Attacking Power Grids with Secure Meters: the case for Breakers and Jammers

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*—Undetectable data attacks on the power grid produces errors in the state estimation that can potentially affect electricity prices as well as make the grid vulnerable to failures. A new hidden attack framework is presented for power grids where all meter measurements are secure from injection of malicious data. An adversary here only jams or blocks meter data from being sent to the control center. Additionally the adversary causes errors in the status of breakers in the grid to change the topological estimate of the grid. Necessary and sufficient conditions for a successful hidden attack in this regime are discussed and an algorithm to determine an optimal attack involving the minimum set of breaker status errors is developed. The efficacy of this novel attack strategy that does not require corruption of any meter data is shown through examples.**

I. Introduction

The operation of the power grid is heavily dependent on collection of accurate measurements from meters distributed throughout the grid. These measurements, which include power injected at buses and flows on transmission lines, are transmitted by Remote Terminal Units (RTU) to the control center and used for real-time state estimation [2] and computation of Locational Marginal Prices (LMP) [1] of electricity. In addition to the measurement data collected from meters, the control center receives topological data from breaker statuses on lines in the grid. The breaker status of a line takes binary values and indicates whether that transmission line is open or closed. These statuses are vital for determining the current network structure of the grid, which is then used with the meter measurements for state estimation. The distributed locations of measurement meters, RTUs and breakers in the grid make them vulnerable to adversaries that can introduce malicious data in them. We consider a new man-in-the-middle topological attack on the power grid in this paper. Here the adversary causes errors in the status of a set of closed breakers and makes them output an open status each. For consistency with meter measurements, the adversary also jams the flow measurements in the lines with intercepted breakers.

The problem of undetectable attacks on state estimation of power grid through injection of malicious data was first studied in reference [3]. The authors of [3] show that IEEE test systems need a few corrupted measurements for a successful undetectable attack and provide a design of such attacks through the use of projection matrices. Following this paper, several different approaches for studying hidden data attacks on the grid have been considered in literature. Reference [4] studies the creation of the optimal attack vector as a mixed integer linear program. The authors of [6] provide a heuristic based detector to detect malicious data attacks. In [5], a framework is developed for analysis of the attack-vector of a constrained adversary using sparse l_0 and l_1 recovery methods. Reference [7] provides a graph based approach to determine optimal hidden attacks and related protection schemes to secure the grid against such attacks. The economic affects of hidden attacks on pricing in the power market are analyzed in [8]. Recently, the authors of [9] have looked at hidden attacks on power grids where attacks on breaker statuses are considered together with malicious data on meter measurements. Using both breaker status corruption and malicious meter data, [9] describes optimal state preserving attacks using minimum number of corrupted locations. The common thread linking the different approaches mentioned above is the introduction of malicious data on meter measurements to produce an undetectable change in state estimation. However, this may be formidable to achieve with modern meters boosted with heightened encryption and security.

In this paper, we present a new attack model which overcomes the difficulty involved in modification of meter readings. The adversary, in our case, changes only the status of a few closed breakers on transmission lines and blocks the communication of flow measurements on those lines to the control center. It is noteworthy that the adversary here does not alter meters for power injection nor does it introduce any malicious data into line flow measurements. Our attack model, thus, extends the scope of hidden attacks to power grids with secure meters as well as to cases where an adversary is resource limited against introducing malicious data in real time. Moreover, exclusion of power injection meters completely from the attack model helps present a realistic attack regime. This is true as power injection measurements on generator buses are normally under secure observation of the owners of generator units and harder to corrupt. Similarly power injection at zero injection buses stay at a constant value of zero and thus cannot be corrupted to prevent detection. In this context, we provide necessary and sufficient conditions to create an undetectable attack on the grid topology and subsequently on state estimation through the comparatively simpler tasks of changing binary breaker statuses and jamming flow measurements on lines alone.

