Electrical Power and Energy Systems 110 (2019) 623–629

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

Partial grid false data injection attacks against state estimation

Harag Margossian*, Mohammad Ali Sayed, Wissam Fawaz, Zahi Nakad

Department of Electrical and Computer Engineering, Lebanese American University, Byblos, Lebanon

ARTICLE INFO

Keywords:
State estimation
False data injection attacks
Power systems

ABSTRACT

The addition of an external communication layer to the power system has left it vulnerable to cyberattacks. False data injection (FDI) can be used to manipulate measurements that are used to estimate the state of the power system. Decisions made based on a false evaluation can result in major disturbances in its operation. Recent studies show how, with full knowledge about the system, these types of attacks can be mounted without being detected. This paper shows how, with knowledge limited only to a specific section of the power system, it is still possible to carry out an undetectable attack. The process of performing the attack and a proof of its undetectability is explained in detail and then illustrated through a case study on the widely adopted IEEE 14 bus system. Last but not least, the paper proposes a method to identify a subset of available measurements to be considered for protection against cyberattacks. This would render the entire network or specific parts of it immune to these attacks.

1. Introduction

The rapid development in renewable energy technologies coupled with their integration into distribution networks is driving advancement in terms of the way a power grid is both monitored and controlled. In point of fact, the grid is currently undergoing a major shift towards more reliance on sensing, control and communication. This paved the way for the emergence of so-called smart grids [1].

In the context of a smart grid, the measurement, control and automation units interact with one another to achieve: (a) reduced power losses [2,3], (b) increased integration of renewable energy [4], (c) reliable protection of power system components [5], (d) quicker restoration of electricity following disturbances [6] and (e) countless other applications. As such, the communication infrastructure will be one of the fundamental components of a smart grid. However, the underlying communication infrastructure lends itself to new security vulnerabilities. As a result, the reliability of the power grid becomes strongly dependent on the reliability and security of its associated communication infrastructure [7].

A substantial amount of data is expected to be collected, transported and analyzed in a smart grid. In this regard, attacks having the potential to compromise the security of the data can be classified into one of two categories, namely passive attacks and active attacks [8]. Passive attacks collect and analyze the data (content and traffic) but do not modify it [9]. Data of interest for passive attacks include private consumer information that can be used to deduce consumers' activities, the type of devices they use and whether or not they are away from home. Active attacks, on the other hand, manipulate the data or introduce false data into the system [10–12]. Injecting false data into the system can be done by altering the control/data messages as they travel to the relays controlling the grid. Given that the control and automation units use measurement data to make their decisions, by targeting these data messages, attackers can cause major disturbances in the power system. Moreover, they can cause specific smart grid applications to fail or even induce network-wide blackouts. These attacks are known in literature as false data injection (FDI) attacks [13].

A particularly critical target for FDI attacks is state estimation (SE), which is an essential tool in the operation of a power system [14]. It is worthwhile noting in this respect that continuously observing all of the power system variables is a cost-prohibitive process. Therefore, there can only be a limited number of measurements gathered from the system. However, the collected measurements may be subject to inaccuracies that are mainly caused by imperfections of the data collecting instrumentation. The aim of SE is thus to get the best estimate of the power system variables of interest based on the limited and possibly noisy measurements available. It is nonetheless possible to detect false measurements by comparing them to their estimated values through the means of the so-called bad data detection (BDD) mechanism [15].

This paper reviews first the current literature pertaining to FDI attacks on SE. Then, it shows that it is possible for an attacker to target partial grids even without having any information about the rest of the power system. This finding corrects one of the misconceptions towards

* Corresponding author.
E-mail address: harag.margossian@lau.edu.lb (H. Margossian).

https://doi.org/10.1016/j.ijepes.2019.03.039
Received 20 June 2018; Received in revised form 23 January 2019; Accepted 18 March 2019
Available online 01 April 2019

this end, found in the open relevant literature. This study then provides valuable insight into the way protected meters can be placed to render the SE immune to FDI attacks, proposing a novel method to effectively select a subset of the measurements to protect.

In Section 2, a summary of the working principles underlying linear SE and BDD is provided along with a survey of the current literature relating to FDI attacks on SE. Section 3 introduces our hypothesis stating that an attacker equipped with limited knowledge about the entire network is capable of mounting a full-fledged attack against a partial grid. That hypothesis is then proven in Section 4 via a motivating example. Section 5 delineates a method aiming at safeguarding the SE in the face of FDI attacks through a systematic selection of measurements to protect against cyberattacks. Finally, Section 6 concludes the paper.

2. Background

2.1. Linear SE and BDD

The purpose of the SE is to estimate a set of state variables x based on which all dependent variables can be calculated. In this paper, the DC power system model [16,17] is used, as is common in SE security analysis papers [11,18–26]. The DC power system model linearizes power flow equations and thus requires less computational resources. This however comes at the expense of a lower computational accuracy. The DC power model is designed around the following assumptions of: a) constant voltages of 1 pu at all buses, b) small phase angle differences between connected buses and c) no transmission losses.

The number of state variables n in this model is equal to $N-1$ such that (assuming that $\theta_1 = 0$ as the slack bus):

$$\boldsymbol{x} = [\theta_2; \theta_3; \cdots; \theta_N] \tag{1}$$

The measurements are defined by the vector $\boldsymbol{z}$ having a size m. The relationship between $\boldsymbol{x}$ and $\boldsymbol{z}$ is given as follows:

$$\boldsymbol{z} = \begin{bmatrix} z_1 \\ \vdots \\ z_m \end{bmatrix} = \begin{bmatrix} h_1(x_1, \cdots, x_n) \\ \vdots \\ h_m(x_1, \cdots, x_n) \end{bmatrix} + \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix} = \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{e} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{e} \tag{2}$$

where $h_i(x_1, \cdots, x_n)$ is the calculated value of z_i based on $\boldsymbol{x}$, $\boldsymbol{e_i}$ is the difference between the measured and calculated values of z_i, and $\boldsymbol{H}$ is a matrix containing the coefficients of $\boldsymbol{x}$ in $\boldsymbol{h(x)}$.

