Optimal Hidden SCADA Attacks on Power Grid: A Graph Theoretic Approach

Deepjyoti Deka, Ross Baldick and Sriram Vishwanath
Department of Electrical & Computer Engineering
University of Texas at Austin
Email: deepjyotideka@utexas.edu, baldick@ece.utexas.edu, sriram@ece.utexas.edu

***Abstract*—Correct estimation of the state variables of a power grid is indispensable for its stable operation. The advent of smart grid has further enhanced the importance of secure real-time monitoring of the state variables. This paper studies hidden data attacks on power systems by an adversary trying to manipulate the state estimator. A novel graph theoretic formulation is developed for the problem of determining the optimum measurements to introduce spurious data for a hidden attack by the adversary. The paper discusses a polynomial-time solvable algorithm to optimally solve this problem under different settings. From the perspective of the system operator, techniques are proposed to help identify critical measurements for protection to prevent such hidden data attacks and to reduce their efficacy. The performance of the algorithms are demonstrated through simulations on IEEE test cases.**

***Index Terms*—Bad data detection, min-cut, power grid observability, SCADA, security, state estimation**

I. Introduction

Real-time Power Grid operation relies on accurate monitoring of the state of its different components. The state vector in a power grid is estimated by using data recorded by measurement units on different buses and lines in the grid. These are used to verify that the line currents and bus voltages operate within their safety margins. These measurements and the state vector estimate are also used to facilitate the calculation of locational marginal prices [3] for electricity pricing in the grid. Thus, correct collection of data from the distributed meters in the grid and accurate estimation of the state variables from these measurements is of utmost importance to the health of the grid. This is highlighted by the fact that one of the principal causes of the 2003 North-East blackout was incorrect telemetry due to an inoperative state estimator [1]. Sophisticated Supervisory Control and Data Acquisition (SCADA) systems are involved in data collection and relaying the measurements to the state estimator of the grid. The presence of meters and data collection units across the grid makes it vulnerable to cyber-attacks and susceptible to malicious measurements. In fact, it has been reported that cyber-hacking had compromised the U.S. electric grid in the past [2]. Such malicious data can often lead to economic losses by faulty electricity pricing [9] and can also create massive blackouts by preventing correct observation of contingencies in the grid.

In this paper, we study the vulnerability of the power grid to such 'hidden' attacks caused by adversaries gaining control of measurement meters. Traditionally, measurements collected from meters located in the power grid suffer from random noise and state estimators involve statistical methods like maximum likelihood criterion and weighted least-square criterion to remove such unwanted noise [4]. However, an adversary in control of several meters could potentially initiate a coordinated attack and change multiple measurements to evade detection by the estimator. Such malicious data attacks will thus be unobservable. [5] first studies this problem of hidden attacks on the power grid which are not detected by tests on the measurement residual. The authors of [5] show that a few measurements are sufficient to enable the adversary to orchestrate a hidden attack. Using techniques from linear algebra, the minimum number of protected measurements needed to prevent any hidden attack is also discussed. Following this, there have been multiple papers on the construction of attack vectors and identifying meter locations for introducing spurious measurements by the attacker. In [7], the authors present a framework for finding the optimal attack vector for the constrained adversary using l_0 and l_1 recovery methods. A constrained attacker is one who tries to manipulate minimum measurements to produce the desired errors in estimation. [6] studies the creation of the optimal attack vector as a mixed integer linear program. Such approaches are NP-hard in general and give approximate solutions through relaxation of the problem statement. Similarly, previous work, such as [8], require assumptions on states of the system for their results.

In this paper, we consider the problem of optimal attack vector construction corresponding to an adversary with limited resources. Following [7], we define the adversary's objective as constructing an attack vector using minimum corrupted measurements in order to produce an undetected error in the estimated state vector. Our approach differs from previous work in this area in that we use graph-theoretic ideas in determining the optimal attack vector and do not require the use of any relaxation of the basic problem statement itself. The solution determined is, hence, optimal and not an approximation. The run-time for such an algorithm is polynomial in the number of nodes (buses) and edges (lines) in the power grid. In addition, the algorithm does not depend on the exact measurement matrix used in state estimation and only uses the adjacency matrix of the associated network-graph. This is significant as the adjacency matrix is often known publicly or can be approximated by an adversary from publicly available

