Information Systems 53 (2015) 201–212

Contents lists available at ScienceDirect

Information Systems

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

Identification of vulnerable node clusters against false data injection attack in an AMI based Smart Grid

Adnan Anwar [a,*], Abdun Naser Mahmood [a], Zahir Tari [b]

[a] School of Engineering and Information Technology (SEIT), The University of New South Wales Australia, Canberra, ACT 2610, Australia
[b] School of Computer Science and IT, RMIT University, Melbourne, VIC 3001, Australia

ARTICLE INFO

Article history:
Received 1 June 2014
Received in revised form
10 November 2014
Accepted 1 December 2014
Available online 8 December 2014

Keywords:
False data injection attack
Radial distribution networks
MatPower
Vulnerable nodes
CFPSO clustering

ABSTRACT

In today's Smart Grid, the power Distribution System Operator (DSO) uses real-time measurement data from the Advanced Metering Infrastructure (AMI) for efficient, accurate and advanced monitoring and control. Smart Grids are vulnerable to sophisticated data integrity attacks like the False Data Injection (FDI) attack on the AMI sensors that produce misleading operational decision of the power system (Liu et al., 2011 [1]). Presently, there is a lack of research in the area of power system analysis that relates the FDI attacks with system stability that is important for both analysis of the effect of cyber-attack and for taking preventive measures of protection.

In this paper, we study the physical characteristics of the power system, and draw a relationship between the system stability indices and the FDI attacks. We identify the level of vulnerabilities of each AMI node in terms of different degrees of FDI attacks. In order to obtain the interdependent relationship of different nodes, we implement an improved Constriction Factor Particle Swarm Optimization (CF-PSO) based hybrid clustering technique to group the nodes into the most, the moderate and the least vulnerable clusters. With extensive experiments and analysis using two benchmark test systems, we show that the nodes in the most vulnerable cluster exhibit higher likelihood of destabilizing system operation compared to other nodes. Complementing research is the construction of FDI attacks and their countermeasures, this paper focuses on the understanding of characteristics and practical effect of FDI attacks on the operation of the Smart Grid by analysing the interdependent nature of its physical properties.

1. Introduction

In recent years, several cyber related attacks, including the sophisticated Stuxnet worm attack [2], have highlighted the importance of security research in the area of Smart Grid infrastructure. It has been shown that a cyber-attack on the Smart Grid can cause devastating impact on our daily life resulting in cascading failures of critical Smart Grid infrastructure and disruption in economy. Sophisticated new attacks have emerged, targeting the increased use of intelligent devices (such as Smart Meters) in today's Advanced Metering Infrastructure (AMI) of the Smart Grid. There are different of kinds of attacks on the Smart Grid, including attacks on data availability, data confidentiality and data integrity. An example of data integrity attack is where a vital component of Smart Grid operational module can be affected by injecting false data into the AMI. Recently, these types of attacks, typically known as False Data Injection (FDI) attacks [3], have drawn significant attention as they can bypass the current security measures and exploit the system operations such as the state estimation process.

* Corresponding author. Tel.: +61 451001357.
E-mail address: Adnan.Anwar@adfa.edu.au (A. Anwar).

http://dx.doi.org/10.1016/j.is.2014.12.001
0306-4379/

State estimator, which is widely used at the utility control centres to calculate the system status during the power system operation, can also be used to filter out the measurement errors and noises [4]. Generally, 'state estimator' can be defined as a computer program which calculates the system states based on the measured data (at different nodes of the Smart Grid) and the equivalent modelled data (based on Kirchhoff's current and voltage laws of physical energy grid). In addition, the Bad Data Detection (BDD) module of the state estimator suppresses any bad data (if exists) based on the residual analysis. Generally, the traditional SE module works based on the principle of Weighted Least Squared (WLS) error minimization method where attack or noise is detected based on the residual analysis [4]. Liu et al. show that the Smart Grid state estimators are now highly vulnerable to the cyber attacks [3]. In the first work of these types of FDI attacks, Liu et al. show that the attack cannot be detected by the residual analysis if certain strategies are followed. Till then, significant research works have been carried out from both attacker's and defender's point of view, discussed below.

Authors in [1] develop some heuristic approaches to exploit the DC state estimation considering both random attacks and targeted attacks. Ozay et al. further extend the work by considering distributed models to generate and detect sparse attack in the state estimation process of the Smart Grid [5]. Different threats of Advance Metering Infrastructure (AMI) are also explored in the literature [6]. Defense strategies of the state estimation module and AMI devices are also well studied [7–10]. For example, a defense strategy based on graphical models to protect Smart Grid against FDI attack is proposed in [7]. In that work, authors consider a dc approximate model of the Smart Grid. Another dc approximate model based protection and detection mechanism is proposed by Yang et al. [8]. Typically, Smart Grid has non-linear power flow characteristics and an ac model of power flow equations can ensure more accurate results. Analysing and comparing with ac model, Hug et al. in [9] show that FDI attacks based on a dc model are more prone to introduce errors in the measurement devices resulting higher probability of detection through BDD technique. To protect AMI, an intrusion Detection framework based on consumption pattern of the end-users is proposed in [10]. Although significant number of research works have been conducted on simulating the FDI attacks [1,5,6] and determining the countermeasures [7–10], there are significant scopes to understand the security vulnerabilities of Smart Grid against FDI based cyber attacks by analysing the physical behaviours of the Smart Grid. Moreover, most of the existing FDI attack simulation and defense strategies are based on the transmission system [3,1,5,7–9] and there is a lack of research works considering power distribution systems. Traditionally, power distribution system has district characteristics from transmission system, e.g., high Resistance to Reactance Ratio, radial network, etc. Therefore, it is important to conduct the vulnerability analysis considering benchmark power distribution systems.

In this work, we have studied the interdependent nature of nodes in a power grid and identified the vulnerable nodes that are most sensitive to False Data Injection (FDI) attacks. We have found that if the attacker specifically targets these highly vulnerable nodes, then the attack will cause much larger impact destabilizing the operation of the power grid than any random selection of nodes. For example, if the same attack vector is introduced as an FDI attack at different measurement nodes, the power system operational states (e.g., Voltage Magnitude and Angle) will vary differently based on the physical properties of the individual nodes. The most vulnerable node identified in our analysis has the largest changes of the operational states and the opposite characteristics are observed for the least vulnerable node. This research is important from both attacker's and system operator's (defender) point of view. Based on the understanding of the node characteristics of the physical Smart Grid, the attacker can decide which node to attack to ensure significant changes of the operational states. On the other hand, the system operator (act as a defender) can emphasis on the real-time monitoring of the vulnerable nodes and introduce proper security measures (e.g., real-time Intrusion Prevention and Detection systems) on those locations. Besides, a distribution system state estimation in a Smart Grid, which has different characteristics from the widely used transmission system state estimation, makes use of AMI measurements instead of pseudo-measurements to enhance the state estimation performance [11]. These AMI measurements are deployed at the end-user nodes. The output of the Smart Grid state estimation will be corrupted if an attacker injects False Data in those AMI measurement devices. In this work, we also conduct vulnerability analysis at different AMI measurement nodes with different degrees of FDI attacks.

Specifically, the contributions of this paper are as follows:

(1) In contrast to existing work on FDI attacks that lack comprehensive power system analysis of the effect of the FDI, in this paper we provide a theoretical study of the relationship between FDI attack vectors and their effect on nodal and system stability (Section 2.3). We show that the Voltage Stability Index (VSI) [12], which is widely used by Power System engineers to determine the system stability [13,14], can also be used to understand the likelihood of system stability under different degrees of FDI based cyber attacks. To the best of our knowledge, this paper, for the first time, considers the voltage stability based indices to understand the cyber-physical vulnerabilities under any information integrity attack (e.g., FDI attacks) of a smart power distribution system.
(2) In order to properly identify nodes with similar levels of vulnerabilities in a complex system, we propose and implement a hybrid clustering algorithm based on the traditional well studied k-means algorithm and the Constriction Factor Particle Swarm Optimization (CF-PSO) to enhance the clustering performance. Experiments performed using test data from UCI repository of machine learning databases show that the CF-PSO based improved clustering outperforms the traditional k-means algorithm and the CF-PSO based clustering. This improved clustering algorithm is then employed to identify nodes that behave similarly based on their physical properties in response to an FDI attack.

