Measurement-driven blind topology estimation for sparse data injection attack in energy system

Highlights

Measurement-driven Blind Topology Estimation for Sparse Data Injection Attack in Energy System

Adnan Anwar,Abdun Naser Mahmood,Zahir Tari,Akhtar Kalam

- The existing works on sparse unobservable attacks where it is assumed that power grid topology [21, 18] or the complete Jacobian matrix [26, 14, 30] is known to the attacker, this work assumes that the attacker has no access to the grid topology matrix or the Jacobian matrix. With the aid of the estimated topology, sparse unobservable attack vectors are then constructed using a completely data-driven approach, which does not require any prior grid information.
- This article solves the unique problem of identifying the topology from the measurement signals only which is later used for adversarial attack analyses. To this end, based on the structural properties of the grid topology matrix, the blind estimation of the topology matrix is modelled as a constraint optimization problem which is then solved using ADMM considering the measurement signals only.
- This paper proposes a novel initialization approach that significantly enhances the estimation accuracy when compared with existing and random initialization approaches.
- This work also utilizes measures from the complex network theory in order to compare the estimation performance. This work demonstrates that the topology of the physical grid can be revealed using the measurement data obtained from the cyber domain.

Measurement-driven Blind Topology Estimation for Sparse Data Injection Attack in Energy System

Adnan Anwar[a], Abdun Naser Mahmood[b], Zahir Tari[c] and Akhtar Kalam[d]

[a]*School of Information Technology, Deakin University, Geelong 3216, Strategic Centre for Cyber Security Research Institute (CSRI), Australia*
[b]*School of Engineering and Mathematical Sciences, La Trobe University, VIC 3086*
[c]*Computer Science and Software Engineering, RMIT University, VIC 3000*
[d]*College of Engineering and Science, Victoria University, Footscray, VIC 3011*

ARTICLE INFO

Keywords:
topology estimation
FDI Attack
measurement
state estimation

ABSTRACT

Smart grid cyber-security has come to the forefront of national security priorities due to the emergence of new cyber threats such as the False Data Injection (FDI) attack. This specific type of attack modifies smart grid measurements to produce wrong system states during the state estimation which is a critical operational functionality. While most of the existing works assume that power grid topology or the Jacobian matrix (that represents measurement and state relationship) is known to the attacker, this work shows that an intelligent attacker can construct a data-driven sparse FDI attack which does not require prior knowledge of system Jacobian or grid topology. In this paper, we show how the power grid topology, which is an important information for sparse attack construction, can be revealed using only measurement signals. The blind topology estimation is formulated as a constrained optimisation problem. The alternating direction method of multipliers (ADMM) is then employed with a novel initialization process for solving this complex problem. The comparative evaluation using graph-theoretic measures indicates that the power grid topology can be revealed with very high accuracy using such an approach. For example, average eigenvalue centrality measures and degree centrality measures show that the estimated topology is around 95.82% and 94.99% accurate compared to the actual topology for the IEEE-14 bus system and 86.47% and 96.34%, respectively for IEEE-30 bus system. Finally, based on the estimated topology we determine the critical set of measurements, which are then utilised for sparse attack construction. We show that only 7.40% and 3.57% sensors are required to construct the sparsest stealthy attacks for the IEEE 14 bus and the 30 bus system, respectively. The findings of this research conclude that an intelligent attacker can construct a very sparse 'stealthy' attack, that can degrade the operational performance significantly, by manipulating a few sensor devices only without any prior system knowledge or information.

1. Introduction

In recent years, the smart grid has been proven vulnerable to sophisticated cyber-attacks [2, 5, 17]. False data injection (FDI) attack is a new type of data integrity attack similar to the man-in-the-middle (MITM) or spoofing attack which has been highlighted in recent smart grid cyber-security researches due to its stealthiness and possible adverse impacts on the power system operation [35, 1, 6]. This class of attacks exploits the sensor (e.g., phasor measurement units) measurements by injecting false information about the grid conditions [1, 26]. As measurement data are widely used in different key operational modules (e.g., state estimator), any corruption in measurements will affect the operational decisions [26, 11]. To ensure data integrity, bad data detectors (BDD) are used in an energy operation centre which detects the presence of any corrupted data by calculating the difference between the measured and estimated system states obtained from the state estimation process. As a result of the strategic FDI injection, the state vectors (e.g., voltage angles) calculated using the state estimation process will be incorrect and misleading. However, due to the intelligent way of choosing the attack vector, the norm of the residual obtained from the state estimation module will appear to be very close to the normal behavior, e.g., the case when there is no false injection [26, 3]. Hence, the attack remains undetected in the existing BDD module. As the obtained states are wrong (which does not correspond to actual physical states of the power grid), any operational decision based on those may have an adverse effect on the power system operation.

Most of the existing stealthy FDI attack strategies assume that the attacker has prior knowledge of system parameters such as line reactance, bus and line connectivity [26, 19, 30]. In practice, it is very difficult to obtain these sensitive information for the following reasons:

a) Obtaining the power system parameters involves getting access to the grid topology maps through intruders or former employees, which is very difficult and challenging for a remote attacker;

b) Power system topological connectivity and electric parameter information are typically stored in a highly secured database server;

c) Historical data of the system topology matrix and parameter information obtained by an insider may be outdated

adnan.anwar@deakin.edu.au (A. Anwar); A.Mahmood@latrobe.edu.au (A.N. Mahmood); zahir.tari@rmit.edu.au (Z. Tari); akhtar.kalam@vu.edu.au (A. Kalam)

www.deakin.edu.au/about-deakin/people/adnan-anwar (A. Anwar); https://scholars.latrobe.edu.au/display/amahmood (A.N. Mahmood); www.rmit.edu.au/contact/staff-contacts/academic-staff/t/tari-professor-zahir (Z. Tari); https://www.vu.edu.au/research/akhtar-kala (A. Kalam)

ORCID(s): 0000-0003-3916-1381 (A. Anwar)

and irrelevant (cannot be used to construct stealthy attack) if the system operating condition changes (e.g., topology reconfiguration) [32, 31].

For these reasons, FDI attack that requires prior knowledge of the energy system Jacobian may not be feasible. Consequently, the attacker may seek an alternative idea of stealthy attack construction based on the measurement data only [33, 20].

Recently, Yu et al. [33] and Kim et al. [20] have demonstrated a *blind* attack construction strategy that does not rely on any prior power system topological and electric line parameter information as required by other FDI attacks [26, 19, 30]. In the blind approaches, the attack is constructed based on the subspace information of the measurements. Yu et al. [33] propose a principal component analysis (PCA) and Kim et al. [20] propose a singular value decomposition (SVD) based subspace estimation technique for stealthy attack construction. In [33], the adversary requires to inject all measurement devices for stealthy attack construction. However, a more practical assumption is that the attacker is most likely able to compromise a limited number of measurement devices [26, 14, 30]. A stealthy FDI attack that requires only a few sensors is called *sparse unobservable FDI attack* or simply *sparse attack* [26, 14, 30]. A sparse attack is more difficult to construct because it involves finding a sparse attack vector that remains hidden in the BDD.

