Electric Power Systems Research 187 (2020) 106490

Contents lists available at ScienceDirect

Electric Power Systems Research

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

Smart grids cyber-physical security: Parameter correction model against unbalanced false data injection attacks☆

Tierui Zou[a], Arturo S. Bretas[*,a], Cody Ruben[a], Surya C. Dhulipala[a], Newton Bretas[b]

[a] Department of Electrical & Computer Engineering, University of Florida, Gainesville, FL 32611-6200 USA
[b] Department of Electrical and Computer Engineering University of Sao Paulo, Sao Carlos, SP, Brazil

ARTICLE INFO

Keywords:
Smart grid
False data injection
System parameters
Cyber physical security

ABSTRACT

This paper presents a correction model for malicious, unbalanced parameter false data injection cyber-attacks. Current state-of-art solutions can detect, identify and correct balanced parameter false data injection cyber-attacks. Thus, they consider all the parameters as equal in error, which means the methods will only work when the same percentage attack happens to each parameter. In this paper, a new correction model using a parameter correction Jacobian matrix, τ, and a Taylor series approximation is presented. A framework for measurement gross error analysis is deployed in processing and analyzing cyber-attacks. Chi-square χ^2 Hypothesis Testing applied to the normalized composed measurement error (CME^N) is considered for cyber-attacks detection, while the largest CME^N error test is used for identification. Validation is performed on the IEEE 14-bus and 118-bus systems. Easy-to-implement model, without hard-to-design parameters, built on the classical weighted least squares solution, highlights potential aspects for real-life implementation.

1. Introduction

As the power grid implements Smart Grid [1] technologies, the many advantages of new metering, controls, and analysis come with added technical challenges. Specifically, the digitalization of the power grid and the increasing dependence on communications systems makes the network more vulnerable to cyber-attacks [2–4]. Cyber-attacks, if not detected and accurately corrected, can lead to misinformation to system operators and potential collapse of the power system [5,6]. While much research has been done to address this concern, science and technology for smart grids cyber-physical security is still seldom.

In any power system, real-time monitoring is a critical process for reliable operation. Currently, physics-based quasi-static system model Power System State Estimation (PSSE) is the main tool for real-time system monitoring [7]. PSSE uses readings of sensors to provide information about the condition of the system. These readings are commonly transmitted to a Supervisory Control and Data Acquisition (SCADA) system, which is where PSSE is performed. The results of PSSE are used in many applications for power systems operation. One of the most important applications is its error processing capability. Measurements that are obviously incorrect or inconsistent are discarded in a pre-filtering step, still a post-processing step called bad data analysis is performed afterwards [8]. The goal of bad data analysis is to detect the existence of bad data among the dataset. Bad data are called Gross Errors (GE) and are modelled as statistically large errors.

As the Smart Grid becomes more of a reality, and more vulnerable to cyber-attacks, the bad data analysis process of PSSE becomes more critical to reliable operation. One type of cyber-attack is the false data injection (FDI), where a subset of data values are modified by an attacker such that the power grid operation is disrupted [9–11]. Most research in this area focus on the detection of measurement FDI [12–17]. However, as illustrated in Fig. 1, a similar strategy can be used by an attacker where instead of attacking the measurements themselves (attack a), the attacker modifies the values of logical status data for switches on the system (attack b), or the stored parameters values of the power system (attack c).

System parameters include values such as transmission line series impedance and shunt capacitance, and are typically values with no dynamics [19]. This data, named here static data, is stored in a database that is not subject to the same pre-processing steps as real-time measurements, meaning if it is compromised, it will not be filtered out or corrected before the PSSE process. Since these parameters are used to build the model of the system, they are most important to the accuracy of PSSE.

Parameter error analysis has been proposed in the previous work [20]. Abur and Expósito [20] uses an augmented state vector based

☆ This work was supported by NSF grant ECCS-1809739.
* Corresponding author.
E-mail address: arturo@ece.ufl.edu (A.S. Bretas).

https://doi.org/10.1016/j.epsr.2020.106490
Received 5 March 2020; Received in revised form 8 May 2020; Accepted 20 June 2020
Available online 04 July 2020

Nomenclature

C	Threshold value of Chi-square distribution
z	Measurement Vector
e	Measurement error vector
τ	Parameter correction Jacobian matrix
$\mathbb{R}^N$	State variables vector space
$\mathbb{R}^m$	Measurement vector space
$J(.)$	Objective function
$h(.)$	Continuous nonlinear differentiable function
σ	Standard deviation
R	Measurement covariance matrix
N	Number of unknown state variables
H	Jacobian matrix of $h(.)$
$\hat{x}$	Estimated state vector
$\hat{z}$	Estimated value of z
x^*	Operating point of state
K	Projection matrix
e_U	Undetectable error
e_D	Detectable error
CME	Composed measurement error
II	Innovation Index
CNE	Composed normalized error
H_p	Jacobian of parameter
g_{k-m}	Conductance from bus k to bus m
b_{k-m}	Series Susceptance from bus k to bus m
b_{k-m}^{sh}	Shunt Susceptance from bus k to bus m
S_{k-m}^{*}	Conjugated complex power flow
I_{k-m}	Complex current in transmission line from bus k to m
P_{k-m}	Real power flow from bus k to m
Q_{k-m}	Reactive power flow from bus k to m
V_k	Voltage at bus k
y_{k-m}	Admittance from bus k to bus m
$P_{k-m(loss)}$	Real power loss from bus k to m
$\lvert E_k - E_m \rvert$	magnitude of the voltage drop from bus k to m
P_k	Real power injection at bus k
Q_k	Reactive power injection at bus k
CME^N	Normalized composed measurement error
$\triangle p$	Parameter error

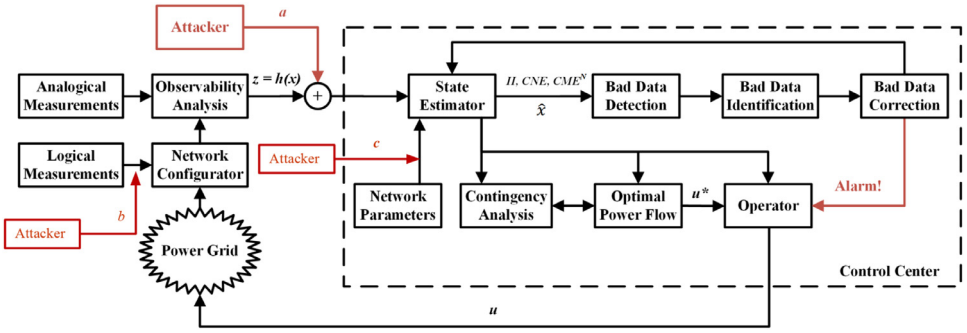

Fig. 1. Various FDI attacks on PSSE (adapted from Bretas et al. [18]).

approach, which can lead to observability issues on low redundancy systems. Furthermore, this approach can't handle multiple simultaneous attacks. In previous work of the authors, parameter cyber-attack correction models have been presented [18,21]. However, these have been limited to either single parameter attacks or multiple attacks of equal magnitude. An intelligent FDI attack otherwise could modify individual parameters in such a way to make the attack as stealthy as possible. For example, rather than modifying only the susceptance parameter value of a transmission line, an attacker could change the susceptance and conductance parameter values of a line. Furthermore, each value could be changed by a different magnitude, making the attack an unbalanced one. One should note that the solution in [21] would only successfully correct both attacks types if they were of the same magnitude percentage (balanced). As in previous works [21], it is not necessary for an attacker to have complete knowledge of the system in order to implement an unbalanced attack on the system parameters. Simple knowledge of the parameters being altered are necessary for an attack. For attacks considered in this paper, that means the attacker needs only information about one or two lines of the system.

This paper presents a model for unbalanced parameter FDI cyber-attacks processing. Presented model considers estimated power losses, and real and reactive power flows measurements. An enhanced cyber-physical security framework for smart grids FDI attacks processing is presented. FDI attacks are detected through a Chi-squared test based on the Innovation concept [18], while considering the extension of the Gauss approach for the solution of an overdetermined set of algebraic non-linear equations [16]. Cyber-attacks are identified with the composed normalized error test [21]. Cyber-attacks are otherwise corrected through a parameter correction Jacobian matrix τ and Taylor series approximation based model. Simultaneous measurement and parameter FDI cyber-attacks are iteratively detected, identified, and corrected. It is vital that all three of these steps are reliable and accurate. Even if a cyber-attack is properly detected and identified, improper correction does not fix the problem at hand. Therefore, a miscorrected attack can still be considered stealthy since the true nature of the attack is not completely known and addressed. The model is tested on the IEEE 14 and 118 bus systems. Comparative test results highlight the model's security and dependability, even when there are simultaneous unbalanced parameter and measurement FDI cyber-attacks, presenting a clear contribution to the state-of-the-art of power systems cyber-physical security.

