On Phasor Measurement Unit Placement against State and Topology Attacks

Jinsub Kim and Lang Tong
School of Electrical and Computer Engineering
Cornell University
Ithaca, New York USA
{jk752, lt35}@cornell.edu

Abstract—Cyber attacks on the SCADA system can mislead the control center to produce incorrect state and topology estimate. If undetected, state and topology attacks can have detrimental impacts on the real-time operation of a power system. The problem of placing secure phasor measurement units (PMUs) to detect such attacks is considered. It is shown that any state or topology attack is detectable if and only if buses with secure PMUs form a vertex cover of the system topology. This condition leads to the countermeasures constructed by available graph algorithms. The examples with IEEE 14-bus, 118-bus, and 300-bus systems demonstrate applications of the countermeasures.

Index Terms—Power system cyber security, false data injection, topology attack, state estimation, phasor measurement units.

I. INTRODUCTION

The communications among participating entities (e.g., control center, substations, consumers, etc.) are essential to smart grid operations. The increasing reliance on communications makes smart grids inevitably vulnerable to cyber attacks. Among many possible cyber attacks, this paper focuses on state and topology attacks [1], [2] in which an adversary aims to mislead the control center with an incorrect state or topology estimate by altering part of meter and network data.

The state and topology estimates are critical inputs to several control center operations including real-time dispatch and real-time pricing. The ability to perturb state or topology estimates allows the adversary to interfere real-time grid operations. For instance, the adversary who can perturb the topology estimate may disguise a connected transmission line as disconnected or vice versa to cause load shedding or a delay in the control center’s response to a contingency event. The effect of state and topology attacks on real-time pricing was also shown to be significant [3]–[5].

In practice, modern power systems employ bad data detectors which raise an alarm if there exists inconsistency among network data (i.e., breaker and switch states) and meter data. For an attack to succeed, the adversary needs to modify both network and meter data such that they are consistent with the “target” state and topology. When the adversary has a power to modify a sufficiently large set of meter, undetectable state and topology attacks might be feasible [1], [2].

This work is supported in part by a grant under the DoE CERTS program, the NSF under Grant CNS-1135844, and a PSERC grant.

This paper considers the role of secure phasor measurement units (PMUs) in detecting state and topology attacks on the power grid. By secure PMUs, we mean that additional security measures (such as encryption and authentication) are implemented so that PMU data are not subject to corruption by man-in-the-middle attacks [6]. Given that PMUs are still at an early stage of deployment, and the cost of deployment remains high, it is important to place secure PMUs carefully in order to maximize the power of detecting cyber attacks. Our goal in this paper is to provide a necessary and sufficient condition that any state or topology attack is detectable and evaluate placement patterns for practical benchmark networks.

A. Related works

The seminal paper by Liu, Ning, and Reiter [1] first introduced a feasible cyber attack on power system state estimation, which we refer to as state attack. In [1], the authors demonstrated that the adversary with an ability to modify certain meter data can perturb the state estimate in an arbitrary degree without being detected by the control center. Many efforts have since been made to analyze the system vulnerability to state attacks and countermeasures. In [7], [8], feasibility of undetectable state attacks was connected to the system observability. Based on the connection, several countermeasures have been developed to prevent undetectable state attacks (see [7], [9]–[12].) Especially, the allocation of secure PMUs to defend against state attacks was studied in [13], [14]. Giani et al. [13] presented a way to assign secure PMUs to disable a certain collection of undetectable state attacks. Kim and Poor [14] proposed a greedy assignment algorithm to make undetectable state attacks infeasible.

A new type of cyber attack to perturb the topology estimate, which we refer to as topology attack, was recently considered in [2], [5]. A necessary and sufficient condition for feasibility of undetectable topology attacks was presented in [2], and a graph-theoretical countermeasure was proposed to assign protection devices on a subset of line flow and injection meters such that undetectable topology attacks become infeasible.

In this paper, we study an optimal countermeasure against both state and topology attacks based on secure PMUs. To the best of our knowledge, our study is the first to consider protection of a grid against joint state and topology attacks.
B. Summary of contributions and organizations

We first prove that an undetectable state attack is feasible only if an undetectable topology attack is feasible. This implies that a countermeasure against undetectable topology attacks is sufficient for protecting the grid from both state and topology attacks.

