53rd IEEE Conference on Decision and Control
December 15-17, 2014. Los Angeles, California, USA

Stealthy Attacks in Power Systems: Limitations on Manipulating the Estimation Deviations Caused by Switching Network Topologies

Shaocheng Wang and Wei Ren

Abstract— **The reliability and robustness of the power system have gained increasing attention as the trend of including more information infrastructures into the current power grid. The stealthy attack is a kind of cyber attack that is undetectable to any residue-based detection scheme. Our previous work [1] has shown that the existence of such attacks can be eliminated by rotationally switching off one of some preselected links which contain a spanning tree of the network graph. In this paper, we extend our previous work, to consider the case when the attack is only stealthy in some of the topologies. The possible consistent deviations of the estimated states are formulated. We show that as the attack is stealthy in more topologies, the flexibility of such deviations is linearly decreased. Several cases are studied to show this trade-off.**

I. INTRODUCTION

There is no doubt that the electric power system, which is one of the most complicated engineered systems, plays a vital role in the modern life. Therefore, its reliability becomes a big concern. The Supervisory Control and Data Acquisition (SCADA) system is in charge of monitoring and controlling the power system. The state estimator, which obtains the measurements from the SCADA system, is in charge of estimating the unknown states in the network. The system operator uses these estimated states as the critical reference for getting knowledge of the system and making the next-step decisions. Some applications such as Optimal Power Flow, Automatic Generation Control and Contingency Analysis are highly dependent on the state estimation [2]. Therefore, it is critical to have an accurate and reliable estimate of the states. Bad estimates will offer the system operator with inaccurate information of the system, which may cause wrong decisions and finally, cause outages in the network.

The idea of the smart grid has gained significant attention and is regarded as the future tendency of the current power network. While it has the advantages of providing a better "situational awareness" by using communications and intelligent technologies, its expansion of the information infrastructures also brings vulnerabilities and shortcomings [3]. In [4], a kind of cyber attacks, namely, the false data injection attack (FDIA) was proposed. The FDIA is launched by injecting malicious data into the meters in order to fool the system operator with the corrupted data. The stealthy attack is defined as a strategically designed FDIA such that it does not trigger the false data alarm whenever the uncorrupted data does not. Countermeasures to disable such attacks are considered in [5], where the strategy of adding protected measurements and verifiable states was proposed. However, such a strategy usually requires the protections on a large number of meters which can be costly, especially with the increase of the grid's size. The *security index*, as the metric for quantifying the minimum effort to corrupt a certain measurement in a stealthy manner, was firstly proposed in [6]. It is essentially a L_0 norm minimization problem and has led to numerous research works [7]–[10]. However, due to its non-convexity, no algorithm that is both accurate and computationally efficient has been found.

Although most of the existing literatures assume a fixed topology for the power network, the topology can be changed for multiple reasons. The positions of the transformer taps may change from time to time, which change the admittance on the transmission lines. The connections among the buses can be changed either intentionally (switching on/off the circuit breakers) or passively (line failures). In recent years, with the trend of including more distributed energy sources, the concept of microgrids was proposed. This motivates the study of the intentional scheduled connection/isolation of the microgrids to/from the main grid (see for example [11]).

Motivated by the aforementioned facts, our previous work studied the effects on the stealthy attacks caused by switching the network topologies [1]. It proposed a necessary and sufficient condition that the topologies have to satisfy in order to eliminate the existence of such attacks via strategically switching among these topologies. In this paper, we extend our previous work. We show that even if the attacker launches an attack that is only stealthy under some of the topologies, it will still have limited flexibility to deviate the estimated states. We formulate this limitation and show the general form of the feasible deviations that can be achieved. Several cases are studied to show how this limitation is related to the decisions that made by both the attacker and the system operator.

II. PRELIMINARIES

A. Graph Theory Background

The topology of a power system network can be described by a graph $\mathcal{G}(\mathcal{V},\mathcal{E})$, where $\mathcal{V}$ and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ are respectively the set of vertices which stands for the buses, and the set of edges which stands for the transmission lines. Due to the fact that power delivered on each transmission line is bidirectional, the graph for describing the power network is undirected. Several fundamental concepts of graph theory are listed as follows:

- A *path* from vertex v_{i_0} to vertex v_{i_t} is a sequence of vertices $v_{i_0},\ldots,v_{i_t}$ such that $(v_{i_j},v_{i_{j+1}}) \in \mathcal{E}$ for $0 \leq j < t$;

Shaocheng Wang and Wei Ren are with the University of California, Riverside, CA 92507, USA. Email: shaocheng.wang@email.ucr.edu, ren@ee.ucr.edu.

- A graph is *connected* if there exists at least one path from every vertex to every other vertex;
- A graph is *disconnected* if it is not connected;
- A *spanning tree*[1] is a minimal set of edges that connect all vertices.

In this paper, we assume the power network associated with $\mathscr{G}(\mathscr{V},\mathscr{E})$ contains $n+1$ buses and l transmission lines. Therefore, $\mathscr{V}=\{v_1,\ldots,v_{n+1}\}$ and $\mathscr{E}=\{e_1,\ldots,e_l\}$. Then a directed incidence matrix $A_0\in\mathbb{R}^{(n+1)\times l}$ can be defined to describe the topology. After arbitrarily assigning the direction of each transmission line without loss of generality, the entries of A_0 are determined in the following way. For each link e_j, the entry in the ith row and jth column of A_0 is $A_0(i,j)=1$ if the direction of e_j starts at bus i, $A_0(i,j)=-1$ if the direction of e_j ends at bus i, $A_0(i,j)=0$ otherwise.