(3) Using the developed stability relationship model and the improved clustering technique, we show that there are certain clusters of nodes in a Smart Grid Distribution System that are more susceptible, e.g., becomes highly unstable, to FDI attacks compared to other nodes in the grid. For example, the average change of nodal voltage magnitude of the most vulnerable cluster is around 506 kV and the least vulnerable cluster experiences around 253 kV, when an equal FDI attack vector is added with the original measurements.

The organization of this paper is as follows: In Section 2, the definitions of VSI and FDI attacks and their relationship are discussed. CF-PSO based Improved Clustering Technique is proposed and evaluated in Section 3. The results and discussions of AMI node vulnerabilities due FDI attacks, considering benchmark test systems, are presented in Section 4. A brief discussion on the protection of the vulnerable nodes against cyber intrusions is presented in Section 5. The paper concludes with some brief remarks in Section 6.

2. Discussion on FDI attacks and voltage stability indices

2.1. Voltage Stability Index (VSI)

Power distribution system has distinct characteristics compared with transmission system, e.g., high Resistance/Reactance ration, radial nature, low voltage and high current level, more power loss compared with transmission systems, etc. [15]. In a power distribution system, voltage stability is a major issue [16].

Generally, substation operates at a higher voltage and the node voltage decreases gradually throughout the distribution feeder. Distribution System Operator (DSO) needs to maintain the voltage profile of each node of the system within a stability margin. Under critical loading condition or any physical disturbance, distribution system may face voltage collapse. In practice, the voltage drops gradually with the increase of the loading and after a certain limit, there is a sharp decrease of the voltage magnitude which changes the frequency and makes the system unstable for operation.

Significant research works have been conducted for voltage stability analysis for both transmission and distribution systems [17]. In this work, we consider a well established voltage stability index proposed by Chakravorty et al. as follows [12]:

$$VSI(N_r) = V_s^4 - 4(P_r X - Q_r R)^2 - 4(P_r R + Q_r X)V_s^2 \quad (1)$$

where $VSI(N_2)$ is the voltage stability index at the receiving end of (N_r) a branch. V_s is the voltage magnitude at the sending end (N_s), R and X are the resistance and reactance of that branch respectively. P_r is the summation of the real power loads of all downstream nodes from the node 'r', the real power load at node 'r' and the real power losses of all downstream branches from the node 'r'. Similarly, Q_r is the summation of the reactive power loads of all downstream nodes from the node 'r', the reactive power load at node 'r' and the reactive power losses of all downstream branches from the node 'r'.

Power flow study, which is basically based on Kirchhoff's current and voltage laws of the physical system, provides the system states, including V_s, P_r and Q_r. Other parameters of Eq. (1), R and X, can be obtained from the power network electric topological database. After a successful power flow solution of system, all parameters of Eq. (1) are known from which the *VSI* index of each node can be calculated.

For a stable operation of the system, i.e., the voltage magnitude larger than the voltage collapse point, the $VSI(N_r) \geq 0$. The node with the minimum *VSI* indicates that it is more prone to voltage collapse compared with other nodes of that system [12].

2.2. FDI attacks on the Smart Grid state estimation

For safe and reliable operation of the power distribution system, operators need to monitor and control the system as it progresses through its various operating states. To reduce measurement errors, state estimation is widely used by power system operators to calculate theoretical values of the system parameters (e.g., Voltage, Current, and Power) and compare against the measurement data. [4]. However, a traditional power distribution system has very limited number of measurement devices, consequently, pseudo-measurements are made instead [18]. Pseudo-measurements are derived from the forecasted consumer demand data which is calculated based on the historical consumption profile of the end users. As forecasted data comes with forecast error and errors due to change in end user behaviour [19], the pseudo-measurements are unreliable for accurate state estimation of a traditional power system. Fortunately, in a Smart Grid context, the real-time AMI measurements can significantly improve the state estimation accuracy by incorporating the actual readings from the Smart Meters [11]. However, FDI attacks through AMI devices may bypass the Bad Data Detection (BDD) module of the state estimator using sophisticated attack strategies [1], discussed below.

2.2.1. FDI attack on DC state estimation

Consider a measurement vector $\mathbf{z}$ for a n-bus systems with m AMI measurements. The measurement vector $\mathbf{z}$ contains measurement noises (which is assumed white Gaussian noise as represented by $\mathbf{e}$), therefore, $\mathbf{z}$ can be written as follows:

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e} \quad (2)$$

here, $\mathbf{H}$ is the calculated function values for the state variables $\mathbf{x}$, typically known as system Jacobian [1]. Now, the state estimation can be formulated as a Weighted Least Square (WLS) error minimization problem as follows:

$$\min \quad \|\mathbf{z} - \mathbf{H}\mathbf{x}\| \quad (3)$$

Under normal operating condition, the measurement data and the equivalent modelled data of those measurement outputs are very close, hence, the error obtained from the state estimation module is very close to zero and lies within the threshold value. In this situation, $\|\mathbf{z} - \mathbf{H}\mathbf{x}\| < \tau$, the Bad Data Detection module of the state estimation detects no Alarms. If an attacker can gain access to the measurement devices including AMI sensors, an attack vector 'a' can be manipulated with the measurement signals such that the

corrupted state becomes $x' = x + c$ and the new corrupted measurement is $z' = z + a$. To keep the attack undetectable, the attacker can choose the attack vector in such a way that $a = Hc$ where c is a vector of non-zero values with the same length of H, as suggested by Liu et al. [3,1]. Therefore, for the new corrupted states x', the manipulated norm of the residual will be

$$\begin{aligned} \|\mathbf{z}' - \mathbf{H}\mathbf{x}'\| &= \|\mathbf{z} + \mathbf{a} - \mathbf{H}(\mathbf{x} + \mathbf{c})\| \text{ (here, } \mathbf{x}' = \mathbf{x} + \mathbf{c} \text{ and } \mathbf{z}' = \mathbf{z} + \mathbf{a}) \\ &= \|\mathbf{z} + \mathbf{a} - \mathbf{H}\mathbf{x} - \mathbf{H}\mathbf{c}\| \\ &= \|\mathbf{z} - \mathbf{H}\mathbf{x}\| \quad (\text{as, } \mathbf{a} = \mathbf{H}\mathbf{c}) \end{aligned}$$

From the above expression, the residual from the corrupted measurements produces the same residual as calculated by the normal system operation. Hence, $\|\mathbf{z}' - \mathbf{H}\mathbf{x}'\|$ will pass the BDD test as $\|\mathbf{z} - \mathbf{H}\mathbf{x}\| < \tau$, and the FDI attack remains undetectable.

2.2.2. FDI attack on AC state estimation

In the previous section, we discussed the stealthy FDI attacks on the DC state estimation. Here, a discussion on *how the state estimation module of the AC system can also be compromised considering the FDI attacks* is presented.