Secondly, we provide a necessary and sufficient graph-theoretical condition for existence of an undetectable state or topology attack. Specifically, it is shown that no undetectable attack exists if and only if the buses with secure PMUs form a vertex cover of the grid topology. The condition implies that finding an optimal countermeasure is equivalent to finding a minimum vertex cover of the topology. The minimum vertex cover problem is NP-complete, but polynomial-time approximation algorithms exist. We construct a countermeasure based on approximation algorithms and demonstrate its application to IEEE 14-bus, 118-bus, and 300-bus systems.

The rest of the paper is organized as follows. In Section II, we present adversary models and mathematical formulation. Section III provides a useful relation between feasibility conditions for undetectable state and topology attacks. Section IV presents a necessary and sufficient graph-theoretical condition for successful protection with secure PMUs. In Section V, we utilize the condition to build countermeasures based on available graph algorithms and demonstrate countermeasures for IEEE test systems. Section VI concludes the paper with remarks.

II. Preliminaries

The control center obtains two types of data from the field meters and sensors deployed throughout the grid. One is the meter data $z \in \mathbb{R}^m$ consisting of bus injection, line flow, and PMU measurements. The second type is the network data $s \in \{0, 1\}^l$ consisting of $l$ breaker status measurements, where each entry represents the measured status of each breaker (0 for open and 1 for closed).

In the absence of communication errors or malicious attacks, $s$ gives true breaker statuses. Each $s \in \{0, 1\}^l$ corresponds to a system topology, which is represented by an undirected graph $\bar{G} = (\bar{V}, \bar{E})$ where $\bar{V}$ is the set of buses, and $\bar{E}$ is the set of connected transmission lines. Specifically, for every physical transmission line between two buses (e.g., $i$ and $j$), $\{i, j\} \in \bar{E}$ if and only if the line is connected. In addition, $\bar{E}_0$ denotes the set of all lines, both connected and disconnected. A subset $\bar{C}$ of $\bar{V}$ is said to form a vertex cover of $(\bar{V}, \bar{E}_0)$ if every $\{i, j\} \in \bar{E}_0$ is incident to at least one vertex in $\bar{C}$ (i.e., $i$ or $j$ are in $\bar{C}$).

In the absence of attack and measurement noise, $z$ is assumed to come from the DC model with the linearized PMU measurements [14], [15]:

$$z = Hx$$

where $x \in \mathbb{R}^n$ is the unknown state vector consisting of voltage phases of all the buses except the slack bus, and $H \in \mathbb{R}^{m \times n}$ is the measurement matrix. To make the presentation concise, the analysis will be provided only for the noiseless model. However, the results in [1], [2] imply that feasibility conditions for undetectable attacks, on which our analysis is mainly based, are the same regardless of the presence of Gaussian measurement noise. Hence, our results can be generalized to the noisy measurement case.

The measurement matrix $H$ in (1) depends on the system topology $\bar{G}$. If an entry $z_k$ of $z$ is the measurement of the line flow from $i$ to $j$ of a connected line $\{i, j\}$, $z_k = B_{ij}(x_i - x_j)$ where $B_{ij}$ denotes the line susceptance and $x_i$ the voltage phase at bus $i$. The corresponding row in $H$ is

$$h_{(i,j)} = \begin{bmatrix} 0 & \cdots & B_{ij} & 0 & \cdots & -B_{ij} & 0 & \cdots & 0 \end{bmatrix}.\,$$

If $z_k$ corresponds to a line flow through a disconnected line, $z_k$ is zero, and the corresponding row in $H$ is a zero row vector. If $z_k$ is the injection measurements at bus $i$, the corresponding row in $H$ is the sum of the row vectors corresponding to all the outgoing line flows from $i$. The linearized PMU measurements from bus $i$ consist of (i) the direct measurement of $x_i$ (i.e., $z_k = x_i$) and (ii) the measurements of all the outgoing line flows from bus $i$ (i.e., the measurements of the line flows from $i$ to $j$ for all $j$ with $\{i, j\} \in \bar{E}_0$) [14], [15].