The specific contributions of this paper towards the state-of-the-art are as follows:

- Unbalanced parameter correction model against false data injection attacks.

- Cyber-physical security framework for detection, identification and correction of false data injection attacks.

The remainder of the paper is organized as follows. Section 2 presents a review on the Smart Grid and the Innovation based quasi-static model weighted least squares state estimation solution. A model for unbalanced parameter cyber-attack correction and a framework for smart grids real-time cyber-security against FDI are presented in Section 3. Case studies are presented in Section 4. Section 5 presents the conclusions of this work.

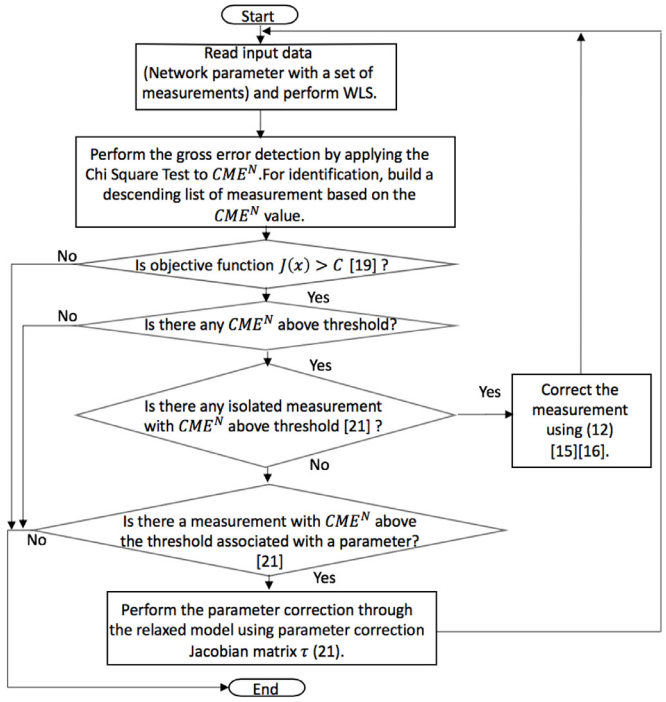

Fig. 2. Data flowchart of the cyber-physical security framework.

2. Background information

2.1. Smart grid

As described in [1], the driving idea towards a Smart Grid is to transform the power system by using Information and Communication Technology (ICT) aiming to create a more sustainable, efficient, and controllable network. ICT allows for two way communication throughout the grid, giving utilities more insight into energy consumption. The Smart Grid will be able to operate distributed generation, reroute the distribution network in real-time though advanced switching equipment enabling self-healing capabilities, and enable real-time monitoring through numerous sensors.

While there are many advantages of the Smart Grid, the increasing amount of ICT leaves the system more vulnerable to cyber-attacks. In [2], relatively simple simulations are run which show that cyber-attacks, gone undetected, can easily trigger widespread outages. Wang et al. [3] discusses the current standards of the power system and concludes that as the Smart Grid is implemented, special care should be taken to address the security of ICT and the algorithms that use the data collected by Smart Grid devices. Ashok and Govindarasu [5], Margossian et al. [6] also show the potential for damaging cyber-attacks through FDI attacks of both real-time measurements or network topology, which is based on mostly static data. Namely, an undetected FDI attack on network topology can lead to violations of system operating limits. This is both damaging to the system equipment and can trigger unnecessary outages.

In real-life, there have already been numerous cases of cyber-attacks which highlight the impact they can have. The first confirmed blackout caused by a cyber-attack on a power grid caused a power outage that affected 225,000 customers in Ukraine [22,23]. Another example of a malicious cyber-attack on a power grid was the Stuxnet malware used to attack the Iran's Nuclear Technology Center [24]. Both cases are examples of how cyber attacks can cause physical harm to the grid, and customers to lose power for an extended period of time.

Table 1
Processing cyber-attacks.

Processing Measurement Cyber-Attack Step 1
$J(x) = 148.57 > C = 132.14$ Attack Detected!
CME^N Descending List

Measurement	II	CME^N
Q_{02-03}	0.9635	6.0474
P_{04-05}	4.0873	−5.8763
Q_{03-02}	0.7432	3.5401
P_{03-02}	6.6220	−3.4331
P_{02-03}	6.4898	3.4063

2.2. Innovation based state estimation theory

A power system with n buses and m measurements can be modeled as a set of non-linear algebraic equations as follow [19]:

$$z = h(x) + e, \tag{1}$$

where $z \in \mathbb{R}^m$ is the measurement vector, $x \in \mathbb{R}^N$ is the state variables vector, $h(x) : \mathbb{R}^N \rightarrow \mathbb{R}^m$, $(m > N)$, is a non-linear differentiable function that relates the states to the measurements, and e is the measurement error vector assumed with zero mean, standard deviation σ and having Gaussian probability distribution. $N = 2n - 1$ is the number of unknown state variables which consist of the voltage magnitudes and angles.

The weighted least squares state estimator searches for the best estimates of the states x which minimizes the cost function as follow:

$$J(x) = \|z - h(x)\|^2_{R^{-1}} = [z - h(x)]^T R^{-1}[z - h(x)], \tag{2}$$

where R is the measurement covariance matrix. $J(x)$ is geometrically a norm in the measurements vector space $\mathbb{R}^m$. Let $\hat{x}$ be the solution of the aforementioned minimization problem, then the estimated measurement vector is $\hat{z} = h(\hat{x})$. The residual is defined as the difference between $\hat{z}$ and z, which means $r = z - \hat{z}$. Linearizing (1) at a certain operating point x^* yields:

$$\triangle z = H \triangle x + e, \tag{3}$$

where $H = \frac{\partial h}{\partial x}$ is the Jacobian matrix of h calculated at the point x^*. $\triangle z = z - h(x^*) = z - z^*$ and $\triangle x = x - x^*$ are the correction of measurement and state vectors, respectively. It is important to note that in the context of a parameter FDI, the values in both h and H will be directly affected [21]. PSSE considers the static data to estimate the system states, however incorrect parameter values will drive PSSE to an incorrect solution.

The state estimation can be formulated as a projection. Let K be a linear operator such that $\triangle \hat{x} = K \triangle z$ and the residual vector $r = \triangle z - \triangle \hat{z}$. Then, the vector $\triangle \hat{z} = H \triangle \hat{x}$ is orthogonal to the residual vector r, since K projects the measurement vector mismatch $\triangle z$ orthogonally in the range space of H, as shown in [14]. Equivalently,

$$< \triangle \hat{z}, r > = (H \triangle \hat{x})^T R^{-1} (\triangle z - H \triangle \hat{x}) = 0, \tag{4}$$

Solving (4) for $\triangle \hat{x}$, one can obtain the following:

$$\triangle \hat{x} = (H^T R^{-1} H)^{-1} H^T R^{-1} \triangle z, \tag{5}$$

In other words, the projection matrix K is the idempotent matrix that has the following expression:

$$K = H (H^T R^{-1} H)^{-1} H^T R^{-1}, \tag{6}$$

The geometrical position of the measurement error in relation to the range space of H provides another way of interpreting the state estimation. Hence, as the measurement vector can be decomposed into two subspaces, it is possible to decompose the measurement error vector into two components as follows:

Table 2
Corrected Parameters using the parameter correction Jacobian matrix τ.