978-1-4799-2358-8/14/$31.00 ©2014 IEEE

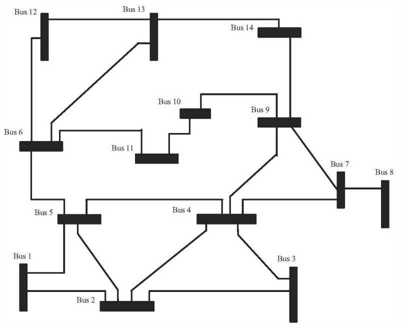

Fig. 1. IEEE 14-bus test system [10]

information unlike the exact measurement matrix which is securely maintained by the power grid system operator. By means of simulations, we demonstrate that current power grids are fairly vulnerable to hidden attacks from even constrained adversaries with limited information. We are unaware of any existing work that presents optimal solution to the hidden attack problem in polynomial time and therefore, believe this to be the first body of work to do so. In addition, we provide algorithms to greedily select a given number of measurements to increase the minimum number of measurements needed by an adversary to cause a hidden attack. In the limiting case, given the prior knowledge of the adversary's resources (maximum number of measurements it can corrupt), the greedy algorithm can aid in the identification of the critical set of protected measurements needed to prevent such hidden attacks.

The rest of this paper is organized as follows. The next section presents a description of the system model used in state estimation in a power grid and problem formulation corresponding to the constrained adversarial attack. The algorithm to determine the optimal solution to this problem is discussed in Section III. Variations of the problem under different initial conditions including pre-existing protected measurements in the grid are discussed in Section IV. We provide greedy algorithms to select existing measurements for protection to prevent hidden attacks on the grid in Section V. Simulations of the algorithms developed on test IEEE bus systems and comparisons with other approaches are reported in Section VI. Finally, concluding remarks and future directions of work are presented in Section VII.

II. Estimation in the Power Grid and Attack Models

We represent the power grid with an undirected graph (V, E) where the set of nodes, V represents the set of buses and the set of edges, E represents the set of transmission lines connecting those buses. Two buses are considered neighbors in the graph when they are connected by a line. Figure 1 shows the graph representation of the IEEE 14-bus test system, which can be found in [10].

There are two kinds of measurements in the power grid in this model: line flow measurements and bus voltage phasor measurements. Meters on lines in E measure the line power-flow while meters on buses in V measure the bus voltage. In addition, a Phasor Measurement Unit (PMU) placed at a bus collects both the bus voltage and power flows in all lines connected to that bus.

We consider the Direct Current (DC) power flow model for measurements in the grid as given by the relation $z = Hx+e$, where $z \in \mathbb{R}^m$ is the vector of measurements. $x \in \mathbb{R}^n$ is the state vector and consists of the voltage phase angles at the buses. H is the measurement matrix which relates the measurements with the state vector and e is the zero mean Gaussian noise vector associated with the measurements. In general, $m > n$ and the system has more measurements than state variables to provide redundancy. Note that, H depends on the topology of the network, the location of the meters and the parameters of transmission lines (like resistance and susceptance). In our case, each measurement can either be of a line flow or a voltage phase angle. If the k^{th} measurement in z corresponds to the flow on line (i, j) between buses i and j, we have

$$z_k = H_k x = B_{ij} x_i - B_{ij} x_j \tag{1}$$

where row H_k is a sparse vector with two non-zero values B_{ij} at the i^{th} position and $-B_{ij}$ at the j^{th} position.

$$H_k = [0..0 \quad B_{ij} \quad 0..0 \quad -B_{ij} \quad 0..0] \tag{2}$$

Similarly, if the voltage phage angle at bus i is measured in z_m, the corresponding row H_m in the measurement matrix is given by $H_m = [0..0 \quad 1 \quad 0..0]$ which is a sparse vector with 1 in the i^{th} position. The measurement matrix is sparse with a maximum of 2 non-zero values per row. To ensure correct estimation, it has full column rank of n. The state estimator outputs the estimated state vector $\hat{x}$ by minimizing the residual $\|z - H\hat{x}\|_2$s with the minimum residual having a magnitude less than a residual threshold λ. Let us consider an adversary corrupting the measurement vector z by adding an attack vector a to generate the new measurements $\hat{z} = z + a$. It is shown in [5] that if a satisfies $a = Hc$ for some $c \in \mathbb{R}^n$, then the residual calculated at the estimator remains the same as before. The estimator outputs an erroneous state vector estimate $\hat{x} + c$, leading to a successful hidden attack by the adversary. [5] constructs the attack vector by using a projection matrix P from the measurement matrix H. The problem of interest here is the case of a constrained adversary with limited resources. Such a adversary will optimally corrupt the minimum number of measurements to organize a successful attack and change the magnitude of at least 1 state variable after the attack. The optimal attack vector a^* is given as the solution of the following optimization problem :

$$\begin{aligned} &\min_{a} \|a\|_0 \\ &\text{s.t.} \quad a = Hc, \ c \neq \vec{0} \end{aligned} \tag{3}$$