There have been few works related to the sparse attacks. Kosut et al. in [21] relate the sparse attacks with network observability and establish a close connection between them. Authors show that the existence of the sparse attack vector depends on the information of the energy grid topological connectivity but not on the electric parameters (e.g., line admittance value). Several work have considered the graph-theoretic analysis using the 'known' power grid topology to demonstrate the successful construction of sparse unobservable attack [21, 18]. However, in contrast to the previous researches, we consider a more realistic situation where the power grid topology is not known to the attacker. To this end, we propose a methodology to reveal the power grid topology based on a data-driven approach using measurement signals only and then utilize it for sparse FDI attack construction. Although some prior works aim to estimate the topology of the power grid [24, 4, 16, 23, 25], none of these researchers investigated the possibility of stealthy attack generation based on the estimated topology. The contribution of this work is listed as follows:

1. In contrast to existing work on sparse unobservable attacks (where it is assumed that power grid topology [21, 18] or the complete Jacobian matrix [26, 14, 30] is known to the attacker), this work assumes that the attacker has no access to the grid topology matrix or the Jacobian matrix. With the aid of the estimated topology, sparse unobservable attack vectors are then constructed using a completely data-driven approach, which does not require any prior grid information. The theory is presented in Section III and experimental evaluation is given in Section IV.C.
2. This article solves the unique problem of identifying the topology from the measurement signals only, which is later used for adversarial attack analyses. To this end, based on the structural properties of the grid topology matrix, the blind estimation of the topology matrix is modelled as a constraint optimization problem which is then solved using ADMM considering the measurement signals only (in Section II.A-II.C).
3. This paper proposes a novel initialization approach that enhances the estimation accuracy significantly when compared with existing and random initialization approaches (demonstrated in Section II.D).
4. This work also utilizes measures from the complex network theory in order to compare the estimation performance (see Section IV.A for comparison). This work demonstrates that the topology of the physical grid can be revealed using the measurement data obtained from the cyber domain.

2. Topology Estimation

In a normal operating condition, the topology of the energy grid remains static. Some related works addressed the challenges of topology estimation [23, 25]. In [24], Li et al. show that the topology of the energy grid can be approximately revealed solely using the correlations of a number of measurement signals obtained from power injection sensors. This process does not require any intervention of the system states. A detailed explanation can be obtained from *Theorem 2* of [24] as proof. This emerging yet challenging problem of topology estimation is possible because of the rich structure of $\mathbf{H}$ matrix that has the following properties, *symmetric* ($\mathbf{H} = \mathbf{H}^T$), *positive semi-definiteness* ($\mathbf{H} \geq \mathbf{0}$) and *null space* ($\mathbf{H1} = \mathbf{0},$ and $\mathbf{H}^T\mathbf{1} = \mathbf{0}$). Let us consider, power injection measurement vector is denoted by $\mathbf{z}$, which is a subset of complete measurement vector $\mathbf{z}_t$. Considering t observations of the injection measurement vectors, the dimension of the measurement matrix $\mathbf{Z}$ becomes a $(N+1) \times t$ matrix. For these t observations, consider the state matrix (voltage angles for DC power flow model) as $\mathbf{\Theta}$ with a structure of $(N+1) \times t$. By assuming $\mathbf{E}$ is the noise matrix, one can write the original measurement model as below:

$$\mathbf{Z} = \mathbf{H\Theta} + \mathbf{E} \tag{1}$$

According to power system load flow theory, the reference bus voltage angle is always considered zero. Hence, $\theta_{\mathbf{ref}} = \mathbf{0}$. By assuming the reference (slack) bus is the first bus, the equality constraint becomes

$$\mathbf{\Theta}^T\mathbf{1}_{ref} = \mathbf{0} \tag{2}$$

Here $\mathbf{1_{ref}}= [1, 0, 0, ..., 0]^T$. for the blind estimation of the $\mathbf{H}$ matrix based on the measurement matrix $\mathbf{Z}$, the system state matrix $\mathbf{\Theta}$ needs to be a full rank matrix, which implies $t \geq N$ with the rank($\mathbf{\Theta}$)= N [24].

2.1. Proposed Solution for Topology Estimation

The power grid topology matrix has some properties including its positive semi-definiteness nature with the null space property, and the matrix is also symmetric. Now, considering the above properties and additional constraints like the slack bus equality constraint of Eqn. 2, we can model the the topology estimation problem as a constraint optimization problem with the sparsity regularization as follows:

$$\begin{aligned} &\min_{\mathbf{H},\mathbf{\Theta}} \|\mathbf{Z}-\mathbf{H\Theta}\|_F^2 + \lambda\|\mathbf{H}\|_1 \\ s.t.\ &\mathbf{H}=\mathbf{H}^T,\ \mathbf{H}\geq\mathbf{0},\ \mathbf{H1}=\mathbf{0},\ \mathbf{H}^T\mathbf{1}=\mathbf{0} \end{aligned} \tag{3}$$

In the above formulation, the regularization parameter for sparsity is defined using λ. In the above formulation, the matrix $\mathbf{H}$ is basically sparse which is bounded by a number of structural equality and inequality constraints presented in Eqn. 3.

2.2. Topology Estimation

To solve the optimization problem defined in Eqn. 3, we use ADMM. According to the definition of ADMM, if $f(x)$ and $g(z)$ are two convex functions which are separable, then ADMM formulation is as belows:

and their convex set $\mathcal{X}$ and $\mathcal{Z}$ respectively, ADMM forms the problem as below [9]:

$$\begin{aligned} &\min_{\mathbf{x}\in\mathcal{X},\mathbf{z}\in\mathcal{Z}} f(\mathbf{x})+g(\mathbf{z}) \\ &\mathbf{Ax}+\mathbf{Bz}-\mathbf{c}=\mathbf{0} \end{aligned} \tag{4}$$

Now, considering the formulation using augmented Lagrangian, the equation is rewritten as:

$$\begin{aligned} L_\rho(\mathbf{x},\mathbf{z},\mathbf{y}) = f(\mathbf{x}) + g(\mathbf{z}) + \mathbf{y}^T(\mathbf{Ax}+\mathbf{Bz}\text{ - }\mathbf{c}) \\ + (\rho/2)\|\mathbf{Ax}+\mathbf{Bz}\text{ - }\mathbf{c}\|_2^2 \end{aligned} \tag{5}$$

In the above formulation, y represents the dual variable whereas ρ represents the augmented Lagrangian parameter. In the above formulation, x and z are the two primal variables. The update steps for x and z are as follows [9]:

$$\mathbf{x}^{k+1} := \arg\min\nolimits_{\mathbf{x}} L_\rho(\mathbf{x},\mathbf{z}^k,\mathbf{y}^k) \tag{6a}$$

$$\mathbf{z}^{k+1} := \arg\min\nolimits_{\mathbf{z}} L_\rho(\mathbf{x}^{k+1},\mathbf{z},\mathbf{y}^k) \tag{6b}$$

Then the update for dual variable will follow [9]:

$$\mathbf{y}^{k+1} := \mathbf{y}^k + \rho(\mathbf{Ax}^{k+1}+\mathbf{Bz}^{k+1}-\mathbf{c}) \tag{7}$$

where $\rho > 0$. Considering $\boldsymbol{\mu} = (1/\rho)\mathbf{y}$, ADMM iteration steps described above can be written in a scaled form as below:

$$\mathbf{x}^{k+1} := \arg\min_{\mathbf{x}\in\mathcal{X}} f(\mathbf{x}) + \frac{\rho}{2}\|\mathbf{Ax}+\mathbf{Bz}^k-\mathbf{c}-\boldsymbol{\mu}^k\|_2^2 \tag{8a}$$

$$\mathbf{z}^{k+1} := \arg\min_{\mathbf{z}\in\mathcal{Z}} g(\mathbf{z}) + \frac{\rho}{2}\|\mathbf{Ax}^{k+1}+\mathbf{Bz}-\mathbf{c}-\boldsymbol{\mu}^k\|_2^2 \tag{8b}$$

$$\boldsymbol{\mu}^{k+1} := \boldsymbol{\mu}^k + \mathbf{Ax}^{k+1} + \mathbf{Bz}^{k+1} - c \tag{8c}$$

Now, the above ADMM formulation is used to reveal the topology of the energy grid blindly based on measurement signals only.