In the power system network, in order to study the phase angle of each bus, one bus is required to be arbitrarily selected as the reference bus. The phase angle of the reference bus is assumed to be zero so that the phase angles of the other buses are measured with respect to the reference bus. Then the truncated incidence matrix $A\in\mathbb{R}^{n\times l}$ can be defined by removing one of A_0's row that corresponding to the reference bus. Some fundamental properties of A and A_0 are listed in the following lemma.

Lemma 1: Let $\mathscr{G}(\mathscr{V},\mathscr{E})$ be the graph associated with $n+1$ nodes. Let A_0 be the associated incidence matrix and A be the truncated version of A_0. Then:

i) $\text{rank}(A_0)=\text{rank}(A)$;
ii) $\mathbf{1}\in\text{Null}\{A_0^T\}$, where $\mathbf{1}\in\mathbb{R}^{|\mathscr{V}|}$ is an all one vector. $\text{Null}\{\cdot\}$ denotes the null space of a matrix;
iii) $\mathscr{G}$ is connected *if and only if* $\text{rank}(A_0)=n$;
iv) $\mathscr{G}$ is disconnected with k components *if and only if* $\text{rank}(A_0)=n-k+1$.

B. State Estimation in the DC Power Model

The DC power model is commonly adopted for the study of the power systems [4]–[10]. Let $x\in\mathbb{R}^n$ be the collection of states of all buses except for the reference bus. Specifically, the states are the phase angles of all other buses relative to the reference bus. Let $z\in\mathbb{R}^m$ be the collection of the measurements including both the power flow on each transmission line and the power injection or load at each bus except for the reference bus. Let $H\in\mathbb{R}^{m\times n}$ be the topology matrix with respect to the original network topology where no transmission line is cut off. Then the relation between the states and the measurements can be written as $z=Hx+w$, where $w\in\mathbb{R}^m$ stands for the measurement noise. In this paper, we assume only one measurement can be obtained on each transmission line or bus and therefore $m=l+n$. Let $D=\text{diag}\{d_1,\ldots,d_l\}\in\mathbb{R}^{l\times l}$ be a diagonal matrix with each nonzero diagonal entries d_i. Here d_i describes the admittance of the ith transmission line, $\forall i=1,\ldots,l$. Then the topology matrix H will have the form of

$$H\triangleq\begin{bmatrix} DA^T \\ ADA^T \end{bmatrix}. \tag{1}$$

[1]Here we focus on the spanning tree in an undirected graph.

Assuming w as a white Gaussian noise with its covariance matrix R, the weighted least-square, minimum variance and maximum likelihood estimation criteria will yield the same estimator as $\hat{x}=(H^TWH)^{-1}H^TWz$, where $\hat{x}\in\mathbb{R}^n$ is the estimate of x and $W=R^{-1}$ is the weighting matrix.

C. Stealthy Attack against Bad Data Detection

The bad data detector is designed to defend against the bad data that may be caused by multiple possible reasons including meter failures or malicious attacks. The residue-based detectors are usually denoted as a function $J(r)$, where $r\triangleq z-H\hat{x}$. Examples include the χ^2 detector and the largest normalized residual test (LNRT). The residue-based detectors are proposed based on the intuition that abnormal data will drive the estimated states away from their true values. That is, the alarm is triggered if $J(r)\geq\tau$, where the threshold τ is designed according to the desired percentage of the false alarm rate. The FDIA is injected to the measurement observed by the system operator [4]. In this case, instead of observing the true measurement z, the operator is only able to see the corrupted data $z_{\text{bad}}\triangleq z+z_a$, where z_a comes from the injected false data. Let $\hat{x}_{\text{bad}}$ be the corrupted estimate of x. Let Δx be the estimation deviation that is introduced by the attacker, i.e., $\Delta x=\hat{x}_{\text{bad}}-\hat{x}$. The stealthy attack is defined as a special case of FDIA when the attacker selects $z_a=H\Delta x$. It follows that for any residue-based detector, $J(r)=J(z_{\text{bad}}-H\hat{x}_{\text{bad}})=J\left((z+z_a)-H(\hat{x}+\Delta x)\right)=J(z-H\hat{x})=J(r)$. This implies that z_{bad} will have the same possibility of triggering the bad data alarm, as that of z. Thus, the stealthy attack requires $z_a\in\text{Im}(H)$, where $\text{Im}(\cdot)$ stands for the column space of a matrix.

III. Problem Formulation

A. Switching Topology Scenario

As the extension of our previous work [1], we keep using the same assumptions and studying the scenario in which the network topology is switching. In [1], the system operator was assumed to be able to intentionally switch on/off one of the selected transmission lines by turns, and therefore change the system topology. That is, each topology is generated by cutting off one link in the graph. Considering the potential issues on the generation-demand balance that might be caused by cutting off links, we do not allow multiple transmission lines to be switched off simultaneously. From the attacker's perspective, it is assumed that the attacker knows all possible topologies but does not know which one is currently adopted by the operator. Moreover, the attacker is also able to compromise a set of measurements that is not protected [5]. As in [1], we assume that the transient stability of the network is guaranteed during the topology switching process. We only consider the network at the steady state for each topology.