This is similar to the attacker's problem in [7], where instead of $c \neq \vec{0}$, the constraint $\|c\|_\infty \geq \tau$ is imposed. Both these problems are related as every solution of Problem 3 can be suitably scaled by τ to give a solution of the problem in [7]. In the next section, we provide our algorithm to design the optimal attack vector using graph theory.

III. Optimal Attack Vector Design

Consider the structure of the sparse m x n measurement matrix H as noted in the previous Section. We augment one extra column h^g to the right of the matrix H to create a modified measurement matrix $\hat{H}$ with

$$\hat{H}_m = \begin{cases} [H_m| -1] & \text{for phase angle measurement} \\ [H_m|\ 0] & \text{for flow measurement} \end{cases}$$

The state vector c is also augmented to form a new state vector $\hat{c} = [c|\ 0]^T$ So, $a = Hc = \hat{H}\hat{c}$. The new formulation $(\hat{H},\ \hat{c})$ is only added to provide a ground phase of 0 such that bus phase angle becomes equivalent to a line flow between the bus and ground. We state and prove a theorem which will enable us to develop the algorithm for determing attack vector.

Theorem 1. *There exists a* $0-1$ *vector* c_{opt} *for the optimal attack vector* a^* *for Problem (3) such that* $\|a^*\|_0 = \|Hc_{opt}\|_0$.

Proof. Consider Problem (3). The optimal attack vector is $a^* = Hc^*$. If c^* is a $0-1$ vector, take $c_{opt} = c^*$. If c is not a $0-1$ vector, construct vector c_{opt} such that $c_{opt}(i) = 1(c^*(i) \neq 0)$, $\forall i \in \{1, n\}$. It follows from the structure of the H matrix that $\|Hc_{opt}\|_0 \leq \|Hc^*\|_0$. As a^* is optimal, it follows that $\|Hc_{opt}\|_0 = \|Hc^*\|_0 = \|a^*\|_0$. □

Consider the modified measurement matrix $\hat{H}$ and the augmented vector $\hat{c}$. We conclude that the optimal attack vector is given by $a^* = \hat{H}\hat{c}_{opt}$, where $\hat{c}_{opt}$ is given by $[c_{opt}|\ 0]^T$.Given that we are concerned only with $\|a^*\|_0$ for the optimal attack vector and $\hat{c}_{opt}$ is a $0-1$ vector, the contribution of a flow measurement in $\|a^*\|_0$ remains the same even if the susceptance B_{ij} of every line in $\hat{H}$ is changed to 1. We, therefore, create an incidence matrix A_H of size m x $(n+1)$ from $\hat{H}$ as follows:

$$A_H(i,j) = 1(\hat{H}(i,j) \geq 0) - 1(\hat{H}(i,j) \leq 0) \tag{4}$$

Note that multiple measurements of the same line-flow or phase angle will lead to multiple edges between two nodes in the associated graph. The main result of this paper, which gives the minimum attack vector for Problem (3) is included in the following theorem.

Theorem 2. *The cardinality of the optimal attack vector in Problem (3) with measurement matrix* H *is equal to the min-cut of an undirected graph* G_H *given by the incidence matrix* A_H.

Proof. It is clear that for any $0-1$ vector $\hat{c}$ of size n x 1, $\|\hat{H}\hat{c}\|_0 = \|A_H\hat{c}\|$. Using Theorem 1, the optimization Problem 3 can be written as

$$\begin{aligned} &\min_a \|a\|_0 \\ \text{s.t.}\quad & a = A_H\hat{c},\ \hat{c} \neq \vec{0}, \hat{c}(n+1) = 0, \hat{c} \text{ is a } 0-1 \text{ vector} \end{aligned} \tag{5}$$

This is the classical min-cut partition problem in graph theory. The minimum value of $\|a\|_0$ is, thus, given by the size of the min-cut of the undirected graph G_H with A_H as incidence matrix. □

Formally, after pre-processing the initial measurement matrix H to generate $\hat{H}$ and subsequently A_H and G_H, the optimal attack vector and its cardinality are given by Algorithm 1.

