $|.|$ is a function on a set and returns the number of elements in it.

In the above definition, condition (1) makes sure that the control center can detect the presence of an attack; condition (2) guarantees that at least two feasible cases exist to obfuscate the control center. In the following, we will first further explain the unidentifiable attack with concrete

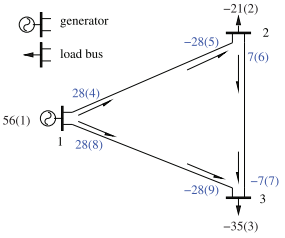


Fig. 1. The meter readings before attack. XX(Y) means that meter Y's reading is XX. A positive value means a power flow comes out of a bus, while a negative value means a power flow goes into a bus.

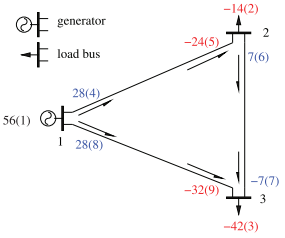


Fig. 2. Type I unidentifiable attack, where meters 2, 3, 5, 9 are compromised (red ones).

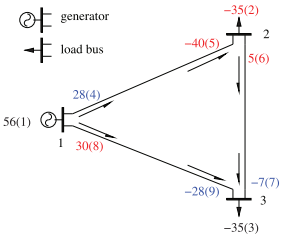


Fig. 3. Type II unidentifiable attack, where meters 2, 5, 6, 8 are compromised (red ones).

examples. Then we will discuss the attack strategy from an attacker's viewpoint.

3.1 Unidentifiable Attack Examples

To further understand the unidentifiable attack, let us consider an ideal case where the measurements have no error except those which are manipulated by an attacker. Suppose there are $m = m_0 + m_1 + m_2$ measurements which can be divided into three sets, M_0, M_1, and M_2, with cardinalities m_0, m_1, and m_2, respectively. Assume that $m_1 \leq r$, $m_2 \leq r$, and an attacker has manipulated the set of measurements in M_1. Obviously, the vector of measurements is not a feasible case, that is, the control center can detect the presence of an attack. Let us further assume that, the measurements $M_0 \cup M_1$ alone are consistent and make the whole system *observable,*[1] so are the measurements $M_0 \cup M_2$. In such a scenario, the control center can conclude that either set M_1 or set M_2 are the compromised measurements. However, the control center has no way to determine the exact set that has been compromised. We call such an attack unidentifiable, since the attack on set M_1 confuses the control center to believe that either set M_1 or set M_2 has been compromised. We say this attack has two feasible cases: one is determined by $M_0 \cup M_1$, and the other is determined by $M_0 \cup M_2$.

In the power system, all meters are interactive to some extent. Therefore, changing one meter usually requires changes of many other meters to make the changes consistent. From the view of an attacker, he intends to change as few meters as possible to generate an unidentifiable attack. In this paper, we focus on two types of unidentifiable attacks, which can lead to bad consequences. One is *load redistribution attack* (Type I), in which the attacker obfuscates the control center whether the power demands on some load buses are redistributed, while the total power demand is unchanged. The other is *load increase attack* (Type II), in which the attacker obfuscates the control center whether the demand on a certain bus is increased, while the demands for other load buses remain the same. Compared to random changes on meter readings that may require to check many times before an unidentifiable attack with bad consequences can be obtained, these two types of attacks empirically require less effort of the attacker.

Let us consider two simple examples that illustrate the two types of unidentifiable attacks above. To simplify our discussion, we use DC model in our examples, but we consider AC model for the rest of the work in this paper.

1. A set of measurements is said to make the system *observable* if the states of all the buses can be determined with these measurements.

Fig. 1 is a three bus power system. On each bus, there is a power injection meter; on each transmission line, there are two power flow meters, with one at each end of the line. In DC model, there is no resistance on transmission lines but only susceptance. The susceptance between buses 1 and 2 is 280 (we omit the unit, and thereafter); that between buses 2 and 3 is 70; and that between buses 1 and 3 is 140. Suppose the load on bus 2 is 21, and the load on bus 3 is 35. Before any attack, the meter readings are consistent as shown in Fig. 1.

Now suppose $r = 4$ and an attacker can manipulate meters {2,3,5,9}. The attacker changes the readings of these four meters to the value shown in Fig. 2. The whole set of data is not consistent, and the control center knows that an attack is present. However, the readings on meters {1,4,6,7,8} are consistent, and they can determine a set of state variables, which corresponds to the load vector $\{bus2, bus3\} = \{21, 35\}$. The readings on meters {1,2,3,5,9} are also consistent, while they can determine a different set of state variables, which corresponds to the load vector $\{bus2, bus3\} = \{14, 42\}$. Under this scenario, even though the control center knows that four meters have been compromised, it has no way to identify which four have been manipulated. The compromised data can either be meters {2,3,5,9}, or meters {4,6,7,8}. That is, there are two feasible cases. One is determined by meters {1,4,6,7,8}, which is $\{56, -21, -35, 28, -28, 7, -7, 28, -28\}$. The other is determined by meters {1,2,3,5,9}, which is $\{56, -14, -42, 24, -24, 10, -10, 32, -32\}$. In this example, the net effect of the attack is to have the control center guess whether there is a 7 unit load redistribution between buses 2 and 3 ({21,35} to {14,42}). To make this load redistribution undetectable, one has to compromise all nine meters except meter 1, which is beyond the attacker's capability. However, we only need to compromise 4 meters to make this attack unidentifiable.

Another similar attack is shown in Fig. 3. In this case, meters {2,5,6,8} are compromised corresponding to the load vector $\{bus2, bus3\} = \{35, 35\}$. Similarly, the compromised data can either be meters {2,5,6,8}, or be meters {1,4,7,9}.