In this paper, we consider 3 types of measurements: (1) voltage angle (θ_i) measurements, (2) active power flow measurements (P_{ij}) and (3) power injection measurements (P_i, generation – load at bus i). Consequently, $\boldsymbol{h(x)}$ is given by:

$$h_i(\boldsymbol{x}) = \begin{cases} \theta_i \quad for \quad \theta_i \\ B_{ij} \times (\theta_i - \theta_j) \quad for \quad P_{ij} \\ \sum_j B_{ij} \times (\theta_i - \theta_j) \quad for \quad P_i \end{cases} \tag{3}$$

where B_{ij} is the susceptance of the line connecting bus i to bus j.

The objective of SE is to determine the best estimate of $\boldsymbol{x}$ given the available measurements. These measurements are assigned weights based on the expected accuracy of their measurement units.

It is common to make the following assumptions regarding the statistical properties of the measurement errors [14]:

- Errors are independent from one another
- Errors follow a Gaussian distribution with an expected value of zero

In a bid to account for these weights, the diagonal matrix $\boldsymbol{R}$ is constructed such that R_{ii} is the inverse of the weight assigned to measurement z_i. The latter is normally chosen as the variance of the measurement.

There are some studies that consider measurement error dependencies [27,28] and state that this improves the accuracy of the state estimation. However, considering measurement error dependencies changes the structure of the $\boldsymbol{R}$ matrix, rendering it a non-diagonal matrix and thus increases SE complexity. In line with the open literature [11,18–26,29,30], in this work, measurement error dependencies are disregarded.

The state estimation problem is then formulated, according to the weighted least squares (WLS) criterion, as follows:

$$minimize \sum_{i=1}^{m} \frac{(z_i - h_i(\boldsymbol{x}))^2}{R_{ii}} \tag{4}$$

which can be rewritten in matrix form as follows:

$$minimize [\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})]^T [\boldsymbol{R}^{-1}] [\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})] \tag{5}$$

The solution in vector form is then given by the vector $\hat{\boldsymbol{x}}$ [11]:

$$\hat{\boldsymbol{x}} = [\boldsymbol{H}^T \boldsymbol{R}^{-1} \boldsymbol{H}]^{-1} \boldsymbol{H}^T \boldsymbol{R}^{-1} \boldsymbol{z} = \boldsymbol{M}\boldsymbol{z} \tag{6}$$

Following the SE, BDD algorithms are normally used to detect false measurements. Several criteria can be used to detect the presence of bad data, but most BDD algorithms rely on measurement residuals. Note that the residuals represent the difference between $\boldsymbol{h(x)}$ and the measurements vector $\boldsymbol{z}$. Those measurements with high resulting residuals are deemed false. To cater to the various measurement accuracies, the vector of residuals $\boldsymbol{r}$ is normalized as follows:

$$\boldsymbol{r} = \left| \frac{\boldsymbol{h}(\hat{\boldsymbol{x}}) - \boldsymbol{z}}{\boldsymbol{\sigma}} \right| \tag{7}$$

where $\boldsymbol{\sigma}$ is the vector of standard deviations of the measurements vector $\boldsymbol{z}$ (i.e. $\sigma_i = \sqrt{R_{ii}}$).

2.2. Related studies: FDI attacks on SE

The framework for FDI attacks that target linear SE is explained in [11]. FDI attacks result in an altered measurement vector $\boldsymbol{z}' = \boldsymbol{z} + \boldsymbol{a}$ where $\boldsymbol{a}$ is the attack vector. Due to this change, the estimated state vector $\boldsymbol{x}$ will deviate from the expected value and become $\boldsymbol{x}'$, such that:

$$\boldsymbol{x}' = \boldsymbol{M}\boldsymbol{z}' \tag{8}$$

For the attack to be successful, however, it will have to remain undetected by the BDD algorithm. This means that the change in the vectors $\boldsymbol{x}$ and $\boldsymbol{z}$, should not lead to a change in the vector $\boldsymbol{e}$ and consequently in the vector $\boldsymbol{r}$. The condition for undetectability can then be written as:

$$\boldsymbol{h}(\boldsymbol{x}') - \boldsymbol{z}' = \boldsymbol{h}(\hat{\boldsymbol{x}}) - \boldsymbol{z} \tag{9}$$

This can be rewritten as:

$$\boldsymbol{H}\boldsymbol{x}' - \boldsymbol{z}' = \boldsymbol{H}\hat{\boldsymbol{x}} - \boldsymbol{z} \tag{10}$$

$$\boldsymbol{H}\boldsymbol{M}\boldsymbol{z}' - \boldsymbol{z}' = \boldsymbol{H}\boldsymbol{M}\boldsymbol{z} - \boldsymbol{z} \tag{11}$$

$$\boldsymbol{H}\boldsymbol{M}(\boldsymbol{z} + \boldsymbol{a}) - (\boldsymbol{z} + \boldsymbol{a}) = \boldsymbol{H}\boldsymbol{M}\boldsymbol{z} - \boldsymbol{z} \tag{12}$$

$$\boldsymbol{H}\boldsymbol{M}\boldsymbol{a} - \boldsymbol{a} = 0 \tag{13}$$

$$(\boldsymbol{H}\boldsymbol{M} - \boldsymbol{I})\boldsymbol{a} = 0 \tag{14}$$

Based on the structure of matrix $\boldsymbol{M}$, it is clear that $\boldsymbol{M}\boldsymbol{H} = [\boldsymbol{H}^T \boldsymbol{R}^{-1} \boldsymbol{H}]^{-1} \boldsymbol{H}^T \boldsymbol{R}^{-1} \boldsymbol{H} = \boldsymbol{I} \Rightarrow \boldsymbol{H}\boldsymbol{M}\boldsymbol{H} = \boldsymbol{H} \Rightarrow (\boldsymbol{H}\boldsymbol{M} - \boldsymbol{I})\boldsymbol{H} = 0$. This means that every column of $\boldsymbol{H}$ is a possible solution to Eq. (14). In fact, it can be shown that any linear combination of the columns of $\boldsymbol{H}$, represented by the vector of coefficients $\boldsymbol{c}$ in what follows, is also a possible solution to Eq. (14). In this way, a successful FDI attack vector $\boldsymbol{a}$ would take the following form:

$$\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c} = c_1 \begin{pmatrix} H_{11} \\ H_{21} \\ \vdots \\ H_{m1} \end{pmatrix} + c_2 \begin{pmatrix} H_{12} \\ H_{22} \\ \vdots \\ H_{m2} \end{pmatrix} + \cdots + c_n \begin{pmatrix} H_{1n} \\ H_{2n} \\ \vdots \\ H_{mn} \end{pmatrix} \tag{15}$$

The new vector of states can then be calculated as [18]:

$$\boldsymbol{x}' = \boldsymbol{Mz}' = \boldsymbol{Mz} + \boldsymbol{Ma} = \hat{\boldsymbol{x}} + \boldsymbol{Ma} = \hat{\boldsymbol{x}} + \boldsymbol{MHc} = \hat{\boldsymbol{x}} + \boldsymbol{c} \quad (16)$$

In [29], FDI attacks against non-linear SE are considered. The authors propose a method that chooses the attack vector based not only on offline data (i.e., information about grid topology, line parameters etc…) but also on online data collected from the grid during the attack (i.e., current measurement values). The authors also show that an attack designed for non-linear SE can also go undetected when targeting linear SE.