Algorithm 1 Optimal Attack Vector through Min-Cut

```
Compute the min-cut of the graph $G_H$
$c \leftarrow \mathbf{1}$
Choose $(n+1)^{th}$ node as root
Remove min-cut edges
Do breadth first path traversal from root
if node $i$ is reached then
    $c(i) \leftarrow 0$
end if
$a^* \leftarrow Hc$
```

The graph traversal after removing the min-cut edges designates 0 to the state variables of buses reachable from the ground node and 1 to the buses in the other partition. The min-cut computation is a well-studied problem in graph theory and is known to have a run time which is polynomial in the number of nodes and edges in the graph [11]. [12] gives a simple algorithm for computing the min-cut in $O(|V|log|V| + |E|)$ time-steps. Here, $|V|$ and $|E|$ represent the number of nodes and edges in the graph.

IV. Optimal Attack Vector Design with Protected Measurements and State Variables

In the case of power grids, it is often true that certain measurements are protected from cyber-attacks by utilizing encryptions or through geographical isolation. Similarly, certain state variables might be protected from adversarial contamination. In such cases, the adversary has the additional constraints of making the values of the attack vector a corresponding to protected measurements and values of c corresponding to protected state variables 0. The optimal attack vector a^* here can be written as the solution of the following optimization problem:

$$\begin{aligned} &\min_a \|a\|_0 \\ \text{s.t.}\quad & a = Hc,\ H^{S_m}c = 0,\ c \neq \vec{0},\ c(i) = 0\ \forall i \in S_v \end{aligned} \tag{6}$$

Here, S_m and S_v are the sets of protected measurements and state variables respectively and H^{S_m} represents the protected rows in the measurement matrix. As outlined in Section III, we generate the undirected graph G_H with incidence matrix A_H from $\hat{H}$. Every measurement in A_H leads to an edge in G_H of unit weight. To include the additional constraints due to protected sets S_m and S_v, we **modify** G_H as follows:

1. Create an edge of infinite weight between ground node and every bus corresponding to protected state variable.
2. Change the weights of every edge with protected flow

measurement to infinity.
The resultant graph generated after this modification is denoted by G_H^*. We list the steps to obtain the optimal attack vector formally in Algorithm 2. In any feasible solution given by Algorithm 2, the buses sharing the protected edges are not included in the min-cut to keep the value of the min-cut below infinity. Thus, the optimal attack vector formed satisfies the constraints due to protection. In the next section, we use the knowledge of optimal attack vector construction to design protection policies that can be adopted to restrict the efficacy of hidden attacks.

Algorithm 2 Optimal Attack Vector with protected measurements and state variables

```
Modify $G_H$ to generate $G_H^*$ using $S_m$ and $S_v$
Run Algorithm 1 on $G_H^*$
```

V. Protection Strategies against Hidden Attacks

Consider Problem 6 with pre-existing secure measurements (set S_m) and state variables (set S_v). For complete protection against hidden attacks, it has been shown in [5] that H^{S_m} should have full column rank where H^{S_m} represents the protected rows in the measurement matrix. For that, the number of protected measurements needs to be greater than n [5], and requires a huge implementation cost. Instead, we look at the problem of augmenting the set of protected measurements S_m with k additional measurements from the unprotected set S_m^c to maximally increase the cardinality of the optimal attack vector and restrict the adversary. We formulate it as follows:

$$\max_{S^* \in S_m^c} \min_{a} \|a\|_0 \tag{7}$$

$$\text{s.t.}\quad a = Hc,\ c \neq \vec{0},\ H^{S_m}c = 0,\ c(i) = 0\ \forall i \in S_v$$
$$H^{S^*}c = 0,\ |S^*| = k,\ \text{where } S^* \text{ is set of new protections}$$

We observe that optimally protecting k new measurements is equivalent to changing the weights of k edges in the modified graph G_H^* (see Section IV) to infinity to increase the min-cut. Solving this NP-hard problem by brute force is impractical given the number of candidate measurements in S_m^c. We provide here a greedy approach for Problem 7 in Algorithm 3 . Here, at each step, the best candidate is greedily selected for protection given the current a^*. After including the best measurement in the protected set S_m, a^* is updated and used in the next step.

Step 4 of Algorithm 3 keeps only the measurements in the current min-cut of G_H^* as candidates in each step as protecting measurements outside the min-cut does not lead to an increase in the size of the min-cut of the updated graph. This step, thus, leads to an reduction in the number of possible candidates from $m - |S_m|$ to $|a\|_0$ without any loss of performance.