In the state estimator of AC systems, the measured power flows are a nonlinear function of system states (e.g., voltage magnitudes and angles). Hence, the AC state estimation can be modelled using the following nonlinear expressions:

$$\min \quad \|\mathbf{z} - \mathbf{h}(\mathbf{x})\| \tag{4}$$

where $\mathbf{z}$ is the measurement vector that can be written as follows:

$$\mathbf{z} = \begin{bmatrix} \mathbf{z}_1 \\ \vdots \\ \mathbf{z}_{n-m} \\ \vdots \\ \mathbf{z}_n \end{bmatrix} = \begin{bmatrix} \mathbf{h_1}(\mathbf{x_1}, \mathbf{x_2}, .., \mathbf{x_3}) \\ \vdots \\ \mathbf{h_{n-m}}(\mathbf{x_1}, \mathbf{x_2}, .., \mathbf{x_3}) \\ \vdots \\ \mathbf{h_n}(\mathbf{x_1}, \mathbf{x_2}, .., \mathbf{x_3}) \end{bmatrix} + \begin{bmatrix} \mathbf{e_1} \\ \vdots \\ \mathbf{e_{n-m}} \\ \vdots \\ \mathbf{e_n} \end{bmatrix} = \mathbf{h}(\mathbf{x}) + \mathbf{e} \tag{5}$$

here, $\mathbf{e}$ is the vector of measurement noise, $\mathbf{x}$ is the vector of system states (generally, voltage magnitudes and angles), $\mathbf{h}(\mathbf{x})$ is the Jacobian matrix which is also represented as J_h. It shows the non-linear relation of the measurements and the system states, as shown below:

$$J_h = \begin{bmatrix} \frac{\partial h_1}{\partial x_1} & \frac{\partial h_1}{\partial x_2} & \cdots & \frac{\partial h_1}{\partial x_{n-1}} & \frac{\partial h_1}{\partial x_n} \\ \frac{\partial h_2}{\partial x_1} & \frac{\partial h_2}{\partial x_2} & \cdots & \frac{\partial h_2}{\partial x_{n-1}} & \frac{\partial h_2}{\partial x_n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{\partial h_{m-1}}{\partial x_1} & \frac{\partial h_{m-1}}{\partial x_2} & \cdots & \frac{\partial h_{m-1}}{\partial x_{n-1}} & \frac{\partial h_{m-1}}{\partial x_n} \\ \frac{\partial h_m}{\partial x_1} & \frac{\partial h_m}{\partial x_2} & \cdots & \frac{\partial h_m}{\partial x_{n-1}} & \frac{\partial h_m}{\partial x_n} \end{bmatrix} \tag{6}$$

Upon gaining the access of a specific measurement device, the attacker can launch a FDI attack which alters the value of measurement data. In order to keep the attacked measurement hidden, at least one state variable needs to be influenced (otherwise, error value obtained from the state estimator (shown in Eq. (4)) will cross the threshold and attack will be detected) [9]. Note that the attacker can only access to the measurement devices but not the system states. Therefore, the attacker will manipulate only the measurements which are directly related to those system states to keep it undetectable [9]. Relation of the measurements and the system states can be found from the Jacobian matrix, J_h as shown in Eq. (6).To this end, the AC state estimation process under the FDI attack can be written as [9]

$$\begin{aligned} &\|\mathbf{z}' - h(\mathbf{x}')\| \\ &= \|\mathbf{z} + \mathbf{a} - h(\mathbf{x} + \mathbf{c})\| \\ &= \left\| \begin{pmatrix} \mathbf{z_n} \\ \mathbf{z_a} + \mathbf{a} \end{pmatrix} - \begin{pmatrix} h(\mathbf{x_n}) \\ h(\mathbf{x_n}, \mathbf{x_a} + \mathbf{c}) \end{pmatrix} \right\| \end{aligned} \tag{7}$$

where $\mathbf{z} = \mathbf{z_n} + \mathbf{z_a}$ and $h(\mathbf{x}) = h(\mathbf{x_n}) + h(\mathbf{x_n}, \mathbf{x_a} + \mathbf{c})$, considering that the terms with subscript '**n**' are normal measurements and system states and the terms with subscript '**a**' are attacked measurements and system states. In order to keep the FDI attack undetectable, $\|\mathbf{z}' - h(\mathbf{x}')\| = \|\mathbf{z} - h(\mathbf{x})\|$ (as, in normal condition $\|\mathbf{z} - h(\mathbf{x})\| < \tau$). Therefore,

$$\begin{aligned} &\|\mathbf{z}' - h(\mathbf{x}')\| \\ &= \|\mathbf{z} - h(\mathbf{x})\| \\ &= \left\| \begin{pmatrix} \mathbf{z_n} \\ \mathbf{z_a} \end{pmatrix} - \begin{pmatrix} h(\mathbf{x_n}) \\ h(\mathbf{x_n}, \mathbf{x_a}) \end{pmatrix} \right\| \end{aligned} \tag{8}$$

solving Eqs. (7) and (8), the value of attack vector, $\mathbf{a}$, can be obtained as follows [9]:

$$\mathbf{a} = h(\mathbf{x_n}, \mathbf{x_a} + \mathbf{c}) - h(\mathbf{x_n}, \mathbf{x_a}) \tag{9}$$

From Eq. (9), to launch an attack vector $\mathbf{a}$, the attacker needs to know the relevant system state values. More information on how the attacker can initiate the undetectable FDI attacks on the state estimation module of an AC system can be obtained from [9].

The observation of Liu et al. [3,1] for DC state estimation and the observation of Hug et al. [9] for AC state estimation can also be applied in the context of AMI based Smart Grids, if we consider the AMI measurements are a subset of the total measurements as shown in Eq. (5). If an attacker gains access to all or a subset of the AMI devices, say, l-AMI devices, he/she can generate an FDI attack by choosing a nonzero attack vector $\mathbf{a} = \{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$ in such a way that the attack vectors at the non-accessible devices become zero (so, $a_i = 0$, where, $i \neq \{AMI\ devices\}$). More insights on how undetectable attacks can be generated and their possible countermeasures are studied in recent works [20,3,1,5,7–9]. It is important to mention that the FDI attacks (where the objective of the attack is to disrupt the system operation) through the AMI devices have two major consequences.

(1) If the FDI attack remains *undetectable* (e.g., residuals are less than a threshold in the traditional Weighted Least Square based estimator), the system states (e.g., voltage magnitude, angle) obtained from the state estimation process will provide wrong information [4]. Real-time or extended real-time operation of the system, e.g., Optimal Power Flow (OPF)

solution or Volt-VAr Control (VVC), will produce misleading operational decisions based on the wrong system states obtained from the state estimation process. This misleading operational decision will degrade the system performance and stability, which may even lead to a large-scale blackout or cascading failure.

(2) In those cases where the FDI attack becomes *detectable* through the residual test, or using other Intrusion Detection Systems, it is still difficult to perform state estimation based on the limited measurements which are not corrupted. Therefore, the system states are unobservable for a portion of the network where the measurements are corrupted [9]. Hence, it is not possible to take operational decisions based on the limited knowledge of the whole system.

Consequently, FDI attacks, whether detected or undetected, will have direct impact on the operation of the Smart Grid. As the scope of this paper is to investigate the effect of FDI attacks on system stability under different degrees of FDI attacks, in the next section, we will show how the relationship of the VSI index and FDI is correlated.

2.3. Relationship of the VSI index and FDI attack vectors

Generally, for real-time or extended real-time operation of SPDS, the electricity distribution operator collects power consumption data from the AMI devices through a SCADA network. If an attacker gains access to any or all of the AMI devices, he/she can manipulate the power consumption data by injecting false information. Let us consider the l-AMI devices are under FDI attacks, therefore, the corrupted real and reactive power measurements, $\mathbf{P}_i^{FDI}$ and $\mathbf{Q}_i^{FDI}$, will be as follows:

$$\mathbf{P}_i^{FDI} = \mathbf{P}_i^0 + \mathbf{a}_i; \quad i\forall\ \{1,2,\ldots,l\} \tag{10}$$

$$\mathbf{Q}_i^{FDI} = \mathbf{Q}_i^0 + \mathbf{a}_i; \quad i\forall\ \{1,2,\ldots,l\} \tag{11}$$

where $\mathbf{P}_i^0$ and $\mathbf{Q}_i^0$ are the actual measured real and reactive powers of i-th AMI devices respectively. $\mathbf{a}_i$ represents the corresponding attack vectors. Now, considering $\mathbf{a}_i = \mathbf{P}_i^0\boldsymbol{\beta}_i$, where $\boldsymbol{\beta}$ is a multiplication factor of actual measurements, Eq. (10) can be written as

$$\begin{aligned}\mathbf{P}_i^{FDI} &= \mathbf{P}_i^0 + \mathbf{P}_i^0\boldsymbol{\beta}_i \\ &= \mathbf{P}_i^0(1+\boldsymbol{\beta}_i) \\ &= \mathbf{P}_i^0\lambda_i \quad (\text{consider},\ 1+\boldsymbol{\beta}_i = \lambda_i)\end{aligned} \tag{12}$$

Similarly,

$$\mathbf{Q}_i^{FDI} = \mathbf{Q}_i^0\lambda_i \tag{13}$$

In Eqs. (12) and (13), we define λ as the degree of attack which can be any real number.