In [19], the authors focus on attacking two measurements rather than the whole SE, while remaining undetected. The proposed attack targets the phase angle of PMUs as this can be done by spoofing their GPS signals and disrupting their synchronization. Knowing the network topology, the attacker can build a Hermitian-complex matrix ($\boldsymbol{W}$) that is a function of the SE verification matrix, the measurement vector and an attack indication matrix that they defined. The authors show that attacking only one measurement or attacking a pair of measurements having a full rank $\boldsymbol{W}$ will result in detection. However, by using a metric called the index of separation, that is constructed from the eigen values of $\boldsymbol{W}$, it is possible to identify pairs of PMUs that can be attacked without detection. A greedy algorithm was developed to maximize the effect of attacks on the system by combining the attacks on different PMU pairs.

In [20], the authors suggest that FDI attacks can be detected if the change in the state variables is large and so they introduce a constraint that limits the change in $\boldsymbol{x}$. The authors also consider that an attack will have a pre-specified set of targets and thus the entries of $\boldsymbol{c}$ will be set to 0 for those phase angles that the attack will not affect. Finally, the authors consider that some measurements might be protected against cyberattacks and thus might not be targetable. In this case, entries of $\boldsymbol{a}$ will be set to 0 for the rows corresponding to the protected measurements. To achieve this, the attack vector is built as a linear combination of the columns of $\boldsymbol{H}$, and matrix operations are used to eliminate the entries corresponding to protected meters while maintaining the effect on the desired targets.

A combination of FDI and availability attacks to perturb the load estimates is considered in [21]. To mount an availability attack, certain measurements are stopped from reaching the grid operator. This would mean that the redundancy of measurements in the SE is reduced and the rows of the $\boldsymbol{H}$ matrix corresponding to these measurements would need to be removed. Then the FDI attack is constructed based on the resulting, smaller matrix. The authors claim that this would reduce the resources needed by the attacker to attack the SE but do not consider the fact that the availability attacks would be a strong indication that an attack is ongoing and this could make the attack more detectable.

This work is extended in [22], where the authors consider two scenarios: one where the attacker has limited resources but full knowledge of the network parameters and another where the attacker has enough resources but imperfect knowledge of the network parameters. With limited resources the attack vector can no longer be constructed using the same methods and needs to be handled as an optimization problem with added constraints. The authors consider the required knowledge for constructing an attack to include the topology of the network, line parameter values (reactance of the lines) and the placement of the measurement units. The authors add that this knowledge can be obtained by recording and analyzing data sent from the measurement units using statistical methods. However, they state that this will result in some deviation from the actual values due to errors in data collection and analysis. This means that the attacker will no longer know the exact $\boldsymbol{H}$ matrix and that an estimation of the matrix is needed to construct the attack vector. The authors say that the residue in this case will have a generalized non-central chi-squared distribution and then calculate the attack detection probability using Monte Carlo simulations. Furthermore, the authors show that the less knowledge the assailant has about the system, the higher the detection rate would be. Finally, through case studies the authors show that the scenario with limited resources can cause more damage than that with imperfect knowledge. It is important to highlight that the authors restrict their study on the imperfect knowledge case to line reactance values and do not consider the case where the attacker has only partial knowledge about the topology of the grid.

Load redistribution attacks are considered in [23]. The authors target load and power flow measurements in order to redistribute the total load that is kept constant, among the different nodes in the network. This is a special case of FDI attacks. The authors claim that a necessary condition for a successful attack against the SE is having full knowledge about the network. For this reason, they restricted their study to the development of a load redistribution attack. The authors show that if the attack targets a specific region of the network and causes the phase angles of all the boundary buses of this region to increase or decrease in the same way, the attack will be undetected. This would mean that the attacker will not need any information about the network beyond the boundary buses. The authors do not consider any phase angle measurements which might compromise the proposed attack model. The authors advance their work in [24] where they propose a method for choosing an optimal attacking region if a specific load bus is to be targeted. They present the problem as a mixed integer linear programming (MILP) problem that minimizes topology, load level, and network parameter information, as well as the number of targeted measurements. Since the authors assume the attacker does not have full information about the entire grid, the solution is suboptimal based on the region that is to be attacked. In [30], the work is extended further to investigate the attack strategy against nonlinear SE.

Increasing measurement redundancy makes carrying out successful FDI attacks more difficult. This is studied in [25]. The authors propose an algorithm that minimizes the number of Phasor Measurement Units (PMUs) to be added as well as the locations to add them based on an impact metric that they define. Their impact metric takes into account the effect of changing the state variables on the dependent variables. It is calculated to quantify the deviation of the system state from the real value due to an undetected FDI attack. This however only increases the cost of carrying out FDI attacks but cannot prevent them.

In [26], the authors consider using protected meters to protect the SE against attacks. The authors argue that the defense and attack budgets are both limited and thus the interaction between the two should be taken into account when choosing which measurements to protect. The problem is then constructed as a mixed integer nonlinear programming (MINLP) problem where the overall defense budget is minimized while protecting the most vulnerable PMUs. This is then extended to become a multi-objective problem that maximizes the required attack budget. The optimization problem was solved using Bender's decomposition to reduce complexity and running time. The proposed method, however, depends on having an understanding of the behavior of the attacker.

3. Partial FDI attacks on SE

In this section the following hypothesis is proposed:

It is possible to carry out a successful full-fledged FDI attack on a partial grid with no knowledge about the rest of the power system.