B. Motivation

Since the attacker does not know the topology that is being adopted, it has to search for an attack that is stealthy in all possible topologies. Therefore the system operator's

objective is to eliminate the possibility of such an attack by adopting an appropriate set of topologies by turns, i.e., selecting an appropriate set of links to cut off by turns. It was shown in [1] that the necessary and sufficient condition is to select a set of links which contains a spanning tree of the network graph. This implies that for a network with $n+1$ buses, the link set should contain at least n entries since it has to contain a spanning tree. With this condition satisfied, there will not exist any feasible stealthy attack.

However, it is still possible for a "smart" attacker to design the attack in a way such that the attack is stealthy in a majority of the topologies. This motivates the work presented in this paper. Based on the scenario as described, in this paper, we study the case when the attacker makes a concession and designs the attack that is stealthy only in some of the topologies preselected by the system operator. Note that the probability of being detected is increasing as the attack is designed to be stealthy in fewer topologies. Moreover, we assume that in order to achieve some destructive objectives, the attack tries to fool the system operator with consistent deviations of the estimated states by injecting the aforementioned partially stealthy attack. That is, the deviations of the corrupted estimates from the real estimates of the states are identical among all topologies in which the attack is stealthy. Note that this is more preferable from the attacker's point of view, since a consistent deviation from the real state is more likely to fool the operator. We consider the following questions. 1) What is the relation between this estimation deviations and the probability of the attack being detected? 2) What do the deviations look like? 3) What are the countermeasures to minimize the effects caused by such attacks?

C. Notations

We use the MATLAB tradition to denote the entries of a matrix/vector. For example, $A(i,j)$ is the ith row, jth column of the matrix A. $z_a(i)$ is the ith entry of z_a. $\mathscr{P} = \{i_1, \ldots, i_n\}$ is a set of n indices such that its corresponding edge set $\mathscr{E}_{\mathscr{P}} = \{e_i | i \in \mathscr{P}\}$ are selected to be cut by the system operator rotationally. $\mathscr{I} = \{i_1, \ldots, i_p\}$ is a set of p indices. Corresponding, the edge set $\mathscr{E}_{\mathscr{I}} = \{e_i | i \in \mathscr{I}\}$. a_i is the ith column of A. $A_{\mathscr{I}} = \left[a_{i_1} | a_{i_2} | \ldots | a_{i_p}\right]$. $A_{\setminus i}$ is the matrix whose columns are identical to that of A except for its ith column being zero. $H_{\setminus i}$ is the topology matrix defined by (1) with respect to $A_{\setminus i}$. $\mathscr{V}_{\mathscr{I}} \subseteq \mathscr{V}$ is the set of buses connected by the links of $\mathscr{E}_{\mathscr{I}}$. $\mathbf{0}$ is an all zero vector with an appropriate dimension. $|\mathscr{V}|$ denotes the cardinality of the set $\mathscr{V}$.

IV. Main Result

In this paper, we only study the scenario in which the attacker tries to "hide" in a subset of the topologies preselected by the system operator. However, we will show that for other cases in which the attacker is also stealthy in some other topologies that are not preselected, can be converted to the case studied in this paper. The detailed explanation is skipped at this point since it requires the conclusion of Corollary 1 that will be given later on. To begin stating our main results, two definitions, namely, trivial and nontrivial topology matrices are given as follows:

Definition 1 (nontrivial topology matrices): Suppose that $|\mathscr{I}| = p$. $\{H_{\setminus i_k} | i_k \in \mathscr{I}\}$ is a set of p nontrivial topology matrices if $\text{rank}(A_{\mathscr{I}}) = p$.

Definition 2 (trivial topology matrix): Let $\{H_{\setminus i_k} | i_k \in \mathscr{I}\}$ be a set of nontrivial topology matrices. Then $H_{\setminus k}$ is a trivial topology matrix spanned by the these nontrivial topology matrices if $\text{rank}([A_{\mathscr{I}} | a_k]) = \text{rank}(A_{\mathscr{I}})$.

From Definition 1, it is clear that $\mathscr{E}_{\mathscr{I}}$ will contain no cycle in $\mathscr{G}(\mathscr{V}, \mathscr{E})$. Similarly, Definition 2 implies that if $\{H_{\setminus i_k} | i_k \in \mathscr{I}\}$ span the trivial topology matrix $H_{\setminus k}$, $\{e_k\} \cup \mathscr{E}_{\mathscr{I}}$ will contain a cycle in $\mathscr{G}(\mathscr{V}, \mathscr{E})$. Since $A_{\mathscr{I}}$ is a submatrix of A, $p \leq \text{rank}(A)$. In this paper, we assume that $\mathscr{G}(\mathscr{V}, \mathscr{E})$ is connected. Therefore $p \leq n$. This implies that the operator can preselect at most n topologies whose associated topology matrices are nontrivial. In the rest of this paper, $\{H_{\setminus i_k} | i_k \in \mathscr{P}\}$ denotes the set of these n nontrivial topology matrices. Let $\{H_{\setminus i_k} | i_k \in \mathscr{I}\}$ be the set of p nontrivial topology matrices associated with the p topologies in which the attack z_a is stealthy. The following definition will be frequently used in the rest of this paper.