2.3. Formulation for Topology Estimation

The problem which we have defined previously in Eqn. 3 can be represented using ADMM in the below form:

$$\min_{\mathbf{H},\mathbf{\Theta},\mathbf{\Pi},\mathbf{\Psi},\mathbf{\Pi}\geq\mathbf{0}} \|\mathbf{Z}-\mathbf{H\Theta}\|_F^2 + \lambda\|\mathbf{\Pi}\|_1 + g(\mathbf{\Psi}) \tag{9a}$$

$$s.t.\ \mathbf{\Theta}-\mathbf{\Psi}=\mathbf{0} \tag{9b}$$

$$\mathbf{H}-\mathbf{\Pi}=\mathbf{0} \tag{9c}$$

$$\mathbf{H1}+\mathbf{1H}=0 \tag{9d}$$

In the above formulation g represents the indicator function of $\{\mathbf{\Psi}|\mathbf{\Psi}^T\mathbf{1}_{ref}=\mathbf{0}\}$, which ensures that the first row of $\mathbf{\Psi}$ becomes zero. At first we form the augmented Lagrangian $L_\rho(\mathbf{H},\mathbf{\Theta},\mathbf{\Pi},\mathbf{\Psi};\boldsymbol{\mu},\boldsymbol{\nu},\boldsymbol{\omega})$ following Eqn. 5. As described in Eqn. 8, the update iterations can be formulated as:

$$\mathbf{\Theta}_{i+1} := \arg\min_{\mathbf{\Theta}} \|\mathbf{Z}-\mathbf{H}_i\mathbf{\Theta}\|_F^2 + \frac{\rho}{2}\|\mathbf{\Theta}-\mathbf{\Psi}_i+\boldsymbol{\mu}_i\|_2^2 \tag{10}$$

The solution of the above equation will be as below:

$$\mathbf{\Theta}_{i+1} := (2\mathbf{H}_i\mathbf{H}_i^T+\rho\mathbf{I})^{-1}(2\mathbf{H}_i^T\mathbf{Z}+\rho\mathbf{\Psi}_i-\rho\boldsymbol{\mu}_i) \tag{11}$$

Then, $\mathbf{\Psi}$ will follow the below updated step,

$$\mathbf{\Psi}_{i+1} := \prod(\mathbf{\Theta}_{i+1}+\boldsymbol{\mu}_i) \tag{12}$$

$\prod$ is operator that indicates the projection onto $\{\mathbf{\Psi}|\mathbf{\Psi}^T\mathbf{1}_{ref}=\mathbf{0}\}$. It means that each element of the first row of $\mathbf{\Psi}$ is equal to zero and the remaining elements are the same. Next, the topology matrix $\mathbf{H}$ is updated as:

$$\begin{aligned} \min_{\mathbf{H}} \|\mathbf{Z}-\mathbf{H\Theta}_{i+1}\|_F^2 + \frac{\rho}{2}\|\mathbf{H}-\mathbf{\Pi}_i+\boldsymbol{\nu}_i\|_F^2 + \\ \frac{\rho}{2}\|\mathbf{H1}+\mathbf{1H}+\boldsymbol{\omega}_i\|_F^2 \end{aligned} \tag{13}$$

The solution of the above equation becomes:

$$\begin{aligned} \mathbf{H}_{i+1} := [2\mathbf{\Theta}_{i+1}\mathbf{\Theta}_{i+1}^T + \rho\mathbf{I} + \frac{\rho}{N}\mathbf{1}^T\mathbf{1}]^{-1} \\ [2\mathbf{\Theta}_{i+1}\mathbf{Z}^T + \rho(\mathbf{\Pi}_i-\boldsymbol{\nu}_i-\boldsymbol{\omega}_i)] \end{aligned} \tag{14}$$

Next, we do the optimization with respect to $\mathbf{\Pi}$ that converts the problem as below:

$$\min_{\mathbf{\Pi},\mathbf{\Pi}\geq\mathbf{0}} \lambda\|\mathbf{\Pi}\|_1 + \frac{\rho}{2}\|\mathbf{H}_{i+1}-\mathbf{\Pi}+\boldsymbol{\nu}_i\|_F^2 \tag{15}$$

The solution of the above formulation is provide in [9]:

$$\mathbf{\Pi}_{i+1} = \mathcal{S}_{\lambda/\rho}(\mathbf{H}_{i+1}+\boldsymbol{\nu}_i) \tag{16}$$

where $\mathcal{S}$ is defined as a soft-thresholding operator as follows:

$$\mathcal{S}_\epsilon(x) := \begin{cases} x-\epsilon * sign(x), & \text{if } |x|>\epsilon \\ 0 & \text{if } |x|\leq\epsilon \end{cases} \tag{17}$$

Finally, the below update steps are used for dual variables:

$$\begin{aligned} \boldsymbol{\mu}_{i+1} &= \boldsymbol{\mu}_i + (\mathbf{\Theta}_{i+1}-\mathbf{\Psi}_{i+1}) \\ \boldsymbol{\nu}_{i+1} &= \boldsymbol{\nu}_i + (\mathbf{H}_{i+1}-\mathbf{\Pi}_{i+1}) \\ \boldsymbol{\omega}_{i+1} &= \boldsymbol{\omega}_i + (\mathbf{H}_{i+1}\mathbf{1}+\mathbf{1H}_{i+1}) \end{aligned} \tag{18}$$

2.4. Initialization of the H matrix

For a static topology matrix, one can observe the variations in the measurement signals which is basically observed because of the variations in the underlying system states. Previously, [13, 33, 20] identified that the correlations among multiple observations of power flow measurements can provide critical information related to the grid topology matrix. Consider, the measurement model represented using Eqn. (1). Now, we obtain the covariance matrix ($\Sigma_{\mathbf{Z}}$) of the measurements $\mathbf{Z}$ as follows [20]:

$$\Sigma_{\mathbf{Z}} \triangleq \mathbf{H}\Sigma_{\mathbf{\Theta}}\mathbf{H}^T + \sigma^2\mathbf{I} \tag{19}$$

where, $\Sigma_{\mathbf{\Theta}}$ is the covariance of $\mathbf{\Theta}$. Under noiseless assumption, $\Sigma_{\mathbf{Z}}$ can be approximated as $\mathbf{H}\Sigma_{\mathbf{\Theta}}\mathbf{H}^T$. So, Eqn. 19 becomes,

$$\Sigma_{\mathbf{Z}} \approx \mathbf{H}\Sigma_{\mathbf{\Theta}}\mathbf{H}^T \tag{20}$$

If the column space of any matrix is represented as $C(.)$, then $C(\mathbf{H}\Sigma_{\mathbf{\Theta}}\mathbf{H}^T)$ is the equivalent of column space $C(\mathbf{H})$ [20]. As our aim is to estimate $\mathbf{H}$ using the procedure discussed in the above sections, we initialize the topology matrix $\mathbf{H}$ with the covariance matrix of the measurement signals ($\Sigma_{\mathbf{Z}}$). Therefore,

$$\mathbf{H}_{ini} = \Sigma_{\mathbf{Z}} \tag{21}$$

where, $\Sigma_{\mathbf{Z}} = \mathbb{E}[(\mathbf{Z}_{inj} - \mathbb{E}[\mathbf{Z}_{inj}])(\mathbf{Z}_{inj} - \mathbb{E}[\mathbf{Z}_{inj}])^T]$ and $\mathbb{E}[.]$ is the expected value.

3. Sparse Unobservable Attack Construction

The attack vector $\boldsymbol{a}$ constructs a *sparse unobservable attack* if $\boldsymbol{a}$ is sparse in nature and satisfies the 'attack feasibility condition', which is represented using equation $\boldsymbol{a} = \mathbf{H}\boldsymbol{c}$ [26, 21]. Here, c is a random vector with the same column length of $\mathbf{H}$ [26]. Being a sparse attack vector, $\boldsymbol{a}$ has very few nonzero components. In other words, only a few sensors need to be compromised. We say, $\boldsymbol{a}$ is a k-sparse unobservable attack vector if $\boldsymbol{a}$ comprises of k specific measurements which satisfy the condition that upon removing the measurements corresponding to those k specific sensors from the vector of all sensor measurements, the network becomes unobservable during the state estimation [20, 21]. The set of sensors that satisfies the above criteria is called a 'critical set of sensors' and denoted as C [27]. More discussion is provided in the next sections.