To prove this hypothesis, the power system is first divided into attacking and non-attacking regions, similarly to [23]. The former is the part of the system that the attacker targets. The attacker is assumed to have full knowledge about this region as well as access to its measurements. On the other hand, the attacker is assumed to have zero knowledge about the non-attacking region and cannot compromise any of its measurements. Those buses that link the two regions together, are henceforth referred to as boundary buses and considered as part of the attacking region.

To differentiate between the two aforementioned regions, Eq. (2) is rewritten as follows:

$$\boldsymbol{z} = \begin{bmatrix} \boldsymbol{z_a} \\ \boldsymbol{z_n} \end{bmatrix} = \boldsymbol{Hx} + \boldsymbol{e} = \begin{bmatrix} \boldsymbol{H_{aa}} & \boldsymbol{H_{an}} \\ \boldsymbol{H_{na}} & \boldsymbol{H_{nn}} \end{bmatrix} \begin{bmatrix} \boldsymbol{x_a} \\ \boldsymbol{x_n} \end{bmatrix} + \begin{bmatrix} \boldsymbol{e_a} \\ \boldsymbol{e_n} \end{bmatrix} \tag{17}$$

where,

- $\boldsymbol{z_a}$, $\boldsymbol{x_a}$, $\boldsymbol{e_a}$ and $\boldsymbol{z_n}$, $\boldsymbol{x_n}$, $\boldsymbol{e_n}$ are the vectors of measurements, states and errors in the attacking and non-attacking regions respectively
- $\boldsymbol{H_{aa}}$ is a matrix containing the coefficients of $\boldsymbol{x_a}$ in the equations of $\boldsymbol{z_a}$
- $\boldsymbol{H_{an}}$ is a matrix containing the coefficients of $\boldsymbol{x_a}$ in the equations of $\boldsymbol{z_n}$
- $\boldsymbol{H_{na}}$ is a matrix containing the coefficients of $\boldsymbol{x_n}$ in the equations of $\boldsymbol{z_a}$
- $\boldsymbol{H_{nn}}$ is a matrix containing the coefficients of $\boldsymbol{x_n}$ in the equations of$\boldsymbol{h_n}$

Note that, because of the nature of Eq. (3), any $h_i(\boldsymbol{x})$ can only be a function of a limited subset of the state vector $\boldsymbol{x}$. For example, if $h_i(\boldsymbol{x})$ corresponds to a phase angle measurement θ_k at bus k, it will only be a function of x_{k-1} (note that x_1 corresponds to θ_2 since bus 1 is assumed to be the slack bus). If it corresponds to a power flow measurement P_{km}, it will be a function of x_{k-1} and x_{m-1}. If it represents an injected power measurement P_k, it will be a function of x_{k-1} and all $\boldsymbol{x}$ corresponding to buses immediately connected to the bus k. This means that $\boldsymbol{H_{an}}$ and $\boldsymbol{H_{na}}$ are sparse matrices with only the entries corresponding to the boundary buses being non-zero.

As explained in Section 2.2, for an FDI attack to remain undetected, the attack vector needs to be a linear combination of the columns of the $\boldsymbol{H}$ matrix. Eqs. (15) and (16) can then be rewritten as follows:

$$\boldsymbol{a} = \begin{bmatrix} \boldsymbol{a_a} \\ \boldsymbol{a_n} \end{bmatrix} = \boldsymbol{Hc} = \begin{bmatrix} \boldsymbol{H_{aa}} & \boldsymbol{H_{an}} \\ \boldsymbol{H_{na}} & \boldsymbol{H_{nn}} \end{bmatrix} \begin{bmatrix} \boldsymbol{c_a} \\ \boldsymbol{c_n} \end{bmatrix} \tag{18}$$

$$\boldsymbol{x}' = \begin{bmatrix} \boldsymbol{x}'_a \\ \boldsymbol{x}'_n \end{bmatrix} = \hat{\boldsymbol{x}} + \boldsymbol{c} = \begin{bmatrix} \boldsymbol{x_a} \\ \boldsymbol{x_n} \end{bmatrix} + \begin{bmatrix} \boldsymbol{c_a} \\ \boldsymbol{c_n} \end{bmatrix} \tag{19}$$

where $\boldsymbol{a_a}$, $\boldsymbol{c_a}$, $\boldsymbol{x}'_a$ and $\boldsymbol{a_n}$, $\boldsymbol{c_n}$, $\boldsymbol{x}'_n$ are the attack vector, vector of coefficients and altered states in the attacking and non-attacking regions, respectively.

Since the attacker has no access to the measurements in the non-attacking region, the following equation logically holds:

$$\boldsymbol{a_n} = \boldsymbol{H_{na}c_a} + \boldsymbol{H_{nn}c_n} = 0 \tag{20}$$

This equation can then be divided into two parts:

$$\boldsymbol{H_{nn}c_n} = 0 \tag{21}$$

$$\boldsymbol{H_{na}c_a} = 0 \tag{22}$$

Based on Eq. (21), $\boldsymbol{c_n} = 0$, is a necessary condition for (20). This means that the phase angles in the non-attacking region must remain unchanged. This differs from the condition suggested in [23] since in the model presented herein, phase angle measurements are considered.

As such, Eqs. (18) and (19) become:

$$\boldsymbol{a} = \begin{bmatrix} \boldsymbol{a_a} \\ 0 \end{bmatrix} = \boldsymbol{Hc} = \begin{bmatrix} \boldsymbol{H_{aa}} & \boldsymbol{H_{an}} \\ \boldsymbol{H_{na}} & \boldsymbol{H_{nn}} \end{bmatrix} \begin{bmatrix} \boldsymbol{c_a} \\ 0 \end{bmatrix} \tag{23}$$

$$\boldsymbol{x}' = \begin{bmatrix} \boldsymbol{x}'_a \\ \boldsymbol{x}'_n \end{bmatrix} = \hat{\boldsymbol{x}} + \boldsymbol{c} = \begin{bmatrix} \hat{\boldsymbol{x}}_a \\ \hat{\boldsymbol{x}}_n \end{bmatrix} + \begin{bmatrix} \boldsymbol{c_a} \\ 0 \end{bmatrix} \tag{24}$$

For Eq. (22) to hold, because of the previously explained nature of the $\boldsymbol{H_{na}}$ matrix, only the entries of $\boldsymbol{c_a}$ that correspond to the boundary buses need to be zero. Eq. (23) is then reduced to:

$$\boldsymbol{a_a} = \boldsymbol{H_{aa}c_a} \tag{25}$$

The attack will then be successful and remain undetected if Eq. (25) is satisfied and $\boldsymbol{c_a}$ (and consequently $\boldsymbol{a_a}$) has zero entries for the boundary buses. Notice that no knowledge of $\boldsymbol{H_{an}}$, $\boldsymbol{H_{na}}$ or $\boldsymbol{H_{nn}}$ is needed to carry out the attack and thus, the proposed hypothesis is verified.

