Implementation of Unobservable State-preserving Topology Attacks

Jiazi Zhang
Dept. of Electrical, Computer, and Energy Engineering
Arizona State University
Tempe, AZ, 85287
Email: jzhan188@asu.edu

Lalitha Sankar
Dept. of Electrical, Computer, and Energy Engineering
Arizona State University
Tempe, AZ, 85287
Email: lalithasankar@asu.edu

Abstract—**This paper studies the vulnerability of AC state estimation (SE) with respect to a class of unobservable state-preserving topology attacks, in which the topology data are changed by attacker while the states remain unchanged. An algorithm based on breadth-first search (BFS) is developed to determine the subset of topology data and measurements required to launch successful unobservable state-preserving topology attacks. It is shown that the proposed algorithm can enable an attacker to obtain the localized topology and corresponding measurement data to mount an attack that bypasses bad data detector and successfully changes topology information of the system in the cyber layer.**

Keywords—***Cyber physical system security, power system state and topology estimation, topology attack, breadth-first search.***

I. Introduction

Topology information plays an essential role in power system operation. In energy management systems (EMSs), various data processing modules including state estimation (SE), contingency analysis (CA), and optimal power flow (OPF) are highly dependent on topology information. Cyber attacks that alter the system topology information can result in wrong solutions within these modules with potential consequences including systematic problems and failures.

There has been much recent interest in understanding the cyber-security challenges facing the electric power system. In [1], the authors introduce a class of false data injection (FDI) attacks for DC SE and show that an attacker with sufficient system knowledge can inject malicious measurements without being detected by existing bad data detection techniques that are subsequent to SE. In [2], Kosut *et al.* demonstrate that the algebraic condition for unobservable FDI attack is equivalent to that of network observability. In [3], the authors focus on FDI attacks on AC SE and introduce a class of unobservable attacks that are limited to a sub-graph of the network. They demonstrate that the knowledge of both system topology and states are required to launch unobservable FDI attacks on AC SE. In [4], the authors demonstrate that unobservable FDI attacks on AC SE can lead to a physical generation re-dispatch when none was needed.

Yet another class of FDI attacks is one that alters topology data in an unobservable manner. In [5], Kim and Tong formally introduce an unobservable topology attack as a specific class of FDI attacks on power systems and evaluate the attack's impact on the locational marginal prices (LMPs). The authors design the attack to alter the system topology estimate by injecting malicious measurements and false line status data. Topology attacks for DC SE are also studied in [6] and [7].

In this paper, we focus on a non-linear system model (*i.e.,* AC SE) and on a class of unobservable topology attacks in which an attacker can change topology information of the system without changing the states. We henceforth refer to such attacks as *unobservable state-preserving topology attacks.* These attacks can be of two types: *line-maintaining* and *line-removing*: for a line-maintaining attack, the attacker changes measurements and line status information to make it appear that line which is not in the system is now shown as active at the control center via SCADA data; the opposite is achieved by a line-removing attack. The paper [5] introduces unobservable state-preserving topology attacks; however the analysis in [5] is restricted to line-removing attacks. To launch such attacks, the authors propose an attack heuristic in which the attacker can set the power flow measurements for a specific line to zero and change the power injection measurements at the end buses of that line.

In this paper, we focus on a class of unobservable state-preserving line-maintaining attacks. We seek to understand the minimum amount of information an attacker needs to launch such attacks. We assume the attacker is aware of a physical outage in the system and changes the resulting SCADA data (prior to SE) to make it appear that the line is in service. We denote such a line as the *target line* hereinafter. Specifically, false line flow measurements need to be created for the target line; however, this cannot be achieved by just adjusting the measurements at the end buses and requires estimating states at those buses as well, since the flow on the outage line has to be computed. For a reliable state estimate, the attacker needs to identify a physical connection (we denote as path hereinafter) between the end buses of the target line, over which it can estimate states with local measurements, and thereby, create an unobservable attack. However, there are multiple such paths in the system. To create an attack with the smallest set of information, the attacker needs to find the shortest path. Since the power system can be represented as an undirected and unweighted graph, algorithms such as Dijkstra's and Bellman-Ford, which are used to find the shortest path in directed and weighted graph, are not suitable in this problem. Therefore, we propose an algorithm based on breadth-first search (BFS), which is generally used for traversing or searching graph data structures [8]. We need such an algorithm to search for the shortest path that connected the end buses of the target line in power system.