3.1. Critical set of measurements

Formally, 'critical set of sensors' is defined as below [12], [20]: Consider a set of measurements and a set of state variables which are represented as $\mathcal{M}$ and $\mathcal{X}$. If it is possible to estimate the states in $\mathcal{X}$ uniquely from the measurements of $\mathcal{M}$, then $\mathcal{X}$ is said to be observable with respect to $\mathcal{M}$. Consider a subset of measurements C in $\mathcal{M}$, which if removed from $\mathcal{M}$, the reduced set of measurements $\mathcal{M}'$ cannot be used to uniquely estimate the states in $\mathcal{X}$. Hence, $\mathcal{X}$ is *unobservable* and the subset of measurements C is defined as a 'critical set of sensors'.

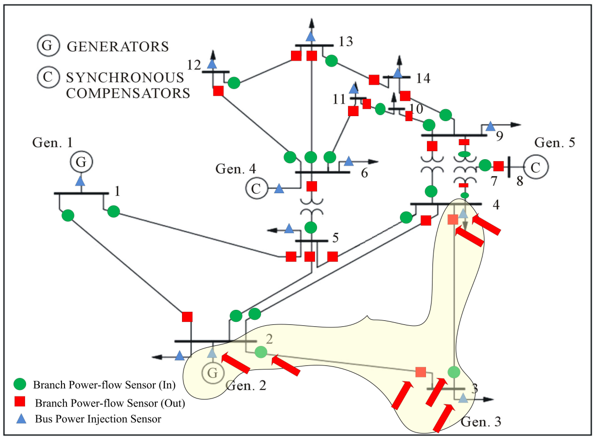

G GENERATORS
C SYNCHRONOUS COMPENSATORS
Gen. 1
Gen. 4
Gen. 5
Gen. 2
Gen. 3
1
2
3
4
5
6
7
8
9
10
11
12
13
14
● Branch Power-flow Sensor (In)
■ Branch Power-flow Sensor (Out)
▲ Bus Power Injection Sensor

Figure 1: Sparse attack construction in 14 bus system. Sensors within the yellow area (marked with red arrow) are the critical sensors for making an unobservable attack that targets bus 3.

3.1.1. *Identification of critical measurements*

Suppose, system state θ_i ($\theta_i \in \boldsymbol{\theta}$) belongs to the bus b. To make the system state θ_i unobservable, the attacker needs to exploit those measurements which are related to the estimation of that system state. To find the critical set of measurements (C_b), we use the following heuristic:

Step 1: Consider the injection measurement at bus b, if exists.

Step 2: Determine the branches incident to bus b.

Step 3: For each of the branches, include the power flow (both inflow and outflow) sensors, if exists.

Step 4: For each of the branches, include the power injection measurements of the remaining node (other than b), if exists.

To explain, we consider the topology of the IEEE 14 bus benchmark system, as shown in Fig. 1. The power flow measurements are marked with 'squares' and 'circles' whereas the injection measurements are marked with 'triangles'. Let us consider that the attacker wants to construct an unobservable attack that targets bus 3. Hence, with the knowledge of the system topology ($\mathbf{H}$) and using the above heuristic, an attacker can find a set of critical sensors (C_3) (within the yellow shaded region). This set of sensors are sufficient to make an unobservable attack $\boldsymbol{a}$, which modifies the estimation of the state x_2 of bus 3 (as the reference bus voltage angle is not considered as a system state, x_1 belongs to bus 2 and so on). Thus, we find $C_3 = \{S_{(2,3)}, S_{(3,2)}, S_{(3,4)}, S_{(4,3)}, S_2, S_3, S_4\}$, where $S_{(i,j)}$ indicates a power flow sensor that measures power flow from node i to node j, and $S_{(i)}$ is an injection sensor that measures power injection at node i, which are marked with red arrow in Fig. 1. This set of sensors also satisfy the spanning-tree observability criteria [22, 28]. This same procedure is applicable to identify a critical set of measurements for any bus (vertices) of the power grid.

3.2. Attack construction

In order to construct a sparse unobservable attack, it is necessary to identify the critical set of measurements. Identification of the critical sets of measurements requires knowledge of the grid topology. In Sec. 2, we have shown how to obtain the estimated topology using the power injection measurement data only. Here, we provide a step-by-step procedure of the sparse unobservable attack construction strategy using the estimated topology.

Step 1-*Estimate the measurement sub-space*: To construct a data-driven sparse unobservable attack, first, we find the measurement subspace using principal component analysis (PCA). In summary: PCA is employed on the measurement matrix to obtain an orthogonal transformation, which produces a set of values of linearly uncorrelated variables (principal components). Then, the first N (which is equivalent to the rank of the measurement matrix) principal components are considered to obtain $\mathbf{H}_{PCA}$, which basically forms a basis matrix of the subspace of possible noiseless measurements [20].

Step 2-*Estimate the topology matrix*: Next, topology estimation is performed using power injection measurements only using the proposed algorithm based on the alternating direction method of multipliers (ADMM) as discussed in Section 2.

Step 3-*Identification of critical measurements*: Based on the estimated topology, the critical sets of measurements are identified using the process discussed in Section 3.1.1.

Step 4-*Sparse unobservable attack construction*: Using any identified critical set of measurements (C_i), it is possible to construct a sparse unobservable attack [20]. In order to do that, first, we remove the rows of $\mathbf{H}_{PCA}$ corresponding to the measurements in the critical set C_i and obtain $\mathbf{H}^r_{PCA}$. Now, our interest is to construct a sparse unobservable attack that will modify only the measurements in C_i. Hence, we calculate the null space of the $\mathbf{H}^r_{PCA}$ using the following simple steps [20]:

1. perform singular value decomposition of $\mathbf{H}^r_{PCA}$ and obtain $\mathbf{H}^r_{PCA} = USV^T$, where U and V are the unitary matrices and S is the diagonal matrix of singular values.
2. find a column $\boldsymbol{c}_v$ in $\boldsymbol{V}$ which corresponds to the smallest singular value in S.
3. this column $\boldsymbol{c}_v$ forms an orthonormal basis for the null space of $\mathbf{H}^r_{PCA}$. Now, sparse unobservable attack vector $\boldsymbol{a}$ is constructed using [20].

$$\boldsymbol{a} = \wp * \mathbf{H}_{PCA}\boldsymbol{c}_v \tag{22}$$

where, $\wp$ (with $\wp \in \mathbb{R}$) is a scalar which controls the magnitude of attack. Impact of $\wp$ on the attack stealthiness is discussed in Section 4.3.1.

Step 5-*Attack Injection*: Finally, the sparse attack vector $\boldsymbol{a}$ is injected with the original measurement vector $\mathbf{z}_t$, which in return produce the attacked measurements as below:

$$\mathbf{z}_{att} = \mathbf{z}_t + \mathbf{a} \tag{23}$$

In the next sections, we demonstrate the performance of the proposed sparse unobservable attack strategy considering a wide range of scenarios.

4. Results and discussion

4.1. Performance of topology estimation

All experiments are validated using IEEE 14 bus and IEEE 30 bus benchmark test systems [34]. The original topology of IEEE 14 bus and 30 bus test systems are obtained using the energy grid simulation tool MATPOWER [34]. This research assumes that an attacker can monitor the injection measurements ($\mathbf{z}$) for multiple observations and at that time there is no topological change of the grid. According to [20], we consider that the system states of multiple observations are independent and identically distributed (i.i.d), which follows a Gaussian distribution, if measurements are taken for a very short amount of time. Here, we consider 100 samples or observations to create a measurement matrix ($\mathbf{Z}$) based on the Eqn. 1. Next, we reveal the topology blindly following Eqn. 3 using the proposed solution. For the ADMM algorithm, *augmented Lagrangian parameter*, denoted as ρ, is the only tuning parameter. For $\rho > 0$, ADMM shows good convergence characteristics as reported in [10]. We chose the optimal value empirically. Considering a range $\rho = [10, 15]$, we found that $\rho = 13$ provides the optimal value when the original topology and estimated topology are very close.