Definition 3 ((p,n)-stealthy attack): Suppose that $\mathscr{I} \subseteq \mathscr{P}$. z_a is a (p,n)-stealthy attack if $z_a \in \cap_{i_k \in \mathscr{I}} \text{Im}(H_{\setminus i_k})$ and $z_a \notin \text{Im}(H_{\setminus i_k})$, $\forall i_k \in \mathscr{P} \setminus \mathscr{I}$.

Before stating our main result, we first state the following lemma that will be used for the proof of our main theorem.

Lemma 2: Suppose that the attacker is able to launch an attack z_a that is stealthy in the p topologies whose associated nontrivial topology matrices form the set $\{H_{\setminus i_k} | i_k \in \mathscr{I}\}$, i.e., $z_a \in \cap_{i_k \in \mathscr{I}} Im(H_{\setminus i_k})$. Then $z_a(i_k) = 0$, $\forall i_k \in \mathscr{I}$.

Proof: From the definition of $H_{\setminus i_k}$, the entries of the i_kth row of $H_{\setminus i_k}$ are all zeros since cutting off the i_kth link will cause the i_kth column of the corresponding incidence matrix $A_{\setminus i_k}$ being all zeros. Thus, if $z_a \in Im(H_{\setminus i_k})$, $z_a(i_k) = 0$. Since this condition has to be satisfied for all of the topologies in which z_a is stealthy, it follows that $z_a(i_k) = 0$, $\forall i_k \in \mathscr{I}$. ■

Theorem 1: Suppose that the attacker launches an attack z_a that is stealthy in $p (p \geq 2)$ topologies. Let $\{H_{\setminus i_k} | i_k \in \mathscr{I}\}$ be the set of the associated nontrivial topology matrices. Then z_a can only be designed in the way such that the deviation of the estimated states Δx satisfies $\Delta x \in \text{Null}\{A^T_{\mathscr{I}}\}$.

Proof: Recall that Δx is caused by injecting the stealthy attack z_a. Then $z_a = H_{\setminus i_k} \Delta x$ holds for all $i_k \in \mathscr{I}$. From Lemma 2, $z_a(i_k) = 0$, $\forall i_k \in \mathscr{I}$. Let $H^{\mathscr{I}}_{\setminus i_k}$ be the submatrix that collects the rows of $H_{\setminus i_k}$ whose indices are in $\mathscr{I}$, i.e., $H_{\setminus i_k}(j,:), \forall j \in \mathscr{I}$. Therefore, since $H^{\mathscr{I}}_{\setminus i_k} \Delta x = 0$ for each $i_k \in \mathscr{I}$, p independent equations can be obtained, i.e., $d_{i_k} a^T_{i_k} \Delta x = 0, \forall i_k \in \mathscr{I}$. Since d_{i_k} is the admittance value on the corresponding transmission line and therefore nonzero, after writing the p equations into a compact matrix form, one can obtain $A^T_{\mathscr{I}} \Delta x = 0$. It follows that $\Delta x \in \text{Null}\{A^T_{\mathscr{I}}\}$. ■

Theorem 1 formulates the limitations on the consistent estimation deviations that can be introduced by the attack z_a, where z_a is stealthy in p topologies associated to p associated nontrivial topology matrices. It is clear that the size of $A^T_{\mathscr{I}}$

increases as p increases. This makes Δx have to satisfy more constraints as well.

Remark 1: When the attack is only stealthy in one of the n topologies ($p=1$), z_a can be designed based on whatever Δx the attacker wants. This brings us back to the case in which the graph topology is fixed. Therefore we assume $p \geq 2$ for the rest of this paper.

Remark 2: When $p=n$, Δx can only be a zero vector due to the fact that $\text{rank}(A_{\mathscr{I}})=n$ leads to $\text{Null}\{A_{\mathscr{I}}^T\}=\emptyset$. It follows that $z_a = H_{\setminus i_k}\Delta x = \mathbf{0}$, $\forall i_k \in \mathscr{I}$. Therefore, it is impossible for the attacker to fool the system operator with an consistent estimation deviation Δx, via injecting an false data z_a that is stealthy in all n topologies preselected by the system operator. Thus the system operator can choose n such topologies to eliminate the existence of the stealthy attack. This is also consistent with the main theorem in [1].

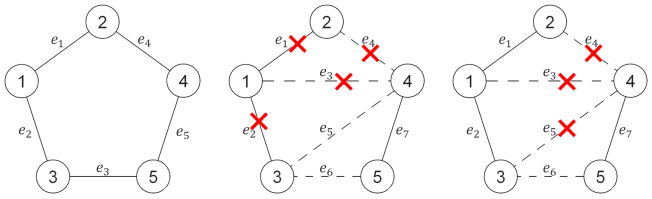
Although in the special case where $p=n$, Theorem 1 leads to the same result as in our previous work, it is not sufficient to prove the main result in [1]. Two theorems are individually proposed from different perspectives. An example is the case when $\mathscr{G}(\mathscr{V},\mathscr{E})$ is a graph that contains only a circle (defined as the *circular* graph in [1]), as shown in Figure 1(a). It is still able to find a stealthy attack even if the operator selects 4 links that form a spanning tree to cut rotationally. This attack, however, will not be able to deviate the estimated states with the same value in different topologies.