Parameter correction Parameter	Database	Erroneous	Presented correction	State-of-the-art correction
			(Approximation error)	**(Approximation error)** [21]
g_{02-03}	1.1350	1.0783	1.1313 (0.326%)	1.1295 (0.485%)
b_{02-03}	−4.7819	−4.5428	−4.7617 (0.422%)	−4.7586 (0.487%)
b^{sh}_{02-03}	0.0219	0.0208	0.0217(0.913%)	0.0217 (0.913%)

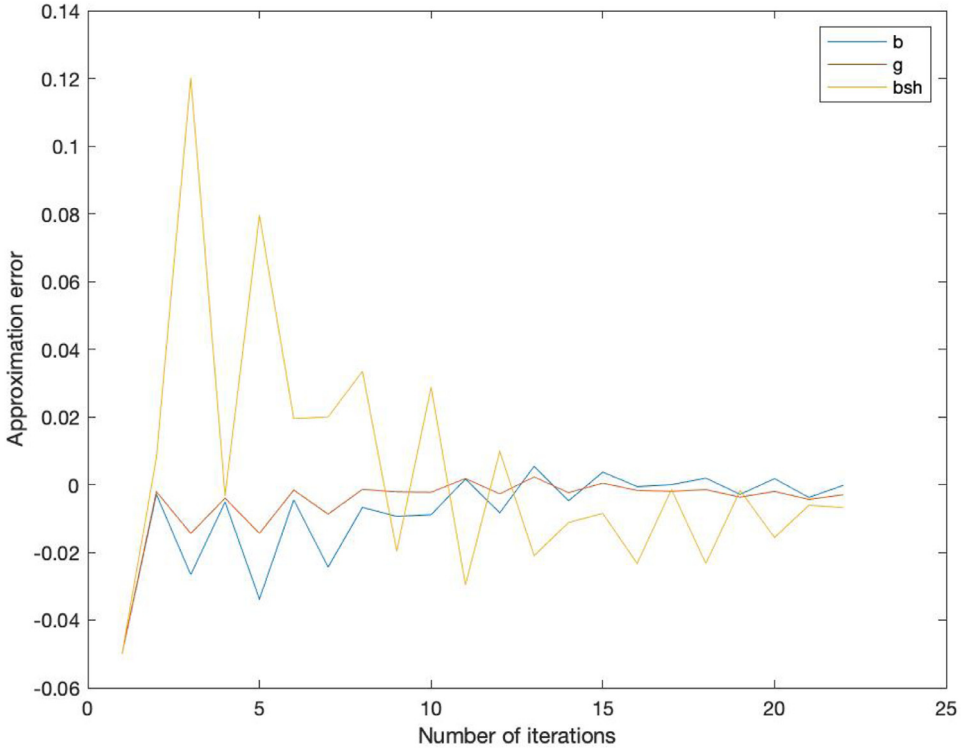

Fig. 3. Correction for line 02–03 using presented model.

$$e = \underbrace{Ke}_{e_U} + \underbrace{(I-K)e}_{e_D}, \tag{7}$$

The component e_D is the detectable error, which is the residual in the classical model, while the component e_U is the undetectable error. e_D is in the orthogonal space to the range space of Jacobian whereas e_U is hidden in the Jacobian space. In order to quantify the undetectable error, the Innovation Index (II) is introduced [17] and is presented in the following:

$$II_i = \frac{\|e_D^i\|}{\|e_U^i\|} = \frac{\sqrt{1-K_{ii}}}{\sqrt{K_{ii}}}, \tag{8}$$

Low Innovation index means there is a large component of error that is not reflected in the residual. Therefore, the residual will be very small even if there is a gross error. By analysing the norm of (7) and substituting in (8), the composed measurement error can be expressed in terms of the residual and the innovation index as follow [17]:

$$CME_i = r_i\left(\sqrt{1+\frac{1}{II_i^2}}\right), \tag{9}$$

If the normalized residual is used instead, one can obtain the Composed Normalized Error (CNE) as follow:

$$CNE_i = r_i^N\left(\sqrt{1+\frac{1}{II_i^2}}\right), \tag{10}$$

Where r_i^N is the normalized residual of meaurement i. Otherwise, CME can be normalized as follow:

$$CME_i^N = \frac{r_i}{\sigma_i}\left(\sqrt{1+\frac{1}{II_i^2}}\right), \tag{11}$$

where σ_i is the standard deviation for measurement i.

2.3. Parameter error analysis

In (1), the possibility of errors in the parameter data is not considered. Instead, if one considers $z = h(x, p) + e$, where p is the parameter in error, this function can be developed into a Taylor Series [21]:

$$z_i = h_{i,0} + \frac{\partial h_i(x,p)}{\partial p}\triangle p, \tag{12}$$

where $\triangle p$ is the parameter error. From (12), the parameter error can be calculated to be as follow:

$$\triangle p = \frac{z_i - h_{i,0}}{H_{p,0}}, \tag{13}$$

where $H_{p,0}$ is the Jacobian of parameters. All the quantities are known, so one can calculate the parameter error through (13), which is called here the relaxed model, since it considers the measurements without error. Through this model one can correct parameter errors using the measurement value of reactive power flow corresponding to the line

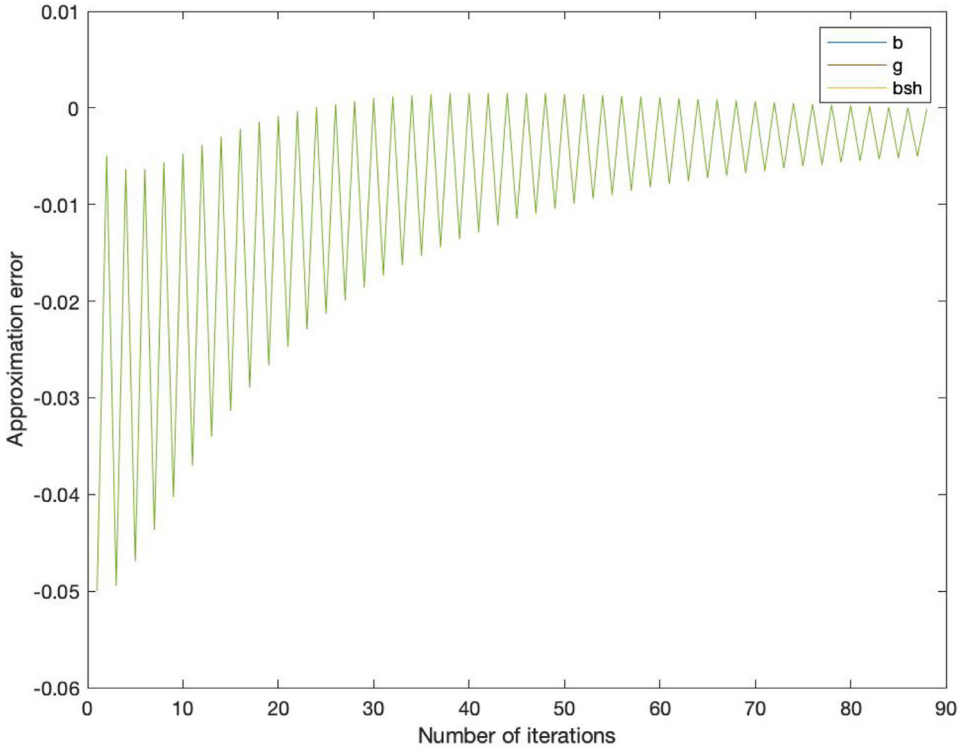

Fig. 4. Correction for line 02–03 using state-of-the-art solution in [21].

Table 3
Processing cyber-attacks.

Processing Measurement Cyber-Attack Step 1 $J(x) = 1078.163 > C = 132.14$ Attack Detected! CME^N Descending List		
Measurement	*II*	CME^N
Q_{02-03}	1.0204	39.0369
Q_{03-02}	0.7220	−37.2976
Q_{03-04}	2.7513	31.3345
Q_{04-03}	3.2326	−30.3003
P_{05}	0.2010	−27.3349
Q_{04-09}	0.8963	22.1735
P_{03-02}	6.3665	−17.7507
Q_{03}	2.0920	17.6771
P_{02-03}	1.8594	17.5790
P_{04-05}	4.1028	−6.9408
P_{03}	4.5145	5.5459

where the parameter attack happened through iterations. However, network parameter values includes three components, which are series conductance g, series susceptance b and shunt susceptance b^{sh}. At the same time, the weights of these three components depend on the network parameter database, so one can only correct the parameter error through this model when these three components have the exactly same percentage attack, lets say, 10% on g, 10% on b, and 10% on b^{sh}. Thus

Table 5
Processing cyber-attacks.

Processing Measurement Cyber-Attack Step 1			
$J(x) = 179.8857 > C = 132.14$ Attack Detected! CME^N Descending List			
Measurement	*II*	CME^N	*CNE*
P_{04-05}	4.1013	−6.9725	−7.1440

unbalanced FDI in parameter values are not considered by this model, for example, 30% on g, 20% on b,and 10% on b^{sh}. To address this issue, an unbalanced correction model is presented in this paper.

3. Unbalanced parameter attack correction model

Consider the conjugate of the complex power flow [19]:

$$\begin{aligned} S^*_{k-m} &= E^*_k I_{k-m} \\ &= y_{k-m} V_k e^{-j\theta_k} \left(V_k e^{j\theta_k} - V_m e^{j\theta_m}\right) + j b^{sh}_{km} V_k^2, \end{aligned} \tag{14}$$

The expressions for the real and reactive power flows can be obtained by identifying the corresponding coefficients of the real and the imaginary parts of (14):

$$P_{k-m} = V_k^2 g_{km} - V_k V_m g_{km} \cos\theta_{km} - V_k V_m b_{km} \sin\theta_{km} \tag{15}$$

$$Q_{k-m} = -V_k^2 (b_{km} + b^{sh}_{km}) + V_k V_m b_{km} \cos\theta_{km} - V_k V_m g_{km} \sin\theta_{km}, \tag{16}$$

Table 4
Corrected Parameters using the parameter correction Jacobian matrix τ .