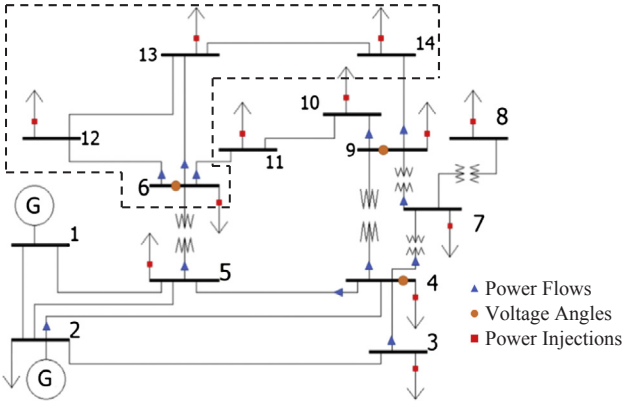

Fig. 1. IEEE 14 bus system.

4. Motivating example

In this section, the partial grid FDI attack under study is demonstrated. The test network used, the process of choosing the attack vector and the state estimation results following the attack are presented and analyzed as well.

4.1. Test network

The modified IEEE 14 bus system [31], commonly adopted in literature for these type of studies [11,21–25], was used. The system is illustrated in Fig. 1, and comprises 14 buses, 13 loads, 2 generators and 27 measurements. The measurements are distributed as follows:

- 12 power flows (shown as $P_{x,y}$ for the power flow of the line connecting bus x to bus y),
- 3 voltage angles (shown as θ_x for the phase angle of bus x), and
- 12 power injections (shown as P_x, for the generation, and L_x, for the load, at bus x)

The measurement values were chosen based on theoretical load flow results. Since actual measurements are noisy and imperfect, a random error, falling within the standard deviation of the measurement units, was introduced to each of the measurements. The standard deviations of the measurements reflect their perceived accuracy levels and are chosen in our work based on sample values reported in [14]. These values are presented in Table 1.

The partial grid to be attacked can be seen within the dotted lines in Fig. 1 and separately in Fig. 2. It comprises 4 buses and 7 measurements. The attacker is assumed to have:

- full knowledge about this section of the grid
- access to all the measurements within the considered section
- no knowledge about or access to anything beyond the section

4.2. Mounting the attack

It is clear from Fig. 1 that the boundary buses of the considered partial grid are buses 6 and 14. This means that any attack vector that would go undetected, should not result in a change in the estimated

Table 1
Standard deviations of measurements.

Measurement type	Standard deviation σ
Voltage angles	0.004
Power flows	0.008
Power injections	0.012

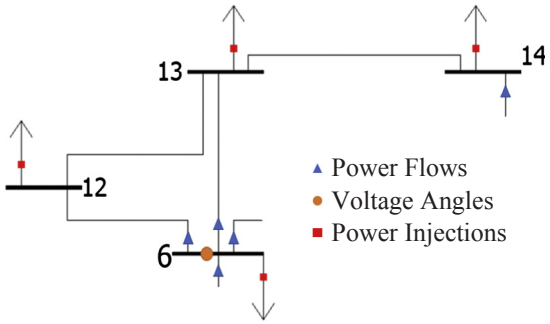

Fig. 2. Section of the grid to be targeted.

phase angles for these two buses.

Based on Eq. (3), the matrix $\boldsymbol{H_{aa}}$ is constructed as follows:

$$\boldsymbol{H_{aa}} = \begin{bmatrix} 3.9091 & -3.9092 & 0 & 0 \\ 7.6764 & 0 & -7.6764 & 0 \\ -20.5811 & 3.9092 & 7.6764 & 0 \\ 3.9092 & -8.9122 & 5.0030 & 0 \\ 7.6764 & 5.0030 & -15.5528 & 2.8734 \\ 0 & 0 & 2.8734 & -6.5719 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

As seen in Section 3, for the attack to remain undetected, the attack vector needs to be calculated based on Eq. (25). As was proposed in [20] for FDI attacks targeting the entire grid, partial grid attacks can also be customized to target: (a) a certain set of measurements, (b) specific estimated states, or (c) a combination of both. To target specific measurements, the attack vector $\boldsymbol{a_a}$ would need to have 0 entries for the non-targeted measurements. Moreover, targeting an estimated state can be done by imposing specific values for the entries of the vector $\boldsymbol{c_a}$.

In this example, the phase angle for bus 13 is targeted and its estimated value is decreased by 0.01 rad. This means that the vector $\boldsymbol{c_a}$ is given as follows:

$$\boldsymbol{c_a} = \begin{bmatrix} 0 \\ 0 \\ -0.01 \\ 0 \end{bmatrix}$$

The vector $\boldsymbol{a_a}$ is then calculated as:

$$\boldsymbol{a_a} = \begin{bmatrix} 3.9091 & -3.9092 & 0 & 0 \\ 7.6764 & 0 & -7.6764 & 0 \\ -20.5811 & 3.9092 & 7.6764 & 0 \\ 3.9092 & -8.9122 & 5.0030 & 0 \\ 7.6764 & 5.0030 & -15.5528 & 2.8734 \\ 0 & 0 & 2.8734 & -6.5719 \\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ -0.01 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0.076764 \\ -0.076764 \\ -0.050030 \\ 0.155528 \\ -0.028734 \\ 0 \end{bmatrix}$$

To check whether or not the changes to the measurements based on this attack vector remain undetected, a full SE (for the entire grid) was carried out. The resulting estimated states, reported in Table 2, confirm that only the targeted phase angle for bus 13 was changed, as identified in bold. Table 3 concurrently shows the original measured, altered (by the attack) and calculated values (after the SE) as well as the normalized residuals for all affected measurements. Despite the resulting load measurement at bus 13 being more than double its actual value and the power flow from bus 12 to 13 that increased to 5.5 times its original value and that from 13 to 14 that dropped to less than half its original value.