The rest of this paper is organized as follows. The next section presents the system model used in state and topology

978-1-4799-3088-3/14/$31.00 ©2014 IEEE

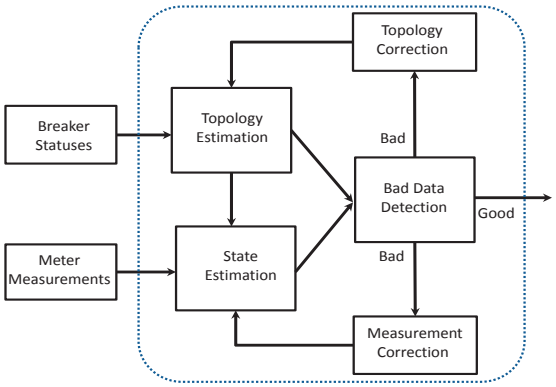

Fig. 1. Generalized State Estimator for a power system

estimation in the grid and description of the attack model. The necessary and sufficient conditions for a hidden attack on the power grid are given in Section III. Section IV includes our proposed algorithm to design the optimal attack strategy for the adversary. We provide case by case examples to demonstrate the selection of minimum number of breakers for a successful hidden attack and also comment on its computational complexity. Finally, concluding remarks and future directions of work are presented in Section V.

II. Estimation in the Power Grid and Attack Model

The control center in the power grid receives two kinds of measurements. The first kind includes topological data from breakers on transmission lines. We denote breaker statuses by the $0-1$ vector b of size n_t times 1 where n_t is the number of transmission lines. Here, breaker statuses of 0 and 1 indicate open and closed transmission lines respectively. The vector b helps create the estimate of the grid topology represented here by the graph $G = (V, E)$, where V (nodes in the graph) denotes the set of buses and E (directed graph edges) represents the set of closed transmission lines connecting those buses. Each edge in E is assigned a random direction such that the flow on that edge is considered positive if it is along the edge direction and negative otherwise. It is noted that every edge in E has a corresponding breaker status of 1. The second kind of measurements at the control center refer to meter data which include power injection measurements at buses and flow measurements on transmission lines. These measurements are used for state estimation based on the network topology determined by the breaker statuses. The overall operation (topology and state estimation together with the associated consistency check for bad data) is called generalized state estimation (GSE) [9], [10] and shown in Figure 1.

We consider the DC model for measurements in the grid [11] here. Let vector z^p be the set of power injection measurements and vector z^f be the set of flow measurements in the grid. If $z \in \mathbb{R}^m$ is the vector of all measurements such that $z = \begin{bmatrix} z^p \\ z^f \end{bmatrix}$, we have

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

Here, $x \in \mathbb{R}^{n_t}$ is the state vector and consists of the flows on all lines in the grid. H is the measurement matrix which depends on the topology derived from the breaker statuses. e is the zero mean Gaussian noise vector associated with the measurements. Here, we consider the collected measurements (z) sufficient for directly estimating the flows on all lines represented in the state vector. Thus, the measurement matrix H has full column rank. Let the k_1^{th} entry in z correspond to the power injection at a bus r with incident transmission lines numbered i and j such that the assigned flow on line i is outgoing from bus r while flow on line j is incoming onto the bus. Then $z(k_1)$ and $H(k_1,)$ (k_1^{th} row in H) are given by:

$$z(k_1) = x(i) - x(j) = [0...1..0.. - 1..0]x = H(k_1,)x \tag{2}$$

where $H(k_1,)$ has a value of 1 and -1 at the i^{th} and j^{th} locations respectively. Generalizing, if $z(k_1)$ measures the power injection on a bus incident by flows in set S, then the elements of the k_1^{th} row in H are given by:

$$H(k_1, i) = \begin{cases} -1 & \text{if } x_i \in S \text{ and incoming on bus} \\ 1 & \text{if } x_i \in S \text{ and outgoing from bus} \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

On the other hand, if $z(k_2)$ gives the flow $x(i)$ on line i, then k_2^{th} row in H has a value of 1 at the i^{th} location and zero everywhere else. Finally, in the presence of noise with covariance Σ, the optimal state vector estimate $\hat{x}$ is given by minimizing the residual $\|\Sigma^{-.5}(z - H\hat{x})\|_2$.