A. Attack model

Fig. 1 illustrates the adversary and state estimation model for the so-called man-in-the-middle attack [6]: the adversary intercepts the remote terminal data $(z, s)$, modifies part of them, and forwards the modified version $(\tilde{z}, \tilde{s})$ to the control center. We take a conservative viewpoint by assuming that the adversary may observe all entries of $z$ and $s$ and modify all of their entries except those coming from the secure PMUs. Although overly conservative, such an assumption makes our protection strategy even robust to the most powerful adversary.

Let $\bar{G}$ be the actual network topology and $H$ its associated measurement matrix. We assume that the actual system is observable; i.e., $H$ has full column rank. We consider an attack aiming to perturb the topology estimate from $\bar{G} = (\bar{V}, \bar{E})$ to $\bar{G}' = (\bar{V}, \bar{E}')$. In contrast to $\bar{G}$, the system with $\bar{G}'$ is allowed to be unobservable (i.e., the corresponding measurement matrix may not have full rank.) For instance, the adversary may aim to mislead the control center that the system topology, which is actually connected, consists of multiple disconnected parts. Note that $\bar{G}$ and $\bar{G}'$ have the same set of vertices. In other words, we consider attacks that only perturb transmission line
connectivities.

The attack has the following structure of data modification (the notation with a bar on a variable denotes the value perturbed by the adversary.)

\[
\bar{s} = s + b \pmod{2}, \\
\bar{z} = z + a(z), \quad a(z) \in A.
\]  

(3)

The adversary adds \( b \in \{0,1\}^l \) to \( s \) such that the topology corresponding to \( \bar{s} \) is the “target” topology \( \bar{G} \). We assume that the adversary can make a proper modification \( b \) for any given target \( \bar{G} \). The attack vector \( a(z) \in \mathbb{R}^m \) is added to \( z \) such that \( \bar{z} \) looks consistent with \( \bar{G} \). In addition, \( a(z) \) also has a role to perturb the state estimate as desired by the adversary. We use the notation \( a(z) \) to emphasize that the adversary can design the attack vector based on the full meter data \( z \). Finally, \( A \subseteq \mathbb{R}^m \) is the set of feasible attack vectors. If \( \mathcal{J}_s \) denotes the set of indices for the entries in \( z \) from secure PMUs, \( A = \{ c \in \mathbb{R}^m : c_k = 0, \forall k \in \mathcal{J}_s \} \). In other words, the adversary may modify all bus injection, line flow, and PMU measurements except those from secure PMUs.

C. Feasibility of undetectable attacks

In assessing whether the grid is vulnerable to an attack, feasibility conditions for undetectable attacks are valuable.

For a state attack, recalling Definition 2.1, an attack \( a \) is undetectable if and only if \( \bar{z} + a(z) \in \text{Col}(\bar{H}) \) for all \( z \in \text{Col}(H) \). Note that \( \bar{z} + a(z) \in \text{Col}(\bar{H}) \) for all \( z \in \text{Col}(H) \) if and only if \( a(z) \in \text{Col}(H) \) for all \( z \in \text{Col}(H) \). In addition, there exists a nonzero function \( a \) with \( a(z) \in \text{Col}(H) \) for all \( z \in \text{Col}(H) \) if and only if \( A \cap \text{Col}(H) \neq \{0\} \). Hence, there exists an undetectable state attack if and only if

\[
A \cap \text{Col}(H) \neq \{0\}.
\]  

(6)

By Theorem 1 in [9], the above condition holds if and only if the grid becomes unobservable after we remove all the meters except the secure PMUs.

For a topology attack, it was shown in [2] that there exists an undetectable topology attack to perturb the topology estimate from \( \mathcal{G} \) to \( \bar{G} \) if and only if

\[
\text{Col}(H) \subset \text{Col}(\bar{H}, A)
\]  

(7)

where \( \text{Col}(\bar{H}, A) \) denotes the vector space spanned by the columns of \( \bar{H} \) and the basis vectors of \( A \). Note that the above condition means that the adversary is able to move any \( z \in \text{Col}(H) \) into \( \text{Col}(\bar{H}) \) by adding a proper \( c \in A \).
III. RELATION BETWEEN FEASIBILITY CONDITIONS

In this section, we prove that the feasibility condition for undetectable state attacks implies the feasibility condition for undetectable topology attacks. It is formally stated as follows.