Parameter correction Parameter	Database	Erroneous	Presented correction	State-of-the-art correction
			(Approximation error)	**(Approximation error)** [21]
g_{02-03}	1.1350	1.2485	1.1293 (0.502%)	−1.9165 (268.854%)
b_{02-03}	−4.7819	−4.5428	−4.7518 (0.629%)	6.9732 (245.824%)
b^{sh}_{02-03}	0.0219	0.0230	0.0217(0.913%)	−0.0353 (261.187%)

Table 6
Corrected measurement using the CNE .

Measurement correction			
Measurement	**Database**	**Erroneous**	**Correction using CNE (Approximation error)** [15,16]
P_{04-05}	−0.6118	−0.6546	−0.6100 (0.294%)

Table 7
Processing cyber-attacks.

Processing Measurement Cyber-Attack Step 1		
$J(x) = 27.5507 < C = 132.14$ No attack Detected!		
Measurement	***II***	$\boldsymbol{CME^N}$
Q_{02-03}	0.9337	−0.5638
Q_{03-02}	0.7199	0.0985
Q_{03-04}	2.6915	−0.0696
Q_{04-03}	3.3602	0.3548
Q_{05}	0.2008	−2.5676
Q_{04-09}	0.8929	0.0073
P_{03-02}	6.4259	0.2503
Q_{03}	2.0793	−0.1400
P_{02-03}	6.3022	−0.0673
P_{04-05}	4.0994	−0.0470
P_{03}	4.6728	−0.4800

Through Eq. (15), one can derive the real power loss of a line:

$$\begin{aligned} P_{k-m(loss)} &= P_{k-m} + P_{m-k} \\ &= g_{km}(V_k^2 + V_m^2 - 2V_kV_m\cos\theta_{km}) \\ &= g_{km}\,|E_k - E_m|^2, \end{aligned} \tag{17}$$

Eqs. (15)–(17) provide a model which correlates the real power flow losses, real power flow, and reactive power flow with system parameters. These equations can be easily organized into matrix format:

$$\begin{pmatrix} |E_k - E_m|^2 & 0 & 0 \\ V_k^2 - V_kV_m\cos\theta_{km} & -V_kV_m\sin\theta_{km} & 0 \\ -V_kV_m\sin\theta_{km} & -V_k^2 + V_kV_m\cos\theta_{km} & -V_k^2 \end{pmatrix} \begin{pmatrix} g_{km} \\ b_{km} \\ b_{km}^{sh} \end{pmatrix} = \begin{pmatrix} P_{k-m(loss)} \\ P_{k-m} \\ Q_{k-m} \end{pmatrix}, \tag{18}$$

(18) is a set of non-linear algebraic equations, which can be linearized through a Taylor series, considering a Newton-Raphson method n_{th} iteration:

$$\begin{pmatrix} |E_k - E_m|^2 & 0 & 0 \\ V_k^2 - V_kV_m\cos\theta_{km} & -V_kV_m\sin\theta_{km} & 0 \\ -V_kV_m\sin\theta_{km} & -V_k^2 + V_kV_m\cos\theta_{km} & -V_k^2 \end{pmatrix}^n \begin{pmatrix} \Delta g_{km} \\ \Delta b_{km} \\ \Delta b_{km}^{sh} \end{pmatrix} = \begin{pmatrix} Z_{P_{k-m(loss)}} - h^n_{P_{k-m(loss)}} \\ Z_{P_{k-m}} - h^n_{P_{k-m}} \\ Z_{Q_{k-m}} - h^n_{Q_{k-m}} \end{pmatrix}, \tag{19}$$

Let the parameter correction Jacobian matrix τ be defined as:

$$\tau = \begin{pmatrix} |E_k - E_m|^2 & 0 & 0 \\ V_k^2 - V_kV_m\cos\theta_{km} & -V_kV_m\sin\theta_{km} & 0 \\ -V_kV_m\sin\theta_{km} & -V_k^2 + V_kV_m\cos\theta_{km} & -V_k^2 \end{pmatrix}, \tag{20}$$

Then the correction for each parameter g, b, or b^{sh} will be done through iterations considering:

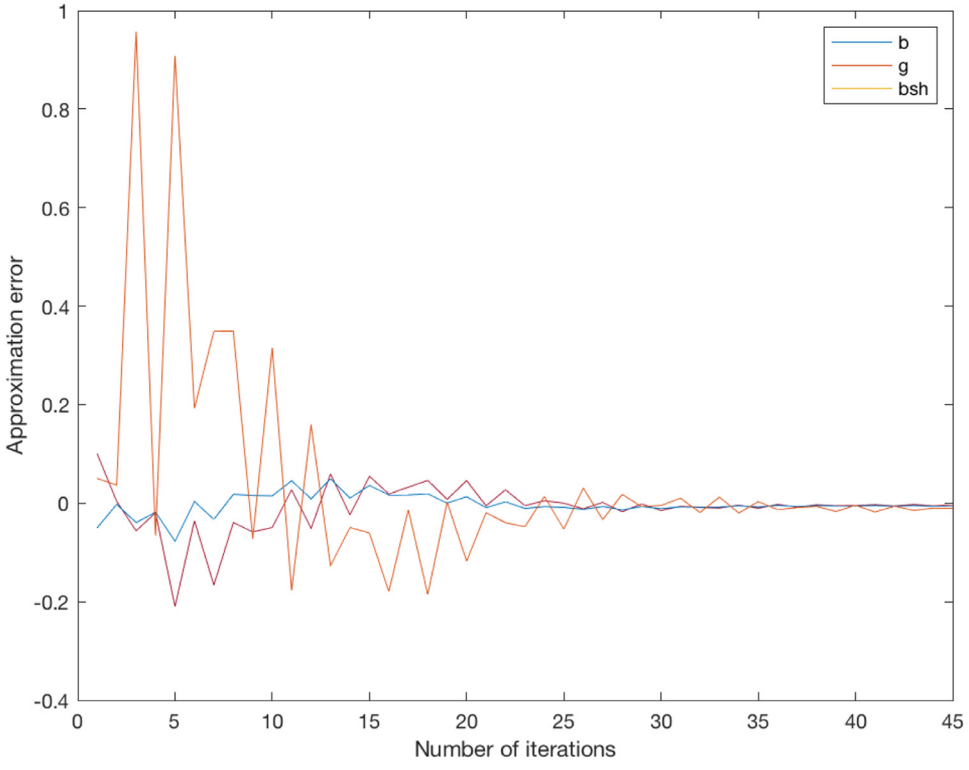

Fig. 5. Correction for line 02–03 using presented model.

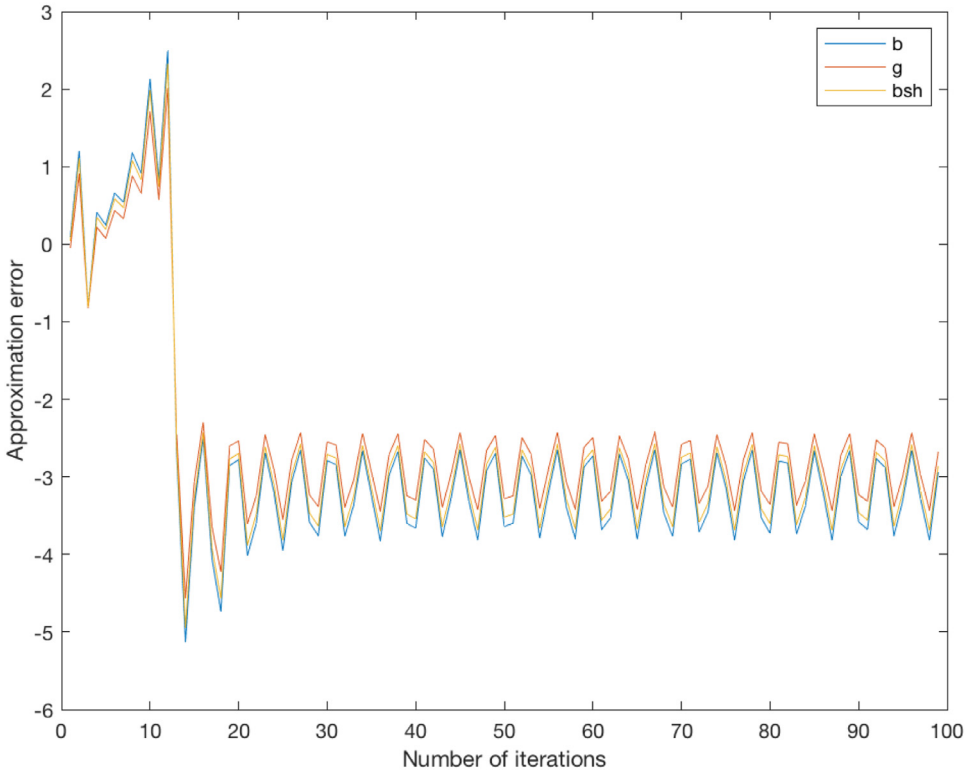

Fig. 6. Correction for line 02–03 using state-of-the-art solution in [21].