4.1.1. Comparative Analysis of Topology Estimation

The 2D grid connectivity or the structure of the estimated topology using the proposed approach (with improved initialization) is shown in Fig. 2-(b) for IEEE 14 bus system. The original grid structure and the estimated grid structure using the proposed method with random initialization are shown in Fig. 2-(a) and Fig. 2-(d), respectively. Fig. 2-(c) shows the estimated grid connectivity obtained from [16]. From Fig. 2, the grid connectivity of the original topology and the estimated topology using the proposed method (with improved initialization) exhibit a very good match (Fig. 2-(a) and (b)). The estimated grid connectivity obtained using the proposed method also shows better similarity with the original grid structure compared with the estimation of [16] (in Fig. 2-(c)) and the method with random initialization (in Fig. 2-(d)).

For the IEEE 30 bus system, the original grid connectivity and the estimated grid connectivity using the proposed method is shown in Fig. 3 and Fig. 4, respectively. The estimated grid connectivity has a very close similarity with the original one except for a few mismatched edges. To quantify the grid estimation performance of the proposed method, we conduct a set of experiments in the following sections using graph-theoretic and eigenvalue analyses.

4.1.2. Accuracy analysis of estimated topology using graph-theoretic metrics

In this section, graph-theoretic metrics are used to compare the original and the estimated graph structures. *Degree centrality* and *eigenvector centrality* have been previously reported as vital measures to study the topological vulnerability of the power grids [7, 29]. In [24], these measures were also used to compare the original and the estimated

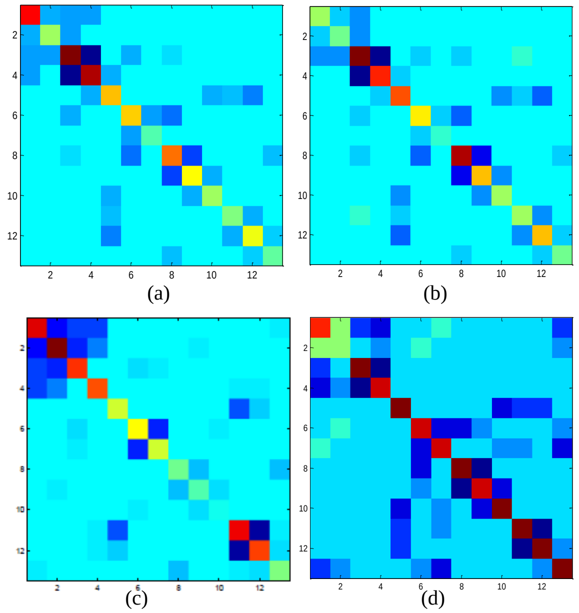


Figure 2: (a) The original topology matrix, (b) Estimated topology matrix using the proposed method with improved initialization, (c) Estimated topology matrix obtained from [15], (d) Estimated topology matrix using the proposed method with random initialization

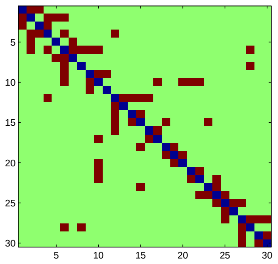


Figure 3: Original topology

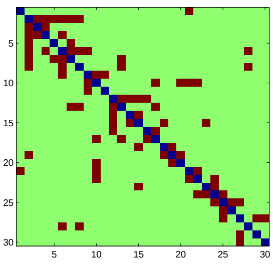


Figure 4: Estimated topology

Table 1
Accuracy of estimated topology using various metrics for IEEE 14 bus system

Performance Indicators	Actual	Estimation	% Acc.
Avg. Eigenvalue Centrality	0.2344	0.2442	95.82%
Degree Centrality	2.8571	3	94.99%
Avg v_{knn}	3.3321	3.4286	97.10%
Graph Energy	20.2847	20.7924	97.49%
Avg. Closeness Centrality	0.0332	0.0348	95.18%

Table 2
Accuracy of estimated topology using various metrics for IEEE 30 bus system

Performance Indicators	Actual	Estimation	% Acc.
Avg. Eigenvalue Centrality	0.1426	0.1233	86.47%
Degree Centrality	2.73	2.83	96.34%
Avg v_{knn}	3.5065	3.5438	98.86%
Graph Energy	41.27	41.16	99.73%
Avg. Closeness Centrality	0.0107	0.0094	87.85%

topologies. Other measures including *closeness centrality*, *average degree of neighboring nodes*, and *graph energy* are also used here to compare the estimation performance [8]. Experiments are performed using the adjacency matrix of the original and the estimated topology considering IEEE 14 bus and 30 bus benchmark systems. The accuracy of the estimated measures are calculated as below:

$$\eta = 1 - \frac{|M_a - M_e|}{|M_a|} \times 100\% \tag{24}$$

where, M_a and M_e are the values of the performance measures obtained using the adjacency matrices of the actual topology and the estimated topology, respectively.

In Table 1 and Table 2, we summarize the values of these graph-theoretic measures to compare the estimation with the original grid for the IEEE 14 and 30 bus systems. From the values of these performance measures, which are summarized in Table 1 and Table 2, it can be concluded that the graph-theoretic indices using the estimated topology is very close compared to the actual topology.

4.2. Identification of critical measurements

we identify the critical measurements for each bus (except the reference bus) of the system which are obtained using: (i) the actual topology and (ii) the estimated topology of the IEEE 14 bus and the IEEE 30 bus systems, respectively following the procedure discussed in Section 3.1.1. To evaluate the accuracy of the identification of the critical measurements, we propose an index Acc_i below,

$$Acc_i = \frac{N_m^i}{N_a^i} \times 100\% \tag{25}$$

where, N_m^i is the total number of matching sensors between the critical sets obtained using the actual and the estimated topologies at bus i, and N_a^i is the total number of critical sensors for bus i that is obtained using the actual topology only. For example, if there are 6 sensors in any critical set of a bus and among them 5 have exact match with the critical set obtained using the estimated topology, then the accuracy is (5/6=) 83.33%. Fig. 5 and Fig. 6 show the accuracy (Acc_i) of identifying critical sets for IEEE 14 bus and 30 bus, respectively. In Fig. 5, critical sensor sets for most of the buses are identified correctly except for the buses 2 and 5. For bus 2, inflow and outflow power measurement sensors of line (2, 5) are missing due to the topology estimation error. The same set of sensors are missing for bus 5 due to the same reason. For all other buses, the obtained critical sensor sets using estimated topology have exact matching (100% accuracy) with the cases that use actual topology. For the IEEE 30 bus system, there is a slight variation in accuracy observed in some buses due to the estimation error of the topology matrix. Other than those small number of buses, the identified critical sensors using actual and estimated topologies have exact matching in most of the buses as shown in Fig. 6.