II. Mathematical Model

In this section, we first introduce the system network and topology processor models. Then we provide a short review of mathematical formulation for AC SE and bad data detection. Throughout, we assume there are n_b buses, n_{br} branches, and n_z measurements in the system.

A. System Network and Topology Processor

The electric power system can be represented by a graph $\mathcal{G} = \{\mathcal{N}, \mathcal{E}\}$ where $\mathcal{N}$ and $\mathcal{E}$ are the sets of buses and lines, respectively. For a specific system, we assume the static topology is $\mathcal{G}_0 = \{\mathcal{N}_0, \mathcal{E}_0\}$ where $\mathcal{N}_0$ and $\mathcal{E}_0$ are the sets of all existing buses and branches, respectively. Then, the static connectivity of the buses with lines can be represented with $n_{br} \times n_b$ "from" and "to" line-to-bus incidence matrices A_{Kf} and A_{Kt}, respectively. If a line k exists to connect bus i to bus j, the $(k,\, i)^{th}$ element of A_{Kf} and $(k,\, j)^{th}$ element of A_{Kt} are 1 and all other entries of A_{Kf} and A_{Kt} are set to zeros. The overall $n_{br} \times n_b$ line-to-bus incidence matrix A_{KN} is calculated using A_{Kf} and A_{Kt} as follows

$$A_{KN} = A_{Kf} - A_{Kt}. \tag{1}$$

At the control center, SCADA collects line status data as a $n_{br} \times 1$ vector s with entries $s_k \in \{0, 1\}$ for $k \in \{1, ..., n_{br}\}$ that indicate the on and off status of circuit-breakers on each line. The data is then passed to a topology processor which maps the real-time power system topology along with network connectivity data. The complete topology information is captured by two matrices Y_{br}, the branch admittance matrix, and Y_{bus}, the bus admittance matrix, defined as

$$Y_{br} = D[\text{diag}(s)A_{KN}], \tag{2}$$

$$\text{and} \qquad Y_{bus} = [\text{diag}(s)A_{KN}]^T D[\text{diag}(s)A_{KN}] \tag{3}$$

where D denotes the $n_{br} \times n_{br}$ branch admittance matrix for $\mathcal{G}_0$, diag$(\cdot)$ denotes an operator that takes an $n \times 1$ vector and creates the corresponding $n \times n$ diagonal matrix with the vector elements along the diagonal.

The topology data is crucial for power system operation. It determines the real-time AC power flow model. Assume $\boldsymbol{V}$ denotes the $n_b \times 1$ complex voltage vector, such that $\boldsymbol{V} = V\angle\theta$, where voltage angle and voltage magnitude, θ and V are both $n_b \times 1$ vectors. The AC power flow model for the system can be written as

$$\begin{bmatrix} S_f \\ S_t \\ S_{bus} \end{bmatrix} = \begin{bmatrix} A_{Kf}\boldsymbol{V} \cdot Y_{br}^{*}\boldsymbol{V}^{*} \\ -A_{Kt}\boldsymbol{V} \cdot Y_{br}^{*}\boldsymbol{V}^{*} \\ \text{diag}\,(\boldsymbol{V}) \cdot Y_{bus}^{*}\boldsymbol{V}^{*} \end{bmatrix} \tag{4}$$

where S_f and S_t are $n_{br} \times 1$ "from" and "to" complex power flow vectors, respectively, S_{bus} is $n_b \times 1$ complex power injection vector, $*$ represents the conjugate of vector [9].

This model is used in the subsequent SE module. In AC SE, the "from" and "to" power flow measurements and the power injection measurements of buses with power injection (generation and/or loads) are used to estimate the states. Therefore, a correct topology information ensures the validity of SE results. Once the line status data is altered by attacker, the topology processor will export incorrect topology information, and hence, lead to wrong estimation results.