Table 8
Processing cyber-attacks.

Processing Measurement Cyber-Attack Step 1 J (x) = 95,762.581 > C = 132.14 Attack Detected!		
CME^N Descending List		
Measurement	*II*	CME^N
Q_{01-05}	1.8983	160.1638
Q_{05-01}	0.7377	−135.9005
Q_{01-02}	2.4522	−103.9931
Q_{01}	1.4556	−103.4556
Q_{02}	3.7805	72.6300
P_{05}	0.1832	−35.7542
Q_{02-05}	0.8061	−60.1611
P_{02}	0.2874	−51.0811
P_{04}	1.2404	−35.7542
Q_{05-02}	1.5040	31.0782
P_{06}	0.7437	−26.5596
Q_{04-02}	2.4309	21.5742
P_{05-01}	7.5007	−21.1503
Q_{03-02}	0.9015	20.6724
P_{04-05}	4.1894	−19.4216
P_{05-04}	4.1787	19.3794
P_{01-05}	7.2439	19.0012

$$\begin{pmatrix} \Delta g_{km} \\ \Delta b_{km} \\ \Delta b_{km}^{sh} \end{pmatrix} = \tau^{-1^n} \begin{pmatrix} Z_{P_{k-m(loss)}} - h^n_{P_{k-m(loss)}} \\ Z_{P_{k-m}} - h^n_{P_{k-m}} \\ Z_{Q_{k-m}} - h^n_{Q_{k-m}} \end{pmatrix}, \tag{21}$$

Model solution converges when a pre-established convergence value is reached. Fig. 2 presents a data flow chart of the cyber-physical security framework considering the parameter error correction model. Gross error detection is performed by applying Chi-Squared Test to CME^N [18]. Identification is done by the composed normalized error test [21]. In this framework, the possibility of either or simultaneous measurement or parameter errors are considered by analyzing the measurement error characteristics [21]. Thus, if there are any isolated measurement errors identified, they are corrected using the *CNE* [15,16]. If a group of measurements associated with the same parameters have high CME^N values, parameter correction is performed by (21) considering the parameter correction Jacobian matrix τ (20).

4. Case study

In this case study, three different FDI attack scenarios are presented. The validation of proposed methodology is done using the IEEE 14-bus and 118-bus systems. The measurement set used for IEEE 14-bus system consists 107 measurements obtained from MATPOWER [25], leading to a global redundancy level GRL = 3.96. For the IEEE 118-bus test system the measurement set consists of 860 measurements, leading to

Table 9
Corrected Parameters using the parameter correction Jacobian matrix τ.

Parameter correction Parameter	Database	Erroneous	Presented correction	State-of-the-art correction
			(Approximation error)	**(Approximation error)** [21]
g_{01-05}	1.0259	1.3337	1.0243 (0.155%)	Unable to converge (∞)
b_{01-05}	−4.2350	−3.3880	−4.2335 (0.035%)	Unable to converge (∞)
b^{sh}_{01-05}	0.0246	0.0271	0.0245(0.406%)	Unable to converge (∞)

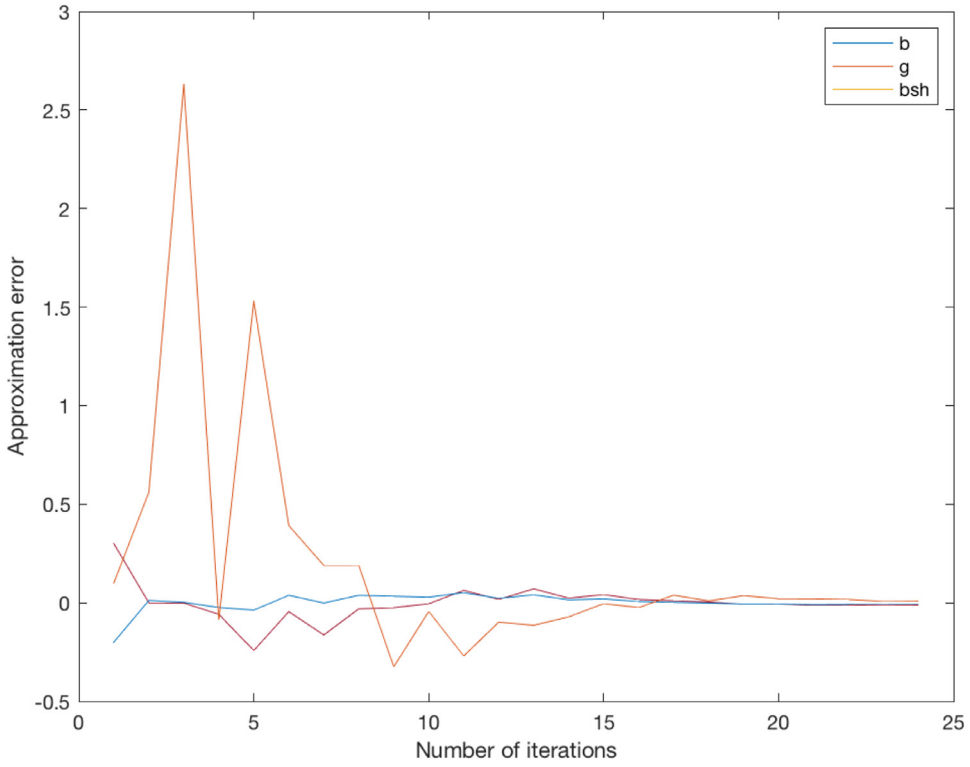

Fig. 7. Correction for line 01–05 using presented model.

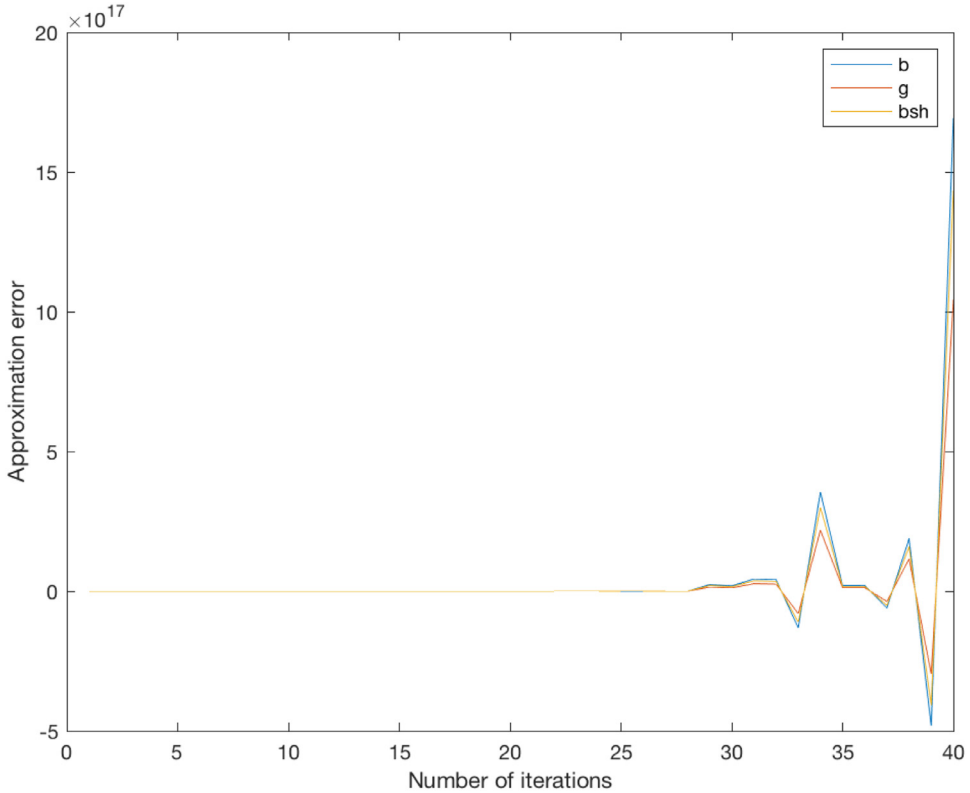

Fig. 8. Correction for line 01–05 using presented model.