**Theorem 3.1:** Let $\mathcal{G}$ denote the true topology and $\mathcal{A}$ the set of feasible attack vectors. If there exists an undetectable state attack (i.e., the condition (6) holds), then there exists $\mathcal{G}$, different from $\mathcal{G}$, such that an undetectable topology attack to perturb $\mathcal{G}$ to $\mathcal{G}$ exists (i.e., the condition (7) holds for $\mathcal{G}$.)

**Proof:** Suppose that the condition (6) holds. Let $\tilde{H}$ denote the submatrix of $\hat{H}$ obtained by selecting the rows corresponding to secure PMU measurements. Then, by Theorem 1 in [9], $\hat{H}$ does not have full column rank. Hence, $N(\hat{H})$, the null space of $\hat{H}$, has a positive dimension. Let $\alpha = [\alpha_1 \cdots \alpha_n]^T$ be an element of $N(\hat{H})$ that is not a zero vector.

Note that $\mathcal{G}$ is a connected graph (due to the assumption that the system with $\mathcal{G}$ is observable), and $\alpha \neq 0$. Using these, one can easily verify that there exists a branch $\{i, j\} \in E$ such that $\alpha_i \neq \alpha_j$. Let $\mathcal{G}$ denote $\langle \mathcal{V}, \tilde{E} \rangle$ with $\tilde{E} = E \setminus \{(i, j)\}$. $\hat{H}$ the measurement matrix for $\mathcal{G}$, and $\tilde{H}$ the submatrix of $\hat{H}$ obtained by selecting the rows corresponding to secure PMU measurements.

For any state $x \in \mathbb{R}^n$, we can choose proper $c \in \mathbb{R}$ such that $\tilde{x} = x + co$ has the same entry for the $i$th and $j$th entries, i.e., $\tilde{x}_i = \tilde{x}_j$. Then, $H\tilde{x} = \tilde{H}\tilde{x}$, and thus $H\tilde{x} = \hat{H}\tilde{x}$. Note that $\hat{H}\tilde{x} = \hat{H}(x + co) = \hat{H}x$ since $\alpha \in N(\hat{H})$. Therefore, $Hx = \hat{H}x \in \text{Col}(\hat{H})$. Because this holds for any $x \in \mathbb{R}^n$, $\hat{H}x \in \text{Col}(\hat{H})$, $\forall x \in \mathbb{R}^n$. In other words, $\text{Col}(\hat{H}) \subseteq \text{Col}(\hat{H})$.

It can be easily shown that $\text{Col}(\hat{H}) \subseteq \text{Col}(\hat{H})$ is equivalent to the condition (7). Therefore, there exists an undetectable topology attack that perturbs $\mathcal{G}$ to $\mathcal{G}$.

**Theorem 3.1** directly leads to the following corollary which implies that preventing undetectable topology attacks is sufficient for protecting the grid from any state or topology attack.

**Corollary 3.1.1:** If an undetectable topology attack does not exist for any target topology $\mathcal{G}$, then an undetectable state attack does not exist.

Note that Theorem 3.1 and Corollary 3.1.1 are general results that are not restricted to the study of grid protection with secure PMUs.

IV. SECURE PMUS AND UNDETECTABLE ATTACKS

In this section, we present a necessary and sufficient graph-theoretical condition for feasibility of undetectable attacks, which characterizes the optimal placement of secure PMUs as a minimum vertex cover of $(\mathcal{V}, E_0)$.

Our analysis is based on the feasibility condition (7) for undetectable topology attacks. By exploiting this condition, we can derive the following graph-theoretical condition for countermeasures against topology attacks.

**Theorem 4.1:** An undetectable topology attack does not exist (i.e., there is no $\mathcal{G}$ satisfying (7)) if and only if the set of buses with secure PMUs is a vertex cover of $(\mathcal{V}, E_0)$.

