Methodology for incisive foraging of high-risk junctions and elimination of injected false data in smart grid

Poulami Ghosh[1], Subrata Biswas[2], Prithwiraj Purkait[3]
[1]Department of Electrical Engineering, St. Thomas' College of Engineering and Technology, Kolkata, India
[2]Department of Electrical Engineering, Netaji Subhash Engineering College, Kolkata, India
[3]Department of Power Engineering, Jadavpur University, Kolkata, India

Article Info

Article history:

Received May 6, 2023
Revised Nov 7, 2024
Accepted Nov 28, 2024

Keywords:

False data injection
High risk junctions
State estimation
Voltage stability index
Weighted least square

ABSTRACT

The present work represents a method for identification of the vulnerable nodes in smart grid as well as assessment of the performance of voltage stability indicator technique with the help of weighted least square scheme. in today's smart grid system, false data injection (FDI) is the major issue to supply uninterruptedly at demand side in advanced metering infrastructure (AMI). The recent blackouts are the consequence of non-identifying FDI as research on FDI is not considered under power system analysis. In our research, vulnerable nodes of a power system network have been identified and a state estimation method was used to eliminate superfluous data for those identified nodes. Voltage stability indicator (VSI) based state estimation have been used successfully to make the smart grid system error free as possible. VSI method has been used first to find the vulnerable nodes of the grid after that the efficient state estimation method i.e. optimal weighted least square (optimal WLS) have been employed to get refined result. Results show that VSI based technique in concurrence with optimal WLS has potential to eliminate undesirable data with sensible level of precision.

Corresponding Author:

Subrata Biswas
Department of Electrical Engineering, Netaji Subhash Engineering College
Techno City, Garia, Kolkata-700152, West Bengal, India
Email: subratab28@gmail.com

1. INTRODUCTION

Smart grid systems are combined with a huge number of devices that are interconnected through a communication network and with a cyber-physical system. So, the heterogeneous network consists of sensor nodes in different layers, and they are very vulnerable due to the openness of data exchange through different channels [1]-[4]. The false data injection attacks (FDIAs) [5] are dangerous. The attacker attacks the smart grid communicating devices or the remote terminal units (RTU) distantly retrieved through the system [6]. FDIs are responsible for changing the smart grid state estimation, and this is the target of the invader. The modified value of data leads to improper judgments in the control room, which results in great fault in the electrical security system [7].

In 2010 computer worm Stuxnet caused an unstable power system operation [8], in 2003 Northeast United States, Ontario Canada, and Midwest, had seen an electrical shutdown of duration of four days in few areas [9], Italy, and parts of Switzerland experienced its major power supply interruption for a duration of 18 hours [9] due to the insecure smart grid system. To improve the safety system of the smart grid system of the nodes of the grid system with the voltage sensitivity index method has been discussed in this paper. Attackers instigate FDIAs by deletion of the measured values acquired through the SCADA arrangement or phasor measurement units (PMUs), which creates a malfunction of the flow of power among buses of the network and the power inserted by the bus. The scheme introduced by Hug and Giampapa [9] can identify conventional bad data, which was created by arbitrary noise, but cannot identify complicated FDIAs.

It is revealed that orthodox approaches on maximum regulated remainders are not capable of identifying well-planned false data injection attacks. So, the attacker may insert a particular attack at the time of measurement and in due course distort the consequences of state estimation [10], [11]. Nowadays, network attacks have become more complicated and sneakier; the FDIA identification scheme applying WLS only cannot identify FDIAs, particularly when while attacker is known and the system information [12]. The weighted extended Kalman filter (WEKF) [13] estimates are supported on present quantity and historical information, and a dynamic threshold. Studying on cost and efficiency of finding methods. The deal of FDIA depending on AC and DC state estimation methodology, is very popular among researchers for smart grid security purposes. Application of FDIAs in the DC prototype offers bulky residues in the process of the AC state estimation, which is improved for detecting FDIAs [14]. FDIAs centered on the AC state estimation prototype were formed in [15] to attack the power supply grid system. The assailant may here create the inaccurate grid state by flow of power and injection of power quantities with no analysis of the current state of a system, and finally vary the state estimation from the safety value as unidentified. With the purpose of decreasing the count of measurements when the attack is created, an FDI attack prototype is endorsed in [16] to alter the grid parameters, and this finally principals to an improved harmonization among the variation in states of the grid plus the alteration of grid parameters.

The attack prototypical created with nonlinear physical limits was offered to attain the secrete consequence and effectively escape of revealing [17]. With AC state estimation arrangements, this is hard to invade for flawless FDIAs, as well as insufficient assaults initiate modifications for the possibility sharing of measured residuals. Hence, a finding technique applying statistical stability for measured residuals is recommended in [18]. Even though the technique may excellently identify FDIAs, this method may not discover an exact position for FDIAs. In smart grid the dynamical prototype has been considered to fight against FDIAs, the fast attack discovery algorithm was recommended in the work [19]. This algorithm discriminates between planned modifications and FDIAs via examining expected statistical possessions. Instantaneously, this technique may be able to find or remove FDIAs with little anticipation. In the work [20], this technique founded on Kullback-Leibler distance (KLD) was useful for identifying FDIAs. The technique regulates the FDIAs reality by matching dissimilarity within possibility distributions among historic and present measurements. The trouble of the identification method starts when it includes a huge historic measured data, as well as finding efficiency can be negotiated to fight trapezoidal attacks. A discovery approach grounded on PMUs measured data of is recommended [21]. This arrangement receives the state estimates achieved by PMUs, SCADA, then implements a stability checking process for identifying FDIAs. This paper suggests a method for optimal WLS that together uses WLS and optimal sampling methods.

The organization of paper is expressed as follows: Section 2 deals with the outline of the problem of this work for finding error free smart grid. The approach for finding voltage stability index (VSI), state estimation methods like AC state estimation idea of FDIA and WLS have also been explained in this section. Section 3 of this work mainly deals with the vulnerable node identification method. In this same segment the estimation method i.e. WEKF which could successfully identify FDIA and proposed method i.e. optimal WLS which supported us to identify the FDIA of smart grid have been discussed. The state deviation process which confirmed the FDIA has also been explained in section 3. In section 4, the performances of the proposed scheme have been described with different outcomes. Section 5 summarizes the findings of the present study and future scope of work.