Now, recall that the VSI of any node of the Smart Grid is defined using Eq. (1). From the definition of VSI, real and reactive power at the r-th node can be written under the normal operational condition as follows:

$$P_r = \sum_{i\forall c} P_L^0 + P_{L(r)}^0 + \sum_{i\forall d} P_{Loss} \tag{14}$$

$$Q_r = \sum_{i\forall c} Q_L^0 + Q_{L(r)}^0 + \sum_{i\forall d} Q_{Loss} \tag{15}$$

where P_L^0 and Q_L^0 are the real and reactive power loads of the energy users, respectively. $P_{L(r)}$ and $Q_{L(r)}$ are the real and reactive power loads of the r-th energy users, respectively. P_{Loss} and Q_{Loss} are the real and reactive power losses of the branches, respectively. Here, c and d represent all bus and branches respectively, beyond the node 'r' where VSI is being calculated.

If 'r' is an AMI measurement node, under an attack scenario Eqs. (14) and (15) can be modified using Eqs. (12) and (13) as follows:

$$P_r = \sum_{i\forall c} P_L^0 + P_{L(r)}^0\lambda_r + \sum_{i\forall d} P_{Loss} \tag{16}$$

$$Q_r = \sum_{i\forall c} Q_L^0 + Q_{L(r)}^0\lambda_r + \sum_{i\forall d} Q_{Loss} \tag{17}$$

Now, depending on the value of λ_r, P_r and Q_r will change, which will impact on the VSI index as defined in Eq. (1). From Eqs. (16) and (17), any injection of false information will increase the value of P_r and Q_r, which will again decrease the value of VSI observed from Eq. (1), as distribution side of the power system has high R/X ratio [21]. Any lower value of the VSI indicates that the system is highly likely to voltage collapse. So, the operators should become concerned about keeping the system within stability margin. From Eq. (1), we see that the VSI depends not only the operational value of P_r and Q_r but also other physical properties of the power grid, which are R and X. Therefore, for the same value of λ (which indicates a same amount of false data injection) at different nodes, the corresponding VSI will vary depending on the values of R and X of the downstream branches of the node being attacked.

In this section, the relationship of VSI and FDI attack is discussed. In Section 4, we show the impact of FDI attacks on the system voltage stability using VSI index. Understanding the overall system vulnerability of all nodes is not possible by looking at the individual VSI index for a single attack vector. Therefore, using different attack vectors, we calculate the VSI values for all nodes of the network and then use a swarm intelligence based improved clustering algorithm to partition the network nodes based on their vulnerabilities. Hence, we use CF-PSO based improved clustering technique in the next section.

3. CF-PSO based improved clustering technique

3.1. Proposed improved clustering technique

k-means is a well known unsupervised clustering algorithm which has a wide range of applications. For n data points and K centroids, the time complexity of k-means algorithm is only $\mathcal{O}(n)$ [22]; therefore, k-means is an efficient clustering algorithm. However, a major problem of k-means is that it may trap in one of the local minima. In the proposed work, the strengths of both k-means and CF-PSO have been exploited to find better solutions than k-means. At the beginning, k-means algorithm is replicated $n/2$ times, where n is the population size of the CF-PSO. Since 'random' initialization is considered as the standard initialization method for the k-means algorithm and performs well for many types of problems [23,24], we use this approach for

initializing k-means. Once the cluster centroids are obtained from the replicated k-means algorithm, we use them as half of the initial population of the swarm. The remaining half swarm population are chosen randomly based on uniform distribution of the solution space, which is widely accepted as the standard initialization technique of PSO [25]. Generally, k-means provides sub-optimal solution most of the times. In those cases, the remaining half input vectors of the swarm (which are generated uniformly throughout the search-space) will still be capable to produce enough diversity in the velocities of the particles to reach to a better solution. The initial swarm structure is given in Fig. 1, where each particle represents K cluster centroids and D refers the dimension of the input data vector. It is worthwhile to mention that the convergence characteristics of PSO depend on the parameter settings of the algorithm.

Algorithm 1.

input: Objective function C_{obj}, swarm size n, CF-PSO parameters
for *each particle* $i = 1, \ldots, n/2$ **do**
  Initialize particle's position $\mathbf{x}_i$ and velocity $\mathbf{v}_i$ using the solution obtained from the replicated k-means output;
end
for *each particle* $i = n/2, \ldots, n$ **do**
  Initialize particle's position $\mathbf{x}_i$ and velocity $\mathbf{v}_i$ randomly;
end
Calculate C_{obj};
Initialize particle's best known position $\mathbf{P}_i$ and swarm's best known position $\mathbf{P}_g$;
while *stopping criterion is false* **do**
  for *each particle* $i = 1, \ldots, n$ **do**
    Update particle's velocity $\mathbf{v}_i$ and position $\mathbf{x}_i$;
    Calculate C_{obj};
    if $C_{obj}(\mathbf{x}_i) < C_{obj}(\mathbf{P}_i)$ **then**
      Update particle's best known position $\mathbf{P}_i$;
      if $C_{obj}(\mathbf{P}_i) < C_{obj}(\mathbf{P}_g)$ **then**
        Update swarm's best known position $\mathbf{P}_g$;
      end
    end
  end
end

In order to determine optimal parameter settings of PSO, Clerc et al. analyse the particles trajectory in a complex solution space (from both algebraic and analytic point of view) and provide a generalized model of the algorithm that contains a set of coefficients to control the systems convergence properties [26]. With the theoretical proofs and extensive experiments, authors in [26] provide the value of 'constriction coefficients' to ensure convergence to a stable point. This variant of PSO with constriction coefficients is known as 'Constriction Factor PSO'. Authors also show that the deleterious effect of the randomness of the PSO algorithm is controlled with the adoption of constriction coefficients. To have a converged behaviour, Clerc et al. suggest the following model [26]:

Position Update Equation (same as the original PSO):

$$\mathbf{x}_i^{t+1} = \mathbf{x}_i^t + \mathbf{v}_i^{t+1} \tag{18}$$

where $x_i(t)$ is the position vector of i-th particle at time t.

Velocity Update Equation (constriction coefficient introduced):

$$\mathbf{v}_i^{t+1} = \chi[\mathbf{v}_i^t + r_1 \cdot \varphi_1 \cdot (\mathbf{p}_i - \mathbf{x}_i^t) + r_2 \cdot \varphi_2 \cdot (\mathbf{p}_g - \mathbf{x}_i^t)] \tag{19}$$

where

$$\chi = \frac{2k}{|2 - \varphi - \sqrt{\varphi^2 - 4\varphi}|} \tag{20}$$

with

$$\varphi = \varphi_1 + \varphi_2 \tag{21}$$

In order to guarantee the convergence, $\varphi > 4$ and $k \in [0, 1]$ [26].

In the CF PSO formulation discussed above, the particles travel towards an optimal solution based on the self-cognition and social-cognition aspects [25]. The exploration capabilities of these particles toward an optimal value depend on the value of 'k' in the formulations (Eq. (20)). For example,

If $k \approx 0$, algorithm converges fast and particles are more prone to local exploitation. That means, particles concentrate a search around a promising area to refine a candidate solution [27]. In this case, there is more possibility to obtain a sub-optimal solution (local minimum) by the algorithm.

If $k \approx 1$, algorithm converges slow and particles are more prone to high degree of exploration. That means, particles explore more region/area of the search space to refine a candidate solution [27]. In this case, the algorithm has more possibility to find an optimal solution (global minimum).

Fig. 1. Swarm structure at the initialization stage.

Based on the convergence criterion, Eberhart et al. shows the performance of Constriction Factor PSO over the popular variants 'adaptive weight PSO' in [28], where $k=1$ and $\varphi=4.1$ is considered which lead to the value of $\chi=0.7298$. In our analysis, we used the similar parameter settings to obtain a converged solution and the total sum of the distance of each instance to the centroid is considered as a cost function. The step-by-step procedure of the proposed solution is described briefly in Algorithm 1.