Algorithm 3 Greedy Solution for Additional Protection

```
1:  for $i = 1$ to $k$ do
2:      $a_{cm} \leftarrow a^*$
3:      for $j = 1$ to $m$ {$m$: total measurements } do
4:          if $a^*(j) \neq 0$ then
5:              $G_{temp} \leftarrow G_H^*$
6:              Protect measurement $j$ in $G_{temp}$
7:              Compute optimal attack vector $a_{temp}$ for $G_{temp}$
8:              if $\|a_{temp}\|_0 \geq \|a_{cm}\|_0$ then
9:                  $cm \leftarrow j$ {current best candidate}
10:                 $a_{cm} \leftarrow a_{temp}$ {current optimal attack vector}
11:             end if
12:         end if
13:     end for
14:     Protect measurement $cm$ in $G_H^*$ and update $a^*$.
15: end for
```

VI. Simulations on IEEE test systems

In this section, we present the performance of our proposed algorithms by simulating their performance on different IEEE test bus systems. All simulations are run in Matlab Version 2009a and averaged to express the results. We first discuss Algorithms 1 and 2 which give the optimal attack vector (a^*) of the adversary. In the IEEE-14 bus system, we place flow measurements on all lines and angle measurements on 60% of the buses selected randomly. We show the trend in average cardinality of the optimal attack vector with increasing fraction of randomly placed protected measurements in Figure 2. We observe that our algorithm is optimal and gives the same result as that given by a brute force approach and much better than the output of a l_1 relaxation of Problem 6. Further, Figure 3 shows the improved performance of Algorithm 2 in designing the optimal attack vector compared to a l_1 relaxation of Problem 6 for 30, 57 and 118 IEEE test bus systems under different system conditions. Next, we discuss the performance of Algorithm 3, which selects k additional protected measurements to maximally increase the cardinality of the adversarial attack vector. Figure 4 compares the performance of our greedy algorithm with the brute force selection of additional measurements for the IEEE 14-bus system. It can be noted that our algorithm, though suboptimal, performs remarkably well over a range of values of k. Following this, we run simulations of Algorithm 3 for IEEE 57, 30 and 118 bus systems and plot the average increase in the cardinality of the optimal attack vector with an increase in the value of k in Figure 5. It can be observed that, despite being sub-optimal, this low complexity algorithm can be used to protect measurements to substantially increase the robustness of the grid .

VII. Conclusion

In this paper, we study the problem of undetected estimation errors in a power grid through injection of spurious measurements into SCADA. We formulate the optimal constrained adversarial attack problem of manipulating minimum measurements for a successful hidden attack and provide a solution for it using a novel graph-theoretic approach. The proposed algorithm presents the *optimal* solution in *polynomial time*, without using any approximation. We prove that our algorithm needs only information about the grid topology (and doesn't

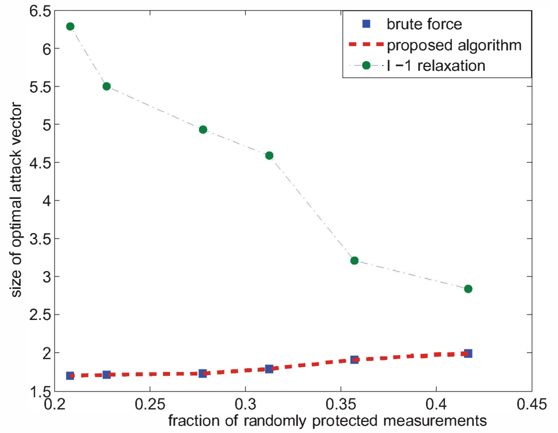

Fig. 2. Optimal hidden attack on IEEE 14-bus system with flow measurements on all lines, voltage measurements on 60% of the buses and fraction of measurements protected

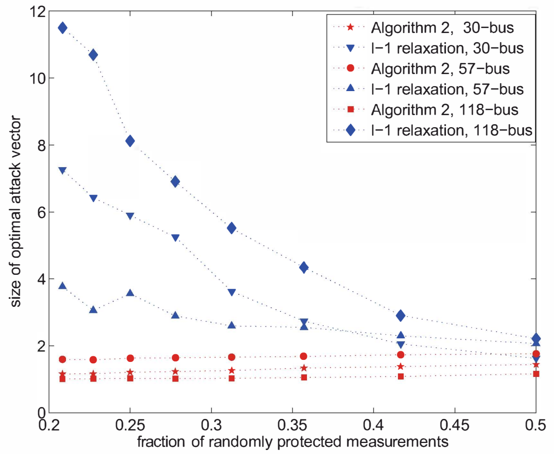

Fig. 3. Optimal hidden attack on IEEE test systems with flow measurements on all lines, voltage measurements on 60% of the buses and fraction of measurements protected