B. State Estimation

Consider an $n_z \times 1$ vector z of nonlinear measurements given as

$$z = h(x, \mathcal{G}) + e \tag{5}$$

where $x = [\theta,\, V]^T$ is the system state vector, and e is an $n_z \times 1$ noise vector which is independent of x and is modeled as Gaussian distributed with 0 mean and σ_i^2 covariance such that the measurement error covariance matrix is given by $R = diag(\{\sigma_i^2\}_{i=1}^{M})$. The function $h(x, \mathcal{G})$ is a vector of nonlinear functions that describes the relationship between the system states and measurements for a topology $\mathcal{G}$. Both the line status data s and the measurements z are collected by the SCADA system. The commonly obtained measurements in the grid are the active and reactive power flows and bus injections.

We use weighted least-squares (WLS) AC SE to calculate the θ and V [10]. The objective of the estimation process is to minimize the sum of the squares of the weighted deviations of the estimated measurements from z. The states are solved as a least square problem with the following objective function

$$\min J(x) = (h(x) - z)^T R^{-1}(h(x) - z), \tag{6}$$

the solution to which satisfies

$$g(\hat{x}) = \frac{\partial J(\hat{x})}{\partial x} = H^T(\hat{x}) \cdot R^{-1} \cdot (h(\hat{x}) - z) = 0 \tag{7}$$

where the system Jacobian matrix $H = \frac{\partial h(x)}{\partial x} \mid_{x=\hat{x}}$, and $\hat{x}$ is the $2n_b \times 1$ estimated state vectors. The WLS solution for this nonlinear optimization problem can be solved iteratively.

C. Bad Data Detection

Measurements collected by SCADA can contain errors, and hence, undermine the accuracy of estimated states. Therefore, bad data detector should be equipped with SE to detect faulty measurements, and hence, protect SE from large errors. The measurement residual vector is used to detect bad data, as

$$r = z - h(\hat{x}, \mathcal{G}) \tag{8}$$

where r is the $n_z \times 1$ residual vector.

The χ^2-detector is utilized to detect bad data. The threshold is determined by the χ^2-test. To bypass the bad data detection, the residuals should satisfy the following relationship

$$r^T R^{-1} r \leqslant \chi^2_{(m-n),p} \tag{9}$$

where $\chi^2_{(m-n),p}$ is the value from χ^2 distribution tables corresponding to a detection confidence with probability p (*e.g.* 95%) and $m - n$ degrees of freedom.

If the threshold in (9) is violated, largest normalized residual method is further used for bad data identification. The identified bad measurement is removed from the measurement vector and the SE is repeated until no bad data is detected.

III. Attack Model

In an unobservable state-preserving topology attack, the attacker aims to maliciously change the system topology from $\mathcal{G}$ to a different "target" topology $\bar{\mathcal{G}} = \{\mathcal{N}, \bar{\mathcal{E}}\}$ without changing the states. In this paper, we only consider topology attacks that perturb line connection $\mathcal{E}$ to $\bar{\mathcal{E}}$; the attacks aiming to split or merge buses are out of scope, *i.e.*, $\mathcal{N}$ remains unchanged. We define the line with status data changed by attacker as *target line* and the end buses of the target line as *target buses.*

As stated in Section I, topology attacks can be of two types: *line-maintaining* and *line-removing*. For a line-maintaining attack, the attacker maliciously alters the line status data of the target line and injects false data to make it appear that line which is not in the original graph $\mathcal{E}$ is now shown as active in $\bar{\mathcal{E}}$; the opposite is achieved by a line-removing attack. To launch a state-preserving topology attack, the attacker injects $n_{br} \times 1$ line status attack vector b and $n_z \times 1$ measurement attack vector a. The line status attack vector b has entries $b_k \in \{-1, 0, 1\}$ for $k \in \{1, ..., n_{br}\}$ such that $b_k = 1, -1,$ and 0, correspond to line-maintaining, line-removing and no attack cases, respectively. This attack modifies (s, z) for topology $\mathcal{G}$ to $(\bar{s}, \bar{z})$ for topology $\bar{\mathcal{G}}$ such that

$$\bar{s} = s + b, \quad \text{and} \quad \bar{z} = z + a. \tag{10}$$

In the absence of noise, the attack vector satisfies

$$a = h(x, \bar{\mathcal{G}}) - h\left(x, \mathcal{G}\right). \tag{11}$$

For a cyber-based topology attack considered here, when the states are preserved, *i.e.*, unchanged, and the system topology except for the target line remains the same, the attacker needs to change the power flow of the target line. To achieve this, the attacker only needs to change the power flow measurements on the target line and power injection measurements on the target buses to make such attack unobservable.