2. THE OUTLINE PROBLEM AND METHODS FOR FINDING ERROR FREE SMART GRID

An outline of the problem of this work is given in the following paragraphs of this section.

- To improve the security system of smart grid, the vulnerable nodes of grid system have been detected with voltage sensitivity index (VSI) method.
- The false data detection technique is based on WEKF and optimal weighted least square (OWLS) which was not previously used in conjunction with detection of FDIA.
- The proposed method is also efficient for detecting the dynamic detection of the FDIA and the performance is very effective here.
- The proposed technique is highly scalable showing a reasonable results and good performance compared to existing work.
- The results obtained from experiment establish that this methodology continues outstanding detection performance of FDIA having variable strengths of attack.

2.1. Voltage stability index

In the distribution network constant voltage level for load end side is to be maintained mandatorily. Distribution operators maintain a constant voltage limit. Generally, voltage drop take place due to increase in load and a decrease in reactive power. Specific research determines the voltage stability index, which can be expressed by the following relation [22], [23].

$$VSI(N_r) = V_s^4 - 4(P_rX - Q_rR)^2 - 4(P_rR - Q_rX)V_s^2 \tag{1}$$

For an uninterrupted distribution system, operators need control on various system parameters. The measuring factors (e.g. current, voltage, and network power) should have error-free parameters. For the error-free measurement state estimation is a frequently used tool in power networks, which also helps to calculate its theoretical value [24].

2.2. AC state estimation

In the AC grid systems, in the state estimator, the power of a network is flowing in the form of a nonlinear function of power system parameters of states like magnitudes of voltage as well as angles. So, AC state estimation may be represented by a subsequent nonlinear relationship: $min\, z - h(x)$, when z being called a vector of measured values, and which is stated by the matrix equation as (2).

$$z = \begin{bmatrix} z_1 \\ \dots \\ z_{n-m} \\ \dots \\ z_n \end{bmatrix} = \begin{bmatrix} h_1(x_1, x_2, \dots x_3) \\ \dots \\ h_{n-m}(x_1, x_2, \dots x_3) \\ \dots \\ h_n(x_1, x_2, \dots x_3) \end{bmatrix} + \begin{bmatrix} e_1 \\ \dots \\ e_{n-m} \\ \dots \\ e_n \end{bmatrix}$$

$$z = h(x) + e \tag{2}$$

In the aforementioned (2), e is represented as a noise vector, x expresses the vector of network states (like magnitudes of voltage and voltage angles), here $h(x)$ is called the Jacobian matrix and is denoted by J_h which expresses the non-linear correlation of the measured data and network parameters of states, as (3).

$$J = \begin{bmatrix} \frac{\partial h_1}{\partial x_1} \frac{\partial h_1}{\partial x_2} \cdots \frac{\partial h_1}{\partial x_{n-1}} \frac{\partial h_1}{\partial x_n} \\ \frac{\partial h_2}{\partial x_1} \frac{\partial h_2}{\partial x_2} \cdots \frac{\partial h_2}{\partial x_{n-1}} \frac{\partial h_2}{\partial x_n} \\ \dots \\ \frac{\partial h_{m-1}}{\partial x_1} \frac{\partial h_{m-1}}{\partial x_2} \cdots \frac{\partial h_{m-1}}{\partial x_{n-1}} \frac{\partial h_{m-1}}{\partial x_n} \\ \dots \\ \frac{\partial h_m}{\partial x_1} \frac{\partial h_m}{\partial x_2} \cdots \frac{\partial h_m}{\partial x_{n-1}} \frac{\partial h_m}{\partial x_n} \end{bmatrix} \tag{3}$$

To gain access to a particular measuring device, a hacker may introduce an FDIA, which is alarming for the magnitude of measured data. For retaining the hacked measurement concealed, minimum one of the state variables is essential should be active. (else, erroneous value gained by state estimator (1) will exceed the onset, and FDI attack will be identified) [9]. The attackers are only able to gain access to measuring devices but not on states of the system. Therefore, the attacker can influence only the measured values which are linked with those system states to retain it untraceable [9]. The link between the measured values and states of network may be established from a Jacobian matrix. J_h (in (3)). The AC state estimation method for FDIA may be restructured as discussed in [9].

$$\left\| z' - h(x') \right\| = \| z + a - h(x + c) \| = \left\| \begin{pmatrix} z_n \\ z_{n+a} \end{pmatrix} - \begin{pmatrix} h(x_n) \\ h(x_n, x_a + c) \end{pmatrix} \right\| \tag{4}$$

Where, $z = z_n + z_a$ and $h(x) = h(x_n) + h(x_n, x_a + c)$, the terms expressed using subscript 'n' are meant for natural measured values of network states and are expressed terms with subscript 'a' are attacked measured values of the network. If the FDI attack is to be kept untraceable:

$$\| z' - h(x') \| = \| z - h(x) \| \tag{5}$$

but, for a normal situation $\| z - h(x) \| < \tau$. Hence, it follows that:

$$\left\|z' - h(x')\right\| = \|z - h(x)\| = \left\|\begin{pmatrix} z_n \\ z_{n+a} \end{pmatrix} - \begin{pmatrix} h(x_n) \\ h(x_n, x_a) \end{pmatrix}\right\| \tag{6}$$

solving (4) and (6), the attack vector value, may be attained as (7) [9].

$$a = h(x_n, x_a + c) - h(x_n, x_a) \tag{7}$$

From the (5), to introduce an attack vector, the hacker should know the pertinent system state values.

Hug and Giampapa [9] observed that AC state estimation may be used in an AMI-dependent smart grids framework. The AMI measured values are a subsection of the entire measured values expressed in (2). If the hacker gains access to entire or a subsection of AMI based devices, e.g., p-AMI devices, he or she can produce a FDI attack through selecting a nonzero attack vector a = {a1, …, am} in the manner so that this attack vectors at non-reachable devices happen to be zero (so, ai= 0, where, i, {AMI devices}).