Table 10
Processing cyber-attacks.

Processing Measurement Cyber-Attack Step 1
J (x) = 4,627.263 > C = 978.3282 Attack Detected!
CME^N Descending List

Measurement	*II*	CME^N
Q_{23-32}	1.4121	−25.5929
Q_{69-47}	2.4033	25.2469
Q_{27-25}	1.5627	−18.4139
Q_{32-23}	1.3423	14.5728
Q_{47-69}	1.6006	−13.0238
Q_{23}	0.4618	9.6543
Q_{25-23}	3.3068	−8.4263
P_{47-69}	5.8944	−7.2040
P_{32}	1.9551	6.6656
P_{69-47}	5.5424	6.4778
Q_{69-70}	1.7417	−5.3168
Q_{72-24}	1.7678	−5.2636
P_{23-32}	4.8832	−5.2139
P_{32-23}	4.9319	5.1730

the GRL = 3.65. System topology and parameters are found in [26].

4.1. Parameter attack scenario I

On the IEEE 14-bus system, a balanced parameter cyber-attack to the series and shunt parameters of line 2–3 (− 5% on parameter g, − 5% on parameter b, − 5% on parameter b^{sh}) is simulated. Attack processing starts with detection, as shown in the data flowchart, where the objective function is higher than the C value for this scenario ($C = \chi^2 = 132.144$), as presented in Table 1. A descending list of CME^N is built after a cyber-attack is detected. The largest CME^N, associated with Q_{02-03}, Q_{03-02}, P_{02-03}, P_{03-02}, characterizes a parameter cyber-attack on line 2–3 [21]. After identification, the net system parameter are corrected using the presented model in (21). Corrected values and comparable results are presented in Table 2. One can see that the balanced parameter attack is successfully corrected using the presented model, from numeric results, the correction presents more accurate performance, considering [21]. Further results in every iteration until convergence are presented in Figs. 3 and 4. The presented model and state of the art algorithm [21] successfully corrects the balanced parameter cyber-attack on line 2–3, however, as one can see the presented model provides accurate and faster convergence rate[21].'s slower convergence rate is expected since it corrects parameters synchronously by considering attacks in all parameters are in same percentage. One should notice that only a green curve is shown in Fig. 4 since all parameters are corrected synchronously, so all three parameter curves are overlapping. Fig. 3 has three separate curves, one for each parameter being corrected.

4.2. Parameter attack scenario II

On the IEEE 14-bus system, we analyze two simultaneous cyber-attacks:

1. A measurement cyber-attack of magnitude 7 σ is added to real power flow from bus 4 to bus 5 (P_{04-05}).
2. An unbalanced parameter cyber-attack to the series and shunt parameters of line 2–3 (10% on parameter g, − 5% on parameter b, 5% on parameter b^{sh}).

Table 12
Processing cyber-attacks.

Processing Measurement Cyber-Attack Step 1
J (x) = 1,272.218 > C = 978.3282 Attack Detected!

CME^N Descending List

Measurement	*II*	CME^N
Q_{69-47}	2.4023	25.4139
Q_{47-69}	2.5183	−11.9623
P_{47-69}	5.8891	−6.5504
Q_{49-69}	2.2762	6.0225
P_{69-47}	5.5366	5.6603
Q_{69-49}	3.2668	5.1741

The FDI attack processing starts with detection, step 1, where the objective function is higher than the C value for this scenario ($C = \chi^2 = 132.144$), as presented in Table 3. Once the attack is detected, a descending list of CME^N is built. By analyzing this list, one can find there are several values above the threshold value $\beta = 3$. The largest values CME^N, related to Q_{02-03}, Q_{03-02}, P_{02-03}, P_{03-02}, P_{03}, Q_{03}, characterizes a parameter cyber-attack on line 2–3 [21]. Then, the net parameter of line 2–3 is corrected using τ in (21). The corrected parameters are shown in Table 4. From Table 4, one can see the final results after convergence, with a small approximation error. After convergence in the correction process, a new state estimation is performed and objective function J(x) is 179.8857, so a new descending list of CME^N is built. The result is shown in Table 5. As seen, the only CME^N value (absolute value) above the threshold is the real power flow of the line 4–5. Therefore, the measurement P_{04-05} is in error. The correction of measurements as shown in the flowchart is performed using their *CNE* values. Corrected measurement is shown in Table 6. After re-running the state estimator, no CME^N value is found to be above the threshold as shown in Table 7. Fig. 5 presents convergence results while applying the presented correction model. Table 4 and Fig. 6 also present the correction results when applying [21]. As one can see, the approximation errors are much larger than the presented correction model.

4.3. Parameter attack scenario III

On the IEEE 14-bus system, an unbalanced parameter cyber-attack to the series and shunt parameter of the line 1–5 (30% on parameter g, 20% on parameter b, 10% on parameter b^{sh}) is simulated. The attack processing starts with detection, the result is shown in Table 8. In Table 8, only values of CME^N above 10 are listed. In this case, the objective function J(x) is 95,762.581, which is extremely large because of this unbalanced parameter FDI attack. Once there is an attack detected, a descending list of CME^N is built. By analyzing this list, one can see the largest value of CME^N is related to the measurement of reactive power flow from line 1–5, and the $CME^N s$ of real power flow as well as the injections on those buses are all above threshold value $\beta = 3$. This situation is characterized as parameter attack on line 1–5 [21]. Then, the

Table 11
Corrected parameters using the parameter correction Jacobian matrix τ.

Parameter correction Parameter	Database	Erroneous	Presented correction (Approximation error)	State-of-the-art correction (Approximation error) [21]
g_{23-32}	2.2169	1.8179	2.2385 (0.974%)	0.4369 (80.292%)
b_{23-32}	−8.0635	−9.0311	−8.0854 (0.271%)	−2.1706 (73.081%)
b^{sh}_{23-32}	0.0587	0.0551	0.0589(0.340%)	0.0133 (77.342%)

Table 13
Corrected parameters using the parameter correction Jacobian matrix τ.

Parameter correction Parameter	Database	Erroneous	Presented correction (Approximation error)	State-of-the-art correction **(Approximation error)** [21]
g_{47-69}	1.0012	1.1314	1.0088 (0.759%)	0.9698 (3.136%)
b_{47-69}	−3.2955	−3.0648	−3.2826 (0.361%)	−2.6270 (20.285%)
b^{sh}_{47-69}	0.0355	0.0383	0.0357(0.563%)	0.0328 (7.606%)

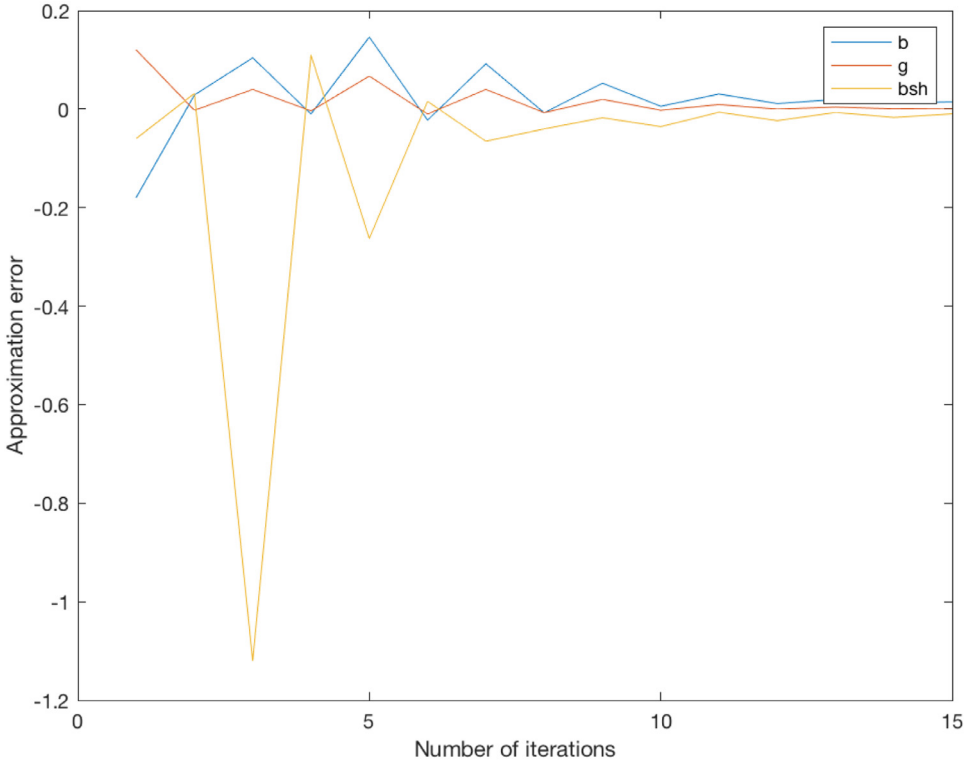

Fig. 9. Correction for line 23–32 using presented model.

correction is performed using τ in (21). Correction results are presented in Table 9, all parameter g, b, and b^{sh} are effectively corrected. Fig. 7 presents convergence results of the unbalanced correction model. As one can see from Table 9 and Fig. 8, when using the state of the art solution [21], this method is unable to converge.