In summary, there is a trade-off between the flexibility of manipulating the estimation deviations and the number of the nontrivial topology matrices associated with the topologies in which the attack is stealthy. On one hand, the attacker prefers to launch an attack that is less possibly detected during the alternations among all possible topologies. This will require Δx to satisfy more constraints with which the attacker may not be able to fool the system operator in the way that it expected. On the other hand, in order to manipulate the estimation deviations in a more flexible manner, the attacker has to take the risk of being detected in more topologies.

Corollary 1: Let z_a be stealthy in p topologies whose associated nontrivial topology matrices forms the set $\{H_{\setminus i_k}|i_k \in \mathscr{I}\}$, i.e., $z_a \in \cap_{i_k \in \mathscr{I}} Im(H_{\setminus i_k})$. Suppose that z_a deviates the state estimates by Δx. Then $z_a = H\Delta x = H_{\setminus k}\Delta x$, where $H_{\setminus k}$ stands for any topology matrix that is spanned by the matrices in $\{H_{\setminus i_k}|i_k \in \mathscr{I}\}$.

Proof: Let A_i be the matrix whose columns are all zeros except for the ith column be a_i. It follows that $A_i = A - A_{\setminus i}$. Let H_i be defined by (1) with respect to A_i. Then $H_i = H - H_{\setminus i}$. Therefore, $z_a = H_{\setminus i}\Delta x = (H-H_i)\Delta x, \forall i \in \mathscr{I}$. Since $\Delta x \in \text{Null}(A_{\mathscr{I}}^T)$ from Theorem 1, $A_i^T \Delta x = 0, \forall i \in \mathscr{I}$. It follows that $H_i \Delta x = 0$, which implies that $z_a = H\Delta x$.

Since $H_{\setminus k}$ is the topology matrix spanned by the topology matrices in $\{H_{\setminus i_k}|i_k \in \mathscr{I}\}$. By Definition 2, $\text{rank}([A_{\mathscr{I}}|a_k]) = \text{rank}(A_{\mathscr{I}})$. This implies that $a_k \in \text{Im}(A_{\mathscr{I}})$ and therefore $\text{Null}([A_{\mathscr{I}}|a_k]^T) = \text{Null}(A_{\mathscr{I}}^T)$. From Theorem 1, $\Delta x \in \text{Null}(A_{\mathscr{I}}^T)$. Thus $\Delta x \in \text{Null}([A_{\mathscr{I}}|a_k]^T)$, which implies that $a_k^T \Delta x = 0$. It follows that $H_k \Delta x = 0$. Therefore, $z_a = H\Delta x = (H-H_k)\Delta x = H_{\setminus k}\Delta x$, which implies that $z_a \in \text{Im}(H_{\setminus k})$. Thus, z_a is also stealthy in the topology to which $H_{\setminus k}$ is associated, i.e. $\mathscr{G}(\mathscr{V},\mathscr{E}_{\setminus k})$. Since this is the case for all trivial topology matrices spanned by the topology matrices in $\{H_{\setminus i_k}|i_k \in \mathscr{I}\}$, one can conclude the proof. ■



(a) (b) (c)

Fig. 1. Topologies for examples

We now explain how problems that are not directly considered by our main results can be converted to problems to which our results are applicable. Definition 3 is defined based on the assumption that $\mathscr{I} \subseteq \mathscr{P}$ which might not always be the case. For example in Figure 1(b), $\mathscr{P}=\{3,4,5,6\}$, as shown by the dashed lines, and $\mathscr{I}=\{1,2,3,4\}$, as shown by the cross marks. It is clear that $\mathscr{I} \nsubseteq \mathscr{P}$ in this case. However, this is equivalent to consider the case as shown in Figure 1(c), where $\mathscr{I}'=\{3,4,5\}$ with $\mathscr{I}'$ similarly defined as that of $\mathscr{I}$ in Figure 1(b). This is due to the fact that $H_{\setminus 1}$ and $H_{\setminus 2}$ are trivial topology matrices spanned by the nontrivial topology matrices $H_{\setminus 3}$, $H_{\setminus 4}$ and $H_{\setminus 5}$. Therefore, by Corollary 1, a feasible z_a such that $z_a \in \cap_{i\in\mathscr{I}}\text{Im}(H_{\setminus i})$ implies that $z_a \in \cap_{i\in\mathscr{I}'}\text{Im}(H_{\setminus i})$. Note that $\mathscr{I}' \subset \mathscr{P}$ in this equivalent case so that our main theorem is applicable. In general, if the operator selects a set of links $\{e_i|i\in\mathscr{P}\}$ which contains a spanning tree of $\mathscr{G}(\mathscr{V},\mathscr{E})$, the set of topology matrices $\{H_{\setminus i}|i\in\mathscr{P}\}$ will contain n nontrivial topology matrices. Moreover, these n nontrivial topology matrices are able to span any topology matrix $H_{\setminus i}, \forall i=1,\ldots,l$. Therefore, our main results in this paper are applicable to any possible cases.