Table 3
List of critical sensors for the sparsest attack

Test sys.	Crit. Set	Bus ID	State	Critical sensors	Sensor location
14 bus	-	8	x_7	$\{S_{(8,7)}, S_{(7,8)}, S_7, S_8\}$	{14 , 34 , 47 , 48}
30 bus	1	11	x_{10}	$\{S_{(9,11)}, S_{(11,9)}, S_9, S_1 1\}$	{ 13 , 54 , 91 , 93}
30 bus	2	13	x_{12}	$\{S_{(12,13)}, S_{(13,12)}, S_1 2, S_1 3\}$	{ 16 , 57 , 94 , 95}
30 bus	3	26	x_{25}	$\{S_{(25,26)}, S_{(26,25)}, S_2 5, S_2 6\}$	{ 34 , 75 , 107 , 108}

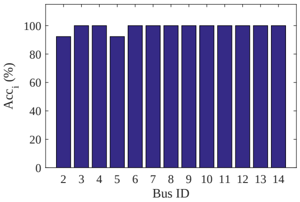


Figure 5: Acc_i for 14 bus

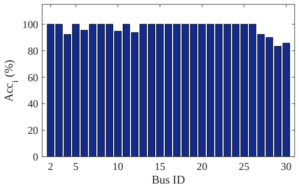


Figure 6: Acc_i for 30 bus

4.3. Performance of attack construction

In this section, we evaluate the attack construction performance. From Fig. 1, we see that 'bus 8' is connected with the grid through line {7, 8} and there are 4 sensors which include 1 inflow and 1 outflow sensor in the line {7, 8} and two injection sensors at node 7 and 8, respectively; these 4 sensors satisfy the spanning-tree observability criteria [28]. After removing the 4 specific sensors, it is possible to construct the sparsest unobservable attack. Following the attack construction strategy of Section 3.2, we perform the data-driven sparsest unobservable attack for IEEE 14 bus test system. In Fig 7, we plot: (i) actual measurements that are not observed by the operator (green circle), (ii) observed measurements (red cross) after the attack, and (iii) estimated measurements (blue diamond). We see in Fig 7 that the observed measurements have distinct values than the actual measurements in four sensors, which are $\{S_{(7,8)}, S_{(8,7)}, S_7, S_8\}$, located respectively in 14, 34, 47, and 48th row of the attacked measurement vector $\mathbf{z}_{att}$, as clearly evident from the figure. We see from Fig. 7 that both of these sets of measurements (observed and estimated) coincide with each other and the estimation error is only $8.6739e^{-26} \approx 0$ (noiseless case). When Gaussian noise of 21 dB is considered, the estimation error is only 33.161, which is well below the threshold of 55.7585 considering a 95% confidence interval. Therefore, the data-driven sparse unobservable attack remains hidden in the BDD. The estimated and actual state variables are also plotted in Fig. 8. The estimated state variable $\hat{\mathbf{x}}_7$ significantly differs from the true state $\mathbf{x}_7$ of 'bus 8' as shown in Fig. 8. Similar to the 14 bus system, the attacker needs to inject only 4 out of 112 sensors for the sparsest unobservable attack construction in the 30 bus test system, which is only 3.57% of the total sensors.

4.3.1. *Stealthiness of the sparsest unobservable attack*

The probability that a sparse unobservable attack is detected by the BDD is investigated in this section. First, we demonstrate the stealthiness of the sparsest unobservable attack. Here we consider 1000 Monte Carlo simulations for the sparsest unobservable attack construction strategy considering: (i) different Gaussian noise levels, and (ii) different attack magnitudes. Experiments are performed for IEEE benchmark 14 bus and 30 bus test systems.

(i) Stealthiness with varying Gaussian noise level: Following the attack construction strategy discussed in Section 3.2, here we generate 1000 attack vectors using Monte Carlo simulations by varying the Gaussian noise SNR between 15 dB to 35 dB for IEEE 14 bus system. The attack vectors are then added with the original measurement signal and tested using the state estimation and the BDD process. The chi-square objective value ($J(\hat{\mathbf{x}})$) for all 1000 attack scenarios are plotted in Fig 9. For IEEE 14 bus system, considering 97.5% confidence interval and 40 as the degree of freedom, the threshold using chi-square distribution becomes 59.3417 (marked using red line in Fig. 9). From Fig. 9, $J(\hat{\mathbf{x}})$ obtained from most of the attack scenarios remain well below the threshold 59.3417. We found that only 2.2% of attacks are being detected by the BDD module and the remaining 97.8% of attacks remain stealthy in the BDD process. We perform a similar type of experiment using the IEEE 30 bus system. The sparsest unobservable attack in IEEE 30 bus system can be constructed using three different sets of critical sensors listed in Table 3. Hence, during the Monte Carlo simulation, we randomly chose one of these three sets and noise SNR between 15 dB to 35 dB. The obtained chi-square objective values ($J(\hat{\mathbf{x}})$) of 1000 attack scenarios are plotted in Fig. 10. Using a similar method like the 14 bus system, the calculated threshold for this experiment is 108.9373. For this test setup, we also observe that almost 97.2% of attacks are below the threshold and capable to deceive the state estimator and BDD.

(i) Stealthiness with varying attack magnitudes: The strength of the sparse unobservable attack depends on the attack magnitudes, which is defined as a ratio between the l_2-*norm* of the attack vector to the l_2-*norm* of the original measurement vector. That means, if the attack magnitude ($\|\mathbf{a}_0\|/\|\mathbf{z}_t\|$) is 3, it indicates that the l_2-*norm* of the attack vector ($\mathbf{a}$) is 3 times the l_2-*norm* of the original measurement vector ($\mathbf{z}_t$). The attack magnitude is controlled by changing the values of $\wp$ in Eqn. 22. In this experiment, for the IEEE 14 bus system, we consider different levels of attack

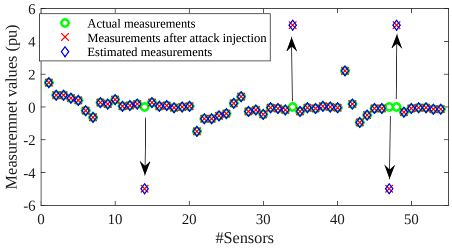


Figure 7: The smallest sparse unobservable attack for IEEE 14 bus system

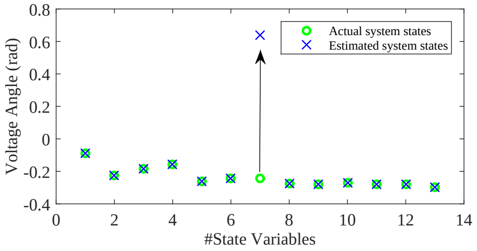


Figure 8: The estimated and the actual state variables for the smallest sparse unobservable attack considering IEEE 14 bus system

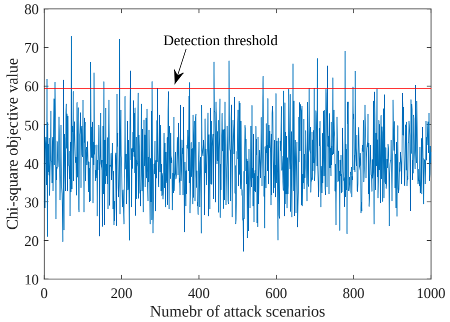


Figure 9: Stealthiness of the sparsest unobservable attack for varying Gaussian noise level using 14 bus system

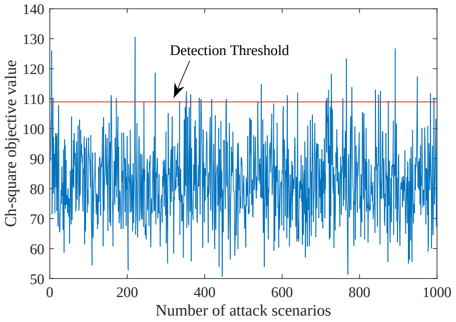


Figure 10: Stealthiness of the sparsest unobservable attack for varying Gaussian noise level using 30 bus system