TABLE 1
The Number of Meters That Are Enough for an Unidentifiable Attack

r	d'
$r \geq d-1$	1
$d-1 > r > d/2$	$d-r$
$r = d/2$	$d/2$
$r < d/2$	impossible

That is, there are two feasible cases: one determined by meters {1,3,4,7,9} and the other by meters {2,3,5,6,8}. In this example, the net effect of the attack is to let the control center guess whether there is a 14 unit load increase on bus 2 (from 21 to 35). Again, only 4 meters need to be compromised to launch this unidentifiable attack, compared to 8 meters for the corresponding undetectable attack.

In each of the example, there are some meters that have the same readings for the different feasible cases of an unidentifiable attack. With more common readings among different feasible cases, fewer meters need to be compromised to launch an unidentifiable attack.

3.2 Best Attack Regions for Unidentifiable Attacks

From an attacker's viewpoint, he is interested in finding a region such that he only needs to compromise as few meters as possible to launch an effective attack, no matter Type I or Type II attack.

First, we have to find a metric to evaluate an attack region. Assume that an attacker needs to compromise d meters in a region to shift from one feasible case to another feasible case, i.e., to launch an undetectable attack. Now, we want to know how many compromised meters are enough to launch an unidentifiable attack in the same region. We denote it by d'. Regarding r, there are four cases in total, listed in Table 1. From the table, we can see that compromising $d/2$ meters is enough to launch an unidentifiable attack, no matter what r is (since the attacker can compromise $d/2$ meters, it means r is at least $d/2$). Thus, we use $d' = d/2$ as the metric to evaluate how good an attack region is.

We use the Jacobian matrix method, similar in [6], to find the best attack region for a bus system. The detail of this method and some attack regions with the values of d' in three IEEE bus systems can be found in Appendix A, which can be found on the Computer Society Digital Library at http://doi.ieeecomputersociety.org/10.1109/TPDS.2012.273. Some of these regions will be further evaluated in Section 7.

4 Optimization Strategy

Under an unidentifiable attack, the control center cannot identify which set of meters is compromised, even though it knows that some meters are compromised. Suppose that under an unidentifiable attack, the control center finds l feasible cases, i.e., $|F'| = l$ (we will present algorithms to find all feasible cases in Section 5). To reduce the damage caused by such an unidentifiable attack, the control center has to consider all l feasible cases, and tries to find a solution such that the damage to the power system is as small as possible before the set of compromised meters can be identified and eliminated (it is possible that the attack cannot be identified without sending power engineers to conduct a physical check).

To evaluate whether a power generation solution is good or not, we need to assess the potential damage such a solution yields to each of l feasible cases. The damage mainly includes the followings:

- *Power shedding on load buses.* There is not enough power supply for load buses such that some load buses get less power than their demands which results in the tripping of circuit breakers to shed some loads.
- *Overloading of transmission lines.* The power flow on a transmission line may go beyond its capacity such that the line trips, possibly resulting in severe consequences, for example, large area blackout.
- *Overpowering on load buses.* A load bus may be fed more power than its demand which can result in the power system operating at higher frequency than it can tolerate, tripping certain circuit breakers and causing blackout.

The cost of the whole power system consists of two components: one is related to the cost of power generation, and the other is related to the cost of damages mentioned above. Any good power generation solution should avoid overloading and overpowering scenarios since they both can cause severe consequences. In our proposed strategy to identify good power generation solutions during an unidentifiable attack, we propose to avoid any potential damages caused by overloading and overpowering by including constraints that prevent overloading and overpowering from occurring. Therefore, we only need to include the power generating cost and the penalty of load shedding in our overall cost. Since all l feasible cases are unidentifiable and equally possible in the view of the control center, it is reasonable to consider the average damage caused by a power generation solution to all feasible attack cases. We are to find a power generation solution such that the sum of the generating cost and the average damage caused by load shedding is minimized

$$min : \sum_{b_j \in G} C_j PG_j + \frac{1}{l} \sum_{k=1}^{l} D_{shed,k}, \tag{1}$$

where $D_{shed,k}$ is defined as follows:

$$D_{shed,k} = \sum_{b_i \in L} C_{shed,i} PS_{k,i}. \tag{2}$$

The constraints are as follows:

1. Power shedding constraints:

$$0 \leq PS_{k,i} \leq PD_{k,i}, \forall b_i \in L, 1 \leq k \leq l, \tag{3}$$

   in which the positive $PS_{k,i}$ guarantees that there is no overpowering.
2. Power flow and power injection constraints:

$$\sum_{j=1}^{n} V_i V_j (G_{ij} cos(\theta_i - \theta_j) + B_{ij} sin(\theta_i - \theta_j)) - PG_i + PD_{k,i} - PS_{k,i} = 0, 1 \leq i, j \leq n, 1 \leq k \leq l, \tag{4}$$

$$\sum_{j=1}^{n} V_i V_j (G_{ij} sin(\theta_i - \theta_j) - B_{ij} cos(\theta_i - \theta_j)) - QG_i + QD_{k,i} - QS_{k,i} = 0, 1 \le i, j \le n, 1 \le k \le l, \tag{5}$$

$$P_{ij} = -V_i^2 G_{ij} + V_i V_j (G_{ij} cos(\theta_i - \theta_j) + B_{ij} sin(\theta_i - \theta_j)), \forall t_{i\_j} \in T, \tag{6}$$

$$Q_{ij} = V_i^2 B_{ij} + V_i V_j (G_{ij} sin(\theta_i - \theta_j) - B_{ij} cos(\theta_i - \theta_j)), \forall t_{i\_j} \in T, \tag{7}$$

$$PL_{ij} = \sqrt{P_{ij}^2 + Q_{ij}^2}. \tag{8}$$

3. Line transmission capacity constraints:

$$-PL_{ij}^{max} \le PL_{ij} \le PL_{ij}^{max}, \forall t_{i\_j} \in T. \tag{9}$$