Theorem 2: Suppose that the attacker is able to launch an (p,n)-stealthy attack. Then it is only able to independently manipulate the estimation deviations on $n-p$ components of the graph $\mathscr{G}(\mathscr{V},\mathscr{E}_{\mathscr{I}})$. Moreover, let $\mathscr{I}_i$ be the set of indices corresponding to the ith component of $\mathscr{G}(\mathscr{V},\mathscr{E}_{\mathscr{I}})$. Then the deviation Δx has the form of $\sum_{i=1}^{n-p}\alpha_i e_{\mathscr{I}_i}$, where $\alpha_i \in \mathbb{R}$ is arbitrary, $\forall i$, and $e_{\mathscr{I}_i} \in \mathbb{R}^n$ is a vector each entry of which is one if its index is in $\mathscr{I}_i$ and zero otherwise.

Proof: It is clear that $A_{\mathscr{I}}$ can be regarded as the truncated incidence matrix which describes the graph $\mathscr{G}(\mathscr{V},\mathscr{E}_{\mathscr{I}})$. Since Theorem 1 shows that the case when $p=n$ will lead to a trivial solution of z_a from the attacker's perspective, we only discuss the case when $p \leq n-1$. Since $\text{rank}(A_{\mathscr{I}}) = p$, it follows that $\dim\{\text{Null}(A_{\mathscr{I}}^T)\} = n-p$, where $\dim\{\cdot\}$ stands for the dimension of a matrix subspace. Suppose that $\mathscr{G}(\mathscr{V},\mathscr{E}_{\mathscr{I}})$ contains k isolated components, then from Lemma 1, we have $k = n-p+1 \geq 2$. By reassigning the indices of buses, without loss of generality, $A_{\mathscr{I}}$ can be written as $A_{\mathscr{I}} = \text{diag}\{[A_{\mathscr{I}_1},\ldots,A_{\mathscr{I}_k}]\}$, where $\mathscr{I}_i \subseteq \mathscr{I}$ is a set of indices with respect to the ith component in $\mathscr{G}(\mathscr{V},\mathscr{E}_{\mathscr{I}})$, $\forall i \in \{1,\ldots,k\}$. Without loss of generality, we let $\mathscr{I}_k$ be the set that contains the index with respect to the reference bus.

It is clear that $\forall i \in \{1,\ldots,k-1\}$, each column of $A_{\mathscr{J}_i}$ contains only two nonzero entries, namely, 1 and -1. Therefore, $A_{\mathscr{J}_i}$ can be regarded as the incidence matrix (similar to A_0) with respect to the graph $\mathscr{G}(\mathscr{V}_{\mathscr{J}_i}, \mathscr{E}_{\mathscr{J}_i})$, where $\mathscr{V}_{\mathscr{J}_i}$ is similarity defined as that of $\mathscr{V}_{\mathscr{J}}$. It follows that $\mathbf{1} \in \text{Null}\{A_{\mathscr{J}_i}^T\}$ from Lemma 1. Moreover, $\text{rank}(A_{\mathscr{J}_i}) = |\mathscr{V}_{\mathscr{J}_i}| - 1$. Thus, $\mathbf{1}$ is the only basis of the left null space of $A_{\mathscr{J}_i}$. This is the case for all $i \in \{1,\ldots,k-1\}$. Therefore for each component that does not contain the reference bus, the attacker can only deviate the estimated states of all included buses with the same value.

Using the same reference bus as that of $\mathscr{G}(\mathscr{V},\mathscr{E})$, it is clear that $A_{\mathscr{J}_k}$ is the truncated incidence matrix (similar to A) with respect to the graph $\mathscr{G}(\mathscr{V}_{\mathscr{J}_k}, \mathscr{E}_{\mathscr{J}_k})$. This implies that $A_{\mathscr{J}_k}$ is a square matrix. Moreover, since the topology matrices associated with the p topologies are nontrivial, the columns of $A_{\mathscr{J}_k}$ are guaranteed to be independent from each other. Therefore $\text{Null}\{A_{\mathscr{J}_k}\} = \emptyset$. This implies that the attacker cannot manipulate any of the state values in the component that contains the reference bus. Recall that $k = n - p + 1$. Therefore the attacker can only independently deviate the estimates of the $n - p$ components that do not contain the reference bus. It follows that the general form of the estimation deviations is $\sum_{i=1}^{n-p} \alpha_i e_{\mathscr{J}_i}$. ■

Theorem 2 describes how exactly the flexibility of manipulating the estimation deviations is limited when the attacker launches a (p,n)-stealthy attack. It is shown that this flexibility can be judged by checking the graph $\mathscr{G}(\mathscr{V},\mathscr{E}_{\mathscr{J}})$. It turns out that this deviation can only be designed in a "component" sense. That is, for each component in the graph $\mathscr{G}(\mathscr{V},\mathscr{E}_{\mathscr{J}})$, the estimation deviations for all included states have to be identical. Moreover, for the component that contains the reference bus, as a special case, the estimation deviations for all included states have to be identical to zeros. Therefore, even though the attacker is possible to launch a feasible attack that is stealthy in some of the preselected topologies, it has to confront the limited flexibility of designing the estimation deviation Δx, especially when it tries to "hide" in more topologies. This trade-off turns out to be linear, as proved in Theorem 2. The conclusions of Theorem 2 instantly leads to the following corollary.

Corollary 2: The possibility of a certain (p,n)-stealthy attack is zero *if and only if* there exists at least one independently verifiable bus in each component of $\mathscr{G}(\mathscr{V},\mathscr{E}_{\mathscr{J}})$ that does not contain the reference bus.