Undetectable attacks can be created, and possible actions to be taken care of are discussed in the recent works [9], [24]-[27]. The FDI attacks (where the attacker's objective is to disorder system function) in AMI-based devices have two main impacts.

i. If FDIA becomes untraceable, like residuals are a smaller amount of an onset value in a weighted least square based estimator, network parameters of indicate (e.g., magnitude of voltage, angle) attained from the state estimation method deliver erroneous information [28]. The erroneous system conditions found from the state estimation method produce confusing operational decisions. These mislead the real-time and prolonged real-time operation in the network, like the solution of optimal power flow (OPF) or volt-VAR control (VVC). This false operative decision will reduce this system's efficiency, stability as well, and consequently, this will cause a significant blackout.
ii. FDI attacks, identified or unidentified, have straight effect in smart grid set-up. In these studies, the influence of FDI attacks on stability of system, in the next segment.

2.3. Weighted least square (WLS) method of state estimation

State estimation in power networks is a significant element in power system energy managing systems. Remote terminal units transmit field measurement data to a state estimator through data transmission systems. A state estimator adequately adjusts state variables of the power system by reducing the sum of residual squares. Few non-linear equations linking the measurements and power system states i.e. bus voltage, and phase angle support for this method. This process is the famous WLS method.

The preliminary WLS equation of state estimation process is given (8).

$$\text{So, } z = h(x) + e \tag{8}$$

The vector z of measured values is $z^T = [z_1\, z_2\, \dots\, z_m]$ and the vector $hh^T = [h_1(x)\, h_2(x)\, \dots\, h_m(x)]$ comprising the non-linear functions $h_i(x)$ is associated with the anticipated value of the measured quantity in state vector x having n variables $x^T = [x_1\, x_2\, \dots\, x_n]$. And e is a vector of measurement errors $e^T = [e_1\, e_2\, \dots\, e_m]$. The measurement errors e_i is supposed to fit the subsequent statistical properties. Primarily, errors with have zero mean has been calculated to find the voltage stability condition by using the following algorithm E (e_i) = 0, i = 1, … m. After that, errors were taken as independent, (E $[e_i e_j]$ = 0 for I ≠ j), in such a way that the covariance matrix is diagonal.

$$Cov(e) = E(ee^T) = R = diag\{\sigma_1^2, \sigma_2^2 \dots \sigma_m^2\}$$

The objective function is denoted by (9).

$$J(x) = \frac{\sum_{i=1}^{i=m}(zi\text{-}hi(x))^2}{R_{ii}} = (zh(x))^T R^{-1}(z - h(x)) \tag{9}$$

The minimization condition of (9) is indicated by:

$$g(x) = \frac{\delta f(x)}{\delta x} = H(x)^T R^{-1}(z - h(x)) = 0$$

where $H(x) = \partial h(x)/\partial x$. The Taylor series expansion of $g(x)$ is expressed as (10).

$$g(x) = g(x^k) + G(x^k)(x - x^k) + \ldots = 0 \tag{10}$$

Where the $k+1$ iterate is correlated to kth iteration via:

$$x^{k+1} = x^k - G(x^k)^{-1}g(x^k) \ldots \tag{11}$$

and $G(x^k)$ is a gain matrix $G(x^k) = \frac{\delta g(x^k)}{\delta x} = H^T(x^k)R^{-1}H(x^k)$. Here, every step of the iteration $g(x^k)$ satisfies $g(x^k) = H^T x^k R^{-1}(z - h(x^k))$.

3. VULNERABLE NODE IDENTIFICATION METHOD

3.1. VSI for vulnerable node identification

In real-time operation SCADA network supports running the data related to the consumption of power to the electrical distribution operator. AMI assistances to deliver these data to electrical operators. If the attacker somehow succeeds in tackling the data and changing the data for power of consumption, he can modify the data of AMI inserting bad data. So, the primary job of smart grid network will be to find the vulnerable nodes in a network. If an attacker somehow accesses the AMI based devices, one can control the data of power consumption by inserting wrong information. Here, we have considered that l-AMI based instruments are attacked by false data information. So, the attacked values of real as well as reactive power measurements, P_i^{FDI} and Q_i^{FDI}, are (12)-(14).

$$P_i^{FDI} = P_i^0 + a_i; i\forall\{1,2,\ldots l\} \tag{12}$$

$$Q_i^{FDI} = Q_i^0 + a_i; i\forall\{1,2,\ldots l\} \tag{13}$$

$$P_i^{FDI} = P_i^0 + P_i^0\beta = P_i^0(1+\beta) \tag{14}$$

where, P_i^0 and Q_i^0 are the correctly measured real and reactive powers of i-th AMI-based devices correspondingly. a_i symbolizes matching attack vectors. Then taking $a_i = P_i^0$, where a_i multiplication factor of actual dimensions, the (8) may be written as (11).

$$P_i^{FDI} = P_i^0 + P_i^0\beta_i = P_i^0\lambda_i \tag{15}$$

Where $\lambda_i = 1 + \beta_i$. Similarly:

$$Q_i^{FDI} = Q_i^0\beta_i \tag{16}$$

in (15) λ is attack degree expressed with any real number.

The VSI for a node in the smart grid is expressed with (1). According to the explanation of VSI, real power and reactive power at rth node may be expressed under regular operative state in this way:

$$P_r = \sum_{i\forall c} P_L^0 + P_{L(r)}^0 + \sum_{i\forall d} P_{LOSS} \tag{17}$$

$$Q_r = \sum_{i\forall c} Q_L^0 + Q_{L(r)}^0 + \sum_{i\forall d} Q_{LOSS} \tag{18}$$

where, P_L^0 and Q_L^0 are the real power and reactive power of the loads of power consumers, correspondingly. $P_{L(r)}$ and $Q_{L(r)}$ are real and reactive power loads of the rth energy consumers, correspondingly. P_{LOSS} and Q_{LOSS} are active and reactive power losses of the divisions correspondingly. In the above equations, c and d signify entire buses and branches correspondingly, beyond node ‘r’ when VSI has been computed.