4. Generator capacity constraints:

$$PG_{g,min} \le PG_g \le PG_{g,max}, \forall b_g \in G, \tag{10}$$

$$QG_{g,min} \le QG_g \le QG_{g,max}, \forall b_g \in G. \tag{11}$$

In the above formulation, $PD_{k,i}$ and $QD_{k,i}$, which are determined by the kth feasible case, are known. $PS_{k,i}$ and $QS_{k,i}$ are variables. V_i and θ_i, $1 \le i \le n$, are auxiliary variables, which connect other variables via (4), (5), (6), and (7). After solving the minimization problem (we use the free software IPOPT [26]), we will get all the variables, including PG_j, $PS_{k,i}$, V_i, and θ_i, $\forall b_j \in G$, $1 \le k \le l$, $1 \le i \le n$. The control center can then determine the amount of power generation on each generator and the amount of power supply on each load bus, and send these quantities as directives to the corresponding generators and load buses. This is how the control center responds to an unidentifiable attack.

5 Analysis of Unidentifiable Attack

When an unidentifiable attack occurs, the control center first has to detect the presence of an attack. One can use any typical bad data detection scheme proposed by previous work to detect the presence of an attack. Given a power system with n buses and m meters in AC model, as mentioned in Section 2, measurements $\mathbf{z} = (z_1, \ldots, z_m)$ are functions of the state variables $\mathbf{x} = (V_1, \ldots, V_n, \theta_1, \ldots, \theta_n)$. That is, $\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e}$, where $\mathbf{h}(\mathbf{x}) = (h_1(\mathbf{x}), \ldots, h_m(\mathbf{x}))$, are defined in the following four cases (assume no error, e.g., $\mathbf{e} = \mathbf{0}$):

1. z is real power injection on bus i:

$$z = \sum_{j=1}^{n} V_i V_j (G_{ij} cos(\theta_i - \theta_j) + B_{ij} sin(\theta_i - \theta_j)). \tag{12}$$

2. z is reactive power injection on bus i:

$$z = \sum_{j=1}^{n} V_i V_j (G_{ij} sin(\theta_i - \theta_j) - B_{ij} cos(\theta_i - \theta_j)). \tag{13}$$

3. z is real power flow from bus i to bus j:

$$z = -V_i^2 G_{ij} + V_i V_j (G_{ij} cos(\theta_i - \theta_j) + B_{ij} sin(\theta_i - \theta_j)). \tag{14}$$

4. z is reactive power flow from bus i to bus j:

$$z = V_i^2 B_{ij} + V_i V_j (G_{ij} sin(\theta_i - \theta_j) - B_{ij} cos(\theta_i - \theta_j)). \tag{15}$$

In case of errors or an attack, the detection scheme will compute L_2 norm $\|\mathbf{z} - \mathbf{h}(\hat{\mathbf{x}})\|_2$, where $\hat{\mathbf{x}}$ is the vector of estimated state variables obtained by a least-squares estimator. Then the L_2 norm is compared with a predefined threshold τ, and an attack is declared only if $\|\mathbf{z} - \mathbf{h}(\hat{\mathbf{x}})\|_2 > \tau$.

Next, the control center should discern if the attack is unidentifiable. It can draw such a conclusion by enumerating all feasible cases for the attack. It is an unidentifiable attack if at least two feasible cases exist; otherwise, it is not. In the following, we first make some assumptions and formulate the case enumerating problem. Then, we describe algorithms to enumerate all feasible cases, including a brute-force search algorithm and an empirical method that can speed up the brute-force search. Finally, we analyze the complexity and performance of the proposed algorithms.

5.1 Assumption and Problem Formulation

We assume that the presence of bad measurements does not make the whole system unobservable, which excludes the scenario of undetectable attacks. And we also assume that a set of meters, say set P, is protected by the power system operator.

Let set A be the set of all meters and set D be the set of bad meters that the control center deduces. With the above assumptions, the problem of finding all feasible cases under an unidentifiable attack can be formulated as follows:

Enumerate all different sets of D such that:

1. The meters in $A \backslash D$ make the whole power system observable.
2. The meters in $A \backslash D$ are consistent; that is, after solving the state estimation for the power system with meters in $A \backslash D$, the norm of residuals of these meters is zero or less than a predefined value τ.
3. $|D| \le r$.
4. $D \cap P = \emptyset$.
5. Different sets of D results in different state variables.[2]

5.2 Enumerating Feasible Cases

Given the assumptions and formulation above, our goal is to find all feasible cases that satisfy all the constraints.

2. This condition is to avoid finding duplicated feasible cases, since it is possible that two different sets of meters produce the same set of state variables.

When r is small, we can use brute-force search to find all feasible cases. However when r is big, the brute-force search becomes very expensive, since its search time grows exponentially with increasing r. However, if one can identify an attack region where the compromised meters are located, then the search space can be reduced and hence the search process can be sped up.