In this work, we take the set of flows on lines as the state vector rather than the set of power injections or voltage phasors. This does not lead to a loss of observability as H is assumed to have full column rank. The estimated set of all line flows can then be used to determine the set of all bus phase angles (θ) using the following relation.

$$x = RM^T\theta \tag{4}$$

Here, R is the diagonal matrix of line susceptance and M is the bus incidence matrix. The use of flows as state vector has a major advantage as the magnitudes of the elements of the measurement matrix H in this case are binary in nature and do not depend on the bus susceptance matrix R. Without any loss of generality, we set the state vector x as $x = \begin{bmatrix} x_o \\ x_u \end{bmatrix}$ such that x_o denotes observed flows on lines equipped with flow measurement meters while x_u corresponds to flows on lines not equipped with flow measuring meters. Similarly, we arrange the flow measurements in z^f in the order of their presence in the vector x_o. Ignoring the noise, we can now rewrite Equation (1) as follows:

$$\begin{bmatrix} z^p \\ z^f \end{bmatrix} = H \begin{bmatrix} x_o \\ x_u \end{bmatrix} \Rightarrow \qquad \begin{bmatrix} z^p \\ z^f \end{bmatrix} = \left[\begin{array}{c|c} H_o^p & H_u^p \\ I_o & 0 \end{array}\right] \begin{bmatrix} x_o \\ x_u \end{bmatrix} \tag{5}$$

Here, sub-matrices H_o^p and H_u^p represent the contribution of flows in x_o and x_u to the power injection measurements z^p. I_o is an identity matrix of size equal to the cardinality of x_o. The same analysis extends to the case with noise as well. For consistency with the breaker statuses given by vector b, we need the estimated flows on lines with open breakers to have

zero values. Mathematically,

$$x(i) - b(i)x(i) = 0 \ \forall i \in \{1, n_t\} \tag{6}$$

Attack Model: An adversary in our case is limited to changing the breaker statuses of *closed* breakers (with values 1) and making them equal to 0. After manipulation by the adversary, the changed vector of breaker statuses (b_{new}) thus follows:

$$b_{new} = b - \hat{b} \tag{7}$$

Here $\hat{b} = \begin{bmatrix} \hat{b}_o \\ \hat{b}_u \end{bmatrix}$ is the adversary's attack vector and has a value of 1 for manipulated breakers and 0 elsewhere. $\hat{b}_o$ and $\hat{b}_u$ are the components of $\hat{b}$ for the set of lines with and without flow measurements respectively. We introduce three diagonal matrices, B_{new}, B_o and B_u with $diag(B_{new}) = b_{new}$, $diag(B_o) = \hat{b}_o$ and $diag(B_u) = \hat{b}_u$. To stay undetected, the adversary also jams/blocks existing flow measurements on the lines with manipulated breakers from being received at the state estimator. Jamming does not raise an alarm at the control center as loss of reception of a few measurements due to communication failures occurs during normal grid operation as well. Now, z_f is updated by removing the jammed flow measurements as shown below:

$$(I_o - B_o)z^f = [(I_o - B_o)|\ 0] \begin{bmatrix} x_o + \Delta x_o \\ x_u + \Delta x_u \end{bmatrix} \tag{8}$$

Here $\Delta x_o = \begin{bmatrix} \Delta x_o \\ \Delta x_u \end{bmatrix}$ denotes the change in estimated state vector x due to the adversary's attack. Since power injection measurements are untouched by the adversary, the expression for z_p from Equation (5) now becomes:

$$z^p = [H^p_o(I_o - B_o)|H^p_u(I_u - B_u)] \begin{bmatrix} x_o + \Delta x_o \\ x_u + \Delta x_u \end{bmatrix} \tag{9}$$

The changes in breaker statuses also cause an update in the consistency requirement given in Equation (6). The new consistency equation is as follows:

$$(1 - b_{new}(i))\,(x(i) + \Delta x(i)) = 0 \ \forall i \in \{1, n_t\} \tag{10}$$

Using the above discussion, we present Problem (11) to determine the minimum set of breakers that need to be changed to create an incorrect estimate of line flows. Formulated as an optimization problem, it provides the design of an optimal attack, given the initial set of measurements z and breaker statuses b in the grid.

$$\begin{aligned} \underset{\Delta x \neq \mathbf{0}}{\text{minimize}} \quad & \|\hat{b}\|_1 \\ \text{subject to} \quad & \hat{b}^T = \begin{bmatrix} \hat{b}_o \\ \hat{b}_u \end{bmatrix}^T \in \{0,1\}^{n_t} \quad \text{(by definition)} \\ & \Delta x \text{ satisfies Equations (8), (9) and (10)} \\ & \text{and } x \text{ is given by Equations (5) and (6)} \end{aligned} \tag{11}$$

In the next section, we discuss the necessary and sufficient conditions for a successful hidden attack in greater detail.