Let us consider ‘r’ represents an AMI measured quantity node which is under the attacker, the (13) and (14) may be changed utilizing (11) and (12) as follows:

$$P_r = \sum_{i\forall c} P_L^0 + P_{L(r)}^0\lambda_r + \sum_{i\forall d} P_{LOSS} \tag{19}$$

$$Q_r = \sum_{i\forall c} Q_L^0 + Q_{L(r)}^0\lambda_r + \sum_{i\forall d} Q_{LOSS} \tag{20}$$

P_r and Q_r will change, if λ_r changes, and it will influence on VSI index shown in (1). From the (19) and (20), any insertion of false data will modify the value of P_r and Q_r, which starts again to reduce the value of VSI observed in (1). At the network distribution end, R/X ratio is very high [29]. A low amount of VSI indicates a failure of voltage of the system. Hence, the grid operatives would maintain the system within the stability boundary.

From (1), VSI depends on resistance R and inductance X of the power grid. So, the equal value of λ (means same quantity of false data insertion) at various nodes, the values of VSI should differ subject to changes of the values of R and X of the downriver branches of different nodes while they are attacked. The following segment describes the connection of VSI and FDI attack. As scope of this paper, VSI has been utilized for searching of vulnerable nodes in IEEE 14 bus topology (Figure 1) as experimental network. Figure 2 shows the vulnerable nodes detected in sample IEEE 14 bus network.

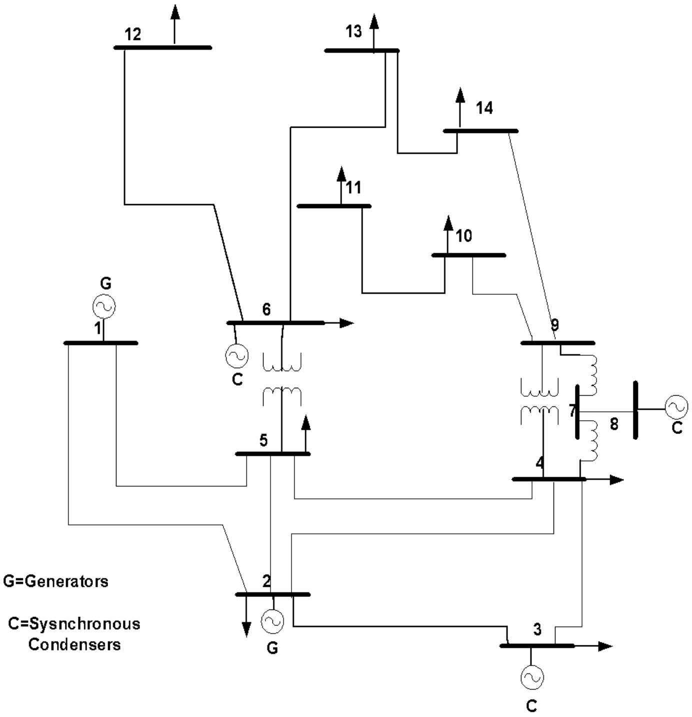

Figure 1. IEEE 14 bus topology

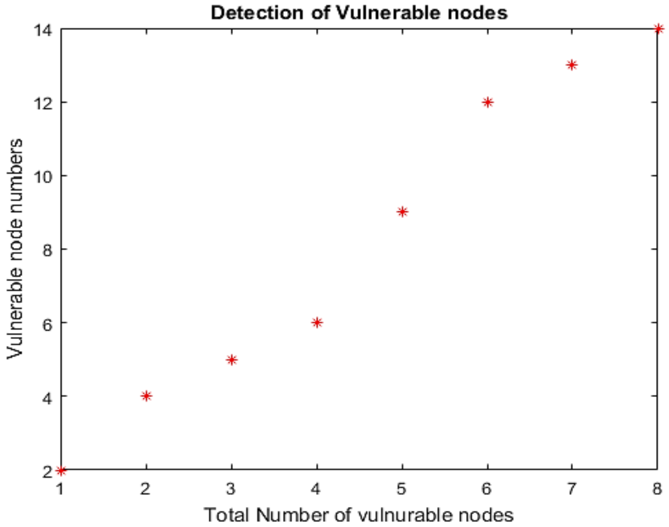

Figure 2. The vulnerable nodes detected in the sample network

3.2. Estimation methods for identification of FDIA

3.2.1. WEKF based measurement

Hu *et al.* [13] tried to simplify the EKF [30] to outstanding estimation result in the presence of FDIAs in the network. WEKF method adaptively reduces the gain value of filter of EKF with the expectation, which certifies the harmed measured values for having a smaller weight for the state estimation technique. The weights foreseen, expected measured values have seen to be enlarged. The bond among the weight matrix W_k of the measured values and the covariance matrix R of the measured noise is $W_k = R^{-1}$. The weight matrix of measured values is expressed as (21).

$$(W_k^{new})^{-1} = W_k^{-1} * e^{|zk-h(x\widehat{_{k|k=1}})|} \tag{21}$$

The performance of state estimation can be successfully explained because with the increment in attack strength, the technique could restrain successfully the attack. When the predicted estimated measurement $h(x\widehat{_{k|k-1}})$ diverges meaningfully from the present measurement zk, the enhancement in predicted remaining vector creates the noise due to measurement which ultimately reduces the Kalman gain. Slight differences among the forecasted and present measurements direct to small fluctuations in the measurement noise. This directs to small variations in Kalman gain and finally to small variations in predictable values. In the presence of FDIAs, the WEKF can restrain the consequences of attacks in an improved manner, eventually raising the mismatch between the WEKF and optimal WLS estimation.