Table 2
Estimated states for the test network with and without the attack.

State	No-attack (radians)	Attack (radians)	State	No-attack (radians)	Attack (radians)
θ_2	−0.0868	−0.0868	θ_9	−0.2778	−0.2778
θ_3	−0.2248	−0.2247	θ_{10}	−0.2831	−0.2831
θ_4	−0.1838	−0.1838	θ_{11}	−0.2767	−0.2767
θ_5	−0.1576	−0.1576	θ_{12}	−0.2831	−0.2831
θ_6	−0.2636	−0.2636	θ_{13}	**−0.2853**	**−0.2953**
θ_7	−0.2456	−0.2456	θ_{14}	−0.3033	−0.3033
θ_8	−0.2458	−0.2458			

Table 3
Measurement residuals – partial FDI attack case.

Measurement	Original value (pu)	Altered Value (pu)	Calculated value (pu)	Normalized residual
$P_{6,12}$	0.082	0.082	0.0766	0.6805
$P_{6,13}$	0.169	0.245764	0.2437	0.2625
L_6	0.114	0.037236	0.0342	0.2500
L_{12}	0.06	0.00997	0.0157	0.4833
L_{13}	0.123	0.278528	0.2816	0.2583
L_{14}	0.144	0.115266	0.1173	0.1666
θ_6	−0.264	−0.264	−0.2636	0.1

4.3. Independence of attack from Non-Attacking region

The attack discussed in the previous section assumes that the attacker has no knowledge about the non-attacking region of the grid. This means that if the partial grid from Fig. 2 was removed and placed in a different grid, as long as the relation between this part and the rest of the grid remains the same, the FDI attack should still be undetected. This section validates this observation.

The alternate network in Fig. 3 is constructed.

Table 4 compares the results for the estimated states, under conditions of attack and no-attack. As shown in bold, once more, only the voltage angle of bus 13 changed as a result of the attack. In fact, the results for the normalized residuals for the affected measurements are identical to those seen in Table 3 and as such are not included again in this section. The attack thus remains undetected in the alternate grid as well.

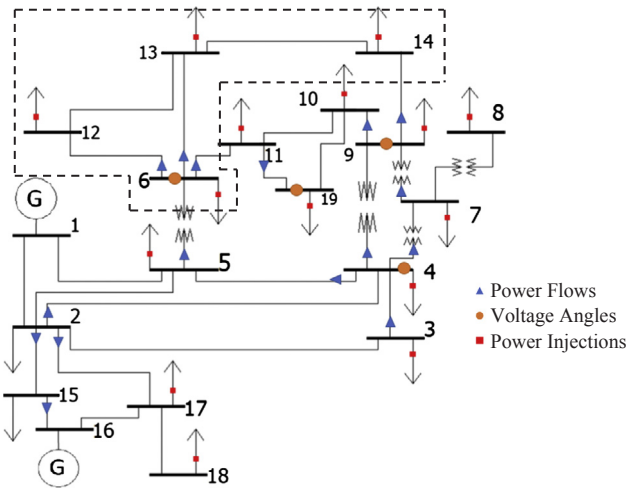

Fig. 3. Alternate system with the same partial grid attack.

Table 4
Estimated states for the alternate network with and without the attack.

State	No-attack (radians)	Attack (radians)	State	No-attack (radians)	Attack (radians)
θ_2	−0.0871	−0.0871	θ_{11}	−0.2772	−0.2772
θ_3	−0.2250	−0.2250	θ_{12}	−0.2835	−0.2835
θ_4	−0.1841	−0.1841	θ_{13}	**−0.2857**	**−0.2957**
θ_5	−0.1579	−0.1579	θ_{14}	−0.3035	−0.3035
θ_6	−0.2639	−0.2639	θ_{15}	−0.0814	−0.0814
θ_7	−0.2459	−0.2459	θ_{16}	−0.0450	−0.0450
θ_8	−0.2460	−0.2460	θ_{17}	−0.0700	−0.0700
θ_9	−0.2780	−0.2780	θ_{18}	−0.0721	−0.0721
θ_{10}	−0.2833	−0.2833	θ_{19}	−0.2830	−0.2830

4.4. Comparison with isolated grid

As seen in Sections 4.2 and 4.3, using the studied attack strategy, it is possible to mount an undetectable attack on a partial grid without having any knowledge about the rest of the network. In this section, a traditional attack is designed for the partial grid without consideration of boundary nodes, thus treating it as an isolated grid.

The same partial grid of Fig. 2 is considered in this case. The attack is designed to simulate a similar impact on the power flows as the attack in Section 4.2, increasing the power flow from bus 6 to bus 13 by a factor of 1.5, decreasing the power flow from bus 13 to 14 by half and increasing the power flow from bus 12 to 13 by a factor of 5.5. However, in this case, recall that the attack is achieved without considering boundary buses. As such, the vector $\boldsymbol{c}$ is given as follows:

$$\boldsymbol{c} = \begin{bmatrix} 0.02 \\ 0.02 \\ 0.01 \\ 0.02 \end{bmatrix}$$

The vector $\boldsymbol{a}$ is then calculated as:

$$\boldsymbol{a} = \begin{bmatrix} \mathbf{-3.9679} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{5.02765} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ 3.9091 & -3.9092 & 0 & 0 \\ \mathbf{7.6764} & \mathbf{0} & \mathbf{-7.6764} & \mathbf{0} \\ 0 & 0 & 0 & -3.6985 \\ -20.5811 & 3.9092 & 7.6764 & 0 \\ 3.9092 & -8.9122 & 5.0030 & 0 \\ 7.6764 & 5.0030 & -15.5528 & 2.8734 \\ 0 & 0 & 2.8734 & -6.5719 \\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0.02 \\ 0.02 \\ 0.01 \\ 0.02 \end{bmatrix} = \begin{bmatrix} \mathbf{-0.07936} \\ \mathbf{0.10055} \\ 0 \\ \mathbf{0.07676} \\ -0.07397 \\ -0.2567 \\ -0.0500 \\ 0.15553 \\ -0.1027 \\ 0.02 \end{bmatrix}$$

Note that the vector $\boldsymbol{a}$ has three additional rows (highlighted in bold) compared to the one in Section 4.2. This is because the vector $\boldsymbol{c}$, in this case, has non-zero values for the entries corresponding to the boundary buses and thus the power flows leaving these buses ($P_{5,6}$, $P_{6,11}$ and $P_{9,14}$) must also be included.

