Improved Protection Scheme for Data Attack on Strategic Buses in the Smart Grid

Charith Wickramaarachchi*, Sanmukh R. Kuppannagari†, Rajgopal Kannan† and Viktor K. Prasanna†
*Department of Computer Science
†Department of Electrical Engineering
University of Southern California
Los Angeles, CA 90089, USA
Email: {cwickram, kuppanna, rajgopak, prasanna}@usc.edu

***Abstract*—Determining voltage phase angles of buses in a Smart Grid is a critical operation in the power system state estimation process. Invalid state estimate of strategic buses can cause a severe socioeconomic impact. In this paper, we present an optimal protection scheme to protect the voltage phase angle estimation of strategic buses in a Smart Grid against data spoofing attacks. We discuss the limitations of the protection scheme presented by Deka et al by identifying a class of attack vectors which cannot be defended against using their protection scheme. We then provide an improved protection scheme to find the minimal set of measurements to protect in order to secure the set of strategic buses against any data spoofing attack. Finally, we discuss tradeoffs and differences in our protection scheme compared with the protection scheme presented by Deka et al.**

I. Introduction

Advances in Internet of Things (IoT) technologies have accelerated the momentum towards smart cyber-physical environments like Smart Grids. The tight coupling of physical and cyber subsystems in Smart Grids makes them vulnerable to complex attacks that utilize both cyber and physical components. Thus security measures for Smart Grids should be designed to make them resilient against such attacks.

A Smart Grid consists of a power system and a communication system. The objective of the power system is to deliver the power generated from power generation units to the consumers. The power system consists of generation, transmission and distribution subsystems. Operating conditions of the power system are continuously monitored at SCADA/EMS (Supervisory Control and Data Acquisition/Energy Management System) systems and managed utilizing the information coming through the communication system. Various sensory devices are deployed across the power system in order to achieve this task. These sensors include: 1) Power injection meters that measure the power flow at generators; 2) Power flow meters and phasor measurement units (PMUs) that measure power flow and voltage phase angles at transmission lines and buses in the transmission subsystem; 3) Smart meters that measure power consumption at consumer sites.

Power system state estimation is a critical process in the power transmission subsystem [1]. State estimation is conducted at EMS/SCADA systems in an online manner using the measurement information coming from different parts of the transmission network [1]. Computed state estimates are then used to manage the power flow of the system to ensure that the system is maintained in a nominal state [1]. Protective measures are taken in emergency situations using the state estimate results. Invalid state estimate can create false demands in power markets [2], [3], increase operational cost [4] and can even cause blackouts [5]. Hence protecting the integrity of the state estimate is of vital importance.

The power system transmission network consists of transmission lines and buses. Determining complex voltage phase angles at these buses is a critical part of the power system state estimation process. This is determined using the power flow and phase angle measurements from power flow meters and PMUs. An adversary may perform a data spoofing attack altering this sensor data to cause an invalid state estimate in the power system. While existing SCADA systems are equipped to detect random spoofing attacks using bad data detectors (BDD), recently Liu et al in [6] showed that well structured hidden data spoofing attacks (HDS) can be formulated to bypass the BDD by carefully selecting the set of measurements to attack [6].

It has been shown in the literature [7] that the number of sensor measurements that need to be protected in order to secure the state estimate of all the buses is the same as the number of buses in the transmission network. Since this can be a costly task, protection schemes to protect the state estimate of strategic subsets of buses in the transmission network have been proposed [8], [9]. In [8], Deka et al presented a polynomial time algorithm using min-cuts to find the minimum set of measurements an adversary needs to attack in order to perform a HDS to compromise a given set of state variables. They extend this method to propose a polynomial time algorithm to find the minimum set of measurements to protect in order to secure a given set of state variables from HDSs. In this paper, we address the limitations of this work and present an alternative protection scheme to secure a set of buses against any HDS.

The main technical contributions of this paper are summarized below:

- We identify the limitations of the protection scheme presented by Deka et al in [8] by providing a counter-example. We identify a class of attack vectors that cannot be defended against using the protection scheme of [8].