5.2.1 Brute-Force Search to Enumerate Feasible Cases

When the maximum number of meters that an attacker can compromise, r, is small, we use brute-force search directly. In a brute-force search, every combination that meets all the constraints in the problem formulation is examined. The brute-force search algorithm works as follows:

Algorithm 1: *Brute-force Search*
Input: r, the attacker's capability;
Set A, the set of all meters;
Set P, the protected set;
Output: A set F that contains all feasible sets of D.
1: $F = \emptyset$;
2: For $i = 1, r$
3: Check every of $\binom{m}{i}$ bad data combinations, D, except those are supersets of any set in F;
4: If $D \cap P = \emptyset$, then
5: If $A \backslash D$ pass the residual test, then
6: Put the bad data set D into F;
7: Endif
8: Endif
9: Endfor

In the above algorithm, the brute-force search actually does not check every combination, as shown in line 3. It does not check the combinations that have already been covered by previous combinations that are included in set F. If we have already found a feasible case with a set of meter readings D being declared as bad, then we do not need to check any other sets of meter readings D', where $D' \supset D$.

5.2.2 Locate Attack Region Then Enumerate Feasible Cases

When r is large, the brute-force search approach becomes expensive. As the compromised meters in an unidentifiable attack are typically clustered, we are to identify the attack region and then enumerate feasible cases which only include meters within the attack region. Such a strategy greatly reduces the search space and hence the search time.

To identify the attack region, we can use existing algorithms based on IBE, such as those discussed in [1]. Though these algorithms cannot exactly identify all the bad data, especially those interacting ones, these algorithms can give us some clues about the attack region.

We propose a three-step scheme for enumerating feasible cases for an unidentifiable attack. In our first step, we use the IBE algorithm since our goal is not to identify all bad data but to roughly locate the attack region. In the IBE algorithm, it first runs the least-squares estimator and then deletes the measurement with the largest residual, until the norm of the residuals is less than a predefined threshold τ. The IBE algorithm works as follows:

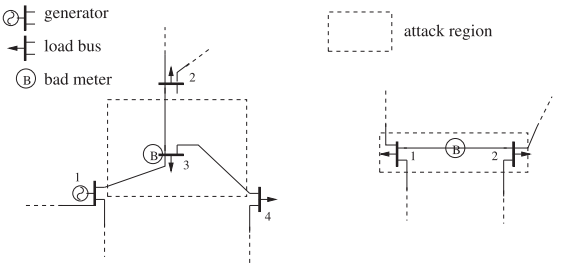


Fig. 4. Attack region illustration. On the left, a meter on bus 3 is declared bad; on the right, a meter on the branch between buses 1 and 2 is declared bad.

Step 1: IBE (Algorithm 2)
1: $D = \emptyset$;
2: $A = \{\text{all meters}\}$;
3: While the norm of residuals of meters in $A \backslash D \geq \tau$
4: Put the meter with the largest residual in D;
5: Run state estimation with $A \backslash D$;
6: Find the meter that has the largest residual;
7: End

After executing *Step 1*, we identify a set of meters, D. We then check where the meters in set D are, and hence can roughly deduce where the attack region is. We define the *attack region*, R, which is a subgraph of the whole power system, using the following algorithm:

Step 2: Attack Region Identification (Algorithm 3)
1: $R = \emptyset$;
2: For meter $a \in D$
3: if a is on bus i
4: $R = R \cup b_i \cup t_{i\_*}$;
5: else if a is on line t_{i_j}
6: $R = R \cup b_i \cup b_j \cup t_{i\_j}$;
7: endif
8: endfor

The rationale for the above algorithm is as follows: If a meter is on a bus, its reading (real/reactive) is the summation of all power flows (real/reactive) incident to that bus according to (4) and (5). If a meter is on a branch, its reading is a function of the state variables of the two end buses according to (6) and (7). For interacting bad data, the bad data nearby a good one can make the good one has the largest residual. Thus, if a data is eliminated in *Step 1*, it is either because the data is bad or its nearby data is bad. Therefore, in the attack region, we include both the data with largest residual and its neighbors that affect it directly. That is, if a meter on a bus is declared bad, we include both that bus and all the branches incident to that bus into the attack region; if a meter on a branch is declared bad, we include that line and two end buses into the attack region. Fig. 4 illustrates how the attack region is defined.

Therefore, by looking at the region where the bad data are located, we can roughly identify the attack region. However, we cannot guarantee that the attack region defined above includes all the bad meters, which is summarized in the following claim.

Claim. By eliminating the measurement with the largest residual until the remaining ones are consistent, the attack

region defined above is not guaranteed to include all bad data.

Remark. The proof is in Appendix B, which is available in the online supplemental material. The example given in our proof in Appendix B, which is available in the online supplemental material, is an extreme case. Consider a power system in AC model, there are 4 meters on each transmission line, with two at each end of the line, one for real power flow, the other for reactive power flow; and there are two injection meters on each bus, one for real power and the other for reactive power. To produce the above attack, the attacker has to compromise more than 2/3 of all meters.[3] If the attacker has that much attack resources, he may be able to launch an undetectable attack which may produce larger damages and hence he may not have the incentive to launch an unidentifiable attack.

After obtaining the attack region, we will do a brute-force search in it. However, this brute-force search algorithm is different from Algorithm 1, since we need to consider the case that the detected attack region does not include all bad data as proved in the above claim. The algorithm is as follows:

Step 3: Brute-force Search in the attack region (Algorithm 4)
Input: R, the detected attack region with $|R|$ meters;
r, the attacker's capability;
Set A, the set of all meters;
Set P, the protected set;
Output: A set F that contains all feasible sets of D.

1: $F = \emptyset$;
2: For i=1, r
3: For every of $\binom{|R|}{i}$ bad data combination, D, except those are supersets of any set in F
4: If $D \cap P = \emptyset$, then
5: If $A \backslash D$ pass the residual test, then
6: Put D into F;
7: Else
8: Run IBE with $A \backslash D$ and update D by including the data with largest residual until passing residual test;
9: Put D in F if $|D| \leq r$;
10: Endif
11: Endif
12: Endfor
13: Endfor

Although the detected attack region may not include all bad data, line 8 in *Step 3* is able to find bad data outside of the detected attack region. The three-step algorithm will usually find all the feasible cases.