Treating this partial grid as an isolated, independent grid, the attack described above will remain undetected. However, if a full SE on the entire grid is carried out, it will result in high measurement residuals for measurements $P_{6,11}$, L_9 and L_{11}, as observed in Table 5. The attack will therefore be detected.

4.5. Impact of network observability

In this sub-section, the impact of the observability of the part-grid on the success of the designed attack is studied. Two scenarios are considered:

- the attacker has access to a measurement but is not sure of its exact location.
- there is a measurement in the partial grid that the attacker is unaware of.

Table 5
Measurement residuals – isolated grid case.

Measurement	Normalized Residual
$P_{6,11}$	3.5754
L_9	3.8399
L_{11}	4.4519

In the first scenario, the attacker does not know the corresponding row of the H matrix of the measurement and cannot accurately calculate its entry in the attack vector. To simulate this, the exact same attack as in Section 4.2 is used, with the addition of the measurement $P_{5,6}$ to the attack vector altered consistently with the other measurements. This results in a high residual for the measurement $P_{5,6}$ and will thus be detected by the BDD algorithm. The residuals for all relevant measurements are given in the following table:

Measurement	Original value (pu)	Altered value (pu)	Calculated value (pu)	Normalized residual
$P_{6,12}$	0.082	0.082	0.0797	0.2813
$P_{6,13}$	0.169	0.245764	0.2458	0.1055
L_6	0.114	0.037236	0.0476	0.8632
L_{12}	0.06	0.00997	0.0216	0.9679
L_{13}	0.123	0.278528	0.2872	0.7201
L_{14}	0.144	0.115266	0.1147	0.0510
θ_6	−0.264	−0.264	−0.2674	0.8440
$P_{5,6}$	0.422	0.4168	0.4363	3.169

In the second scenario, the attacker uses the H_{aa} matrix but without one of its rows. Since this measurement might contradict the compromised measurement vector, the attack may be detected. To simulate this, once again, the same attack as in 4.2 is used but ignoring measurement $P_{6,13}$ in the attack. This results in particularly high residuals for $P_{6,13}$ and L_{13} leading consequently to detection by the BDD algorithm. The residuals for all relevant measurements are given in the following table:

Measurement	Original value (pu)	Altered value (pu)	Calculated value (pu)	Normalized residual
$P_{6,12}$	0.082	0.082	0.0677	1.7902
$P_{6,13}$	0.169	0.169	0.2147	5.7182
L_6	0.114	0.037236	0.0628	2.1289
L_{12}	0.06	0.00997	0.0143	0.3638
L_{13}	0.123	0.278528	0.2412	3.1135
L_{14}	0.144	0.115266	0.1122	0.2586
θ_6	−0.264	−0.264	−0.2627	0.3327

In conclusion, it is clear from the above results that observability is required to carry out a successful partial FDI attack. Any measurement whose exact nature is not known cannot be used and full knowledge of the partial grid is required.

5. FDI attack mitigation

In this section, we rely on the definition of a protected meter as provided in [18], to propose a defense strategy against FDI attacks targeting the SE. Note that, a protected meter is a measurement unit that is secure and whose data cannot be compromised.

For an FDI attack to be undetected, in the presence of protected meters, the entries of the attack vector $\boldsymbol{a}$ corresponding to these measurements must be zero. After removing the rows with non-zero entries, Eq. (25) becomes as follows:

$$0 = \boldsymbol{H_p c} \tag{26}$$

where $\boldsymbol{H_p}$ is a submatrix of $\boldsymbol{H}$, including only the rows corresponding to the protected meters.

Eq. (26) represents a homogeneous system of equations. If this system has any solution other than the trivial solution $\boldsymbol{c} = 0$, then an

attack is possible. Therefore, to make sure that an attack is not successful, the only solution to these equations must be the trivial solution.

A homogeneous system of equations always has non-trivial solutions if it has more unknowns than equations. Thus, the first condition for complete protection against attacks is to have the number of protected meters be at least equal to the number of states n. Choosing the number of protected meters to be equal to n, the system of equations will have no non-trivial solutions, if and only if, the determinant of $\boldsymbol{H_p}$ is not zero (i.e. $\boldsymbol{H_p}$ is invertible). Note that, the $\boldsymbol{H_p}$ matrix is invertible if all its rows are linearly independent. Hence, if n independent measurements are protected, the system will be immune to attacks.

For example, the test network defined in Section 4.1 has 13 state variables and so, 13 independent measurements need to be protected. By performing QR decomposition [32] of the matrix $\boldsymbol{H}$, one can find a possible set of independent rows, the corresponding measurements are identified to be:

- Power flow measurements (from – to bus): 2–4, 3–4, 4–5, 4–7, 4–9, 5–6, 6–11, 6–12, 6–13, 9–10, 9–14
- Power injection measurements (bus): 5, 7

Once the measurement units to be protected are identified, and in case of a limited budget, further optimization can be made to reduce the number of units to be protected. This is similar to what was proposed in [25], except that in this case the complexity of the problem is significantly reduced as only a subset of the measurements need to be considered. Otherwise, it is also possible to first identify areas in the network that are of high importance or are particularly vulnerable (as in [33]) and consequently apply the proposed mitigation technique only to those areas.

If the partial grid from Fig. 2 is identified as an important area, then 4 independent measurements would need to be protected. These measurements are identified, by finding a set of independent rows of the matrix $\boldsymbol{H_a}$, to be:

- Power flow measurements (from – to bus): 6–12, 6–13
- Power injection measurements (bus): 6, 13

This method has the advantage of restricting the number of measurements to be protected to 13 out of the total of 27 measurements for the full grid and to 4 out of 7 for the partial grid.

6. Conclusion

This paper showed, mathematically, that it is possible to compromise the results of the SE through FDI attacks targeting a specific part of the power system. This can be achieved, without having any knowledge about the network or access to any measurements beyond the targeted partial grid. The findings were tested and verified on the IEEE 14 bus system. After designing an attack vector based on the measurements and characteristics of the partial grid, the BDD algorithm was used on the original IEEE 14 bus system and a modified system with 19 buses (that includes the same partial grid) and, in both cases, no attack was detected.