A. Line-removing vs. Line-maintaining attacks

For line-removing attack, as stated in [5], when the attacker sets the target line status to zero, the "from" and "to" power flow measurements should also be changed to zero. The modified power injection measurements for bus i are

$$\begin{aligned} P_i^a &= P_i - P_{ij} \\ Q_i^a &= Q_i - Q_{ij} \end{aligned} \tag{12}$$

where P_{ij} and Q_{ij} are the physical active and reactive "from" power flows of line ij, respectively. The modified power injection measurements on bus j obey (12), as well. An example of such attack is shown in Fig. 1(a). In this case, to create a precise attack, the line flow P_{ij} and Q_{ij} have to be estimated using all the relevant SCADA measurements. A heuristic way to creating such attacks is to use just the local power flow measurements at both ends of the target line. This is proposed in [5] and the authors have demonstrated its performance via simulation.

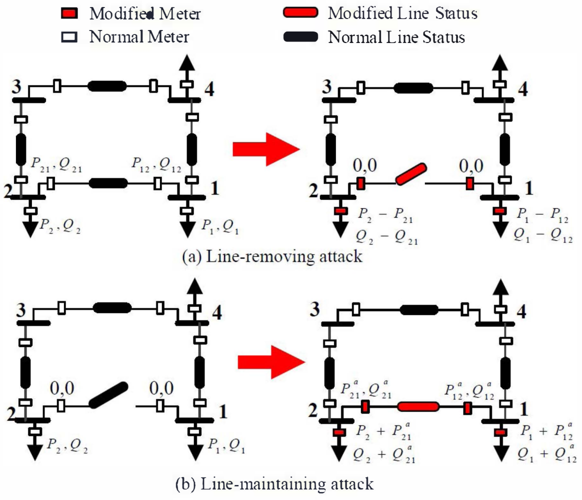
In contrast, we argue that for a line-maintaining attack, such a heuristic will not work. This is because for a line-maintaining attack, the actual "from" and "to" power flows on the target line are already zero since the target line is out. When the attacker sets the target line status to 1, the "from" and "to" power flow measurements should be non-zero since the line appears active at control center. The modified "from" power flow measurements P_{ij}^a and Q_{ij}^a should satisfy

$$\begin{aligned} P_{ij}^a = V_i^2(g_{si} + g_{ij}) - V_iV_j(g_{ij}cos(\theta_i - \theta_j) \\ +b_{ij}sin(\theta_i - \theta_j)) \\ Q_{ij}^a = -V_i^2(b_{si} + b_{ij}) - V_iV_j(g_{ij}sin(\theta_i - \theta_j) \\ -b_{ij}cos(\theta_i - \theta_j)) \end{aligned} \tag{13}$$

where b_{ij} and g_{ij} are the susceptance and conductance of the target line, respectively, b_{si} and g_{si} are the shunt branch susceptance and conductance of bus i, respectively. The modified "to" power flow measurements P_{ji}^a and Q_{ji}^a also obey (13). From (13), we can see that to calculate the false power flow measurements on the target line, the attacker needs to estimate the states. For the power injection measurements for bus i, since the power injection for bus i should equal to the sum of all line power flows from bus i, the measurements should be modified as

$$\begin{aligned} P_i^a &= P_i + P_{ij}^a \\ Q_i^a &= Q_i + Q_{ij}^a \end{aligned} \tag{14}$$

where P_i and Q_i are the physical active and reactive power injection measurements, respectively; P_i^a and Q_i^a are the injection measurements modified by attacker. The power injection measurements on bus j also satisfy the relationship in (14). An example of such an attack is shown in Fig. 1(b).