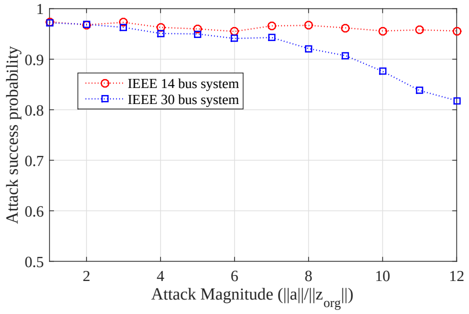


Figure 11: Attack success probability for varying attack magnitudes

magnitudes starting from 1 to 12. For each of these attack magnitude level, we perform 1000 Monte Carlo simulations for different SNRs (20 to 35 dB) values and calculate their corresponding $J(\hat{\mathbf{x}})$. Using the chi-square threshold for this test setup, the probability of successful attack construction is calculated. This procedure is repeated for all attack magnitude levels and plotted in Fig. 11. From the figure, we see that the probability of successful attack construction is over 0.95, even when the l_2-*norm* of the attack vector (**a**) is large, e.g., 12 times the original measurements. Similar steps are followed to investigate the attack performance with varying attack magnitudes for the IEEE 30 bus test system. The probability of successful attack construction is also plotted in Fig. 11. We see that the probability of successful attack construction decreases gradually with the increase of the attack magnitudes. In this case, the stealthy attack can be constructed with a probability over 0.95 even when the attack magnitude is 5. From this experiment and Fig. 11, we can summarize that the stealthiness of the attack construction is sensitive to the attack magnitude under the Gaussian noise assumption. However, an attacker can still construct a stealthy attack with a high success rate (over the probability of 0.95) with a high attack magnitude (the l_2-*norm* of the attack vector (**a**) is around 12 times and 5 times the original measurements for the 14 bus and 30 bus IEEE benchmark systems, respectively).

4.3.2. Stealthiness of the k-sparse unobservable attack

In the above sections, the stealthiness of the sparsest unobservable attack is discussed. Here, we investigate the stealthy characteristics of the k-sparse unobservable attack. Based on the identified set of critical sensors, we construct a k-sparse unobservable attack that corrupts one or more system states following the procedure discussed in Section 3. First, we discuss the experimental setup and results obtained using IEEE 14 bus system. To accomplish the task, we perform 100 trials of experiments where we randomly choose a system state for each trial. Then, we simulate 1000 Monte Carlo runs in each experimental trial considering different SNR (15 dB to 35 dB) values and attack magnitudes (up to 5), which produces 1000 chi-square objective values ($J(\hat{\mathbf{x}})$). Using these values and the chi-square detection threshold (with 97.5% confidence), the probability of successful attack construction is calculated for each trial. This procedure is repeated for all 100 trials and the results are reported in Fig 12. From Fig 12, most of the trials have a high attack

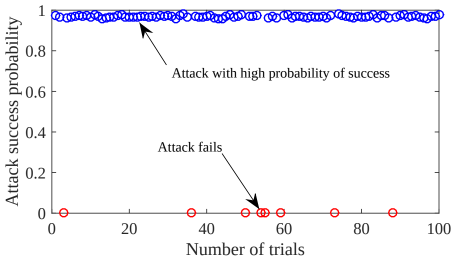


Figure 12: Investigation on the stealthiness of the k-sparse unobservable attacks using 14 bus system

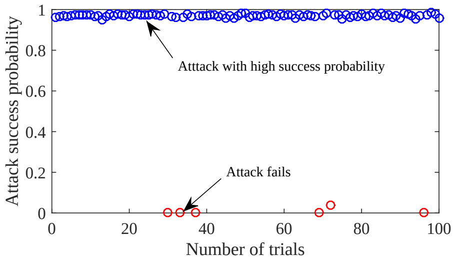


Figure 13: Investigation on the stealthiness of the k-sparse unobservable attacks using 30 bus system

success probability (over 97%) and only a few trials are unsuccessful. These unsuccessful trials are related to those k-sparse attack vectors where the list of critical sensors are not accurately estimated due to the mismatch in previously estimated topology. Similar to the IEEE 14 bus system, the stealthiness of the k-sparse unobservable attack is investigated using IEEE 30 bus system. The results are plotted in Fig 13. From this figure, we also observe that most of the attacks are successful with high probability. On average, the attack success rate is 92.25% for the IEEE 30 bus system considering all the trials. In summary, this section investigates the stealthiness of the k-sparse attack strategy using the information obtained from the estimated topology. We find the attacks are successful with high probability in any individual trial (over 99% for the 30 bus system) and also over 92.25% (for the 14 bus system) on an average (from all trials) considering different estimation errors, Gaussian noise cases and different attack magnitudes.

5. Conclusion

In this paper, we investigated the sparse FDI attack construction strategy without any prior knowledge of system Jacobian or power grid topology. Here, we demonstrated that it is possible to construct stealthy attacks even when an attacker has access to only a limited number of measurement devices to inject false data. In order to construct a stealthy and sparse FDI attack, the attacker needs to know the grid topological connectivity. We demonstrated how to reveal the power grid topology from the measurement signals only. In this work, the estimation problem is formulated as an optimisation problem where the ADMM method is used for solving the problem. The comparative evaluation using visualization and graph-theoretic measures indicated that the proposed solution reveals the topology with high accuracy when compared to the actual one. Finally, based on the estimated topology we determined the critical set of measurements, which were then utilised for sparse attack construction. We showed that only 7.40% and 3.57% sensors are required to construct the sparsest stealthy attacks for the IEEE 14 bus and the 30 bus system, respectively.

The finding from this research was very significant as it clearly points out that the topological properties of the physical grid can be revealed using the measurement data obtained from the cyber domain. Moreover, an intelligent attacker can make use of the estimated physical grid information to create an FDI attack that injects false information only into a fraction of all available measurement devices, which makes the attack more practical, hence likely.

References

[1] Ahmed, S., Lee, Y., Hyun, S., Koo, I., 2019. Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest. IEEE Transactions on Information Forensics and Security 14, 2765–2777.

[2] Alexopoulos, T.A., Korres, G.N., Manousakis, N.M., 2020. Complementarity reformulations for false data injection attacks on pmu-only state estimation. Electric Power Systems Research 189, 106796.

[3] Anwar, A., Mahmood, A., 2014. Vulnerabilities of smart grid state estimation against false data injection attack, in: Renewable Energy Integration. Springer. Green Energy and Technology, pp. 411–428.

[4] Anwar, A., Mahmood, A., Pickering, M., 2016. Estimation of smart grid topology using scada measurements, in: 2016 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 539–544.

[5] Anwar, A., Mahmood, A.N., 2016. Anomaly detection in electric network database of smart grid: Graph matching approach. Electric Power Systems Research 133, 51 – 62.

[6] Anwar, A., Mahmood, A.N., Pickering, M., 2017. Modeling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements. Journal of Computer and System Sciences 83, 58 – 72.

[7] Bompard, E., Pons, E., Wu, D., 2012. Extended topological metrics for the analysis of power grid vulnerability. IEEE Systems Journal 6, 481–487.

[8] Bounova, G., de Weck, O., 2012. Overview of metrics and their correlation patterns for multiple-metric topology analysis on heterogeneous graph ensembles. Phys. Rev. E 85, 016117.

[9] Boyd, S., Parikh, N., Chu, E., Peleato, B., Eckstein, J., 2011a. Distributed optimization and statistical learning via the alternating direction method of multipliers. Found. Trends Mach. Learn. 3, 1–122.

[10] Boyd, S., Parikh, N., Chu, E., Peleato, B., Eckstein, J., 2011b. Distributed optimization and statistical learning via the alternating direction method of multipliers. Found. Trends Mach. Learn. 3, 1–122.

[11] Bretas, A.S., Bretas, N.G., Carvalho, B., Baeyens, E., Khargonekar, P.P., 2017. Smart grids cyber-physical security as a malicious data attack: An innovation approach. Electric Power Systems Research 149, 210 – 219.

[12] Clements, K.A., Krumpholz, G.R., Davis, P.W., 1981. Power system state estimation residual analysis: An algorithm using network topology. IEEE Transactions on Power Apparatus and Systems PAS-100, 1779–1787.