4.4. Parameter attack scenario IV

On the IEEE 118-bus system, we analyze two simultaneous cyber-attacks:

1. Unbalanced parameter FDI attack to the series and shunt parameter of the line 23–32 (− 18% on parameter g, 12% on parameter b, − 6% on parameter b^{sh}).
2. Unbalanced parameter FDI attack to the series and shunt parameter of the line 47–69 (13% on parameter g, − 7% on parameter b, 8% on parameter b^{sh}).

In this case, the parameter of two lines are simultaneously attacked ($line_{23-32}$ and $line_{47-69}$). Different percentage FDI attacks are injected in each parameter of each line. The first processing of the framework is detection. Results are presented in Table 10. In Table 10, one can see that the objective function J(x) is 4,627.263, which is much higher than threshold value C (978.3282), thus an attack is detected. A descending list of CME^N is built, the largest absolute value of CME^N which is 25.5929 in this list is related to reactive power flow from line 23–32. As one can see, the CME^N value of corresponding real power flow and injection related to line 23–32 are also above the threshold value. This situation is characterized as a parameter attack on line 23–32 [21]. The correction process is implemented until convergence. The results for correction are shown in Table 11. After the correction for net parameter of line 23–32, a new state estimation process is performed, and a new descending lists of CME^N is built in Table 12 since the objective function value 1,272.218 is still higher than threshold value C(978.3282). One will notice the largest value of CME^N is related to reactive power flow in line 69-47 and the corresponding $CME^N s$ of real power flow (positive and negative direction) are also above threshold value. Then a parameter attack of line 69-47 is identified [21]. Correction is performed and the results of this correction are shown in Table 13.

Further information of correction using the presented model is illustrated in Fig. 9. One can see the corrected values of each parameter are very close to the original values after convergence.

On the other hand, additional correction results in every iteration for line 23–32 using the state of art solution [21] are shown in Fig. 10 and Table 11. The system is able to converge. However, each parameter converges to an incorrect value. To illustrate the performance of the presented model, comparable results of line 47–69 correction are presented in Figs. 11 and 12. It is interesting to point out that even though the correction method in [21] does correction for the errors on line 47–69, it does a poor job on line 23–32. This shows that simultaneous

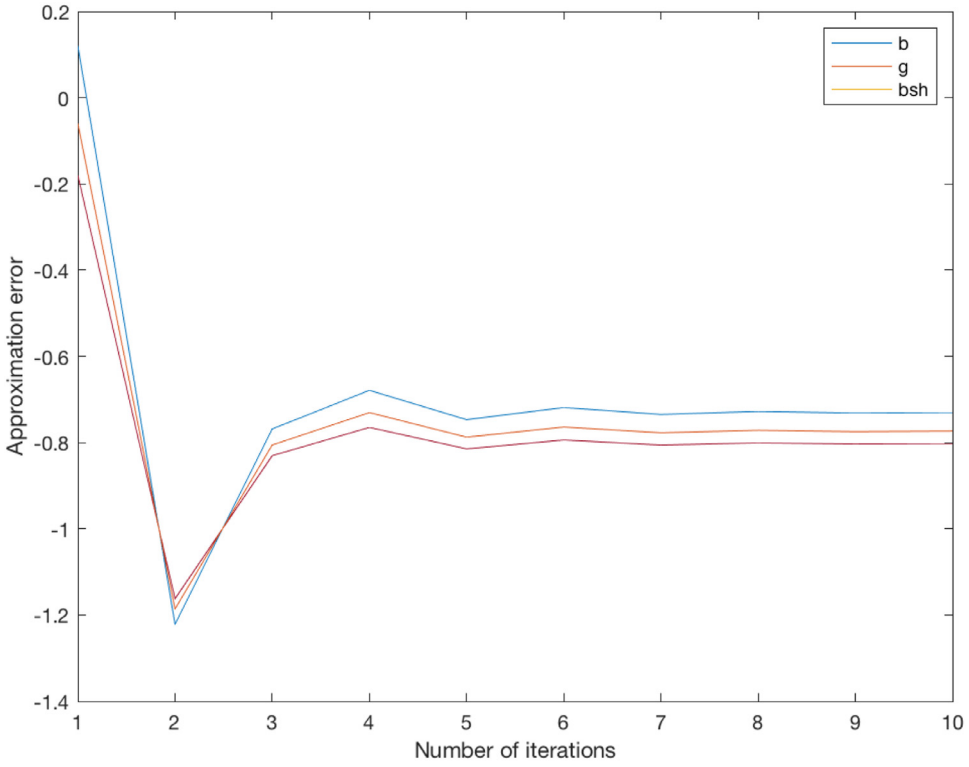

Fig. 10. Correction for line 23–32 using state-of-the-art solution in [21].

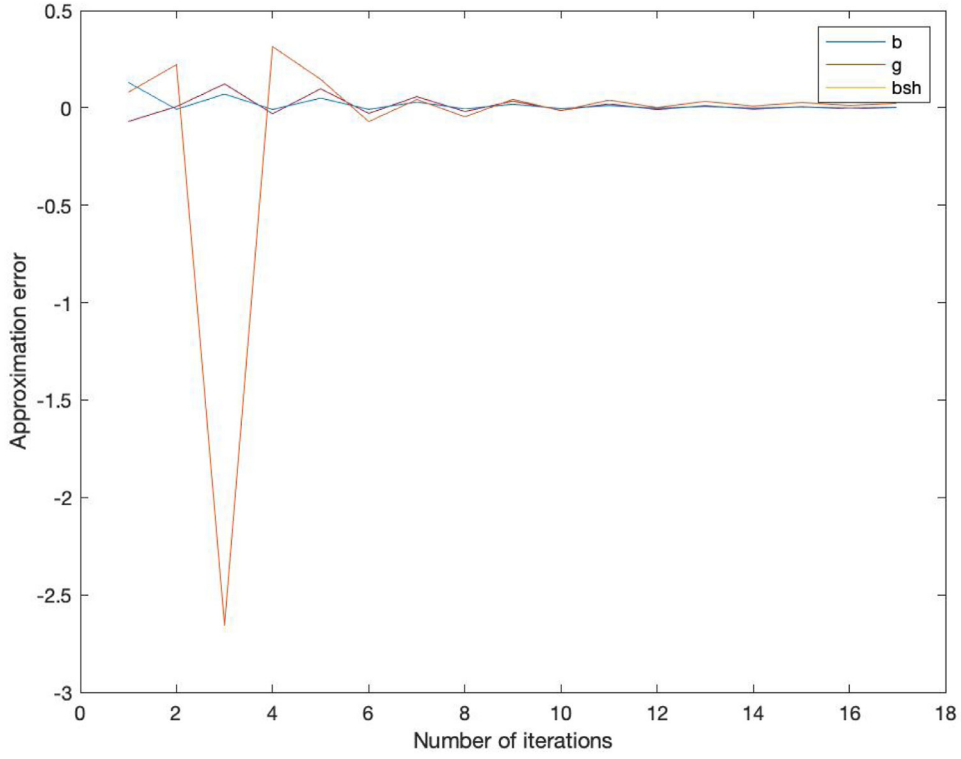

Fig. 11. Correction for line 47–69 using presented model.

attacks can have an impact on the system even if one of the attacks is identified and corrected decently well under the current method. The proposed method is able to accurately correct both of line parameters, nullifying the cyber-attacks impact on state estimation dependent applications.

5. Conclusion

This paper presents a correction model for malicious unbalanced parameter FDI cyber-attacks. A smart grids cyber-physical security framework for FDI attacks processing is further presented. State-of-the-art solutions only model parameters under the same percentage of FDI.