The paper also proposed a method to choose which measurement units to protect, in order to prevent undetectable FDI attacks targeting the SE. It was shown that, for a comprehensive defense strategy, the number of independent measurement units protected, needs to be equal to the number of state variables of the SE. In case of a limited budget, it was proposed to resort to optimization techniques to determine, from among the identified units, which ones to protect.

Acknowledgments

This project has been jointly funded with the support of the National Council for Scientific Research in Lebanon CNRS-L and the Lebanese American University.

References

[1] Mohassel Ramyar Rashed, et al. A survey on advanced metering infrastructure. Int J Electr Power Energy Syst 2014;63:473–84.
[2] Marah Rim, El Hibaoui Abdelaaziz. Algorithms for Smart Grid management. Sustain Cities Soc 2018;38:627–35.
[3] Klaimi Joelle, et al. A novel loss-based energy management approach for smart grids using multi-agent systems and intelligent storage systems. Sustain Cities Soc 2018;39:344–57.
[4] Hossain MS, et al. Role of smart grid in renewable energy: an overview. Renew Sustain Energy Rev 2016;60:1168–84.
[5] Eissa MM. New protection principle for smart grid with renewable energy sources integration using WiMAX centralized scheduling technology. Int J Electr Power Energy Syst 2018;97:372–84.
[6] Pickett Bruce, et al. Reducing outages through improved protection, monitoring, diagnostics, and autorestoration in transmission substations (69 kV and above). IEEE Trans Power Delivery 2016;31(3):1327–34.
[7] Sun Chih-Che, Hahn Adam, Liu Chen-Ching. Cyber security of a power grid: state-of-the-art. Int J Electr Power Energy Syst 2018;99:45–56.
[8] Komninos Nikos, Philippou Eleni, Pitsillides Andreas. Survey in smart grid and smart home security: issues, challenges and countermeasures. IEEE Commun Surv Tutorials 2014;16(4):1933–54.
[9] Laughman Christopher, et al. Power signature analysis. IEEE Power Energy Mag 2003;99(2):56–63.
[10] Rahman Md Ashfaqur, Mohsenian-Rad Hamed. False data injection attacks with incomplete information against smart power grids. 2012 IEEE Global Communications Conference (GLOBECOM). IEEE; 2012.
[11] Liu Yao, Ning Peng, Reiter Michael K. False data injection attacks against state estimation in electric power grids. ACM Trans Inform System Security (TISSEC) 2011;14(1):13.
[12] Skopik Florian, et al. A survey on threats and vulnerabilities in smart metering infrastructures. Int. J. Smart Grid Clean Energy 2012;1(1):22–8.
[13] Liu Xuan, Li Zuyi. False data attack models, impact analyses and defense strategies in the electricity grid. Electricity J. 2017;30(4):35–42.
[14] Gomez-Exposito Antonio, Abur Ali. Power system state estimation: theory and implementation. CRC Press; 2004.
[15] Wu Yiming, et al. Bad data detection using linear WLS and sampled values in digital substations. IEEE Trans Power Delivery 2018;33(1):150–7.
[16] Stott Brian, Jardim Jorge, Alsaç Ongun. DC power flow revisited. IEEE Trans Power Syst 2009;24(3):1290–300.
[17] Zhang Cong, et al. DC power flow analysis incorporating interval input data and network parameters through the optimizing-scenarios method. Int J Electr Power Energy Syst 2018;96:380–9.
[18] Deng Ruilong, et al. False data injection on state estimation in power systems—attacks, impacts, and defense: a survey. IEEE Trans Ind Inf 2017;13(2):411–23.
[19] Andrade Sergio Barreto, et al. Undetectable PMU timing-attack on linear state-estimation by using rank-1 approximation. IEEE Trans Smart Grid 2016.
[20] Liang Gaoqi, et al. False data injection attacks targeting DC model-based state estimation. 2017 IEEE power & energy society general meeting. IEEE; 2017.
[21] Pan Kaikai, et al. Combined data integrity and availability attacks on state estimation in cyber-physical power grids. 2016 IEEE International Conference on Smart Grid Communications (SmartGridComm). IEEE; 2016.
[22] Pan Kaikai, et al. Data attacks on power system state estimation: limited adversarial knowledge vs. limited attack resources. arXiv preprint arXiv:1708.08355; 2017.
[23] Liu Xuan, Li Zuyi. Local load redistribution attacks in power systems with incomplete network information. IEEE Trans Smart Grid 2014;5(4):1665–76.
[24] Liu Xuan, et al. Modeling of local false data injection attacks with reduced network information. IEEE Trans Smart Grid 2015;6(4):1686–96.
[25] Yang Qiang, et al. PMU placement in electric transmission networks for reliable state estimation against false data injection attacks. IEEE Internet Things J 2017;4(6):1978–86.
[26] Deng Ruilong, Xiao Gaoxi, Rongxing Lu. Defending against false data injection attacks on power system state estimation. IEEE Trans Ind Inf 2017;13(1):198–207.
[27] Caro Eduardo, Conejo Antonio J, Minguez Roberto. Power system state estimation considering measurement dependencies. IEEE Trans Power Syst 2009;24(4):1875–85.
[28] Caro Eduardo, et al. Multiple bad data identification considering measurement dependencies. IEEE Trans Power Syst 2011;26(4):1953–61.
[29] Rahman Md Ashfaqur, Mohsenian-Rad Hamed. False data injection attacks against nonlinear state estimation in smart power grids. 2013 IEEE Power and Energy Society General Meeting (PES). IEEE; 2013.
[30] Liu Xuan, Li Zuyi. False data attacks against AC state estimation with incomplete network information. IEEE Trans Smart Grid 2017;8(5):2239–48.
[31] Christie Rich. Power systems test case archive. Electrical Engineering dept.., University of Washington; 2000.
[32] Golub Gene H, Van Loan Charles F. Matrix computations. JHU Press; 2012.
[33] Anwar Adnan, Mahmood Abdun Naser, Tari Zahir. Identification of vulnerable node clusters against false data injection attack in an AMI based smart grid. Inform Syst 2015;53:201–12.