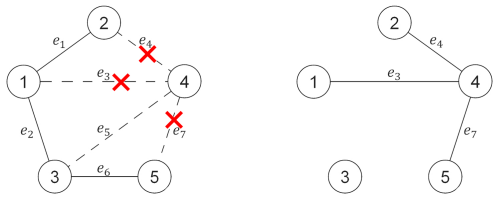
The proof of Corollary 2 is straightforward and omitted here for the sake of saving space. This corollary is motivated by the fact that Δx for all buses in the same component of $\mathscr{G}(\mathscr{V},\mathscr{E}_{\mathscr{J}})$ have to be identical. Therefore by guaranteeing that at least one state can be independently verified (the state value can be directly observed by some methods that are independent from the state estimator, see [5] for details), it is obtained that $e_{\mathscr{J}_i} = \mathbf{0}, \forall i \in \{1,\ldots,n-p\}$. Thus $\Delta x = \mathbf{0}$. It follows that $z_a = H\Delta x = \mathbf{0}$ from Lemma 2.

Corollary 2 also explains why the estimation deviations of the states that belong to the component, which includes the reference bus, have to identically be zero. This is because of the state value of the reference is assumed to be zero in order to show the angles of other buses relative to it. Therefore by Theorem 2, all states in the same component of $\mathscr{G}(\mathscr{V},\mathscr{E}_{\mathscr{J}})$ will have zero deviations. From this perspective, the reference bus plays the role of a verifiable state.

TABLE I

PARAMETERS OF STUDIED CASES

Case #	$\mathscr{P}$	Ref	$\mathscr{I}$	Δx_1	Δx_2	Δx_3	Δx_4	Δx_5
1	3,4,5,7	v_5	3,4,7	0	0	α	0	N/A
2	3,4,5,7	v_5	3,4,5	α	α	α	α	N/A
3	3,4,5,7	v_4	3,4,5	0	0	0	N/A	α
4	1,2,4,6	v_4	1,2,6	α	α	α	N/A	α



(a) $\mathscr{G}(\mathscr{V},\mathscr{E})$ (b) $\mathscr{G}(\mathscr{V},\mathscr{E}_{\mathscr{J}})$

Fig. 2. Study of Case 1 in Table I

V. CASE STUDIES

From Theorem 2, an (n,p)-stealthy attack is only able to independently deviate $n-p$ components in $\mathscr{G}(\mathscr{V},\mathscr{E}_{\mathscr{J}})$. However, the number of buses in each component of $\mathscr{G}(\mathscr{V},\mathscr{E}_{\mathscr{J}})$ is dependent on both the system operator's selection of $\mathscr{P}$ and the attacker's selection of $\mathscr{I}$,where $\mathscr{I}$ and $\mathscr{P}$ are similarly defined as that of the example shown in Figure 1(b). Moreover, since an (p,n)-stealthy attack is not able to deviate the estimated states of all buses that included in the same component with the reference bus, the location of the reference bus in $\mathscr{G}(\mathscr{V},\mathscr{E})$ will also contribute to the limitation as described in Theorem 2. Motivated by these intuitions, in this section, we use $\|\Delta x\|_0$, which stands for the number of nonzero entries of Δx, as the metric to evaluate how the limitations on the estimation deviation Δx is affected by the selection of $\mathscr{P}$, $\mathscr{I}$ and the reference bus in $\mathscr{G}(\mathscr{V},\mathscr{E})$.

A. Scenario without Verifiable State

The parameters of all cases that studied in this scenario are listed in Table I, in which the "Ref" stands for the reference bus for each case. It is assumed that for each case, a $(3,4)$-stealthy attack is launched with the listed choice of $\mathscr{I}$ and $\mathscr{P}$. Δx_i denotes the deviated estimates of the ith bus. Note that this deviation is undefined for the reference bus and therefore marked as "N/A" in the table. $\alpha \in \mathbb{R}$ is arbitrary.

The details for case 1 is shown in Figure 2 as an example. Similar figures can be easily derived for other cases in Table I. We omit them here for the interest of space. In Figure 2(a), the dashed lines form the link set $\{e_i | i \in \mathscr{P}\}$, which is decided by the operator. The cross marks show the link set $\{e_i | i \in \mathscr{I}\}$, which is decided by the attacker. Figure 2(b) shows the graph $\mathscr{G}(\mathscr{V},\mathscr{E}_{\mathscr{J}})$, which is the critical graph used to judge the general form of the deviations of the estimated states Δx.