(a) Line-removing attack

(b) Line-maintaining attack

Fig. 1. Examples of unobservable state-preserving topology attacks.

IV. Unobservable State-preserving Line-maintaining Attacks with Local Information

We assume the attacker has the following capabilities:

1) Attacker has knowledge of the topology $\mathcal{G}$ of the entire network.
2) Attacker has the capability to observe measurements only for a sub-network $\mathcal{S}$ of $\mathcal{G}$ and perform SE for $\mathcal{S}$. The choice of $\mathcal{S}$ is described in detail in the sequel.
3) Attacker has the capability to change both the line status data of the target line and the measurements on both target line and target buses.

For the system, we assume that the power system is observable prior to the attack.

For nonlinear measurement model and AC SE, the attacker cannot construct a only with the knowledge of system configuration. In fact, recent work in [3], [4] show that attack vector constructed with DC measurement model can be detected when the system uses AC SE. To this end, we model a sophisticated attacker who attacks the line status data and measurements of the target line and the power injection measurements on the end buses of target line (target buses) by first estimating the system states $\hat{x}_{\mathcal{S}}$ for $\mathcal{S}$ using AC SE. Let $I_{\mathcal{T}}$ represent the set of measurements the attacker needs to modify to launch an attack. The resulting modified measurement vector $\bar{z}$ input to SE has entries

$$\bar{z}_i = \begin{cases} z_i\,, & i \notin I_{\mathcal{T}} \\ h_i(\hat{x}_{\mathcal{S}}, \bar{\mathcal{G}})\,, & i \in I_{\mathcal{T}} \end{cases} \tag{15}$$

For line-maintaining attacks, equations (13)–(14) imply that the voltage magnitudes and voltage angle difference of the target buses are required to form the unobservable attack vector. Thus, the attacker has to obtain a good estimate of the voltage magnitudes and voltage angle difference of the target buses. Since the target line is physically disconnected, the attacker needs to find a sub-network of the physical system to estimate states on the target buses. Such a sub-network should contain at least one physical path that connects the two target buses. By using power flow measurements on the lines of the path, attacker can estimate the voltage magnitudes and voltage angle differences of the buses on the path, and thus, obtain a good estimate of the states of the target buses. For clarification, consider the example shown in Fig. 2. In this case, the target line is the line connecting bus 1 and 2. The goal of attacker is to obtain a good estimate of states on target buses 1 and 2. Assume bus 1 is the reference bus. Attacker can use power flow measurements on the line connecting bus 1 and 4 to calculate V_4 and $\triangle\ \theta_{14} = \theta_1 - \theta_4$. Then, the V_3 and $\triangle\ \theta_{43} = \theta_4 - \theta_3$ can be estimated with power flow measurements on the line connecting bus 4 and 3 and the estimated $V_4\angle\theta_4$. It is the same for estimation of V_2 and $\triangle\ \theta_{32} = \theta_3 - \theta_2$. Then, attacker can obtain a good estimation of voltage magnitudes V_1 and V_2, and voltage angle difference$\triangle\ \theta_{12}$ =$\triangle\ \theta_{14}$+ $\triangle\ \theta_{43}$+ $\triangle\ \theta_{32}$, and hence, calculate the modified measurements.

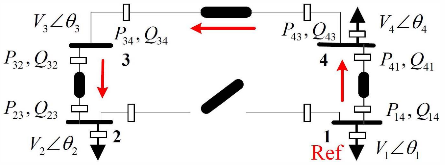


Fig. 2. Illustration of a sub-network for unobservable state-preserving attack

For a specific target line, there are multiple paths between the two target buses in the system. To reduce the cost of attacks, attacker needs to analyze the system topology $\mathcal{G}$ and find the shortest path between the two target buses. Thus, the attack can be launched by estimating a minimal set of measurements.