- We provide an improved protection scheme to find the minimal set of measurements to protect in order to secure a set of buses against any HDS.

II. Background

Following [8], we consider the DC power flow model for state estimation. The power grid transmission network consists of buses and transmission lines. The states of the power system are represented by state variables consisting of voltage magnitudes and phase angles at buses. Voltage magnitudes can be directly measured using sensors deployed at buses while phase angles are estimated using the active power flow measurements collected from sensors [10]. In this paper, two types of measurements are considered: 1) Power flow measurements of transmission lines, 2) Voltage phase angles directly measured at buses. Power flow measurements are measured by power flow meters and voltage phase measurements can be directly measured through phase measurement units.

In the DC power flow model, the relationship between measurements and state variables is governed by:

$$z = Hx + e \tag{1}$$

$z \in \mathbb{R}^m$ is a vector of measurements, $x \in \mathbb{R}^n$ is a vector of state variables $(m > n)$. H is the measurement matrix and $e \in \mathbb{R}^m$ represents measurement errors (noise). Assuming a gaussian error distribution with co-variance R, state estimate x can be obtained by:

$$x = (H^T R H)^{-1} H^T R z = Pz \tag{2}$$

Power systems consist of a bad data detector that is capable of detecting and removing bad data from the measurements. However, in [6] Liu et al. showed that existing bad data detectors are only capable of detecting unstructured random errors from the measurements.

The attack model used by an attacker is as follows: An attacker formulates an attack by introducing an attack vector a to the vector of measurements z so that $\bar{z} = z + a$. It is shown in [6] that some *structured* attacks with $a = Hc$ can bypass the bad data detector, introducing an error $c \in \mathbb{R}^n$ to the state estimates. Attackers should have access to the topology of the network and access to the measurements to conduct such attack. Since the power system communication network is an isolated system and it is very hard to manipulate data at the SCADA due to physical security. Attackers will have to physically access the sensors to inject bad data. Generally, these sensors are protected by guards or using surveillance equipment. But due to the large number of sensors in transmission networks and limited budgets, it is hard to protect all the sensors. As shown in [7] the number of measurements that needs to be protected in order to secure the state estimate of all buses is same as the number of buses in the transmission network.

In [8] Deka et al proposed a method to find the minimum cardinality attack vector to attack a given set of state variables S_{atck} such that the attack will produce a non-zero change in the state estimate of all the state variables in the set S_{atck}.

First, a graph G_H is constructed from the transmission network using following rules:

1 Each state variable associated with a bus is represented by a vertex.
2 Each flow meter is represented by an edge $e = (u, v)$ where u and v are buses incident to the measured transmission line.
3 A new vertex: *reference vertex* is introduced connecting each bus with a phase measurement to the *reference vertex* by adding new edges.
4 A new vertex: *attack vertex* is introduced connecting each bus in S_{atck} to the *attack vertex* by adding new edges.
5 Each edge that represents a secured measurement has infinite weight and each unsecured edge has a unit weight.

Figure 1 illustrates an example 6-bus transmission network and G_H constructed using the above mentioned steps.

They stated a method to find the attack vector with minimum cardinality in **Lemma 1**:

Lemma 1: [8] *The attack vector of minimum cardinality is given by the minimum cut of the undirected graph G_H which separates nodes in S_{atck} from the 'reference node'.*

Extending **Lemma 1** Deka et al, proposed a method to find the minimum set of measurements that needs to be protected in order to protect a given set S_{atck} from such attacks. They argue that *protection is possible if and only if the weight of the minimum cut between the 'reference node' and the 'attack node' becomes unbounded or infinite.* Hence they argue that the minimum set of measurements to protect in order to secure a given S_{atck} can be found in polynomial time [8]:

Theorem 1: [8] *The minimum measurements that need to be protected to secure the set S_{atck} against any hidden false data spoofing attack is given by the unprotected edges in the minimum cost path from the $attack\ vertex$ to the $reference\ vertex$ in G_H, where the cost of an edge is given by the reciprocal of its edge weight.*

III. Protection Scope

In this section, we demonstrate the limitations of the protection scheme presented in [8].