**Proof:** See Appendix.

**Theorem 4.1** implies that any secure PMU placement that guarantees detection of topology attacks must form a vertex cover of $(\mathcal{V}, E_0)$, the graph with all transmission lines (both connected and disconnected lines). In addition, placing secure PMUs to a vertex cover is sufficient for a countermeasure. Note that the vertex cover condition does not depend on the true topology $\mathcal{G}$.

Recalling Corollary 3.1.1, one can easily see that the vertex cover condition in Theorem 4.1 is necessary and sufficient for preventing both undetectable state attacks and undetectable topology attacks, as stated below.

**Corollary 4.1.1:** An undetectable topology attack and an undetectable state attack do not exist if and only if the set of buses with secure PMUs is a vertex cover of $(\mathcal{V}, E_0)$.

**Corollary 4.1.1** leads to the following corollary regarding the optimal placement of secure PMUs.

**Corollary 4.1.2:** Placing the minimum number of secure PMUs to disable undetectable state and topology attacks can be achieved by placing secure PMUs on the minimum vertex cover of $(\mathcal{V}, E_0)$.

V. OPTIMAL PLACEMENT OF SECURE PMUS

Corollary 4.1.2 implies that finding an optimal countermeasure is equivalent to finding a minimum vertex cover of $(\mathcal{V}, E_0)$. Unfortunately, the minimum vertex cover problem is NP-complete [18], and there is no known polynomial-time algorithm. However, many polynomial-time approximation algorithms have been developed for decades (see [19] and references therein), and we may employ them to build a suboptimal countermeasure in a polynomial time.

One popular approximation algorithm with $O(|\mathcal{V}|\|E_0\|)$ complexity is a greedy approach that chooses the vertex with the maximum degree first [19]. Table I shows its pseudocode. Specifically, in each iteration, the algorithm (i) chooses a vertex with the maximum degree in the remaining graph and (ii) removes all the edges incident to the vertex from the graph. The algorithm terminates when there is no line.

<table>
<thead>
<tr>
<th>Greedy-Vertex-Cover($\mathcal{V}, E_0$):</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: $C \leftarrow \emptyset$</td>
</tr>
<tr>
<td>2: while $E_0 \neq \emptyset$</td>
</tr>
<tr>
<td>3: select a vertex $i$ with the maximum degree in $(\mathcal{V}, E_0)$</td>
</tr>
<tr>
<td>4: $C \leftarrow C \cup {i}$</td>
</tr>
<tr>
<td>5: remove all edges incident to $i$ from $E_0$</td>
</tr>
<tr>
<td>6: end</td>
</tr>
<tr>
<td>7: return $C$</td>
</tr>
</tbody>
</table>

In $(\mathcal{V}, E_0)$, the degree of $i \in \mathcal{V}$ is the number of lines incident to $i$. |
left in the graph. It has the approximation ratio\(^3\) of \(\sum_{i=1}^{\Delta} \frac{1}{i}\) where \(\Delta\) is the maximum degree of the graph. Since power system topologies are sparse in general, \(\Delta\) is expected to be small. Note that the greedy approach is just one among numerous possible options, and we may employ a different approximation algorithm depending on the system topology characteristics (e.g., maximum degree, sparsity). We may even use multiple approximation algorithms simultaneously and pick the best result.

We demonstrate the countermeasures for IEEE 14-bus, 118-bus, and 300-bus systems, constructed by the aforementioned greedy approach. Fig. 2 shows the secure PMU assignments by the countermeasure for IEEE 14-bus system, and Table II presents the number of secure PMUs used by the countermeasure for each system. One can observe that the fraction of buses with secure PMUs is about a half in all three cases.

Kim and Poor [14] demonstrated that protection against undetectable state attacks can be achieved by locating secure PMUs at about a third of buses. Hence, Table II suggests that the additional protection against topology attacks necessitates placing additional secure PMUs.

VI. CONCLUSION

We considered the problem of locating secure PMUs to detect state and topology attacks. A necessary and sufficient graph-theoretical condition was provided, and an optimal countermeasure was characterized as a minimum vertex cover of the grid topology.