3.2. Evaluation of the proposed improved clustering technique

To evaluate the performance of the CF-PSO based improved clustering method, 'shuttle' dataset [29] from NASA is used. The benchmark dataset is available from UCI repository of machine learning databases. The shuttle dataset has 58 000 data instances and contains 9 numerical attributes. In this experiment, the dataset has been used to evaluate the performance of the k-means, CF-PSO and the proposed CF-PSO based improved clustering approaches. The algorithms have been implemented in Matlab platform using a PC of Intel(R) core i7 at 3.7 GHz. The results obtained from 30 individual runs of each algorithm have been summarized in Table 1, where maximum number of iteration is considered 1000. From Table 1, we observe that the proposed method has better solution accuracy than any of the individual algorithms (either the k-means algorithm or the CF-PSO based clustering) for any number of clusters. In order to test the statistical significance, we conduct an unpaired two tailed *t*-test with 95% confidence interval. Optimal objective function values obtained from the proposed method show statistically very significant in one case and extremely statistically significant in the remaining five cases. In Fig. 2, the convergence characteristics of the clustering algorithms using k-means, CF-PSO and the proposed approach are shown which is obtained averaging the values of 30 individual trails. From Fig. 2 and Table 1, it can be seen that both the k-means and CF-PSO based clustering trap in a sub-optimal solution. On the other hand, CF-PSO based improved clustering technique avoided being locally stuck and finds better solutions as shown in Fig. 2.

4. Results and discussion

In this section, at first, we discuss about the benchmark test systems. Then we calculate the VSI of each node of the test systems. After that, the most and the least vulnerable nodes are identified. To understand the overall node vulnerability characteristics of the whole system, we cluster the nodes which exhibits the similar behaviours. Finally, we show the characteristics of different clusters with different degrees of FDI attack.

4.1. Benchmark test systems and analysis tool

In this work we consider two benchmark systems, the 33-bus and the 69-bus distribution test systems, which are widely used in distribution system analysis (e.g., [30,31]). Test system data are obtained from [32,12], respectively. 33-bus distribution test system has a total user demand of 3715 kW and 2300 kVAr. Total system power loss is approximately 203 kW. This test system has 33 buses and 32 line sections. On the other hand, the 69-bus distribution test system has a total user demand of 3790 kW and 2690 kVAr. Total system power loss is approximately 225 kW. This test system has 69 buses and 68 line sections. For analysis purpose, we used Matlab based power system simulation tool MatPower [33].

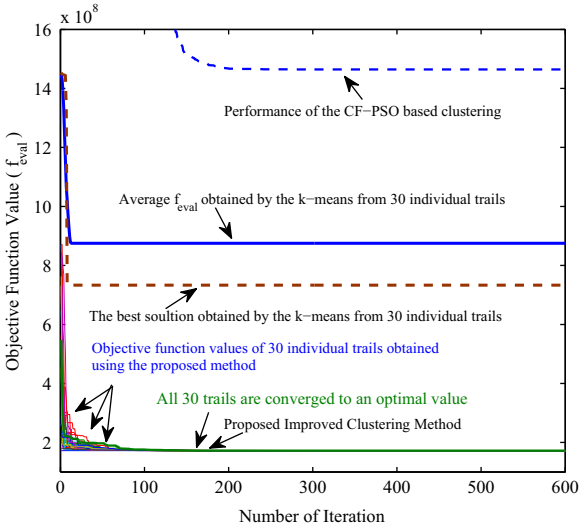

Fig. 2. Convergence characteristics of different algorithms.

Table 1
Objective function value using the 'Shuttle' dataset.

# *k*	Algorithm	Mean	Best	*t*-Statistics	Decision
3	CF-PSO	1.46e+09	1.46e+09	$P<0.0001$	Ext. sig.
	k-Means	8.76e+08	7.31e+08	$P<0.0001$	Ext. sig.
	Proposed technique	**1.74e+08**	**1.72e+08**	–	–
5	CF-PSO	1.46e+09	1.46e+09	$P<0.0001$	Ext. sig.
	k-Means	1.75e+08	1.37e+08	$P=0.0021$	Very sig.
	Proposed technique	**1.02e+08**	**9.70e+07**	–	–
7	CF-PSO	1.46e+09	1.46e+09	$P<0.0001$	Ext. sig.
	k-Means	1.14e+08	7.76e+07	$P<0.0001$	Ext. sig.
	Proposed technique	**6.07e+07**	**5.97e+07**	–	–

4.2. Identification and clustering of the most and the least vulnerable nodes

First, we calculate the VSI of each node (except the substation bus) of both 33-bus and 69-bus test systems using Eq. (1) at the normal loading condition (that means, no attack vector is added in this situation). The calculated VSI values are reported in Table 2. For the 33-bus test system, Node 18 has the minimum VSI value of 0.697 and Node 2 has the maximum VSI value of 1.001. From the definition (Eq. (1)), VSI ≥ 0 for stable operation of the distribution system. Therefore, Node 2 is the most stable node and Node 18 is the weakest node in terms of susceptibility to voltage collapse. These nodes are marked bold in Table 2. For the 69-bus test system, Node 65 has the minimum VSI value of 0.6868 and Node 6 has the maximum VSI value of 1.03. Therefore, Node 6 is the most stable node and Node 65 is the weakest node in terms of voltage collapse. These nodes are also marked bold in Table 2.

Now, for both the test systems, we investigate the impact of FDI attacks at different AMI nodes including the most and the least sensitive node. Therefore, we increase the value of λ from 1 to 3 at Eqs. (16) and (17) for all AMI nodes. Here, $\lambda=1$ indicates that there is no attack generated and a value more than 1 represents a positive injection of false data. The degree of FDI attack increases as the value of λ increases. Here $\lambda=3$ means that the manipulated measurement data value is 3 times of the original measurement. The vulnerabilities of different AMI nodes under FDI attacks are shown in Figs. 3 and 4 for the 33 bus and the 69 bus test systems. Here, different coloured lines represent the VSI variations of different AMI nodes under the attack scenario. From the simulation results, shown in Fig. 3, we see that the weakest nodes (Node 18 for 33 bus system) have maximum deviations under different degrees (λ) of FDI attacks. As the VSI value becomes close to zero, the likelihood of voltage collapse increases. From Fig. 4, similar behaviour is observed. Node 65, the weakest node of 69 bus test system, shows the maximum change in VSI index under the attack scenario. Therefore, from Figs. 3 and 4, the weakest nodes identified by the VSI analysis are more prone to voltage collapse when AMI nodes are subjected to false data injections. Hence, we consider them as the most vulnerable nodes in terms of FDI attacks. Although we observed the variations of VSI values with the change of attack magnitude, we can further study the FDI attack impact on the voltage profile of the whole system. Therefore, we conduct a power flow study for both test systems considering $\lambda=1$, 2, and 3 using MatPower [33]. From the results of the power flow analysis, we report the voltage profiles of all nodes in Figs. 5 and 6 respectively for

Table 2
VSI Values of 33 bus and 69 bus test systems.

33 bus		69 bus			
Node no.	VSI	Node no.	VSI	Node no.	VSI
2	**1.001183558**	2	1.000133855	36	0.999787505
3	0.993689984	3	0.999999984	37	1.000363923
4	0.936298948	4	1.000106274	38	0.999623751
5	0.908106398	5	1.002629811	39	0.998539621
6	0.884778834	**6**	**1.031391209**	40	0.998182879
7	0.814521166	7	0.996659059	41	1.000949841
8	0.803092175	8	0.933706109	42	0.996546452
9	0.787249246	9	0.92127326	43	0.994370056
10	0.766353073	10	0.931350386	44	0.994095508
11	0.745899728	11	0.898308982	45	0.994421459
12	0.74334671	12	0.901761311	46	0.993638668
13	0.740013304	13	0.889270507	47	0.999558556
14	0.719505544	14	0.878522362	48	1.004128465
15	0.71218474	15	0.867950479	49	1.009405242
16	0.70780161	16	0.849462496	50	0.981106863
17	0.703790169	17	0.84879974	51	0.9171632
18	**0.697148284**	18	0.842631258	52	0.916933249
19	0.98839113	19	0.84420139	53	0.923167388
20	0.987499424	20	0.841982645	54	0.914395114
21	0.97227965	21	0.841578645	55	0.90680066
22	0.969497182	22	0.838225297	56	0.88991075
23	0.934835912	23	0.838428828	57	0.936559475
24	0.922420936	24	0.838473117	58	0.817351506
25	0.896340976	25	0.837969612	59	0.758624139
26	0.813994098	26	0.837029921	60	0.747143315
27	0.807615835	27	0.836610189	61	0.738413813
28	0.801867787	28	0.999758829	62	0.693720904
29	0.762763157	29	0.999976451	63	0.693138299
30	0.734825189	30	0.99981996	64	0.696533024
31	0.72378435	31	0.999118159	**65**	**0.686773817**
32	0.709813456	32	0.999321801	66	0.890429745
33	0.706791537	33	0.999456952	67	0.890016253
		34	0.998742216	68	0.879893784
		35	0.997184601	69	0.877503133