[13] Esmalifalak, M., Nguyen, H., Zheng, R., Han, Z., 2011. Stealth false data injection using independent component analysis in smart grid, in: IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 244–248.

[14] Giani, A., Bitar, E., Garcia, M., McQueen, M., Khargonekar, P.,

Poolla, K., 2013. Smart grid data integrity attacks. IEEE Transactions on Smart Grid 4, 1244–1253.

[15] Kekatos, V., Giannakis, G., Baldick, R., 2014. Grid topology identification using electricity prices, in: IEEE PES General Meeting.

[16] Kekatos, V., Giannakis, G.B., Baldick, R., 2016. Online energy price matrix factorization for power grid topology tracking. IEEE Transactions on Smart Grid 7, 1239–1248.

[17] Khare, G., Mohapatra, A., Singh, S., 2021. A real-time approach for detection and correction of false data in pmu measurements. Electric Power Systems Research 191, 106866.

[18] Kim, J., Tong, L., 2013. On topology attack of a smart grid: Undetectable attacks and countermeasures. IEEE Journal on Selected Areas in Communications 31, 1294–1305.

[19] Kim, J., Tong, L., Thomas, R., 2014. Data framing attack on state estimation. IEEE Journal on Selected Areas in Communications 32, 1460–1470.

[20] Kim, J., Tong, L., Thomas, R., 2015. Subspace methods for data attack on state estimation: A data driven approach. IEEE Transactions on Signal Processing 63, 1102–1114.

[21] Kosut, O., Jia, L., Thomas, R.J., Tong, L., 2011. Malicious data attacks on the smart grid. IEEE Transactions on Smart Grid 2, 645–658.

[22] Krumpholz, G.R., Clements, K.A., Davis, P.W., 1980. Power system observability: A practical algorithm using network topology. IEEE Transactions on Power Apparatus and Systems , 1534–1542.

[23] Li, T., Werner, L., Low, S.H., 2020. Learning graphs from linear measurements: Fundamental trade-offs and applications. IEEE Transactions on Signal and Information Processing over Networks 6, 163–178.

[24] Li, X., Poor, H., Scaglione, A., 2013. Blind topology identification for power systems, in: IEEE International Conference on Smart Grid Communications (SmartGridComm).

[25] Liu, J., Srikantha, P., 2019. Decentralized topology reconfiguration in multiphase distribution networks. IEEE Transactions on Signal and Information Processing over Networks 5, 598–610.

[26] Liu, Y., Ning, P., Reiter, M.K., 2011. False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. 14, 13:1–13:33.

[27] Monticelli, A., 1999. State Estimation in Electric Power Systems: A Generalized Approach. Springer US.

[28] Mori, H., Tsuzuki, S., 1991. A fast method for topological observability analysis using a minimum spanning tree technique. IEEE Transactions on Power Systems 6, 491–500.

[29] Nasiruzzaman, A.B.M., Pota, H.R., Anwar, A., 2012. Comparative study of power grid centrality measures using complex network framework, in: IEEE Power Engineering and Optimization Conference (PEDCO), pp. 176–181.

[30] Ozay, M., Esnaola, I., Vural, F., Kulkarni, S., Poor, H., 2013. Sparse attack construction and state estimation in the smart grid: Centralized and distributed models. IEEE Journal on Selected Areas in Communications 31, 1306–1318.

[31] Rahman, M.A., 2012. False Data Injection Attacks with Incomplete Information. Ph.D. thesis. Texas Tech University.

[32] Rahman, M.A., Mohsenian-Rad, H., 2012. False data injection attacks with incomplete information against smart power grids, in: IEEE Global Communications Conference (GLOBECOM), pp. 3153–3158.

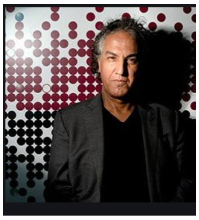
[33] Yu, Z.H., Chin, W.L., 2015. Blind false data injection attack using pca approximation method in smart grid. IEEE Transactions on Smart Grid 6, 1219–1226.

[34] Zimmerman, R., Murillo-Sanchez, C., Thomas, R., 2011. MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education. IEEE Transactions on Power Systems 26, 12–19.

[35] Zou, T., Bretas, A.S., Ruben, C., Dhulipala, S.C., Bretas, N., 2020. Smart grids cyber-physical security: Parameter correction model against unbalanced false data injection attacks. Electric Power Systems Research 187, 106490.

Adnan Anwar is a Lecturer in Cyber Security at the School of Information Technology. Previously he has worked as a Data Scientist at Flow Power. He has over 8 years of research, and teaching experience in universities and research labs including NICTA, La Trobe University, and University of New South Wales. He received his PhD and Master by Research degree from UNSW. He is broadly interested in the security research for critical infrastructures including Smart Energy Grid, SCADA system, and application of machine learning and optimization techniques to solve cyber security issues for industrial systems. He has been the recipient of several awards including UPA scholarship, UNSW TFR scholarship, best paper award and several travel grants including ACM and Postgraduate Research Student Support (PRSS) travel grants. He has authored over 30+ articles including journal (mostly in Q1), conference articles and book chapters in prestigious venues.

Dr. Abdun Mahmood received his PhD from the University of Melbourne, Australia, in 2008 the MSc (Research) degree in computer science and the B.Sc. degree in applied physics and electronics from the University of Dhaka, Bangladesh, in 1999 and 1997, respectively. Dr. Mahmood had an academic career in University since 2000, working at University of Dhaka, RMIT University, UNSW Canberra and currently in La Trobe University as an Associate Professor (Reader). Dr. Mahmood leads a group of researchers focusing on Machine Learning and Cybersecurity including Anomaly Detection in Smart Grid, SCADA security, Memory Forensics, and False Data Injection. He has published his work in various IEEE Transactions and A-tier international journals and conferences.



Zahir Tari is a full professor in Distributed Systems at RMIT University (Australia). He received a bachelor's degree in Mathematics from University of Algiers (USTHB, Algeria) in 1984, M.Sc. in Operational Research from University of Grenoble (France) in 1985 and Ph.D. degree in Computer Science from University of Grenoble (France) in 1989. Zahir's expertise is in the areas of system's performance (e.g. P2P, Cloud, Edge, IoT) as well as system's security (e.g. SCADA, Smart Grid, Cloud, IoT). He is the co-author of several books (John Wiley, Springer) and he has edited over 25 conference proceedings. Zahir is also a recipient of over $10M$ in funding from ARC (Australian Research Council) and lately part of a successful 7th Framework AU2EU (Australia to European) bid on Authorization and Authentication for Entrusted Unions. Finally, Zahir is an associated editor of ACM Computing Surveys and was an associate editor of the IEEE Transactions on Computers (TC), IEEE Transactions on Parallel and Distributed Systems (TPDS) and IEEE Magazine on Cloud Computing.

Aktar Kalam has been at Victoria University (VU) since 1985. He is a former Deputy Dean of the Faculty of Health, Engineering and Science and Head of Engineering of the College of Engineering and Science. Currently, he is the Head of External Engagement. He is also the current Chair of the Academic Board in the Engineering Institute of Technology, Perth, Australia. Professor Kalam has wide experience in educational institutions and industry across four continents. He received his B.Sc. and B.Sc. Engineering from Calcutta University and Aligarh Muslim University, India. He completed his MS and PhD at the University of Oklahoma, USA and the University of Bath, UK. Professor Kalam has conducted research, provided industrial consultancy and published more than 542 publications on his area of expertise. He has written 26-plus books in the area. More than 35 PhD students have graduated under his supervision. Professor Kalam provides consultancy for major electrical utilities, manufacturers and other industry bodies in his field of expertise. He is a Fellow of EA, IET, AIE, a life member of IEEE and a member CIGRE AP B5 Study Committee.