PMU measurements are considered essential for analyzing dynamic phenomena, and they are more frequently available and more valuable to state estimation than other traditional measurements (e.g., power flow and injection measurements). Hence, the control center naturally has more incentives to secure PMU units than other measurement units. Our study reflects such practical aspects and provides a protection strategy based solely on secure PMU units.

We assumed that the control center employs a primitive consistency test—the noiseless version of the \(J(x)\)-test—as a detection algorithm, and our countermeasure guarantees detection of attacks by making a certain subset of data trustworthy. Even though such a primitive test can reflect practical bad data detectors well, it would be worthwhile to further investigate how we can enhance the bad data detector to achieve more accurate and economic countermeasures.

Lastly, we have employed the linearized DC model in our analysis. The DC model allows a succinct characterization of conditions for undetectable attacks. However, it is a good approximation of the nonlinear AC model only if all bus voltage phasors are sufficiently close to \(1\angle0^\circ\). Therefore, it is necessary to analyze the effectiveness of the countermeasures designed based on the DC model (including the one presented in this paper) in the nonlinear AC model.

ACKNOWLEDGEMENT

We appreciate the anonymous reviewers for their thoughtful and constructive comments.

APPENDIX

Proof of Theorem 4.1

(i) Sufficiency: Suppose that the set of buses with secure PMUs form a vertex cover. We will prove that an undetectable attack does not exist. Assume that there exists an undetectable attack to modify the topology estimate from \(\mathcal{G} = (\mathcal{V}, \mathcal{E})\) to \(\tilde{\mathcal{G}} = (\mathcal{V}, \tilde{\mathcal{E}})\) with \(\tilde{\mathcal{E}} \neq \mathcal{E}\). Then, the condition (7) implies that \(\text{Col}(\mathcal{H}) \subseteq \text{Col}(\tilde{\mathcal{H}}, \mathcal{A})\). We will show that a contradiction arises.

- Case I: Suppose that \(\tilde{\mathcal{E}} \nsubseteq \mathcal{E}\). Then, there exists a line \(\{i, j\}\) in \(\mathcal{E}\), which is not in \(\tilde{\mathcal{E}}\). Because secure PMUs form a vertex cover of \((\mathcal{V}, \mathcal{E}_0)\), either \(i\) or \(j\) should have a secure PMU on it. Without loss of generality, assume there is a secure PMU at \(i\). Then, the measurements from the secure PMU include a measurement for the line flow from \(i\) to \(j\). Let \(k\) denote the row index of \(\mathcal{H}\) corresponding to the line flow from \(i\) to \(j\), measured by the secure PMU at bus \(i\).

First, since \(\{i, j\}\) is connected in \(\mathcal{G}\), the \(k\)th row of \(\mathcal{H}\) is \(h_{(i,j)}\) as defined in (2). Secondly, since \(\{i, j\}\) is disconnected in \(\mathcal{G}\), the \(k\)th row of \(\tilde{\mathcal{H}}\) is a zero row vector. Third, every element of \(\mathcal{A}\) has a zero in the \(k\)th entry, because the \(k\)th entry corresponds to a secure PMU measurement. These three observations imply that \(\text{Col}(\mathcal{H})\) cannot be included in \(\text{Col}(\tilde{\mathcal{H}}, \mathcal{A})\). And, this contradicts with \(\text{Col}(\mathcal{H}) \subseteq \text{Col}(\tilde{\mathcal{H}}, \mathcal{A})\).

---

\(^3\)The approximation ratio is defined as the maximum (over all input graphs) of the ratio of the size of the vertex cover found by the algorithm divided by the size of the minimum vertex cover.
- Case II: Now, suppose that $\mathcal{E} \subseteq \tilde{\mathcal{E}}$. Then, there exists $\{i, j\} \in \tilde{\mathcal{E}} \setminus \mathcal{E}$. Let $x \in \mathbb{R}^n$ be an arbitrary state vector with $x_i \neq x_j$. We will prove that $Hx \notin \text{Col}(\tilde{H}, A)$, which implies $\text{Col}(H) \nsubseteq \text{Col}(\tilde{H}, A)$ and thus contradicts with $\text{Col}(H) \subseteq \text{Col}(\tilde{H}, A)$.