III. Necessary Conditions for Hidden Attack

From Problem (11), we observe that a successful hidden attack using vector $\hat{b} = \begin{bmatrix} \hat{b}_o \\ \hat{b}_o \end{bmatrix}$ needs to satisfy Equations (8), (9) and (10). From the equations for line flow measurements in (5) and (8), we have

$$(I_o - B_o)\Delta x_o = \mathbf{0} \tag{12}$$

We now combine equations for injection measurements in (5) and (9) with (12) to get

$$H^p_o B_o x_o + H^p_u B_u x_u = H^p_u (I_u - B_u)\Delta x_u \tag{13}$$

Using the fact that only closed breakers are attacked by the attack vector $\hat{b}$, (6) and (10) can be written in terms of B_o and B_u to give

$$B_o[x_o + \Delta x_o] = \mathbf{0}, B_u[x_u + \Delta x_u] = \mathbf{0} \tag{14}$$

It is worth noting that jamming of line flows gives (13), while Equations (12) and (14) arise from need for consistency between flow measurements and breaker statuses. The conditions necessary and sufficient to conduct a successful attack ($\Delta x \neq \mathbf{0}$) that satisfies the known flow and injections measurements are given by Equations (12), (13), (14).
Further, the phase angles corresponding to the set of line flows are given by Equation (4). The estimated new line flows after the adversary's attack will thus be permissible if there is a corresponding new set of phase angles that satisfy the following relation.

$$x + \Delta x = RB_{new}M^T(\theta + c) \tag{15}$$

Here c is the change in the set of phase angles and B_{new} is the diagonal matrix of updated breaker statuses. Additionally, to guarantee that no bus has open breakers on all of its incident lines, the following needs to hold:

$$M_{abs} b_{new} \neq \mathbf{0} \tag{16}$$

Here, each entry in matrix M_{abs} is the magnitude of the corresponding entry in the bus incidence matrix M. For each bus in the grid, the corresponding row in M_{abs} gives the lines incident on it. We now look at different cases and discuss the possibility of existence of a hidden attack in each case.

Type 1: Attacking only lines WITHOUT flow measurements

In this case, breakers on lines with flow measurements are not intercepted. Thus, the corresponding attack vector for those lines satisfy $\hat{b}_o = \mathbf{0}$ and $B_o = [0]$. The following theorem states that a successful hidden attack using breakers on lines without flow measurements alone does not exist.

Theorem 1. *There does not exist any solution to the Problem (11) with $\hat{b}_o = \mathbf{0}$.*

Proof. We note that a successful attack needs to satisfy Equation (13). Plugging $B_o = [0]$ in (13), we have

$$\begin{aligned} & H^p_u B_u x_u = H^p_u (I_u - B_u)\Delta x_u \\ \Rightarrow \quad & H^p_u \Delta x_u = H^p_u B_u [x_u + \Delta x_u] \\ \text{Using (14), } & H^p_u \Delta x_u = \mathbf{0} \end{aligned} \tag{17}$$

From the structure of measurement matrix H given in (5), we observe that full column rank of H implies full column rank of H_u^p. Thus the only solution to (17) is given by $\Delta x_u = \mathbf{0}$. Moreover, the necessary condition (12) and $B_o = [0]$ give $\Delta x_o = \mathbf{0}$. This implies that $\Delta x = \left[\begin{smallmatrix}\Delta x_o \\ \Delta x_u\end{smallmatrix}\right] = \mathbf{0}$ and no hidden attack exists that can create a change in state estimation. Hence Proved. □

Further, we use Theorem 1 to claim the following corollary regarding the need for jamming measurements in creating a successful hidden attack.

Corollary 1. *There does not exist any hidden attack that consists of intercepting breakers without jamming measurements.*

Proof. We assume that all lines with closed breakers have a non-zero flow. If flow measurements cannot be jammed then the breakers on the lines with flow measurements should not be changed to prevent inconsistency between flow and breaker status. Thus, $\hat{b}_o = \mathbf{0}$. Using Theorem 1, we conclude that no hidden attack is possible. □

Type 2: Attacking only lines with flow measurements
In this case, breakers on lines without flow measurements are not attacked. This gives us $\hat{b}_u = \mathbf{0}$ and $B_u = [0]$.