3.3. Optimal WLS

3.3.1. A weighted least-squares approximation

In this research paper, we start with the discrete norm least-squares method. The common form of the discrete norm is shown in (22).

$$\|v\|_n := (\tfrac{1}{n}\textstyle\sum_{i=1}^{n} w^i \left|v(x^i)\right|^2) \tag{22}$$

The above equation will be used now for the weighted least-squares estimator. Here, sampling measured value dµ, usually varies from $d\rho$ has been applied and can be written as (23).

$$wd\mu = d\rho \tag{23}$$

Here w is considered as positive function described universally on X. So $fx\omega^{-1}dp = 1$, and we here reflect weighted least-square method where weights have been considered as follows: $wi = w(xi)$. Here we select the norm so that, the norm $\|v\|_n$ approaches $\|v\|$ as n improves. When $d\mu = d\rho$ and $w \equiv 1$ indicates standard least-squares method evaluated by Theorem 1.1. It is to be noted that varying the sampling values are a usual practice scheme for decreasing the difference in Monte Carlo methods, which includes importance sampling. L_j denotes $L^2(X, d\rho)$ orthonormal basis of V_m and with this an introduction of new function can be mentioned as (24).

$$x \rightarrow k_{m,w}(x) := \textstyle\sum_{j=1}^{m} w(x)\left|L_j(x)\right|^2 \tag{24}$$

Which is dependent on V_m, $d\rho$, and w.

$$K_{m,w} = K_{m,w}\,(V_m, d\rho, w) := \left\|k_{m,w}\right\|L^\infty \tag{25}$$

It is to be noticed that, as $\sqrt{w}L_j$ are an $L^2(X, d\mu)$ orthonormal basis of $\sqrt{w}V_m$ where space consists of functions $\sqrt{wg}$ with $g \in V_m$, we obtain $\int x^{k_m,wd\mu=m}$ and thus $K_m, w \geq\ m$.

3.3.2. Optimal sampling

Theorem 2.1 in leads the study with usual way aiming for optimal sampling scheme for weighted least-square method. Let us consider:

$$w := \frac{m}{k_m} = \frac{m}{\sum_{j=1}^{m}\left|L_j\right|^2} \tag{26}$$

for any value of w, one may test out that:

$$d\mu := \frac{k_m}{m}\,d\rho \tag{27}$$

is the probability measure on X as $\int x^{k_m d\rho = m}$. Furthermore, for the specific choice $k_m, w = wk_m = m$. Therefore:

$$k_m, w = m. \tag{28}$$

thus, we conclude that result is subsequent result of above theorem. This theorem displays that above selection of w and dμ permits for attaining nearest-optimal estimates which reduces weighted least-squares estimator, below nominal condition which selects n so that it becomes least of order $m\ ln(m)$.

3.4. Identification process with state deviation

The power flow calculation of power system is executed for k, and calculated result is included for deviation error following Gaussian distribution which is the measurement system. At this condition two numbers of state estimation approaches offered above are applied to evaluate the system state. Primarily, for comparing the deviations among two estimates the consistency test is applied. The formula is given by (29).

$$x\hat{}sk\ -\ x\hat{}d\ k\ 2\ \leq\ \tau a \tag{29}$$

Here $x\hat{}sk$ and $x\hat{}d\ k$ symbolizes the forecast state estimates using optimal WLS and WEKF respectively. The consistency check threshold is expressed with $\tau a.$ The value of τa is fixed by measurement error as well as correctness of state estimation outcome. As forecasted value is designed by means of Holt's two parameter approach, unexpected deviations in generator and load are not accepted in system. For removing false identifications due to sudden change in generator output or changes in load, the residues from the calculated estimates and the original measured value are ensured. The technique of residual test is given by (30).

$$zk\ -\ h\ (x\hat{}s\ k)\ 2\ \leq\ \tau b \tag{30}$$

Here $h\ (x\hat{}s\ k)$ can be expressed as estimated measured value found from the optimal WLS; the identification threshold of bad data is τb, and tolerance error of the chi-square distribution decides the result also. If the power grid is attacked with FDIA, the test results regarding consistency of the state estimation achieved through these two estimation approaches WEKF and optimal WLS are much higher than the threshold values. It ensures the presence of FDIAs. Ultimately, the forecast estimate values obtained applying WEKF are undergone through residual tests to determine the presence of FDIAs. If the threshold value of the optimal WLS test is lesser than the outcome of residual test, the presence of FDIA is sure in the system. Conversely, if threshold of chi-square test is greater than outcome of a residual test, then the consistency test result is interrupted, lastly it is determined that the system is attack-free.

4. RESULTS AND DISCUSSION

For experimental purpose MATLAB R2018b has been selected for simulation and analysis. The power flow of the network was evaluated applying significant data obtained by MATPOWER 7.1 power simulation platform. In this experiment, Gaussian noise has been included in power flow results. Here the mean value is selected 0 and the variance of 0.010. In the result section, the outcome regarding identification of projected method has been established from the simulation results. According to the proposed scheme, attack vector has been injected as FDIA in IEEE-14 bus network. Firstly, the FDIA nodes are detected by VSI method. Secondly after FDIA in smart grid the state estimation results applying WEKF, and proposed method (optimal WLS) have been compared. Lastly, the presence of FDIA has been determined by the proposed identification approach in IEEE-14 bus system.

The VSI index method was applied in IEEE-14 bus system with injected false data in some nodes. The experimental result with VSI is shown in Table 1. The VSI has efficiently detected the vulnerable nodes. Table 2 (column 1) shows all the meter measurements (taken as before attack) along with the estimates generated by WEKF and proposed method. Figure 3 illustrates the experimental results for the voltage magnitude of IEEE-14 bus system. The curves indicate voltage magnitudes for the different methods of state estimation with the proposed scheme. The proposed scheme establishes a very good, estimated value compared to the other methods. Table 3 explains data (voltage phase) which were obtained by all the meter measurements (taken as before attack) along with the estimating methods which are generated by WEKF and proposed method. Figure 4 illustrates the experimental results for the voltage phase of IEEE-14 bus system. The curves specify voltage phases for the different methods of state estimation with the proposed scheme which establishes a very good, estimated value than the other methods.