Assume that $Hx \in \text{Col}(\tilde{H}, A)$. Then, $Hx = \bar{H}y + a$ for some $y \in \mathbb{R}^n$ and $a \in A$. Let $\mathcal{J}_R$ denote the row indices of $H$ corresponding to the line flow measurements of lines in $\mathcal{E}$ from the secure PMUs. Let $\tilde{H}$, $\bar{H}$, and $\tilde{a}$ denote the submatrices of $H$, $\tilde{H}$, and $a$, respectively, where the submatrices are obtained by selecting only those rows with indices in $\mathcal{J}_R$. Then,

$$\tilde{H}x = \bar{H}y + \tilde{a}.$$  

First of all, $\tilde{a}$ is a zero vector, because all measurements corresponding to the indices in $\mathcal{J}_R$ are from the secure PMUs. Hence, $\tilde{H}x = \bar{H}y$. Secondly, $\mathcal{E} \subset \mathcal{E}$ implies that $\bar{H} = \tilde{H}$. Therefore, $Hx = \bar{H}y$. In addition, since $(\mathcal{V}, \mathcal{E})$ contains a spanning tree and the secure PMUs form a vertex cover, $\bar{H}$ has full column rank (by the spanning tree criterion in [20]). Hence, $x = y$, and we have $Hx = \tilde{H}x + a$.

Because the secure PMUs form a vertex cover, at least one of $i$ and $j$ has a secure PMU on it. Without loss of generality, assume $i$ has a secure PMU on it. Let $k$ denote the row index of $H$ corresponding to the line flow from $i$ to $j$, measured by the secure PMU at bus $i$. Since the $k$th row corresponds to a secure PMU measurement and $a \in A$, the $k$th row of $a$ is zero. The $k$th row of $Hx$ is also zero, because the line $\{i, j\}$ is disconnected in $\mathcal{G}$ (i.e., $\{i, j\} \notin \mathcal{E}$). However, since $\{i, j\}$ is connected in $\mathcal{G}$, the $k$th row of $\tilde{H}x$ is $B_{ij}(x_i - x_j)$, which is nonzero since $x_i \neq x_j$. This contradicts with $Hx = \tilde{H}x + a$. Hence, $Hx \notin \text{Col}(\tilde{H}, A)$, and thus $\text{Col}(H) \nsubseteq \text{Col}(\tilde{H}, A)$.

(ii) Necessity: Suppose that the set of buses with secure PMUs is not a vertex cover. It suffices to show that there exists $\tilde{\mathcal{G}} = (\bar{\mathcal{V}}, \bar{\mathcal{E}})$ such that an attack to modify the topology estimate from $\mathcal{G}$ to $\tilde{\mathcal{G}}$ is undetectable.

Since the set of buses with secure PMUs is not a vertex cover, there exists a line $\{i, j\}$ such that both $i$ and $j$ do not have secure PMUs on them. We define $\tilde{\mathcal{G}} = (\bar{\mathcal{V}}, \bar{\mathcal{E}})$ such that if $\{i, j\} \in \mathcal{E}, \tilde{\mathcal{E}} \equiv \mathcal{E} \setminus \{\{i, j\}\}$, and if $\{i, j\} \notin \mathcal{E}, \tilde{\mathcal{E}} \equiv \mathcal{E} \cup \{\{i, j\}\}$. It can be easily seen that $\tilde{H}x - Hx$ has nonzero entries only at the entries corresponding to the injections at $i$ and $j$ and line flows through the line $\{i, j\}$ (both directions) (see [5]) for more explanation about the structure of $\tilde{H}x - Hx$. Note that those entries are not from secure PMUs, because both $i$ and $j$ do not have secure PMUs on them. Hence, $\tilde{H}x - Hx \in A$.

Therefore, for any $z = Hx \in \text{Col}(H)$, setting $a(z) \triangleq (\tilde{H} - H)x = (\tilde{H} - H)(H^TH)^{-1}H^Tz$ renders $z + a(z) \in \text{Col}(\tilde{H})$. Hence, the attack $a$ to modify $\mathcal{G}$ to $\tilde{\mathcal{G}}$ is undetectable, and the proof is completed.

\section*{References}