Type 3: Attacking all lines with closed breakers
This is the general case where closed breakers on all lines with or without flow measurements can be attacked.
Now, we prove a theorem which states that the cardinality of an optimal attack of Type 2 is never greater than that of an optimal attack of Type 3. In other words, we claim that restricting the attack to lines with flow measurements alone is as good a strategy as attacking breakers on both lines with and without flow measurements.

Theorem 2. *The optimal solution of Problem (11) gives a successful attack of Type 2 with $\hat{b}_u = \mathbf{0}$ that involves breakers on lines with flow measurements alone.*

Proof. Any successful attack satisfies the conditions given in (12), (13) and (14). For an attack of Type 2, $B_u = [0]$ holds and the condition $B_u[x_u + \Delta x_u] = \mathbf{0}$ becomes trivially true. This leads to fewer constraints on Δx_u in Problem (11) for an attack of Type 2 as compared to an attack of Type 3. Thus an optimal attack of type 2 is given by a relaxation of Problem (11) and its cardinality does not exceed that of an attack of Type 3. Hence proved that the optimal solution is achieved through an attack of Type 2. □

In the next section, we comment on the complexity of Problem (11) and discuss solution techniques to design a successful attack.

IV. Design of Optimal Attack Vector

We first design an optimal attack that satisfies the conditions given in Equations (12), (13), (14). After determining such an attack, Equations (15) and (16) are checked to decide if the attack is permissible by an assignment of phase angles. We assume here that *the sum of flows on a "proper subset" of all connected lines incident on a bus is not zero.* Mathematically, if S_i is the set of lines incident on a bus i in the grid, our assumption can be stated as

$$\forall S' \subset S_i, S' \neq S_i, \quad \Sigma_{k \in S'} x(k) \neq 0 \tag{18}$$

Note that E denotes the set of all lines in the grid with closed breakers. We label the set of lines in E with flow measurement meters by E_o and the set of lines in E without flow measurement meters by E_u. Thus, $E_o \bigcup E_u = E$. Theorem 2 states that the optimal hidden attack comprises of manipulating breakers on lines in set E_o.

Consider a bus i in the grid installed with a power injection meter such that all connected lines incident on it belong to the set E_o and have their flows measured. Let an adversary corrupt the breakers of a proper subset of lines incident on bus i and jam the associated flow measurements. Opening the breakers on all lines incident on bus i is of course not permitted by Equation (16) to preserve observability. Due to assumption (18), the total outgoing flow on the attacked lines do not cancel out and the necessary condition given in Equation (13) is not satisfied by the attack. Thereby, we conclude that under assumption (18), the following holds:

Lemma 1. *If all lines incident on a bus with a power injection meter belong to the set E_o, then the corresponding values of $\hat{b}_o$ for those lines are 0 and none of the lines are included in the hidden attack.*

Consider, now, a line in set E_o such that it is not incident on a bus with power injection measurement at either of its ends. It follows immediately that attacking the breaker and jamming the flow measurement on that line will go undetected as the attack will not affect any other measurement in the grid and is consistent. Such attacks on individual lines in E_o are termed **Trivial Attacks**. We assume here that *at least one of the two buses connected by each line in set E_o has a meter for power injection measurement.* This assumption prevents all trivial attacks in the grid. The lines of set E_o, under this assumption, can thus be decomposed into two disjoint set, E_o^1 consisting of lines incident on one bus with injection measurement, and E_o^2 consisting of lines incident on two buses with injection measurement. Hence, $E_o^1 \bigcup E_o^2 = E_o$.