Table 1. Vulnerable node detection using VSI

Bus No.	VSI	Stability status	Bus No.	VSI	Stability status
1	1.0000	Stable	8	1.0000	Stable
2	-54.1942	Vulnerable	9	-97.5199	Vulnerable
3	1.0000	Stable	10	1.0000	Stable
4	-23.8973	Vulnerable	11	1.0000	Stable
5	-22.1350	Vulnerable	12	-8.2894	Vulnerable
6	-42.1593	Vulnerable	13	-76.7224	Vulnerable
7	1.0000	Stable	14	-98.1856	Vulnerable

Table 2. Comparison table for voltage magnitude of WEKF and the proposed method after FDI

Bus No.	Measured value in P. U		Methodology used		Bus No.	Measured value in P. U		Methodology used	
	Before FDI	After FDI	WEKF [13]	Proposed method		Before FDI	After FDI	WEKF [13]	Proposed method
1	1.068	1.2134	1.15	1.07	8	1.0287	1.1347	1.06	1.023
2	0.9899	1.0959	1.08	0.99	9	0.9763	1.088	1.07	0.976
3	0.9518	1.0645	1.05	0.96	10	0.9758	1.0873	1.07	0.979
4	0.9579	1.0716	1.061	0.958	11	0.9932	1.1025	1.1	0.98
5	0.9615	1.0749	1.06	0.96	12	1.0009	1.1091	1.1	1.001
6	1.0185	1.125	1.115	1.019	13	0.994	1.1028	1.1	1.03
7	0.9919	1.1028	1.1	1.01	14	0.9647	1.0772	1.05	0.97

Table 3. Comparison table for voltage phase of WEKF and the proposed method after FDI

Bus No.	Measured value in degree		Methodology used		Bus No.	Measured value in degree		Methodology used	
	Before FDI	After FDI	WEKF [13]	Proposed method		Before FDI	After FDI	WEKF [13]	Proposed Method
1	0	0	0	0	8	-13.39	-11.39	-14.39	-13.1
2	-4.97	-4.86	-4.9	-4.92	9	-14.91	-12.91	-15.91	-14.62
3	-12.75	-12.89	-12.8	-12.73	10	-15.4	-13.4	-16.4	-15.11
4	-10.3	-8.3	-11.3	-10.01	11	-14.9	-12.9	-15.9	-14.61
5	-8.76	-6.76	-9.76	-8.47	12	-15.7	-13.7	-16.7	-15.41
6	-14.5	-12.5	-15.5	-14.21	13	-15.5	-13.5	-16.5	-15.21
7	-13.3	-11.3	-14.3	-13.01	14	-16.08	-14.08	-17.08	-15.79

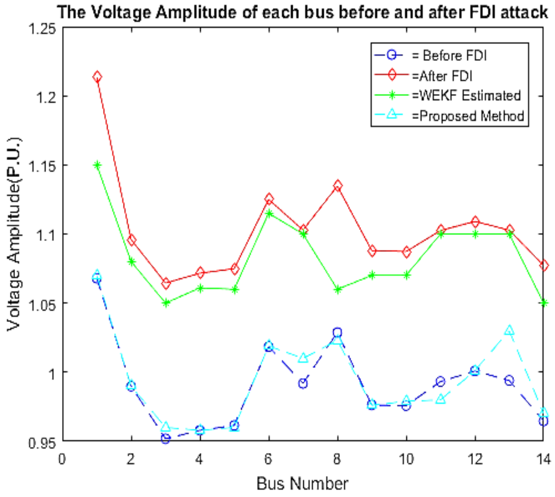

Figure 3. Comparison of voltage amplitude at each bus before and after FDI attack

4.1. Comparison of RMSE values for different methods

The paper also applies the root mean square error (RMSE) for determining the estimators- WLS, WEKF and optimal WLS performance. The RMSE is also used here to find the strength of state estimation while WLS, WEKF as well as optimal WLS are under FDIA attack. The RMSE computes the estimation error for WLS, WEKF and optimal WLS estimators by means of deviation between anticipated estimation and the real value. The anticipated estimated value for bus voltage is matched with real value while network is attacked. Computation of RMSE may be performed with the following equation. The RMSE computed by estimated error of every bus has been cited in Table 4. From Table 4, RMSE obtained by optimal WLS estimation is expressively lower compared to RMSE of the WEKF estimation. So, in presence of FDIA, the optimal WLS presents enhanced performance for estimation than the WEKF and WLS.

$$RMSE = \sqrt{\frac{1}{N}\sum_{j=1}^{N}(\hat{x_j} - x_j)^2} \tag{31}$$

Here N denotes the bus numbers; $\hat{x_j}$ denotes anticipated estimated voltage for the jth bus. The estimate errors for the voltage parameter for every are shown in Table 5. These data of voltage values have been taken while the smart grid is under attack. In Table 5, the estimate error of optimal WLS is found to be minimal when grid is under the injection of false data state. So optimal WLS shows an improvement for estimation performance over WEKF while smart grid faced attack by FDIA. The column of proposed method in Table 5 and Table 5 using optimal WLS shows very good results as optimal weight least method uses selection of w and dμ which permits the user for attaining nearest optimal estimates of abridged weighted least-squares estimator. Here the minimum condition is that n is minimal for the order $m\ ln(m)$.