5.3 Performance Analysis

Given a power system with m measurements and an attacker with capability r, the brute-force search (Algorithm 1) is $O(\binom{m}{r})$. This is huge when m and r are both large. Therefore, Algorithm 1 only works for either a small power system or an attacker with very limited capability.

3. For an n bus system with $|T|$ branches, there are $2n + 4|T|$ meters. The attack has to compromise a portion of $\frac{2n+4|T|-(2n-1)}{2n+4|T|} > \frac{2}{3}$, since $|T|$ is usually greater than n.

When Algorithm 1 is not applicable, we should utilize the three-step scheme (Algorithms 2-4). Suppose there are $|R|$ meters in the located attack region R, then the complexity is $O(\binom{|R|}{r})$, which is much smaller than that of brute-force search, given that the compromised measurements in an unidentified attack is usually clustered and $|R|$ is much less than m. If the attack region R is not connected, i.e., there are more than one attack regions, we can apply Algorithms 2-4 on each connected attack region.

Our method is better than all existing bad data detection methods in power system under an unidentifiable attack, since they cannot work in case of such attack. In an unidentifiable attack, there are more than one feasible cases. All existing methods can only find one solution, which means that they can at most find one feasible case. The attacker is always able to manipulate a set of measurements such that the set of bad measurements identified by an existing method is different from the set of manipulated measurements. Therefore, none of them can work in the scenario of an unidentifiable attack. In this sense, our method has already greatly eliminated false positive (FP) and false negative (FN) which all existing methods have. However, since our algorithms are heuristic, they may still have FP and FN. If the detected attack region contains all the bad data, there will be neither FP nor FN. Even if the detected attack region does not contain all the bad data, Algorithm 4 is able to find some bad data outside of the detected attack region. We believe that these two facts will reduce the rate of FP and FN. As shown in the evaluation in Section 7, there is neither FP nor FN in dealing with the six unidentifiable attacks created with Matpower [27].

6 Direct Meter Verification to Eliminate Feasible Cases

In this section, we investigate how a control center with limited resources for verifying meter readings should strategize such that it can either identify a particular feasible case as the real attack scenario or reduce the number of feasible cases from all feasible cases. By limited resources, we mean the maximum number of meters that the control center can verify.

Suppose the control center has found l feasible cases given an unidentifiable attack. Now the control center has limited resources to verify only a small number of meters, say s meters. From the perspective of the control center, it is interested in either finding which one of l feasible cases is the real attack case, or excluding as many feasible cases from the l feasible cases. The issue the control center faces is which meters should be chosen for reading verification to maximize its interest.

This problem can be formulated as a set cover problem with some restrictions. The detailed formulation process and how it is solved can be found in Appendix C, which is available in the online supplemental material.

7 Evaluation

In this section, we present the results of several experiments that we conduct. First, we generate six unidentifiable attacks in three bus systems. Second, we locate the attack

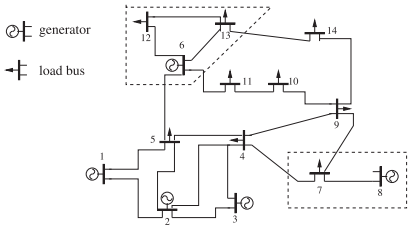


Fig. 5. The topology of 14-bus system in Matpower.

TABLE 2
Type I Attack in 14-Bus System

Meters	Before attack	After attack
PI on bus13	−13.5	**−3.5**
PL from bus6 to bus12	8.05	**12.32**
QL from bus6 to bus12	3.31	**4.43**
PL from bus13 to bus6	−17.93	**−14.34**
QL from bus13 to bus6	−9.99	**−9.33**
PL from bus12 to bus13	1.87	**−3.96**
QL from bus13 to bus12	−1.53	**−2.41**

region and enumerate all possible cases using Algorithms 2-4 presented in Section 5; at the same time, we show that the IBE method does not correctly identify the set of bad data, especially if the bad data interact with one another. Finally, we evaluate the operating cost of the power system based on the optimization strategy we present in Section 4. Our results show that the optimization strategy, we propose for dealing with unidentifiable attacks, is a viable solution. Here we only detail the evaluation on IEEE 14-bus system. The evaluation on IEEE 9-bus and 30-bus systems can be found in Appendix D, which is available in the online supplemental material.

7.1 Generating Unidentifiable Attacks

We generate one Type I attack and one Type II attack in 14-bus system, whose topology is shown in Fig. 5. We generate malicious data using the Matpower tool [27], which is developed to solve power flow problems. We first input one load vector into Matpower and record the first set of meter readings. Then, we feed another load vector into Matpower and record the second set of meter readings. Comparing the two sets of readings, some of them are the same in both sets while others are different. We merge the two sets of readings as follows: for those meter readings that are different in these two cases, we keep some obtained from the first set, and some from the second set. In this way, we can get an unidentifiable attack scenario with two feasible cases.

We still consider the two types of attack scenarios illustrated in Section 3 using the AC model. For Type I load redistribution attack scenario, we introduce the second feasible case by increasing the load on one bus by a certain amount and decreasing the load on another bus by the same amount. Thus, together with the original case, we obtain an unidentifiable attack with two feasible cases. For Type II load increase attack scenario, we introduce the second feasible case by increasing the load only on one bus by a certain amount; similarly, we get an unidentifiable attack with two feasible cases.