We now focus on lines without flow measurement meters. As considered for set E_o, we assume that a power injection meter exists on at least one of the two buses connected by each line in set E_u. Like E_o, we divide E_u into two sets. The set of lines in E_u that have only one of their ends incident on a bus with injection measurement is denoted E_u^1, while remaining set of lines ending in buses with injection measurements at both ends is called E_u^2. Here, $E_u^1 \bigcup E_u^2 = E_u$. Unique state estimation using flows and injection measurements given by Equation (1) necessitates that the following lemma holds:

Lemma 2. *Each bus installed with a meter for power injection measurement can have a maximum of one line in E_u^1 incident on it.*

We now show the design of an attack for a bus with a line in E_u^1 incident on it. Consider the example shown in Figure 2. Here the power injection at bus a (colored red) is measured by a meter while the power injections at buses b, c and d (colored

solid black) are not measured. Lines (a, b) and (a, d) (solid lines) have flow measurement meters while line (a, c) (dashed line) does not have a flow measurement meter and belongs to set E_u^1. Notice that if an adversary changes the breaker status on line (a, b) and jams the flow measurement (i_{ab}), we have $\Delta i_{ab} = -i_{ab}$. This leads to a change in the estimated flow on line (a, c) given by $\Delta i_{ac} = (P_a - i_{ab} - i_{ad}) - (P_a - i_{ad}) = i_{ab}$. Conditions (12), (13) and (14) necessary for a successful attack are satisfied by this attack. We conclude that *a bus with injection measurement connected to a line in set E_u^1 permits an attack if it is also connected to a line in set E_o^1*. We call this class of attacks **Simple Attacks**. The cardinality of such an attack is 1.

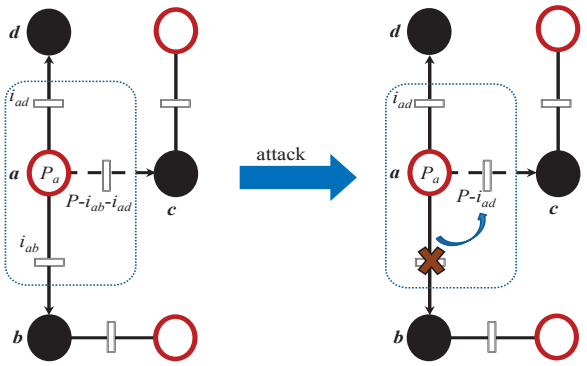

Fig. 2. Example of class **Simple Attack**. Solid Black Circles represent buses without injection measurement. Red Circles represent buses with injection measurements. Solid Lines have power flow measurements while flows on dashed lines are not measured. Rectangular blocks on lines represent breakers. A crossed breaker represents manipulation of its status and jamming of line flow measurement.

Consider now the lines in set E_u^2. These include all lines without flow measurements that are connected to buses with injection meters on both ends. Unlike the case for lines in E_u^1, a bus can have multiple incident edges belonging to E_u^2. In fact, buses connected by edges in E_u^2 form a graph G_u^2 (not necessarily connected) as shown in Figure 4. Each node in graph G_u^2 represents a bus with an installed injection meter while the edges represent lines without flow measurements. We first state the following theorem regarding nodes in graph G_u^2.

Theorem 3. *Buses with power injection meters that are connected by lines in E_u^2 form a tree in graph G_u^2.*

Proof. It suffices to show that there exists no cycle comprising of edges in E_u^2. Assume that such a cycle exists. One can then have an additional flow of certain magnitude (Δ) circulating through the edges in the cycle without affecting the injection measurements at the buses in G_u^2. Note that lines in E_u^2 do not have installed flow measurements. Thus, the additional flow in the cycle does not affect the observed set of measurements $z = \begin{bmatrix} z^p \\ z^f \end{bmatrix}$. This implies that multiple solutions to estimation of x exist if there are cycles in G_u^2 which contradicts the fact that the measurement matrix H has full column rank. Hence proved that the connected nodes in G_u^2 lie on trees. □

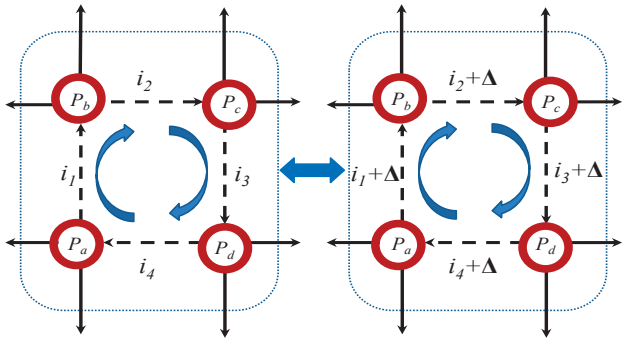

Fig. 3. Example of non-unique state estimate for cycle formed by lines without flow measurements. Red colored circles represent buses with injection measurements. Dashed Lines do not have flow measurements. For the same set of measurements, an extra current of Δ can flow in the circle leading to multiple solutions of state estimation.