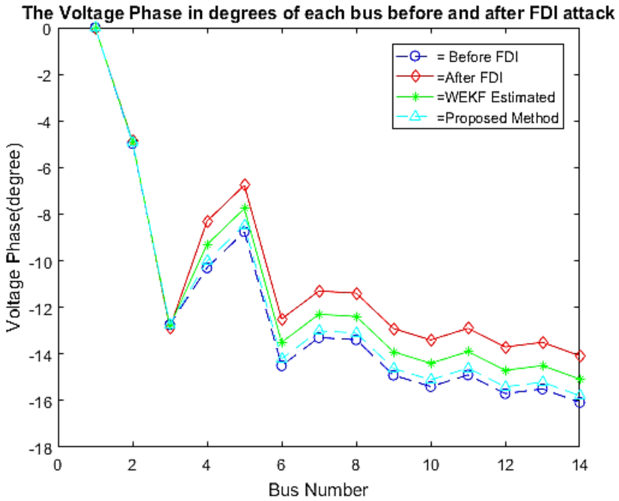

Figure 4. Comparison of voltage phase angles at each bus before and after FDI attack

Table 4. RMSE of voltage amplitude

Algorithm	RMSE
WLS	0.1094
WEKF [13]	0.0054
Optimal WLS	0.00038

Table 5. Estimated error of WLS, WEKF, and proposed optimal WLS and proposed method

Bus No.	WLS method (RMSE)	WEKF [13] (RMSE)	Proposed method (RMSE)	Bus No.	WLS method (RMSE)	WEKF [13] (RMSE)	Proposed method (RMSE)
1	8.23×10^{-2}	-3.1×10^{-3}	5.41×10^{-4}	7	10.90×10^{-2}	5.5×10^{-3}	1.54×10^{-4}
2	10.20×10^{-2}	5.3×10^{-3}	4.20×10^{-4}	8	11.44×10^{-2}	5.8×10^{-3}	1.37×10^{-4}
3	9.94×10^{-2}	4.2×10^{-3}	3.76×10^{-4}	9	10.96×10^{-2}	3.9×10^{-3}	1.89×10^{-5}
4	12.14×10^{-2}	5.1×10^{-3}	3.29×10^{-4}	10	10.94×10^{-2}	6.1×10^{-3}	1.55×10^{-5}
5	12.16×10^{-2}	6.2×10^{-3}	2.69×10^{-4}	11	11.75×10^{-2}	5.2×10^{-3}	5.43×10^{-5}
6	11.47×10^{-2}	7.5×10^{-3}	2.12×10^{-4}	12	11.64×10^{-2}	3.7×10^{-3}	6.46×10^{-6}
7	10.90×10^{-2}	5.5×10^{-3}	1.54×10^{-4}	13	11.71×10^{-2}	4.1×10^{-3}	6.76×10^{-6}
8	11.44×10^{-2}	5.8×10^{-3}	1.37×10^{-4}	14	12.05×10^{-2}	7.2×10^{-3}	7.55×10^{-6}

5. CONCLUSION

This paper recommends a technique based on VSI index and state deviation to efficiently identify and pinpoint the FDIA. To pinpoint the FDIA the VSI index algorithm has been implemented. Using a discrete optimal sampling weighting function to the orthodox WLS method, the detection performance due to the FDIA attack is blocked efficiently. The consistency test for WLS, WEKF as well as optimal WLS estimation were executed to primarily decide the presence of false data injection attack within network. With the intention of dropping this value for error finding rate, residual test was also executed. For reducing the redundancy of the network, efficient chi-square test has been executed. Ultimately, the experimental results establish the outstanding enactment of proposed scheme to identify FDIA. As future work, diverse FDIA of smart grid network, like time synchronization attack as well as interception attacks can be considered.

FUNDING INFORMATION

There is no funding involved: Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Poulami Ghosh	✓	✓	✓	✓	✓	✓		✓	✓	✓				
Subrata Biswas		✓				✓		✓	✓	✓	✓	✓	✓	
Prithwiraj Purkait	✓		✓	✓		✓			✓	✓	✓	✓	✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis

I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting

Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

No conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] H. Khurana, M. Hadley, Ning Lu, and D. A. Frincke, “Smart-grid security issues,” *IEEE Security & Privacy Magazine*, vol. 8, no. 1, pp. 81–85, Jan. 2010, doi: 10.1109/MSP.2010.49.

[2] Y. Zhang, L. Wang, and Y. Xiang, “Power system reliability analysis with intrusion tolerance in SCADA systems,” *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 669–683, Mar. 2016, doi: 10.1109/TSG.2015.2439693.

[3] B. Alohali, K. Kifayat, Q. Shi, and W. Hurst, “Replay attack impact on advanced metering infrastructure (AMI),” in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 175, pp. 52–59, 2017, doi: 10.1007/978-3-319-47729-9_6.

[4] P. H. Mirzaee, M. Shojafar, H. Cruickshank, and R. Tafazolli, “Smart grid security and privacy: From conventional to machine learning issues (threats and countermeasures),” *IEEE Access*, vol. 10, pp. 52922–52954, 2022, doi: 10.1109/ACCESS.2022.3174259.

[5] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer, “Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions,” *IEEE Signal Processing Magazine*, vol. 29, no. 5, pp. 106–115, Sep. 2012, doi: 10.1109/MSP.2012.2185911.

[6] Y. Dafalla, B. Liu, D. A. Hahn, H. Wu, R. Ahmadi, and A. G. Bardas, “Prosumer nano grids: a cybersecurity assessment,” *IEEE Access*, vol. 8, pp. 131150–131164, 2020, doi: 10.1109/ACCESS.2020.3009611.

[7] M. Du, G. Pierrou, X. Wang, and M. Kassouf, “Targeted false data injection attacks against AC state estimation without network parameters,” *IEEE Transactions on Smart Grid*, vol. 12, no. 6, pp. 5349–5361, Nov. 2021, doi: 10.1109/TSG.2021.3106246.

[8] R. McMillan, “Siemens: Stuxnet worm hit industrial systems,” PC World. [Online]. Available: http://www.pcworld.com /businesscenter/article/205420/siemens_stuxnet_worm_hit_industrial_systems.html.

[9] G. Hug and J. A. Giampapa, “Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks,” *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012, doi: 10.1109/TSG.2012.2195338.

[10] J. Shi, S. Liu, B. Chen, and L. Yu, “Distributed data-driven intrusion detection for sparse stealthy FDI attacks in smart grids,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 3, pp. 993–997, Mar. 2021, doi: 10.1109/TCSII.2020.3020139.

[11] C. Pei, Y. Xiao, W. Liang, and X. Han, “A deviation-based detection method against false data injection attacks in smart grid,” *IEEE Access*, vol. 9, pp. 15499–15509, 2021, doi: 10.1109/ACCESS.2021.3051155.