Consider the transmission network of Figure 1. Assume all transmission lines have flow measurements and buses 1, 2, 3 have phase measurements. Let S_{atck} be $\{1, 2, 3, 4, 5, 6\}$. Assuming unit susceptance magnitude at each transmission line and using equation (1), the relationship between measurements and state variables for this transmission network is as stated in equation (3). Here $z_{(i,j)}$ represents flow measurement in line (i, j), z_i the phase measurement at bus i and x_i the state variable of bus i.

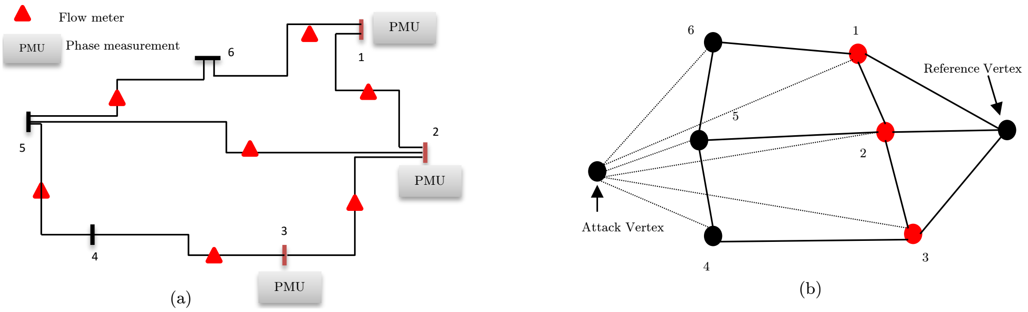


Fig. 1: On the left (a) is a 6-Bus transmission network. Each transmission line consists of flow meters and buses 1, 2, 3 have phase measurements (PMUs)(colored in red). On the right (b) is the G_H constructed from the transmission network following the steps mentioned in Section II.

$$\begin{bmatrix} z_{(1,2)} \\ z_{(1,6)} \\ z_{(2,3)} \\ z_{(2,5)} \\ z_{(3,4)} \\ z_{(4,5)} \\ z_{(5,6)} \\ z_1 \\ z_2 \\ z_3 \end{bmatrix} = \begin{pmatrix} -1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \times \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix} \quad (3)$$

Now according to Theorem 1 [8], protecting any of the phase measurements at buses 1, 2 or 3 should protect S_{atck} from any hidden data spoofing attack. Consider a scenario where we choose to protect measurement 1 (z_1). One can show that state variables 4, 5, 6 will be affected by a hidden data spoofing attack if an attacker uses the attack vector a below:

$$a = \begin{bmatrix} 0 & -1 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^T \quad (4)$$

The counter-example above can be generalized to arbitrary transmission network topologies by using the following assumption from [8]: for a successful HDS, a non-zero change should be observed in each and every state variable of the set S_{atck}. Let $P_{\{i\}}$ denote the submatrix of P consisting only of rows indexed by a given index set $\{i\}$. Then we have,

Proposition 1: There exists a structured attack vector a and a set S_{atck} such that $c = P_{\{i\}}a$, $i = S_{atck}$ and c is an $|S_{atck}| \times 1$ vector and $1 < ||c||_0$ which cannot be defended against by the protection scheme defined by Theorem 1.

Proof: (by contradiction) Assume that the protection scheme defined by Theorem 1 can defend against any structured attack defined in Proposition 1. Alternatively, there cannot be any attack vector a for any set S_{atck} for which $1 < ||c||_0$. Let the minimum number of measurements be protected as determined by Theorem 1 be l. Let $||S_{atck}|| = k$ with $k > l$ (we will show later why this assumption is valid). Let the attack vector a have non-zero values for each meter measurement except for the ones protected using the protection scheme defined by Theorem 1. Hence, only the protected meter measurements can be relied upon to make state estimation.