We use a BFS algorithm to identify the shortest path that connects the target buses. The *minimal observation sub-network* $\mathcal{S}$ denotes the connectivity of the buses and lines on the shortest path. The physical power grid $\mathcal{G}$ is represented as an unweighted and undirected graph in which an edge is a line and a node is a bus. We assign one of the target buses as the *starting bus* and the remaining target bus is the *destination bus*. The procedure to determine $\mathcal{S}$ is as follows:

Algorithm 1 BFS for shortest path connecting target buses

Input: $\mathcal{G}$, *starting bus*, *destination bus*

Output: shortest path connecting the *starting bus* and the *destination*

1) Set the *starting bus* as the *in progress bus* and the rest buses as *unvisited buses*. Set the level of the current set of *in progress buses* as $k = 0$.
2) Search all *unvisited buses* that are connected (by a branch) to the set of *in progress buses*. Mark such *unvisited buses* as the *in progress buses* and the previous set of *in progress buses* as *visited buses*. Set the level of the current set of *in progress buses* as $k = k + 1$. If the *destination bus* is in the set of *in progress buses*, that means the *shortest path tree* has been identified, go to step 3. Otherwise, repeat step 2.
3) Backtrack from the *desination bus* to the *starting bus* level-by-level, and identify the shortest path. If there is more than one shortest path, repeat step 3 until all shortest paths are identified.

Once $\mathcal{S}$ is found, the attacker can assign one of the target buses as a slack bus, collect and use the power flow measurements $z_{\mathcal{S}}$ for all buses and lines in $\mathcal{S}$ to perform local SE to minimize the estimate error as:

$$J_{\mathcal{S}}(x_{\mathcal{S}}) = (h(x_{\mathcal{S}}, \mathcal{S}) - z_{\mathcal{S}})^T R_{\mathcal{S}}^{-1}(h(x_{\mathcal{S}}, \mathcal{S}) - z_{\mathcal{S}}), \tag{16}$$

for which the solution is

$$g(\hat{x}_{\mathcal{S}}) = \frac{\partial J(\hat{x}_{\mathcal{S}})}{\partial x_{\mathcal{S}}} = H^T(\hat{x}_{\mathcal{S}}) \cdot R_{\mathcal{S}}^{-1} \cdot (h(x_{\mathcal{S}}, \mathcal{S}) - z_{\mathcal{S}}) = 0 \tag{17}$$

where $H = \frac{\partial h(x_{\mathcal{S}}, \mathcal{S})}{\partial x_{\mathcal{S}}} \mid_{x_{\mathcal{S}} = \hat{x}_{\mathcal{S}}}$ is the system Jacobian matrix. The WLS solution for this nonlinear optimization problem can be solved iteratively. Then attacker can calculate the modified measurements with (15).

Since the power system is a complex geographically distributed network, attacker may be limited to a subset of the network static topology. Under such conditions, this method can also be applied to find the minimal observation sub-network.

In practice, to launch an unobservable state-preserving line-maintaining attack, attackers are limited to finite sets of target lines due to the following reasons:

1) The power injection measurements can only be altered by redistributing loads in cyber layer. Attacker cannot change generator output data due to direct communication between control center and power plant.
2) The power injection for no load buses cannot be altered, since load occurring in no load buses can be immediately detected by operator.
3) Any attacks that can lead to negative loads in cyber layer can be detected.

4) The significant alteration of the system such as system dividing to several islands (line-removing attack) or islands combining to a whole system (line-maintaining attack) can lead to operator's intervention.

Therefore, to launch a successful line-maintaining attack, attacker should analyze the system topology and operation states prudently to choose a target line. The following three classes of lines should be avoided as target lines:

1) Single critical line or critical pairs of lines.
2) Lines that once being attacked can lead to negative loads in cyber layer.
3) Lines that connected to no load buses.

In Section V, we illustrate the attack design and the algorithm performance with an IEEE 24-bus reliable test system (RTS).

V. Numerical Results

In this section, we use the IEEE 24-bus RTS shown in Fig. 3 as the test system. We assume that the measurements in the test system are: (a) active and reactive power flows on both ends of all lines; and (b) active and reactive power injection on buses with loads and/or generation; *i.e.*, overall, the number of total measurements in the test system is 192. We run our simulations with MATLAB R2014a and MATPOWER 4.1.