The proof of Theorem 3 is easily elucidated though a simple example presented in Figure 3.

We now focus on trees in graph G_u^2 that consist of nodes connected by lines in E_u^2. It follows from Theorem (2) that an optimal attack for a tree in G_u^2 consists of attacking lines with flow measurements that are incident on the tree nodes. Given any tree in G_u^2, notice that if the adversary attacks lines in set E_o^1 incident on the tree nodes such that the sum of all flow outgoing through the targeted lines is zero, the attack goes undetected. This happens as estimated flows on lines in E_u^2 connecting the tree nodes change to absorb the flows on the attacked lines. The sum of outgoing flows on the attacked lines must be zero here for satisfaction of Equations (13) and (14). An example of an attack on a tree with three buses is depicted in Figure 4. Here the sum of outgoing flows on the targeted lines (marked with crosses in the figure) is $i_1 + i_3 - i_6 = 0$ and a successful attack results. Such attacks that can be conducted on trees in G_u^2 are termed **Tree-based Attacks**. The cardinality of a tree based attack is at least 2 and greater than that of a simple attack.

Hardness of Tree-based Attacks: The following theorem states that computing an optimal tree-based attack as described above is NP-hard.

Theorem 4. *Determining the optimal tree-based attack on the grid is equivalent to a Knapsack Problem and is NP-hard.*

Proof. Proof Steps: Consider the example in Figure 4. It is clear that optimal hidden attack on a tree in graph G_u^2 is given by selection of the smallest set of flow measurements on lines in E_o^1 incident on the tree such that the sum of the outgoing flows on the considered lines is zero. This is equivalent to a special case of Knapsack problem called Subset-sum problem [12]. In the equivalent formulation, positive and negative weights for the Knapsack are given by the outgoing flow measurements. For the entire graph G_u^2, the optimal hidden attack is determined by considering all its trees and is NP-hard as the Knapsack problem is NP-hard. □

It is worth mentioning here that the Knapsack problem is

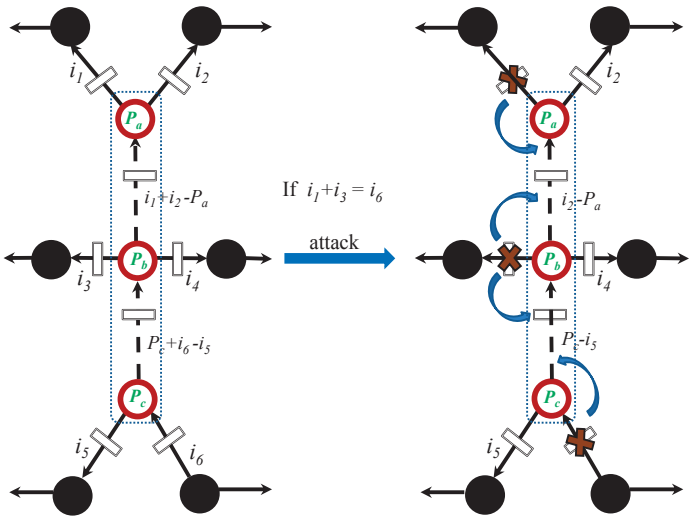

Fig. 4. Example of class **Tree-based Attack**. Solid Black Circles represent buses without injection measurement. Red Circles represent buses with injection measurements. Solid Lines have power flow measurements while flows on dashed lines are not measured. Rectangular blocks on lines represent breakers. A crossed breaker represents manipulation of its status and jamming of line flow measurement. Total outgoing flow on attacked lines is 0.

one of the most well-studied problems in combinatorial optimization and hence several approximate techniques for it exist, including ones based on dynamic programming. An adversary can use such approximations to determine the optimal hidden attack, if it exists. We now combine the insights obtained in this section and formulate Algorithm 1 for designing the optimal hidden attack. This provides the adversary with a solution to Problem (11). In Algorithm 1, Step 3 removes lines from the candidate attack set as discussed in Lemma 1. Step 6 selects a simple attack if it exists. Following Theorem 4, Step 14 finds a tree-based attack by solving a Knapsack Problem. Finally the last step determines the permissibility of the attack by checking the presence of phase angle assignments to guarantee the change in estimated line flows.