Consider the equation,

$$z = H_{\{T\},\{S_{atck}\}}x + e \quad (5)$$

$H_{\{T\},\{S_{atck}\}}$ denotes the submatrix of H with rows corresponding to all the protected meters T and columns corresponding to the state variables S_{atck}. Now, $H_{\{T\},\{S_{atck}\}}$ is an $l \times k$ matrix with $l < k$. So the rank of $H_{\{T\},\{S_{atck}\}} = l$. This implies that there exists $k - l$ state variables in the set S_{atck} which are linearly dependent upon l independent state variables. If the l independent state variables do not change, it is not possible to detect any changes in the remaining $k - l$ variables. Hence, there exists c such that $||c||_0 = k - l$. Choosing k, l such that $k - l > 1$ contradicts the assumption that the protection scheme can defend against any structured attack defined in Proposition 1.

Now we show why choosing k, l such that $k - l > 1$ is a valid assumption. As per the protection scheme of Theorem 1, each node in S_{atck} is joined to the attack node with an edge. So the minimum number of meters l to be protected will be: $\min\{dist(ref, s), s \in S_{atck}\} + 1$ where $dist(u, v)$ gives the minimum distance between nodes u, v. So, for any S_{atck} where $||S_{atck}|| = k > 2 + \min\{dist(ref, s), s \in S_{atck}\}$, the assumption that $k - l > 1$ is valid $\blacksquare$.

Theorem 1 [8] defines a protected path in graph G_H. Proposition 1 implies that the protection scheme described in [8] is limited, as shown below.

Theorem 2: The protection scheme proposed in [8] will only protect the state variables represented by the vertices in the protected path from *attack vertex* to *reference vertex* against any HDS.

Proof: The protection scheme provided by **Theorem 1** only secures all the measurements in the shortest path from reference vertex to the set of vertices in S_{atck}. Let $u \in S_{atck}$ denote the vertex at the end point of this shortest path. Every cut that separates any vertex in the shortest path from reference vertex v to u will thus have a protected edge with infinite weight. However, it can be clearly seen that there can be cuts not containing any protected edges that separate other vertices in the set $S_{atck} \backslash u$ from the reference vertex v, thereby making them vulnerable to HDS ■.

Thus the protection scheme proposed in [8] (Theorem 1) only makes it impossible for an attacker to attack **all** the state variables in S_{atck} at once. However it might be possible to attack a subset of the state variables associated with S_{atck} which is a fundamental limitation in the protection scheme.

IV. Improved Protection Strategy

We now provide a scheme for optimal protection against any data spoofing attack where it can protect all the state variables associated with S_{atck}. The proposed method to find the protection scheme is given by **Theorem 3** below.

Theorem 3: The minimum measurements that need to be protected to secure the set S_{atck} against any hidden false data injection attack is given by the unprotected edges in a minimum Steiner tree that connects *reference vertex* in G_H to all the vertices that represent S_{atck}.

Proof: According to Deka et al. in [8] the attack vector to attack a given set S_{atck} is given by the cut that separates the vertices associated with S_{atck} with the reference vertex. If we need to protect each state variable associated with S_{atck}, all the cuts in G_H that separate any vertex in S_{atck} with reference vertex should have an edge with infinite weight. It is clear that to achieve this condition there should be a protected path from each vertex in S_{atck} to the reference vertex. In other words edges in a subgraph that connect each vertex in S_{atck} and reference vertex represents a set of measurements to protect in order to protect S_{atck} from HDS. The minimum set of measurements is therefore given by the unprotected edges in a minimum Steiner tree that connects *reference vertex* in G_H to all the vertices that represent S_{atck}. ■.

Figure 2 illustrates the protection provided by two protection schemes using IEEE 14 bus dataset.