[12] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan, “Sparse malicious false data injection attacks and defense mechanisms in smart grids,” *IEEE Transactions on Industrial Informatics*, vol. 11, no. 5, pp. 1–12, Oct. 2015, doi: 10.1109/TII.2015.2475695.

[13] P. Hu, W. Gao, Y. Li, F. Hua, L. Qiao, and G. Zhang, “Detection of false data injection attacks in smart grid based on joint dynamic and static state estimation,” *IEEE Access*, vol. 11, pp. 45028–45038, 2023, doi: 10.1109/ACCESS.2023.3273730.

[14] M. A. Rahman and H. Mohsenian-Rad, “False data injection attacks against nonlinear state estimation in smart power grids,” in *2013 IEEE Power & Energy Society General Meeting*, IEEE, 2013, pp. 1–5, doi: 10.1109/PESMG.2013.6672638.

[15] R. Deng, P. Zhuang, and H. Liang, “False data injection attacks against state estimation in power distribution systems,” *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2871–2881, May 2019, doi: 10.1109/TSG.2018.2813280.

[16] C. Liu, H. Liang, and T. Chen, “Network parameter coordinated false data injection attacks against power system AC state estimation,” *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1626–1639, Mar. 2021, doi: 10.1109/TSG.2020.3033520.

[17] N. N. Tran, H. R. Pota, Q. N. Tran, and J. Hu, “Designing constraint-based false data-injection attacks against the unbalanced distribution smart grids,” *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 9422–9435, Jun. 2021, doi: 10.1109/JIOT.2021.3056649.

[18] G. Cheng, Y. Lin, J. Zhao, and J. Yan, “A highly discriminative detector against false data injection attacks in AC state estimation,” *IEEE Transactions on Smart Grid*, vol. 13, no. 3, pp. 2318–2330, May 2022, doi: 10.1109/TSG.2022.3141803.

[19] S. Nath, I. Akingeneye, J. Wu, and Z. Han, “Quickest detection of false data injection attacks in smart grid with dynamic models,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 10, no. 1, pp. 1292–1302, Feb. 2022, doi: 10.1109/JESTPE.2019.2936587.

[20] G. Chaojun, P. Jirutitijaroen, and M. Motani, “Detecting false data injection attacks in AC state estimation,” *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2476–2483, Sep. 2015, doi: 10.1109/TSG.2015.2388545.

[21] J. Zhao, G. Zhang, and R. A. Jabr, “Robust detection of cyber attacks on state estimators using phasor measurements,” *IEEE Transactions on Power Systems*, vol. 32, no. 3, pp. 2468–2470, May 2017, doi: 10.1109/TPWRS.2016.2603447.

[22] M. Chakravorty and D. Das, “Voltage stability analysis of radial distribution networks,” *International Journal of Electrical Power & Energy Systems*, vol. 23, no. 2, pp. 129–135, Feb. 2001, doi: 10.1016/S0142-0615(00)00040-5.

[23] T. Zabaiou, L. Dessaint, and I. Kamwa, “Preventive control approach for voltage stability improvement using voltage stability constrained optimal power flow based on static line voltage stability indices,” *IET Generation, Transmission & Distribution*, vol. 8, no. 5, pp. 924–934, May 2014, doi: 10.1049/iet-gtd.2013.0724.

[24] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 1–33, May 2011, doi: 10.1145/1952982.1952995.

[25] A.-S. K. Pathan, *The state of the art in intrusion prevention and detection*, 2014, doi: 10.1201/b16390.

[26] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, “Sparse attack construction and state estimation in the smart grid: centralized and distributed models,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1306–1318, Jul. 2013, doi: 10.1109/JSAC.2013.130713.

[27] S. Bi and Y. J. Zhang, “Graphical methods for defense against false-data injection attacks on power system state estimation,” *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1216–1227, May 2014, doi: 10.1109/TSG.2013.2294966.

[28] A. Anwar and A. N. Mahmood, “Vulnerabilities of smart grid state estimation against false data injection attack,” in *Green Energy and Technology*, vol. 0, no. 9789814585262, 2014, pp. 411–428, doi: 10.1007/978-981-4585-27-9_17.

[29] W. H. Kersting, *Distribution system modeling and analysis*. CRC Press, 2017. doi: 10.1201/9781315120782.

[30] R. Zhang, Q. Zhang, Z. Wang, and H. Sun, “Detection of false data injection attack in smart grid based on iterative Kalman filter,” in *2021 China Automation Congress (CAC)*, IEEE, Oct. 2021, pp. 6083–6088, doi: 10.1109/CAC53003.2021.9728537.

BIOGRAPHIES OF AUTHORS

Poulami Ghosh is currently working as assistant professor in Electrical Engineering Department of St. Thomas' College of Engineering and Technology. She received the M.Tech. degrees in Engineering from Jadavpur University, Kolkata, India in 2007. Her research includes the cyber security in smart grid system. She can be contacted at email: ghoshpoulami81@gmail.com.

Subrata Biswas is currently working as associate professor in Electrical Engineering Department of Netaji Subhash Engineering College, Kolkata, India. He received the M.E.E. and Ph.D. degrees in Engineering from Jadavpur University, Kolkata, India in 2006 and 2017 respectively. He has co-authored more than 35 research papers. His research includes the condition monitoring of power equipment, advanced signal processing technique in power system, high-voltage engineering, and partial discharge diagnostics. He can be contacted at email: subratab28@gmail.com.

Prithwiraj Purkait is a professor of Power Engineering Department, Jadavpur University, Kolkata, India. He obtained his B.E.E, M.E.E, and Ph.D. degrees from Jadavpur University, Kolkata, India in 1996, 1999, and 2002 respectively. He was involved in postdoctoral research and further as visiting academic in the University of Queensland, Australia during 2002-2003, 2005, and 2007. He has published about 100 research papers and has authored five books. His current research includes transformer insulation condition assessment techniques, motor and drives fault diagnosis techniques, and advanced signal processing applications in high-voltage engineering. He can be contacted at email: prajpurkait@gmail.com.