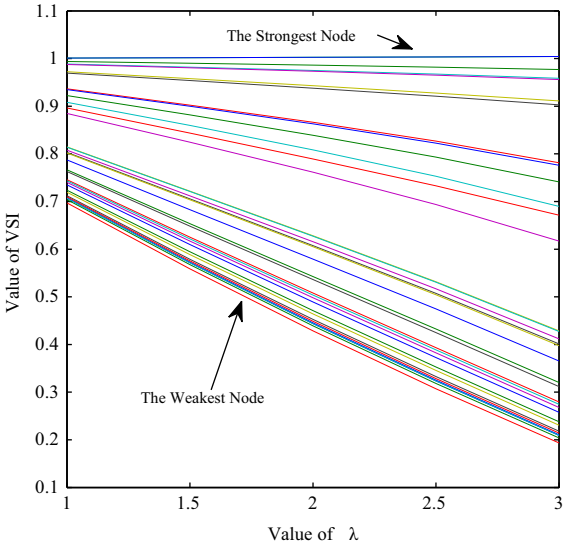

Fig. 3. VSI of all AMI nodes for the 33 bus test system. (For interpretation of the references to colour in this figure caption, the reader is referred to the web version of this paper.)

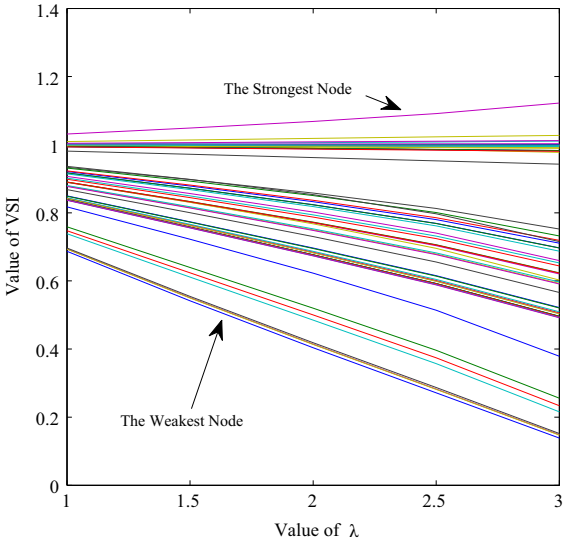

Fig. 4. VSI of all AMI nodes for the 69 bus test system. (For interpretation of the references to colour in this figure caption, the reader is referred to the web version of this paper.)

the 33 bus and the 69 bus systems. From the voltage profiles, we also notice that Node 18 at 33 bus test system and Node 65 at 69 bus test system are the most vulnerable nodes for any value of λ. From Figs. 5 and 6, we also observe that the impact of FDI attack varies from node to node depending on their physical properties. So, it is important to group the nodes with similar characteristics. In order to do that, we vary the value of λ from 1 to 3 with a step size of 0.5, calculate and store the value of VSI for each node of the 33 bus test system. Now, we perform the CF-PSO based hybrid clustering developed in Section 3. Here, we are interested to group the vulnerable nodes into 3 clusters – the cluster of the least vulnerable nodes, the moderate vulnerable nodes and the most

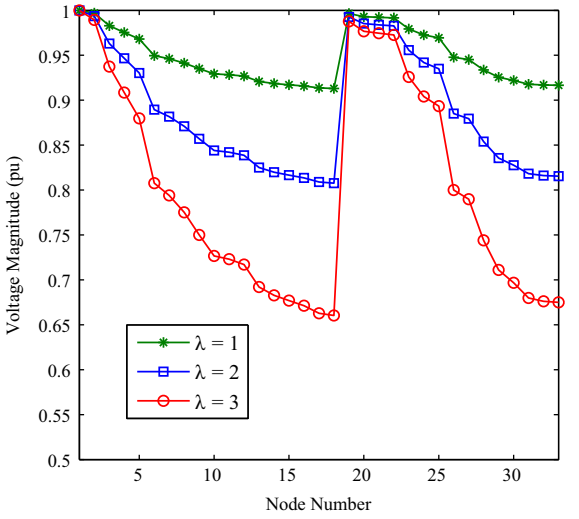

Fig. 5. Voltage magnitude of all AMI nodes for 33 bus test system.

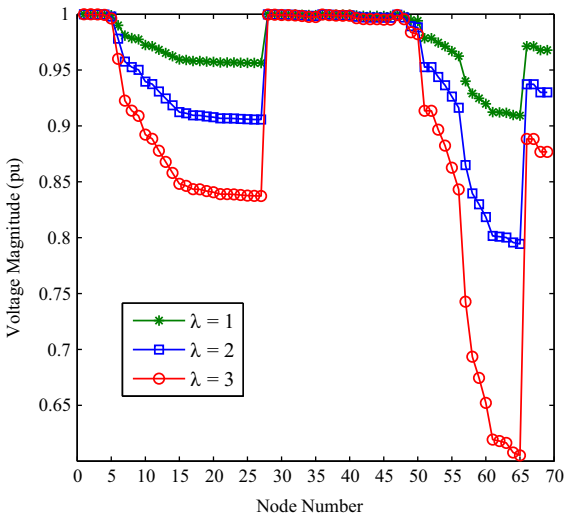

Fig. 6. Voltage magnitude of all AMI nodes for 69 bus test system.

vulnerable nodes. The proposed CF-PSO based hybrid clustering algorithm will make 3 clusters based on the VSI data. The output obtained from the clustering algorithm is given in Table 3 and can be visualized from Fig. 7. From Table 3, we see that Nodes 7 to 18 and Nodes 26 to 33 are the most vulnerable nodes in terms of FDI attacks. Now, if we again observe the voltage profiles of different nodes of the 33 bus test system (Fig. 5), we see that the nodes in the above described cluster have more deviations of voltage magnitudes than other nodes of the remaining clusters. In Fig. 7, red colour is used to visualize the nodes in the most vulnerable cluster. Blue and green indicate the nodes which belongs to the moderate and the least vulnerable clusters. Similarly, we conduct experiments for the 69 bus test systems. The nodes of the most, average and the least vulnerable clusters are given in Table 4 and visualized in Fig. 8. The Nodes 59 to 65 belong to the cluster of the most vulnerable nodes, marked red dots in the Fig. 8. Nodes of this most vulnerable cluster show maximum voltage deviations in Fig. 6.

5. Protecting the vulnerable nodes

In this section, we discuss the defensive techniques that can be used to secure the most vulnerable nodes identified by the proposed method. To prevent non-legitimate access into smart metering devices, advanced authentication schemes and different Intrusion Prevention Systems (IPS) can be used. If an attacker manages to bypass these preventive security techniques and compromise the devices connected with the vulnerable nodes, an Intrusion Detection System (IDS) is then necessary to identify the attacks launched by the intruder and take mitigating actions.

Table 3
Vulnerable node clustering of 33 bus test system.