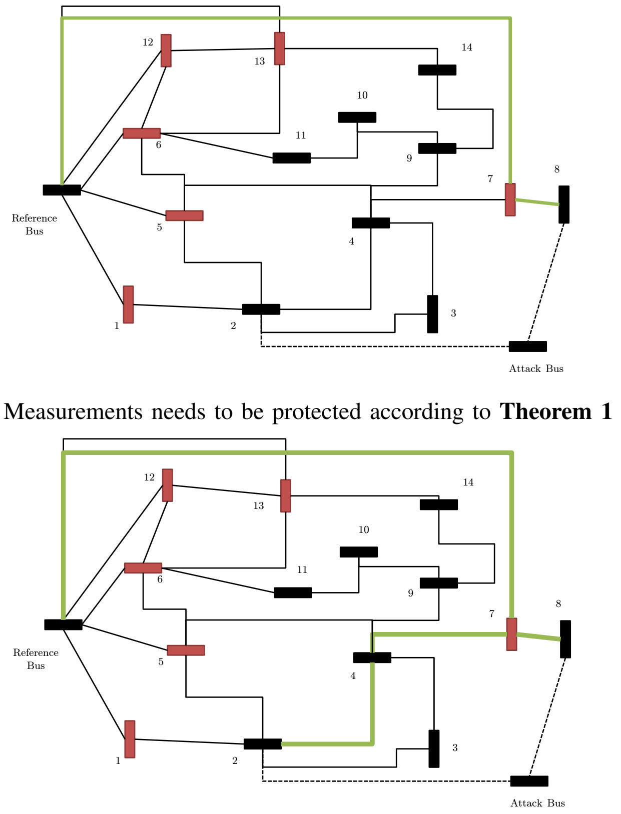
V. Related Work

In this section, we describe some of the existing work in the literature closely related to the work presented in this paper.

As mentioned before, Liu et al. in [6] first showed a limitation in SCADA systems which enables attackers to formulate an undetectable attack that can bypass the BDD subsystem. They showed that the residual r used by BDD will be unaffected if the attacker employs a structured attack vector $a = Hc$ as shown below:

$$r = \parallel z + a - H(x + c) \parallel = \parallel z - Hx \parallel \tag{6}$$

In [11] Kosut et al showed a relationship between attack vectors that can conduct an HDS and network observability [12]. They showed that an attack vector can conduct a HDS if and only if *the network becomes unobservable when the meters associated with the nonzero entries of attack vector are removed from the network*. Extending this work, Bobba et al in [7] showed that it is sufficient and required to protect a basic set of measurements in order to secure the state variables associated with all the buses in the transmission network.



(a) Measurements needs to be protected according to **Theorem 1**

(b) Measurements needs to be protected according to **Theorem 3**

Fig. 2: Comparison of set of measurements that needs to be protected in order to protect buses 2 and 8 using a 14 bus transmission network. Red colored buses represent buses with direct phase measurements. Measurements represented by bold green lines denotes the measurements that need to be protected in order to protect the state estimate of buses 2 and 8.

Since the cardinality of a set of basic measurements in a transmission network is the same as the number of buses, protection schemes to protect the state estimate associated with subsets of buses have been proposed [8], [9]. The set of states to be protected can be derived in various ways, data driven influence based metrics as shown in [13] is one such example. While our work addresses the limitations of the protection scheme proposed in [8], in [9] Bi et al also present a graphical method similar to the work of [8]. In this work, they consider a system which consists of power injection measurements and power flow measurements whereas our work focuses on a system with direct phaser and power flow measurements. Bi et al show that in their setting the minimum set of measurements that needs to be protected in order to secure a given subset of buses is given by a variant of the minimum Steiner tree problem in a graph constructed from the transmission network.

VI. Evaluation

A. Setup

We evaluated both protection schemes using simulations on an IEEE 14 Bus test case dataset [14]. We implemented the a tool to compute minimum Steiner tree as an integer linear program based on [15] using Gurobi solver [16]. Graph Stream Project [17] was used for shortest path calculations. All the experiments were conducted in an Intel Core i5 3.20 GHz computer with 16GB RAM.

In these evaluations, we randomly assigned PMUs to the buses. We considered the cases where 25%, 50% and 75% of the buses have PMUs.

B. Results and Discussion

We used three evaluation metrics to compare the protection schemes provided by **Theorem 1** and **Theorem 3**.

1 Protection coverage
2 Protection cost
3 Computation time

Protection coverage is defined as the number of buses protected from any HDS as a result of protecting the measurements given by the protection method. We define the protection cost to be the number of measurements that are protected by the protection method. Computation time is defined as the time to compute the set of measurements that needs to be protected.