TABLE 3
Type II Attack in 14-Bus System

Meters	Before attack	After attack
PL from bus7 to bus8	0	**−10.00**
PL from bus8 to bus7	0	**10.00**

TABLE 4
The Deleted Sets and Compromised Set for Attacks in 14-Bus System

Attack	Deleted set	Compromised set
Type I	$bs12\_1$, $br19\_3$, $br12\_3$ $br13\_1$, $br19\_2$, $br13\_2$ $br12\_4$	$bs13\_1$, $br12\_1$, $br12\_2$ $br13\_3$, $br13\_4$, $br19\_1$ $br19\_4$
Tpye II	$bus7\_1$, $bus8\_1$	$br14\_1$, $br14\_3$

Two unidentifiable attacks are generated in 14-bus system, one for each type. For the Type I attack, the compromised meters are listed in Table 2, and the rest meters remain intact and their readings are omitted. The meter readings before the attack is based on the real power load vector $\{bus12, bus13\} = \{6.1, 13.5\}$, and the meter readings after the attack are based on the real power load vector $\{bus12, bus13\} = \{16.1, 3.5\}$; the loads in other buses have the same values as those in the Matpower distribution package. For the Type II attack, the compromised data are listed in Table 3. The meters readings before the attack is based on the real power $bus7 = 0$, and the readings after the attack is based on the real power $bus7 = 10$; the loads in other buses have the same values as those in the Matpower distribution package.

7.2 Locate the Attack Region and Enumerate Feasible Cases

For the two attacks listed above, we first use Algorithm 2 to get the deleted set D. The deleted set for each attack is listed in Table 4, where where $bsxx\_1/2$ means PI/QI on bus xx, respectively, and $brxx\_1/2/3/4$ means the PL/QL on the from-bus and to-bus of branch xx, respectively. In the table, $br12 = (bus6, bus12)$, $br13 = (bus6, bus13)$, and $br19 = (bus12, bus13)$. To show the effectiveness of IBE, we also list the real compromised set for each attack.

As we can see in Table 4, the IBE method cannot identify the real compromised measurements, and there is even no common element between the deleted set and the compromised set. This illustrates that the IBE method cannot identify the interacting bad measurements. Neither can other bad data detection methods, such as NQC, HIT, and COI mentioned in Section 2, as explained in Section 5.3.

Next, we apply Algorithm 3 on the deleted set listed in Table 4 to get the attack region. Though the deleted sets do not even contain one real compromised measurement, the attack regions obtained from Algorithm 3 do contain all the compromised measurements. The attack regions are shown in the dashed rectangle or trapezoid in Fig. 5.

Finally, we apply Algorithm 4 directly to enumerate all feasible cases. For both of the unidentifiable attacks, we are able to find out that there are only two feasible cases for each attack, just as same as described in Section 7.1. Furthermore, we can tell the attack type of each attack after obtaining its feasible cases. Let us take the Type II

TABLE 5
The Cost Comparison for Type I Attack in 14-Bus System

	If case 1	If case 2	Average
Solution 1	8083	Over-loaded	NA
Solution 2	8594	8594	8594
Our solution	8573	8595	8584

TABLE 6
The Cost Comparison for Type II Attack in 14-Bus System

	If case 1	If case 2	Average
Solution 1	8083	10208	9146
Solution 2	Over-powered	8486	NA
Our solution	8087	10081	9084

attack in 14-bus system as an example to show the effectiveness of Algorithm 4. In the 14-bus system, there are 14 buses and 20 branches. As we assume 4 meters on each branch and 2 meters on each bus, there are 108 meters in total. To calculate the time complexity of the enumerating algorithms in Section 5, let us further assume that the attacker can at most compromise 8 meters and there is no protected meter in the power system ($P = \emptyset$). For the brute-force search algorithm, the search space of $\sum_{i=1}^{8}\binom{108}{i}$, is still huge, not to mention all the computations required for state estimation and residual checking. While in the attack region, there are only 16 meters. By localizing the attack region first, the search space is greatly reduced to at most $\sum_{i=1}^{8}\binom{16}{i}$. Actually, the search space is even far smaller than $\sum_{i=1}^{8}\binom{16}{i}$ for two reasons. The first is that we have already found one feasible case via the IBE method. The second is, once a feasible case is found, the brute force search can skip some combinations. For instance, if a solution with three bad data has been identified, we do not need to check all bad data combinations which include these three bad data.

7.3 Cost Optimization

We evaluate our optimization problem using the two unidentifiable attacks we discussed in Section 7.1. For each of the unidentifiable attacks, we have already known that there are two feasible cases and what they are. Thus, we only need to feed these feasible cases into the objective function (1) and try to minimize it. We use the free software IPOPT [26] to solve the nonlinear optimization problem. In our analysis, we set the power shedding cost as five times as the cost of the most expensive generator. This setting is reasonable, since the power shedding cost must be higher than the cost of any generator; otherwise, the generator will choose not to satisfy the load demand even it still has available capacity.

7.3.1 Type I Attack in 14-Bus System

In this attack, we change 7 meters as shown in Table 2. Under this unidentifiable attack, the control center may either conclude that the power demands of buses 12 and 13 are 6.1 and 13.5 (case 1), or they are 16.1 and 3.5 (case 2). In the original Matpower packet, all line capacities are 9,900 MVA. To examine the impact of line capacities, we adjust the line capacities for the following branches: branches 12, 13, and 19 to 10, 25, and 10 MVA, respectively. The cost comparison is listed in Table 5, in which solution 1 is the optimal solution based on case 1, and solution 2 is the optimal solution based on case 2. "Overload" means that if the control center gets a solution based on case 1 but it is actually case 2, then some branches will exceed their line capacities. As we can see, our solution is the best, given that the control center cannot favor one case over the other.