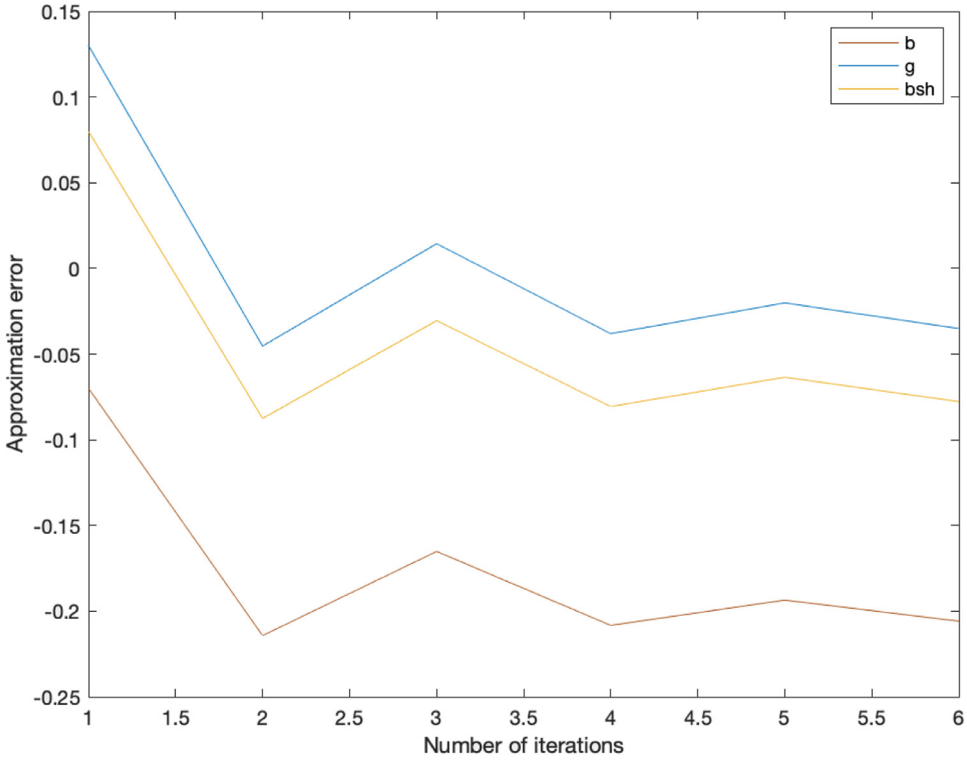

Fig. 12. Correction for line 47–69 using state-of-the-art solution in [21].

Case studies considering the IEEE 14-bus and IEEE 118-bus highlights presented model parameter correction precision with approximation errors smaller than 1%, while state-of-the-art model [21] fails to converge or converges to incorrect values. The advantage of presented model in regards to the state-of-the-art is that it allows correction of either balanced or unbalanced parameter FDI attacks. Still, the SE software does not require major changes for the implementation of the correction model. With the presented correction model, parameter attacks that could be considered stealthy using the state-of-the-art are no longer stealthy, preventing the potential for damage to the system and outages.

CRediT authorship contribution statement

Tierui Zou: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Writing - original draft, Visualization. **Arturo S. Bretas:** Conceptualization, Methodology, Software, Writing - original draft. **Cody Ruben:** Software, Writing - review & editing, Visualization, Investigation. **Surya C. Dhulipala:** Software, Investigation, Visualization, Writing - review & editing. **Newton Bretas:** Supervision, Investigation, Visualization, Writing - review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

References

[1] P. Bansal, A. Singh, Smart metering in smart grid framework: a review, 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), (2016), pp. 174–176, https://doi.org/10.1109/PDGC.2016.7913139.

[2] A. Stefanov, C. Liu, Cyber-power system security in a smart grid environment, 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), (2012), pp. 1–3, https://doi.org/10.1109/ISGT.2012.6175560.

[3] Y. Wang, B. Zhang, W. Lin, T. Zhang, Smart grid information security - a research on standards, 2011 International Conference on Advanced Power System Automation and Protection, vol. 2, (2011), pp. 1188–1194, https://doi.org/10.1109/APAP.2011.6180558.

[4] S. Bi, Y.J.A. Zhang, Graph-based cyber security analysis of state estimation in smart power grid, IEEE Commun. Mag. (99) (2017) 2–9.

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

[6] H. Margossian, M.A. Sayed, W. Fawaz, Z. Nakad, Partial grid false data injection attacks against state estimation, Int. J. Electr. Power Energy Syst. 110 (2019) 623–629, https://doi.org/10.1109/PDGC.2016.7913139.

[7] Y. Liu, P. Ning, M.K. Reiter, False data injection attacks against state estimation in electric power grids, ACM Trans. Inform. Syst. Secur.(TISSEC) 14 (1) (2011) 13, https://doi.org/10.1109/ISGT.2012.6175560.

[8] S.A. Zonouz, K.M. Rogers, R. Berthier, R. Bobba, W.H. Sanders, T.J. Overbye, SCPSE: Security-oriented cyber-physical state estimation for power grid critical infrastructures. IEEE Trans. Smart Grid 3 (4) (2012) 1790–1799, https://doi.org/10.1109/APAP.2011.6180558.

[9] S. Li, Y. Yılmaz, X. Wang, Quickest detection of false data injection attack in wide-area smart grids, IEEE Trans. Smart Grid 6 (6) (2015) 2725–2735.

[10] S. Li, Y. Yilmaz, X. Wang, Sequential cyber-attack detection in the large-scale smart grid system, Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on, IEEE, 2015, pp. 127–132.

[11] Q. Wang, W. Tai, Y. Tang, M. Ni, S. You, A two-layer game theoretical attack-defense model for a false data injection attack against power systems, Int. J. Electr. Power Energy Syst. 104 (2019) 169–177.

[12] P. Chen, S. Yang, J.A. McCann, J. Lin, X. Yang, Detection of false data injection attacks in smart-grid systems, IEEE Commun. Mag. 53 (2) (2015) 206–213.

[13] S.K. Singh, K. Khanna, R. Bose, B.K. Panigrahi, A. Joshi, Joint-transformation-based detection of false data injection attacks in smart grid, IEEE Trans. Ind. Inf. 14 (1) (2018) 89–97.

[14] N.G. Bretas, S.A. Piereti, A.S. Bretas, A.C. Martins, A geometrical view for multiple gross errors detection, identification, and correction in power system state estimation, IEEE Trans. Power Syst. 28 (3) (2013) 2128–2135.

[15] N. Bretas, A. Bretas, S. Piereti, Innovation concept for measurement gross error detection and identification in power system state estimation, IET Gener. Transm. Distrib. 5 (6) (2011) 603–608.

[16] N.G. Bretas, A.S. Bretas, The extension of the gauss approach for the solution of an overdetermined set of algebraic non linear equations, IEEE Trans. Circuits Syst. II (2018).

[17] N. Bretas, A. Bretas, A.C. Martins, Convergence property of the measurement gross error correction in power system state estimation, using geometrical background, IEEE Trans. Power Syst. 28 (4) (2013) 3729–3736.

[18] A.S. Bretas, N.G. Bretas, B. Carvalho, E. Baeyens, P.P. Khargonekar, Smart grids cyber-physical security as a malicious data attack: an innovation approach, Electr. Power Syst. Res. 149 (2017) 210–219.
[19] A. Monticelli, State Estimation in Electric Power Systems: A Generalized Approach, Springer Science & Business Media, 2012.
[20] A. Abur, A. Expósito, Power System State Estimation: Theory and Implementation, Power Engineering (Willis), CRC Press, 2004. https://books.google.com/books?id=NQhbtFC6_40C
[21] A.S. Bretas, N.G. Bretas, B.E. Carvalho, Further contributions to smart grids cyber-physical security as a malicious data attack: proof and properties of the parameter error spreading out to the measurements and a relaxed correction model, Int. J. Electr. Power Energy Syst. 104 (2019) 43–51.
[22] D. Volz, U.s. government concludes cyber attack caused ukraine power outage, 2016, https://www.reuters.com/article/us-ukraine-cybersecurity/u-s-government-concludes-cyber-attack-caused-ukraine-power-outage-idUSKCN0VY30K.
[23] P. Fairley, Upgrade coming to grid cybersecurity in U.S., 2016, https://spectrum.ieee.org/energy/the-smarter-grid/upgrade-coming-to-grid-cybersecurity-in-us?bt_alias=eyj1c2vyswqioiaimmnjzjayndytmdlkos00mzliltlizmqtnzm0yze0zwjjzjlkin0%3D.
[24] K. Zetter, An unprecedented look at stuxnet, the world's first digital weapon, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.
[25] R.D. Zimmerman, C.E. Murillo-Sánchez, D. Gan, Matpower: a matlab power system simulation package, Manual, Power Systems Engineering Research Center, Ithaca NY, 1 (1997).
[26] R. Christie, Power systems test case archive, Electrical Engineering Dept., University of Washington, (2000).