According to **Theorem 1**, in the sub-optimal protection method (S-OPT) provided by Deka et al [8], the set of measurements to protect is given by the edges in the shortest path from attack vertex to reference vertex. Since the edges from attack vertex do not represent any measurement, protection cost will be one less than the number of edges in the shortest path from the attack vertex to the reference vertex. According to **Theorem 2**, the set of buses protected by this method is given by the buses represented by vertices in this protected path. We can exclude reference vertex and attack vertex as they do not represent any buses. The cardinality of these protected set of buses (Protection coverage) will be equal to the protection cost as a result.

Similarity, as stated in **Theorem 3** the optimal protection scheme (OPT) is given by the set of measurements represented by the edges in the minimum Steiner tree that connects the vertices that represent S_{atck} with the reference vertex. Since the number of edges in a tree is one less than its number of vertices, protection cost of the OPT will be as same as the protection coverage.

Figure 3 shows how protection cost/protection coverage change with increasing $\mid S_{atck} \mid$. As expected, we can observe that in the optimal protection scheme protection cost and protection coverage increase with $\mid S_{atck} \mid$. It can be seen that the protection cost and protection coverage is independent of $\mid S_{atck} \mid$ when the sub-optimal protection scheme provided in **Theorem 1** is used. This is due to that fact that protection scheme provided in **Theorem 1** only guarantees to protect a single bus in $\mid S_{atck} \mid$ from HDS.

Figure 4 shows how the computation time changes with increasing $\mid S_{atck} \mid$. We observe that the computation time for the OPT protection scheme is higher than the S-OPT protection scheme. This is due to the NP-Hard nature of the minimum Steiner tree problem [18]. Due to the computational intractability of finding the minimum Steiner tree on real scale transmission networks, approximate algorithms [15], [19] can be used. Even though the approximate Steiner tree solutions will not provide the optimal solution in terms of the protection cost, as discussed in the proof of **Theorem 3**, any Steiner tree (or sub-graph) that connects reference vertex with vertices that represent $\mid S_{atck} \mid$ will provide complete protection from any HDS.

PMU placement in power grids is gaining traction since its induction. Placement strategies of PMUs have been discussed in the literature [20]. As shown in **Theorem 3**, the set of measurements to protect is given by the edges in the minimum Steiner tree that connects the vertices that represent S_{atck} with reference vertex. As a result, placing secure PMUs at each bus in S_{atck} will protect them from HDS with minimum protection cost. Further analysis on optimal PMU placement to ensure network observability and protecting all buses against HDS have been discussed in the literature [21].

VII. Summary

In this paper, we identified a limitation in the protection scheme provided by Deka et al in [8], to protect a set of buses in power grid against hidden data spoofing attacks. We presented an improved protection scheme that addressed this limitation. Analysis on protection schemes was provided theoretically and discussed using evaluation results.

VIII. Acknowledgment

This work has been funded by US NSF under grant ACI-1339756 and Northrop Grumman Corporation under grant 003570-00001.

References

[1] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC press, 2004.

[2] L. Jia, R. J. Thomas, and L. Tong, "Impacts of malicious data on real-time price of electricity market operations." Citeseer.

[3] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 659–666, 2011.

[4] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1731–1738, 2012.

[5] ——, "Modeling load redistribution attacks in power systems," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382–390, 2011.

[6] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

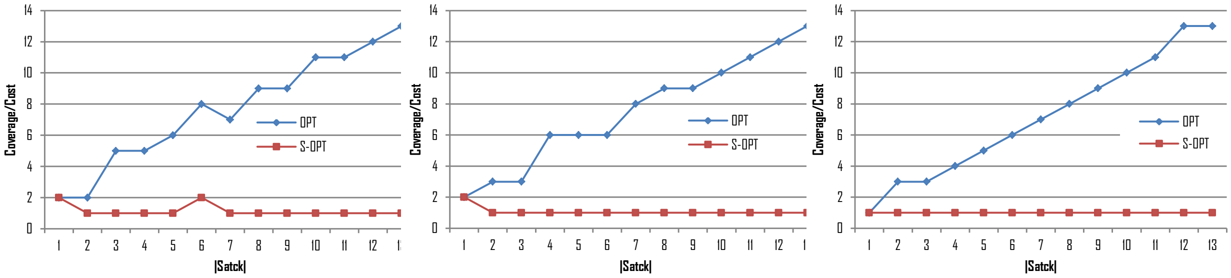
[7] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation."