7.3.2 Type II Attack in 14-Bus System

Table 3 shows the type II attack in 14-bus system. The two feasible cases are as follows: the real power demand on bus 7 is either 0 (case 1) or 10 (case 2). In this example, we do not change any line capacity. The cost comparison is listed in Table 6, where "overpowered" means that if the control center gets a solution based on case 2 but it is actually case 1, then some buses will get more power than their demands. As we can see, our solution is still the best, given that the control center cannot favor one case over the other.

8 Conclusion

In this paper, we introduce the concept of unidentifiable attack in power system, which is a new type of attack never proposed before. In such an attack, the control center cannot obtain a deterministic state estimation, since there may be several feasible cases and the control center cannot simply favor one over the others. We also discuss a strategy that an attacker can use to identify good attack regions where he can find meters to compromise for an identifiable attack. We then formulate an optimization strategy from the perspective of the control center to deal with an unidentifiable attack such that the average damage caused by the attack can be minimized. Furthermore, we propose a three-step scheme that allows us to find all feasible cases under an unidentifiable attack, in which we locate attack region first and hence significantly reduce the search space when compared to the search space using the brute-force search scheme directly. We also discuss a strategy that the control center can use to reveal the real case if it only has limited resources to verify some meters. Finally, we evaluate and validate our optimization strategy and enumerating scheme using 9-bus, 14-bus, and 30-bus power systems.

Nomenclature

Indices:
- i, j: bus index
- k: feasible case index
- g: generator index

Sets and elements:
- L: set of load buses
- G: set of generator buses
- A: set of all meters
- $\mathbf{z}$: the vector of all meter measurements
- $\mathbf{z}_a$: the measurement vector under attack
- P: set of protected meters
- D: set of bad meters
- B: set of all buses, $B = L \cup G$
- b_i: bus i
- T: set of transmission lines
- t_{i_j}: transmission line between buses i and j
- t_{i_*}: transmission lines incident to bus i

Constants:

m:	total number of meters, $m = \|A\|$
l:	total number of feasible cases
n:	total number of buses, $n = \|B\|$
r:	capability of the attacker
s:	number of meters an operator can verify
C_g:	generating cost of generator g
$C_{shed,i}$:	power shedding cost of load bus i
G_{ij}:	conductance between bus i and bus j
B_{ij}:	susceptance between bus i and bus j
$PG_{g,min}$:	min real capacity of generator g
$PG_{g,max}$:	max real capacity of generator g
$QG_{g,min}$:	min reactive capacity of generator g
$QG_{g,max}$:	max reactive capacity of generator g
PL_{ij}^{max}:	max line capacity between bus i and j
$PD_{k,i}$:	real demand on bus i in case k
$QD_{k,i}$:	reactive demand on bus i in case k

Variables:

$\mathbf{x}$:	the vector of state variables
θ_i:	voltage phase of bus i
V_i:	voltage amplitude of bus i
PG_g:	real power generated by generator g
QG_g:	reactive power generated by generator g
$PS_{k,i}$:	real power shedding on bus i in case k
$QS_{k,i}$:	reactive shedding on bus i in case k
P_{ij}:	real power flow between bus i and j
Q_{ij}:	reactive power flow between bus i and j
PL_{ij}:	power flow between bus i and j
$D_{shed,k}$:	total real power shedding cost for case k

ACKNOWLEDGMENTS

The authors would like to thank all the reviewers for their helpful comments. This project was supported in part by US National Science Foundation grants CNS-1117412 and CAREER Award CNS-0747108.

REFERENCES

[1] F. Schweppe and J. Wildes, "Power System Static-State Estimation, Part I II & III," *IEEE Trans. Power Apparatus and Systems,* vol. PAS-89, no. 1, pp. 130-135, Jan. 1970.

[2] H. Merrill and F. Schweppe, "Bad Data Suppression in Power System Static State Estimation," *IEEE Trans. Power Apparatus and Systems,* vol. PAS-90, no. 6, pp. 2718-2725, Nov. 1971.

[3] T. Van Cutsem, M. Ribbens-Pavella, and L. Mili, "Hypothesis Testing Identification: A New Method for Bad Data Analysis in Power System State Estimation," *IEEE Trans. Power Apparatus and Systems,* vol. PAS-103, no. 11, pp. 3239-3252, Nov. 1984.

[4] E. Asada, A. Garcia, and R. Romero, "Identifying Multiple Interacting Bad Data in Power System State Estimation," *Proc. IEEE Power Eng. Soc. General Meeting,* 2005.

[5] A. Monticelli, F. Wu, and M. Yen, "Multiple Bad Data Identification for State Estimation by Combinatorial Optimization," *IEEE Trans. Power Delivery,* vol. TPD-1, no. 3, pp. 361-369, July 1986.

[6] Y. Liu, M. Reiter, and P. Ning, "False Data Injection Attacks against State Estimation in Electric Power Grids," *Proc. 16th ACM Conf. Computer and Comm. Security (CCS),* 2009.

[7] Z. Qin, Q. Li, and M. Chuah, "Unidentifiable Attacks in Electric Power Systems," *Proc. IEEE/ACM Third Int'l Conf. Cyber-Physical Systems,* 2012.

[8] Y. Yuan, Z. Li, and K. Ren, "Modeling Load Redistribution Attacks in Power System," *IEEE Trans. Smart Grid,* vol. 2, no. 2, pp. 382-390, June 2011.

[9] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious Data Attacks on Smartgrid State Estimation: Attack Strategies and Countermeasures," *Proc. IEEE First Int'l Conf. Smart Grid Comm. (SmartGridComm.),* 2010.