Clusters	Nodes	Comment
Cluster 1	7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18 26, 27, 28, 29, 30, 31, 32, 33	The most vulnerable cluster
Cluster 2	4, 5, 6 23, 24, 25	The moderate vulnerable cluster
Cluster 3	2, 3, 19 20, 21, 22	The least vulnerable cluster

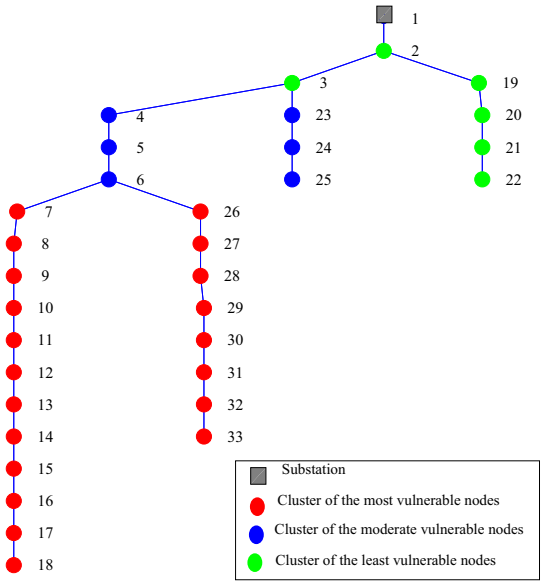

Fig. 7. Vulnerable node clustering of the 33 bus test system. (For interpretation of the references to colour in this figure caption, the reader is referred to the web version of this paper.)

Table 4
Vulnerable node clustering of 69 bus test system.

Clusters	Nodes	Comment
Cluster 1	59,60,61 62,63,64,65	The most vulnerable cluster
Cluster 2	8,9,10,11,12,13,14,15,16,17,18,19,20,21,22 23,24,25,26,27,51,52,53,54,55,56, 57,58,66,67,68,69	The moderate vulnerable cluster
Cluster 3	2,3,4,5,6,7,28,29,30,31,32,33,34,35,36 37,38,39,40,41,42,43,44,45,46,47, 48,49,50	The least vulnerable cluster

5.1. Device authentication

Authenticity of devices and data traffic is one of the earliest and an essential step towards ensuring secured communication. Generally, communication between the AMI devices and the EMS/DMS is delay sensitive and traffic intensive. On the other hand, state estimation procedure needs near real-time operation. Therefore, authentication schemes in a SCADA connected Smart Grid should maintain minimal message exchange among different grid devices and coordinating agents like EMS/DMS while security should be assured. Li and Cao points out that the Smart Grid Intelligent Electronic Devices (IED), e.g., AMI meters often have limited storage [34]. To solve the storage problem, a new One-Time Signature (OTS) based multicast authentication is proposed that also shorten authentication delay and reduce computational cost significantly [34]. Fouda et al. proposed a lightweight message authentication scheme based on Diffie–Hellman exchange protocol [35] that can ensure desirable security requirements under a Smart Grid consideration. To handle the FDI data integrity attacks (e.g., man-in-the-middle attack, message alteration and modification), Li et al. propose a Merkle-Tree-Based Authentication Scheme that is more lightweight than the traditional Rivest–Shamir–Adleman (RSA) based authentication [36]. Therefore, one effective solution to protect the vulnerable nodes against the FDI attacks is to ensure proper device authentication schema maintaining the Smart Grid security requirements.

5.2. Intrusion detection and prevention systems (IDPS)

Intrusion Prevention System (IPS) monitors the network traffic online to prevent network intrusions by identifying malicious activities. Not only monitoring network traffic, but also it takes preventive actions. For example, after identifying malicious packets, IPS can reject it or delete it. In an Intrusion Detection System (IDS), the event logs of malicious activities are stored with detailed information for future analyses. For both the cases, alarm is generated to alert the system operators. IPS and IDS can be installed in the EMS/DMS to monitor the complete network or can be installed in any specific device of interest. Generally, Smart Grid has a large number of nodes and it is not possible to install IDS/IPS at each node as it will increase the computational, storage and economic cost significantly. Therefore, a practical solution is to install IDS/IPS only to the vulnerable nodes. In the following section, we discuss some recent techniques which are proposed to detect FDI attacks and to protect the Smart Grid.

Liu et al. propose two methods, based on nuclear norm minimization and low rank matrix factorization, for detecting FDI attacks [37]. In that work, the temporal correlation of time-series measurements and the spatial nature of FDI

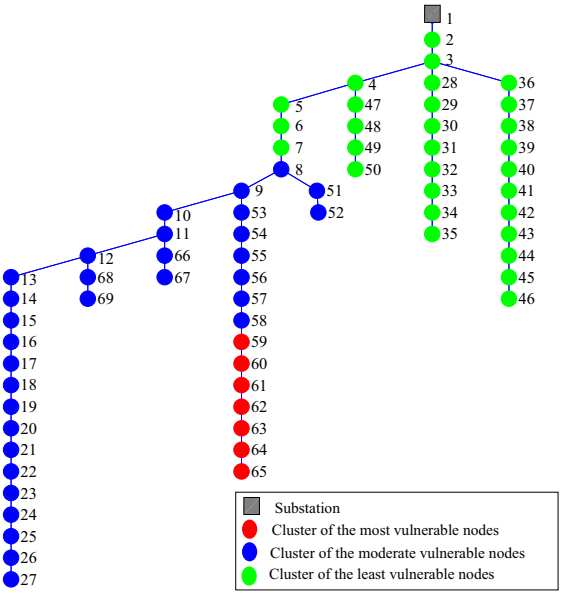

Fig. 8. Vulnerable node clustering of the 69 bus test system. (For interpretation of the references to colour in this figure caption, the reader is referred to the web version of this paper.)

attacks are also studied considering missing observation values along with different attack ratios. Lo et al. in [38] develops a hybrid detection framework for AMI based Smart Grid. Authors suggest that the network observability and attack detection rate can be improved significantly by proper deployment of grid sensors. Authors in [39] propose a defense strategy to protect some important nodes using CUSUM algorithm. To protect the vulnerable nodes against malicious FDI attacks, a graphical method based defense strategy is proposed in [40]. Machine learning approach based attack detection method is proposed by Esmalifalak et al. in [41].

Generally, intrusion detection systems are two types: (i) signature based and (ii) anomaly based. In a signature based IDS, information are compared against attack signatures, which are typically stored in a database, to identify the malicious data. On the contrary, anomaly based IDS uses a threshold to compare the normal and abnormal patterns, any deviation from threshold is considered as an anomaly. The threshold is typically calculated based on some statistical analyses. In an IT domain, signature based IDS are very effective as there is an abundance of signatures [42]. For a SCADA connected Smart Grid, new types of cyber threats are increasing. The existing power grid infrastructure, which is built couple of decades ago, is not prepared for this. Therefore, anomaly detection technique based on signature may not effective as the signature of the new cyber intrusions, like FDI attacks, may not be available in the database. Hence, an anomaly based IDS may be a good solution to protect the vulnerable nodes of the Smart Grid. Yang et al. highlights that power grid covers a large geographical area which makes it very difficult to monitor and control [39]. Hence, the cyber-attack defence strategies installed to the most vulnerable nodes obtained by the proposed method may be a good solution to ensure the protection of a SCADA connected Smart Grid.

6. Conclusion

In this paper, the interdependent nature of nodes in the power grids is studied and a method, based on voltage stability index, is utilized to identify the node characteristics in terms of voltage collapse. Hence, we show a relationship between the voltage stability indices and the false data injection attacks. We establish that nodes which are more prone to voltage collapse (less VSI value) are more vulnerable in terms of FDI attacks. Considering the end user nodes as AMI nodes (e.g., having Smart Meters), we conduct extensive experimental analyses to show the impact of FDI attacks by studying the physical properties of the Smart Distribution Grids. From our experiments, it is evident that injection of similar amount of false information does not have same impact on every node. Hence, it is important to identify similar nodes that exhibit similar characteristics under FDI attack. In order to avoid trapping into local minima of finding the best clusters that describe similar node behaviour, we perform CF-PSO based hybrid clustering to obtain the nodes of the most, the moderate and the least vulnerable clusters for two benchmark test systems. Our future work will address the protection and the detection strategies of the most vulnerable AMI nodes, which is under preparation.