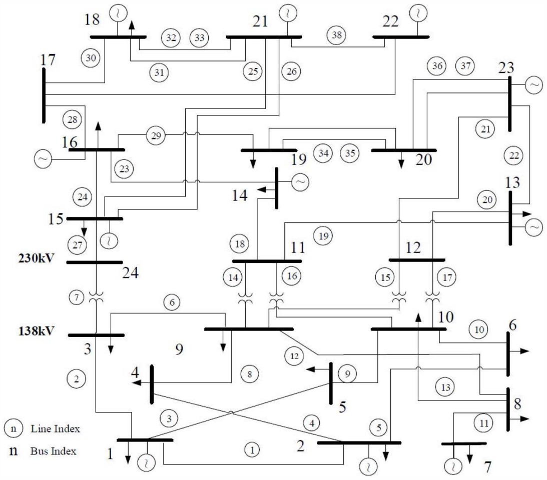


Fig. 3. IEEE 24-bus reliable test system.

A. Feasible Target Line Selection

In this subsection, we analyze the test system to identify all feasible target lines for unobservable state-preserving line-maintaining attacks. We first exclude critical lines and the lines that connected to a no load buses in the system. For the rest lines, we perform a whole network SE and use the estimated states to calculate the attack vector. We check the modified loads in cyber layer for each line and exclude the lines that can lead to negative loads. TABLE I demonstrates all the lines we exclude from the set of feasible target lines and the reason for exclusion. Overall, for line-maintaining attacks, there are 8 feasible target lines in the test system, for which the line indices are #2, #5, #8, #9, #12, #13, #34, #35.

TABLE I. Classification of infeasible target lines for undetectable state-preserving line-maintaining attack

Infeasible Reason	Infeasible Target Line
Critical Line	#11
Connect to No Load Bus	#7, #14−#22, #25−#28, #30−#33, #36−#38
Lead to Negative Load	#1, #3, #4, #6, #10, #23, #24

B. Minimal Observation Sub-network

In this subsection, we exhaustively illustrate the minimal observation sub-network of each feasible target line according to the algorithm introduced in Section IV. The details of each minimal observation sub-network for each target line are demonstrated in TABLE II. The minimal number of lines and buses (denote as n_{Sl} and n_{Sb}, respectively) inside the minimal observation sub-network for each target line is illustrated in Fig. 4. That is the minimal information the attacker needs to observe before launching a successful attack. Since the system is under full monitoring redundancy, there are 4 measurements which are active and reactive power flow measurements on both "from" and "to" ends placing on a line. Therefore, the minimum number measurements the attacker needs to access is the minimum number of observation measurements along the path, as well as the measurements placed on the target line and the target buses, *i.e.*, $4n_{Sl} + 8$.

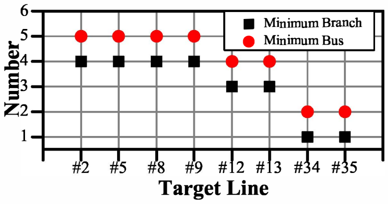


Fig. 4. Number of branches and buses of the minimal observation sub-network of each target line

TABLE II. Minimal observation sub-network for all feasible target lines

Target Line #	Branches of Minimal Observation Sub-network	Connectivity of Buses
2	#1, #4, #8, #6	1⇒2⇒4⇒9⇒3
5	#1, #3, #9, #10	2⇒1⇒5⇒10⇒6
8	#4, #1, #5, #6	4⇒2⇒1⇒3⇒9
9	#3, #1, #5, #10	5⇒1⇒2⇒6⇒10
12	#13, #16, #14	8⇒10⇒11⇒9
13	#12, #14, #16	8⇒9⇒11⇒10
34	#35	19⇒20
35	#34	19⇒20

From these results, we can see that the minimal observation sub-network for each target line is relatively small compared with the whole network topology even for a small system such as IEEE 24-bus RTS. The largest minimal observation sub-network in the test system consists of 4 branches and 5 buses, in which the total observation measurements number is 16. The number of measurements of this sub-network that attacker need to access inside is 24, which is 12.5% of the test system. Therefore, it is possible for attacker to launch such attacks with only a small subset of information of the system.