[10] T. Kim and H. Poor, "Strategic Protection against Data Injection Attacks on Power Grids," *IEEE Trans. Smart Grid,* vol. 2, no. 2, pp. 326-333, June 2011.

[11] L. Mili, M. Ribbens-Pavella, and T. Van Cutsem, "Bad Data Identification Methods in Power System State Estimation-A Comparative Study," *IEEE Trans. Power Apparatus and Systems,* vol. PAS-104, no. 11, pp. 3037-3049, Nov. 1985.

[12] Z. Fadlullah, M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, "Toward Intelligent Machine-to-Machine Communications in Smart Grid," *IEEE Comm. Magazine,* vol. 49, no. 4, pp. 60-65, Apr. 2011.

[13] M. Fouda, Z. Fadlullah, N. Kato, R. Lu, and X. Shen, "A Lightweight Message Authentication Scheme for Smart Grid Communications," *IEEE Trans. Smart Grid,* vol. 2, no. 4, pp. 675-685, Dec. 2011.

[14] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications," *IEEE Trans. Parallel and Distributed Systems,* vol. 23, no. 9, pp. 1621-1631, Sept. 2012.

[15] H. Wang, B. Sheng, and Q. Li, "TelosB Implementation of Elliptic Curve Cryptography over Primary Field," Technical Report WM-CS-2005-12, College of William and Mary, 2005.

[16] H. Wang and Q. Li, "Efficient Implementation of Public Key Cryptosystems on MICAz and TelosB Motes," Technical Report WM-CS-2006-7, College of William and Mary, 2005.

[17] H. Wang, B. Sheng, C.C. Tan, and Q. Li, "WM-ECC: An Elliptic Curve Cryptography Suite on Sensor Motes," Technical Report WM-CS-2007-11, College of William and Mary, 2007.

[18] Y. Yuan, Z. Li, and K. Ren, "Quantitative Analysis of Load Redistribution Attacks in Power Systems," *IEEE Trans. Parallel and Distributed Systems,* vol. 23, no. 9, pp. 1731-1738, Sept. 2012.

[19] T. Gamage and B. McMillin, "NondeducibilitY-Based Analysis of Cyber-Physical Systems," *Critical Infrastructure Protection III,* vol. 311, pp. 169-183, 2009.

[20] H. Wang, C. Tan, and Q. Li, "Snoogle: A Search Engine for the Physical World," *Proc. IEEE INFOCOM,* 2008.

[21] S. Ren, Q. Li, H. Wang, X. Chen, and X. Zhang, "Analyzing Object Detection Quality under Probabilistic Coverage in Sensor Networks," *Proc. Int'l Workshop Quality of Service (IWQoS),* 2005.

[22] Z. Ling, J. Luo, W. Yu, X. Fu, D. Xuan, and W. Jia, "A New Cell Counter Based Attack against TOR," *Proc. 16th ACM Conf. Computer and Comm. Security (CCS),* 2009.

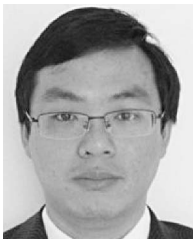
[23] D. Xuan, R. Bettati, and W. Zhao, "A Gateway-Based Defense System for Distributed DoS Attacks in High-Speed Networks," *Proc. IEEE Workshop Information Assurance and Security,* vol. 1, 2001.

[24] M. Ding, F. Liu, A. Thaeler, D. Chen, and X. Cheng, "Fault-Tolerant Target Localization in Sensor Networks," *EURASIP J. Wireless Comm. and Networking,* vol. 4, p. 19, 2007.

[25] K. Xing, M. Ding, X. Cheng, and S. Rotenstreich, "Safety Warning Based on Highway Sensor Networks," *Proc. IEEE Wireless Comm. and Networking Conf.,* vol. 4, 2005.

[26] A. Wachter and L. Biegler, "On the Implementation of an Interior-Point Filter Line-Search Algorithm for Large-Scale Nonlinear Programming," *J. Mathematical Programming: Series A and B,* vol. 106, pp. 25-57, 2006.

[27] R. Zimmerman, C. Murillo-Sánchez, and R. Thomas, "MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education," *IEEE Trans. Power Systems,* vol. 26, no. 1, pp. 12-19, Feb. 2011.



Zhengrui Qin received the BS degree in the Geophysics Department from Peking University, China, and the MS degree in the Department of Physics and Astronomy from Dartmouth College. He is currently working toward the PhD degree in the Department of Computer Science at the College of William and Mary. His research interests include SmartGrid and cognitive radio. He is a student member of the IEEE.

Qun Li received the PhD degree in computer science from Dartmouth College. He is currently working as an associate professor in the Department of Computer Science at the College of William and Mary. His research interests include wireless networks, sensor networks, RFID, pervasive computing systems, smart grid, wireless health, and social networks. He received the NSF Career award in 2008. He is a senior member of the IEEE.

Mooi-Choo Chuah received the first class honors bachelor's degree in electrical engineering from thte University of Malaya, Malaysia, and the master's and PhD degrees from the University of California, San Diego. She is the director of Wireless Infrastructure and Network Security Laboratory and an associate professor of the Computer Science and Engineering Department at Lehigh University. Prior to joining Lehigh, she spent 12 years at Bell Laboratories, Lucent Technologies, Holmdel, New Jersey, where she conducted researches in future wireless system design, network security, resource, and mobility management design. Her current research interests include next generation wired/wireless network design, mobile computing, mobile health, and Smart Grid. She has been awarded 60 US patents and 15 international patents. She is a senior member of the IEEE and a member of Sigma Xi society.