V. Conclusion

In this paper, we study hidden attacks on state estimation on power grids where all meters are protected from introduction of malicious data. We present a new attack model where the adversary corrupts only the breaker statuses on transmission lines and jams the communication of flow measurements on the attacked lines. We discuss necessary and sufficient conditions for the existence of hidden attacks of this regime. We develop an algorithm to help determine the optimal attack strategy that requires changing the minimum number of breaker statuses in the grid and describe its operation through case by case test examples. The important conclusion from this work is that even grids completely protected by secure measurements are vulnerable to hidden attacks and, further, that such attacks can in fact be conducted by adversaries armed only with generic information regarding the grid structure. Formulating stronger attack strategics and analyzing protection schemes against our attack framework are the focus of our current work.

Algorithm 1 Optimal Attack Vector $\hat{b}^*$ for Problem (11)

Input: Measurements $z = \begin{bmatrix} z^p \\ z^f \end{bmatrix}$, measurement matrix H, breaker statuses b, $G = (V, E)$, $E = E_o^1 \bigcup E_o^2 \bigcup E_u^1 \bigcup E_u^2$

1: Candidate set $E_{cand} \leftarrow E_o^1$, $\hat{b}^* \leftarrow \mathbf{0}$, $m \leftarrow 0$.
2: Remove lines in E_{cand} that connect nodes of degree 1.
3: For each node with injection meter connected only by lines in E_o, remove all its incident lines from E_{cand}.
4: **for** $len = 1$ **to** size(E_u^1) **do**
5: $j_{bus} \leftarrow$bus with injection meter connected to len^{th} line.
6: **if** some line k incident on j_{bus} belongs to E_{cand} **then**
7: $len \leftarrow$ size(E_u^2), $\hat{b}^*(k) \leftarrow 1$, $m \leftarrow 1$.
8: **end if**
9: **end for**
10: **if** $m < 1$ **then**
11: Create graph G_u^2 with buses with power injection measurements and lines in E_u^2.
12: $len \leftarrow \infty$. $S_{tree} \leftarrow$ trees in G_u^2.
13: **for** $i = 1$ **to** size(S_{tree}) **do**
14: $S_{temp} \leftarrow$ least lines of E_{cand} incident on i^{th} tree such that sum of outgoing flows is 0.
15: **if** $len >$ size(S_{temp}) **then**
16: $len \leftarrow$ size(S_{temp}). $\hat{b}^* \leftarrow \mathbf{0}$, $\hat{b}^*(S_{temp}) \leftarrow 1$.
17: **end if**
18: **end for**
19: **end if**
20: Check Equations (15) and (16).

References

[1] A. L. Ott, "Experience with PJM market operation, system design, and implementation", *IEEE Trans. Power Syst.*, vol. 18, no. 2, 2003.
[2] A. Abur and A. G. Expósito, "Power System State Estimation: Theory and Implementation", New York: Marcel Dekker, 2004.
[3] 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.
[4] 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.
[5] T. Kim and V. Poor, "Strategic Protection Against Data Injection Attacks on Power Grids", *IEEE Trans. Smart Grid*, vol. 2, no. 2, 2011.
[6] 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.
[7] D. Deka, R. Baldick, and S. Vishwanath, "Optimal Hidden SCADA Attacks on Power Grid: A Graph Theoretic Approach", *ICNC*, 2014.
[8] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets", *Proc. IEEE SmartGridComm*, 2010.
[9] J. Kim and L. Tong, "On topology attack of a smart grid: Undetectable attacks and countermeasures", *IEEE J. Select. Areas Commun.*, vol. 31, no. 7, 2013.
[10] O. Alsac, N. Vempati, B. Stott, and A. Monticelli, "Generalized state estimation", *IEEE Trans. Power Systems*, vol. 13, no. 3, 1998.
[11] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*, CRC, 2000.
[12] S. Martello and P. Toth, *Knapsack Problems: Algorithms and Computer Implementations*, Wiley, 1990.