For case 1, since it is a $(3,4)$-stealthy attack, it is only able to deviate one component in $\mathscr{G}(\mathscr{V},\mathscr{E}_{\mathscr{J}})$. As shown in Figure 2(b), bus 3 is the only bus that belongs to the component that does not contain the reference bus v_5. Therefore, only Δx_3 can be deviated with an arbitrary value α. If follows that $\|\Delta x\|_0 = 1$. For case 2, the only difference from case 1 is the selection of $\mathscr{I}$. As a result, however, the estimated states of all buses are deviated with the same value and therefore $\|\Delta x\|_0 = 4$. This is because in $\mathscr{G}(\mathscr{V},\mathscr{E}_{\mathscr{J}})$ of case 2, the reference bus is isolated from all other buses. Then all buses are included in the component that does not contain the reference bus. Therefore, given the objective to be deviating more numbers of states from the attacker's perspective, the selection of $\mathscr{I}$ in case 2 is more preferred by the attacker. In case 3, all parameters stay the same as that of case 2 except that the reference bus is selected as bus 4 instead of bus 5. However, by simply changing the reference bus, only one estimate of states can be deviated. Actually, in this case, any possible $(3,4)$-stealthy attack is only able to deviate one estimated state since all buses are directly connected to the reference bus in $\mathscr{G}(\mathscr{V},\mathscr{E}_{\mathscr{J}})$. Therefore, case 3 is the most preferable case form the operator's perspective. In case 4, using the same reference bus as that of case 3, the selection of $\mathscr{P}$ is changed. It turns out that by selecting $\mathscr{I}$ listed in Table I, the estimates of all states will be deviated, i.e., $\|\Delta x\|_0 = 4$. Thus, this is the least preferable case that the operator should consider.

Therefore, using $\|\Delta x\|_0$ as the metric, we summarize the following two criteria for the system operator to select the location of the reference bus in $\mathscr{G}(\mathscr{V},\mathscr{E})$, and the n links to cut rotationally, in the scenario when there is no verifiable state. 1) In $\mathscr{G}(\mathscr{V},\mathscr{E}_{\mathscr{J}})$, the reference bus should be directly connect to as much buses as possible. As shown in the comparison between case 2 and case 3. 2) The reference bus should act as the "root" of the spanning tree that formed by the n links whose indices are in $\mathscr{P}$. Moreover, each branch of the spanning tree should have as few vertices as possible, as shown in the comparison between case 3 and case 4.

B. Scenario with Verifiable State

When there exist independently verifiable states [5], the strategy for the operator to select $\mathscr{P}$ will be changed significantly. A certain (p,n)-stealthy attack will be impossible if $n-p$ verifiable buses are added in the way described in Corollary 2. However, it is the attacker's decision to select which p of the n topologies to "hide" in. The comparison between case 1 and case 2 in the former scenario has shown that by selecting different $\mathscr{I}$ the attacker will significantly change the number of estimated states that could be deviated. Therefore, the operator should try to find a solution to minimize $\|\Delta x\|_0$ regardless of the selection of $\mathscr{I}$ by the attacker. Suppose that bus 5 is verifiable in case 4 shown in Table I, $\|\Delta x\|_0 \equiv 0$ for any possible $(3,4)$-stealthy attack. Note that in the scenario without any verifiable state, case 4 is one of the least preferable strategies for the operator to select $\mathscr{P}$. Case 3 in Table I, however, which is the optimal strategy in the former scenario, becomes the last strategy that operator would consider in this scenario. This is because for the scenario with verifiable states, in order to make $\|\Delta x\|_0 \equiv 0$ hold for any possible $(3,4)$-stealthy attack in case 3, all buses should be verifiable except for the reference bus. This implies that the existence of the verifiable states can significantly change the strategies for selecting $\mathscr{P}$ and the reference bus.

VI. Conclusions & Future Work

We extended our previous work [1] which studied the scenario of using the scheme of switching topologies to defend against the stealthy FDIAs in power system. It is shown that even if the attack is still feasible to be stealthy in a majority of the preselected topologies, there is a linear trade-off between the flexibility of manipulating the estimation deviation, and the possibility of not being detected. The general form of the consistent deviation of the estimated states are formulated as well. It turns out that this deviation can only be designed in a "component" sense. Several cases are studied to show how the deviation can be affected by the decision made by both the attacker and the operator.

Our future directions include the analysis of the transient stability during the switching among topologies, the minimum effort to learn the current topology from the attacker's perspective, and specifically formulating the objective for optimally selecting the topology set from the operator's perspective.

References

[1] S. Wang and W. Ren, "Stealthy false data injection attacks against state estimation in power systems: Switching network topologies," in *American Control Conference, 2014*, June 2014, pp. 1572–1577.

[2] A. Ali and E. Antonio, *Power System State Estimation*. Marcel Dekker, Inc., 2004.

[3] Y. Mo, T.-H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber physical security of a smart grid infrastructure," *Proceedings of the IEEE, Special Issue on Cyber-Physical Systems*, vol. 100, no. 1, pp. 195–209, Jan 2012.

[4] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 13:1–13:33, Jun. 2011. [Online]. Available: http://doi.acm.org/10.1145/1952982.1952995

[5] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in *Preprints of the First Workshop on Secure Control Systems, CPSWEEK*, vol. 2010, 2010.

[6] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010, Stockholm, Sweden*, 2010.

[7] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 214–219.

[8] K. C. Sou, H. Sandberg, and K. Johansson, "Computing critical k -tuples in power networks," *Power Systems, IEEE Transactions on*, vol. 27, no. 3, pp. 1511–1520, 2012.

[9] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 645–658, 2011.

[10] K. Cheong Sou, H. Sandberg, and K. H. Johansson, "On the exact solution to a smart grid cyber-security analysis problem," 2011.

[11] B. Kroposki, R. Lasseter, T. Ise, S. Morozumi, S. Papatlianassiou, and N. Hatziargyriou, "Making microgrids work," *Power and Energy Magazine, IEEE*, vol. 6, no. 3, pp. 40–53, 2008.