C. Undetectability of Attacks

In this subsection, we test the unobservable state-preserving line-maintaining attacks with both global information and local information on the test system. In our simulation, we use MATPOWER to generate measurements and perform state estimation. The default setting of the IEEE 24-bus system in MATPOWER is utilized for simulation. We assume the system is operating under optimal power flow and the loads of the system are constant. The errors for all measurements are assumed to be $e_i \sim N\left(0,\, 0.01\right)$ and the χ^2 detector threshold is chosen for a 95% confidence in detection.

We test 1000 trials for each target line with two attack regimes, *global information regime* and *local information regime*. The global information regime is that attacker can observe all measurements in the system and perform AC SE with whole network topology and measurements. While the local information regime is that attacker can only observe the measurements inside the minimal sub-network $\mathcal{S}$ and perform AC SE with topology and measurements of $\mathcal{S}$. In each trial, the measurements are generated by adding random Gaussian noise to the actual power flows and injections of the test system. The attacker first uses both global and local information regime to obtain the estimated states. Then the attack vectors are calculated with both regimes, and added to the corresponding measurements to get two sets of corrupted measurements. We use these corrupted measurements to perform AC SE of the whole network to obtain residuals and use χ^2-test with the residuals. If the residual is greater than the threshold, we assume this trial as detected trial. We calculate the detection probability as $p_{\text{detection}} = \frac{\#\text{detection trials}}{\#\text{trials}}$. The detection probabilities of attacks with both global information and local information for each target line are demonstrated in Fig. 5. The blue dash and dot line represents the 5% false alarm constraint of the χ^2 detector.

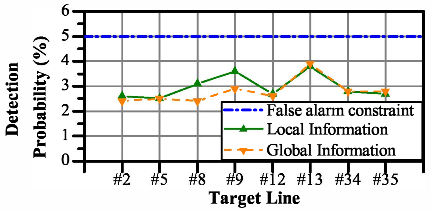


Fig. 5. Detection probability (1000 trials) of unobservable state-preserving line-maintaining attacks on both global information and local information (false alarm const. = 5%)

From Fig. 5, we can see that for most target lines, the detection probabilities of attacks generated with global information are lower than those with local information. However, both of them are lower than the false alarm constraint, which means the proposed attacks will not be detected.

VI. Conclusion and Future Work

In this paper, we focus on unobservable state-preserving topology attacks, especially the line-maintaining attacks. We propose an algorithm based on BFS to find the minimum local information required to perform such attacks. We have shown that our proposed algorithm can enable an attacker to obtain the localized topology and corresponding measurement data to mount an attack that bypasses bad data detector and successfully changes topology information of the system in the cyber layer.

One possible extension is to study a more sophisticated class of topology attacks in which both topology information and system states are changed by attacker in an unobservable manner. Moreover, we will also study the consequences of topology attacks on physical power system. It is crucial to identify the anomalies caused by such unobservable topology attacks in modules subsequent to SE, and thereby, develop the detection modules and resiliency mechanisms to detect and mitigate such topology attacks.

References

[1] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ser. CCS '09, Chicago, Illinois, USA, 2009, pp. 21–32.

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

[3] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012.

[4] J. Liang, O. Kosut, and L. Sankar, "Cyber-attacks on ac state estimation: Unobservability and physical consequences," in *IEEE PES General Meeting*, Washington, DC, July 2014.

[5] J. Kim and L. Tong, "On topology attack of a smart grid," in *Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES*, Washington, DC, February 2013, pp. 1–6.

[6] M. Rahman, E. Al-Shaer, and R. Kavasseri, "Impact analysis of topology poisoning attacks on economic operation of the smart power grid," in *Distributed Computing Systems (ICDCS), 2014 IEEE 34th International Conference on*, June 2014, pp. 649–659.

[7] A. Ashok and M. Govindarasu, "Cyber attacks on power system state estimation through topology errors," in *Power and Energy Society General Meeting, 2012 IEEE*, July 2012, pp. 1–8.

[8] S. Even, *Graph Algorithms (2nd ed)*. Cambridge University Press, 2011.

[9] R. D. Zimmerman and C. E. Murillo-Sánchez, "Matpower 5.1 user's manual," 2015.

[10] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*. New York: CRC Press, 2004.