References

[1] Y. Liu, P. Ning, M.K. Reiter, False data injection attacks against state estimation in electric power grids, ACM Trans. Inf. Syst. Secur. 14 (1) (2011). 13:1–13:33.
[2] R. McMillan, Siemens: Stuxnet worm hit industrial systems, COMPUTERWorld.
[3] Y. Liu, P. Ning, M. K. Reiter, False data injection attacks against state estimation in electric power grids, in: Proceedings of the 16th ACM Conference on Computer and Communications Security, CCS '09, ACM, New York, NY, USA, 2009, pp. 21–32.
[4] A. Anwar, A. Mahmood, Vulnerabilities of smart grid state estimation against false data injection attack, in: J. Hossain, A. Mahmud (Eds.), Renewable Energy Integration, Green Energy and Technology, Springer, Singapore, 2014, pp. 411–428.
[5] M. Ozay, I. Esnaola, F. Vural, S. Kulkarni, H. Poor, Sparse attack construction and state estimation in the smart grid: centralized and distributed models, IEEE J. Sel. Areas Commun. 31 (7) (2013) 1306–1318.
[6] D. Grochocki, J. Huh, R. Berthier, R. Bobba, W. Sanders, A. Cardenas, J. Jetcheva, Ami threats, intrusion detection requirements and deployment recommendations, in: IEEE Third International Conference on Smart Grid Communications (SmartGridComm), 2012, pp. 395–400.
[7] S. Bi, Y.J. Zhang, Graphical methods for defense against false-data injection attacks on power system state estimation, IEEE Trans. Smart Grid 5 (3) (2014) 1216–1227.
[8] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, W. Zhao, On false data-injection attacks against power system state estimation: modeling and countermeasures, IEEE Trans. Parallel Distrib. Syst. 25 (3) (2014) 717–729.
[9] G. Hug, J. Giampapa, Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks, IEEE Trans. Smart Grid 3 (3) (2012) 1362–1370.
[10] P. Jokar, N. Arianpoo, V. Leung, Intrusion detection in advanced metering infrastructure based on consumption pattern, in: IEEE International Conference on Communications (ICC), 2013, pp. 4472–4476.
[11] M. Baran, T. McDermott, Distribution system state estimation using ami data, in: IEEE Power Systems Conference and Exposition, 2009.
[12] M. Chakravorty, D. Das, Voltage stability analysis of radial distribution networks, Int. J. Electr. Power Energy Syst. 23 (2) (2001) 129–135.
[13] M. Moradi, M. Abedini, A combination of genetic algorithm and particle swarm optimization for optimal DG location and sizing in

distribution systems, Int. J. Electr. Power Energy Syst. 34 (1) (2012) 66–74.
[14] M. Arun, P. Aravindhababu, A new reconfiguration scheme for voltage stability enhancement of radial distribution systems, Energy Convers. Manag. 50 (9) (2009) 2148–2151.
[15] A. Anwar, H. Pota, Loss reduction of power distribution network using optimum size and location of distributed generation, in: 21st Australasian Universities Power Engineering Conference (AUPEC), 2011.
[16] F.A. Viawan, Voltage control and voltage stability of power distribution systems in the presence of distributed generation (Ph.D. thesis), Chalmers University of Technology, 2008.
[17] T. Zabaiou, L.-A. Dessaint, I. Kamwa, Preventive control approach for voltage stability improvement using voltage stability constrained optimal power flow based on static line voltage stability indices, IET Gener. Transm. Distrib. 8 (5) (2014) 924–934.
[18] M. Baran, A. Kelley, A branch-current-based state estimation method for distribution systems, IEEE Trans. Power Syst. 10 (1) (1995) 483–491.
[19] J. Wu, B. Zhang, H. Li, Z. Li, Y. Chen, X. Miao, Statistical distribution for wind power forecast error and its application to determine optimal size of energy storage system, Int. J. Electr. Power Energy Syst. 55 (2014) 100–107.
[20] A. Anwar, A. Mahmood, Cyber security of smart grid infrastructure, in: A.-S.K. Pathan (Ed.), The State of the Art in Intrusion Prevention and Detection, CRC Press, Taylor & Francis Group, USA, 2014, pp. 139–154.
[21] W. Kersting, Distribution System Modeling and Analysis, Electric Power Engineering, CRC Press, USA, 2002.
[22] S. Das, A. Abraham, A. Konar, Automatic clustering using an improved differential evolution algorithm, IEEE Trans. Syst. Man Cybern. Part A: Syst. Hum. 38 (1) (2008) 218–237.
[23] J. Pena, J. Lozano, P. Larranaga, An empirical comparison of four initialization methods for the k-means algorithm, Pattern Recognit. Lett. 20 (10) (1999) 1027–1040.
[24] P.S. Bradley, U.M. Fayyad, Refining Initial Points for K-Means Clustering, in: Jude W. Shavlik (Ed.), Proceedings of the Fifteenth International Conference on Machine Learning (ICML '98), Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 1998, pp. 91–99.
[25] J.F. Kennedy, J. Kennedy, R. Eberhart, Y. Shi, Swarm Intelligence, The Morgan Kaufmann Series in Evolutionary Computation, Morgan Kaufmann Publishers, 2001.
[26] M. Clerc, J. Kennedy, The particle swarm – explosion, stability, and convergence in a multidimensional complex space, IEEE Trans. Evol. Comput. 6 (1) (2002) 58–73.
[27] F. Van den Bergh, An analysis of particle swarm optimizers (Ph.D. thesis), University of Pretoria, 2001.
[28] R. Eberhart, Y. Shi, Comparing inertia weights and constriction factors in particle swarm optimization, in: Proceedings of the 2000 Congress on Evolutionary Computation, vol. 1, 2000, pp. 84–88.
[29] J. Mertz, P.M. Murphy, UCI machine learning repository. ⟨http://archive.ics.uci.edu/ml⟩.
[30] M. Aman, G. Jasmon, A. Bakar, H. Mokhlis, M. Karimi, Optimum shunt capacitor placement in distribution system a review and comparative study, Renew. Sustain. Energy Rev. 30 (0) (2014) 429–439.
[31] R. Rao, K. Ravindra, K. Satish, S. Narasimham, Power loss minimization in distribution system using network reconfiguration in the presence of distributed generation, IEEE Trans. Power Syst. 28 (1) (2013) 317–325.
[32] B. Venkatesh, R. Ranjan, H. Gooi, Optimal reconfiguration of radial distribution systems to maximize loadability, IEEE Trans. Power Syst. 19 (1) (2004) 260–266.
[33] R. Zimmerman, C. Murillo-Sanchez, R. Thomas, MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education, IEEE Trans. Power Syst. 26 (1) (2011) 12–19.
[34] Q. Li, G. Cao, Multicast authentication in the smart grid with one-time signature, IEEE Trans. Smart Grid 2 (4) (2011) 686–696.
[35] M. Fouda, Z. Fadlullah, N. Kato, R. Lu, X. Shen, A lightweight message authentication scheme for smart grid communications, IEEE Trans. Smart Grid 2 (4) (2011) 675–685.
[36] H. Li, R. Lu, L. Zhou, B. Yang, X. Shen, An efficient Merkle-tree-based authentication scheme for smart grid, IEEE Syst. J. 8 (2) (2014) 655–663.
[37] L. Liu, M. Esmalifalak, Q. Ding, V. Emesih, Z. Han, Detecting false data injection attacks on power grid by sparse optimization, IEEE Trans. Smart Grid 5 (2) (2014) 612–621.
[38] C.-H. Lo, N. Ansari, Consumer: a novel hybrid intrusion detection system for distribution networks in smart grid, IEEE Trans. Emerg. Top. Comput. 1 (1) (2013) 33–44.
[39] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, W. Zhao, On false data-injection attacks against power system state estimation: modeling and countermeasures, IEEE Trans. Parallel Distrib. Syst. 25 (3) (2014) 717–729.
[40] S. Bi, Y.J. Zhang, Graphical methods for defense against false-data injection attacks on power system state estimation, IEEE Trans. Smart Grid 5 (3) (2014) 1216–1227.
[41] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, Z. Han, Detecting stealthy false data injection using machine learning in smart grid, Syst. J., http://dx.doi.org/10.1109/JSYST.2014.2341597, in press.
[42] S. Sridhar, M. Govindarasu, Model-based attack detection and mitigation for automatic generation control, IEEE Trans. Smart Grid 5 (2) (2014) 580–591.