[8] D. Deka, R. Baldick, and S. Vishwanath, "Data attack on strategic buses in the power grid: Design and protection," in *PES General Meeting—Conference & Exposition, 2014 IEEE*. IEEE, 2014, pp. 1–5.

[9] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *Smart Grid, IEEE Transactions on*, vol. 5, no. 3, pp. 1216–1227, 2014.

[10] J. J. Grainger and W. D. Stevenson, *Power system analysis*. McGraw-Hill, 1994.

[11] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 220–225.

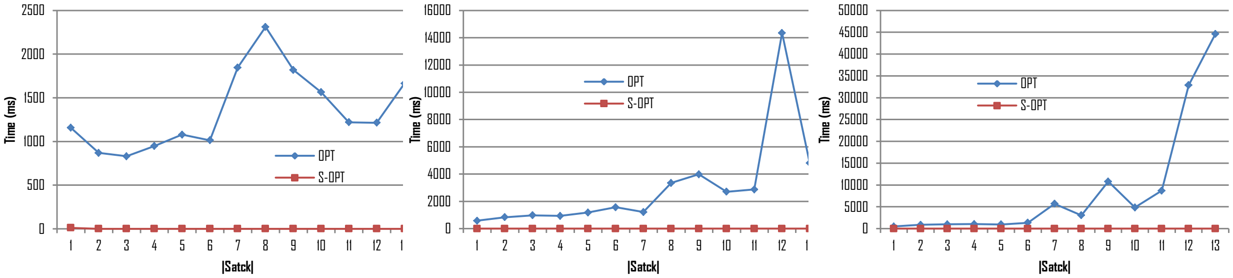


(a) PMUs placed at 25 % of buses

(b) PMUs placed at 50 % of buses

(c) PMUs placed at 75 % of buses

Fig. 3: Comparison of protection cost/coverage between optimal (OPT) and sub-optimal (S-OPT) protection methods.



(a) PMUs placed at 25 % of buses

(b) PMUs placed at 50 % of buses

(c) PMUs placed at 75 % of buses

Fig. 4: Comparison of computation time for optimal (OPT) and sub-optimal (S-OPT) protection methods.

[12] G. Krumpholz, K. Clements, and P. Davis, "Power system observability: a practical algorithm using network topology," *IEEE Transactions on Power Apparatus and Systems*, vol. 4, no. PAS-99, pp. 1534–1542, 1980.

[13] M. Misyrlis, C. Chelmis, R. Kannan, and V. K. Prasanna, "Sparse causal temporal modeling to inform power system defense," *Procedia Computer Science*, vol. 62, 2016.

[14] "Liines smart power grid test case repository," http://amfarid.scripts.mit.edu/Datasets/SPG-Data/index.php, accessed: 2016-07-1.

[15] V. V. Vazirani, *Approximation algorithms*. Springer Science & Business Media, 2013.

[16] "Gurobi optmizer," http://www.gurobi.com/, accessed: 2016-07-1.

[17] "Graphstream: A dynamic graph library," http://graphstream-project.org/, accessed: 2016-08-01.

[18] R. M. Karp, *Reducibility among combinatorial problems*. Springer, 1972.

[19] L. Kou, G. Markowsky, and L. Berman, "A fast algorithm for steiner trees," *Acta informatica*, vol. 15, no. 2, pp. 141–145, 1981.

[20] N. M. Manousakis, G. N. Korres, and P. S. Georgilakis, "Taxonomy of pmu placement methodologies," *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 1070–1077, 2012.

[21] Q. Yang, R. Min, D. An, W. Yu, and X. Yang, "Towards optimal pmu placement against data integrity attacks in smart grid," in *2016 Annual Conference on Information Science and Systems (CISS)*. IEEE, 2016, pp. 54–58.