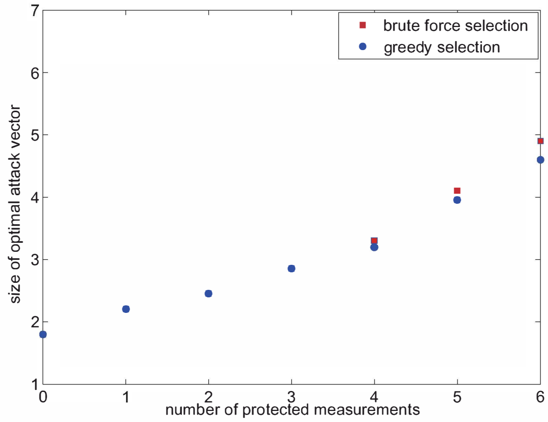

Fig. 4. Protection of additional measurements in IEEE 14-bus system with flow measurements on all lines, voltage measurements on 60% of the buses and 1/6% of measurements initially protected

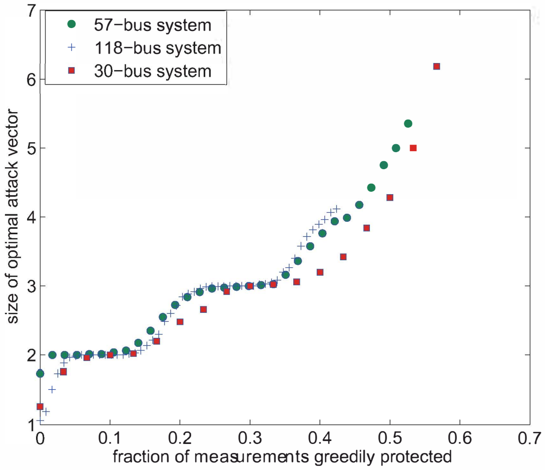

Fig. 5. Greedy protection of additional measurements in IEEE test systems with flow measurements on all lines, voltage measurements on 60% of the buses and 1/6% of measurements initially protected

require the actual line susceptance in the grid). We also develop a greedy algorithm to protect additional measurements to reduce the efficacy of hidden attacks in the grid. Numerical simulations on IEEE test cases are used to show the advantages of our proposed algorithms and compare them to other approaches. This work on low-complexity algorithms can be extended to include other adversarial attack models with different constraints and objectives. Another extension includes the placement of limited number of secure phasor measurement units (PMUs) to improve protection against hidden attacks. This is the focus of our current work.

References

[1] B. Liscouski and W. Elliot, “Final report on the August 14, 2003 blackout in the United States and Canada: Causes and Recommendations”, *A report to US Department of Energy*, 40, 2004.

[2] S. Gorman, “Electricity grid in U.S. penetrated by spies”, *Wall St. J.*, 2009.

[3] A. L. Ott, “Experience with PJM market operation, system design, and implementation”, *IEEE Trans. Power Syst.*, vol. 18, no. 2, 2003.

[4] A. Abur and A. G. Expósito, “Power System State Estimation: Theory and Implementation”, New York: Marcel Dekker, 2004.

[5] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids”, *Proc. ACM Conf. Comput. Commun. Security*, 2009.

[6] O. Vukovic, K. C. Sou, G. Dan, and H. Sandberg, “Network-aware mitigation of data integrity attack on power system state estimation”, *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 6, 2012.

[7] T. Kim and V. Poor, “Strategic Protection Against Data Injection Attacks on Power Grids”, *IEEE Trans. Smart Grid*, vol. 2, no. 2, 2011.

[8] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, “Limiting false data attacks on power system state estimation”, *Proc. Conf. Inf. Sci. Syst.*, 2010.

[9] L. Xie, Y. Mo, and B. Sinopoli, “False data injection attacks in electricity markets”, *Proc. IEEE SmartGridComm*, 2010.

[10] R. Christie, “Power system test archive”, Available: http://www.ee.washington.edu/research/pstca.

[11] L. R. Ford and D. R. Fulkerson, “Maximal flow through a network”, *Can. J. Math.*, 1956.

[12] M. Stoer and F. Wagner, “A simple min-cut algorithm”, *J. ACM*, 44(4), 1997.