Electric Power Systems Research 149 (2017) 210–219

Contents lists available at ScienceDirect

Electric Power Systems Research

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

Smart grids cyber-physical security as a malicious data attack: An innovation approach[☆]

Arturo S. Bretas[a,*], Newton G. Bretas[b], Breno Carvalho[a], Enrique Baeyens[c], Pramod P. Khargonekar[d]

[a] Department of Electrical & Computer Engineering, University of Florida, Gainesville, FL 32611-6200, USA
[b] Department of Electrical & Computer Engineering, University of Sao Paulo, Sao Carlos, SP 13566-590, Brazil
[c] Department of Systems Engineering and Automation, University of Valladolid, Valladolid 47002, Spain
[d] University of California, Irvine, CA 92697-5615, USA

ARTICLE INFO

Article history:
Received 18 January 2017
Received in revised form 5 April 2017
Accepted 17 April 2017

Keywords:
Smart grids
Cyber-physical systems security
State estimation
Innovation concept
Bad data analysis

ABSTRACT

This paper presents an analytical methodology for smart grids cyber-physical security based on gross error analysis. The presented methodology is built on the Weighted Least Square (WLS) state estimator (SE) formulation. Although cyber-physical security is a wide subject, in this paper Cyber-Attacks are modeled as bad data. Detection, identification and correction of multiple and simultaneous cyber-attacks on power grid's SCADA system, or network database, are investigated. Cyber-attack detection is made through a Chi-square (χ^2) Hypothesis Testing (HT) applied to the composed measurement error (*CME*). Composed errors are estimated with measurements' innovation index (*II*). Cyber-attack identification is made through the Largest Normalized Error Test property. Cyber-attack correction is made considering cyber-attack type and using the composed normalized error (*CNE*). One important advantage of the presented method is it does not require a previous knowledge of how the attack was performed, as far as it is restricted to a change of measurements, parameters or topology, since the error is estimated and then the bad data is corrected. A significant advantage of this correction is that it avoids potential local or global unobservable conditions, since it does not delete any measurement of the measurement set. Validation of the proposed methodology is made on the IEEE 14-bus and 57-bus systems. Simulations show the reliability and robustness of the proposed methodology even when the cyber-attack occurs simultaneously on SCADA data and network database.

Published by Elsevier B.V.

1. Introduction

The US Power Grid is one of the largest and most complex structures ever built and it is a critical infrastructure for the country. In the near future, the progressive proliferation of Smart Grid Technologies will greatly increase the capabilities and the flexibility of the Grid by increasing its connection to cyber-attack-related vulnerabilities [18].

Recently, the first confirmed blackout caused by a cyber-attack in a power grid left about 225,000 customers in Ukraine without electricity [19,18]. Even though the identities of the perpetrators of the attack remain uncertain, this event reinforces the critical interest in US Power Grid vulnerabilities and countermeasures [20,21]. It was reported that one malware which is under suspicion of having caused the aforementioned massive blackout was found in several systems that operate in US Power Grid [18,22], and just recently, a cyber-attack attempt to Burlington Electric, one of Vermont's electrical utilities [23], was discovered. Another famous case of cyber-attack on electrical utilities is the malware Stuxnet, which caused malfunction of critical equipment in Iran's Nuclear Technology Center [24]. In addition to being a subject of National Security, blackouts can have huge economic impact. The estimated cost of the 2003 Northwest blackout ranges from $4 to $10 billion U.S. dollars in the United States, and $2.3 billion Canadian dollars in Ontario [25]. Considering smart grids cyber-physical security, several researches have been published in the recent past. The paper by Liu et al. [1] is one of the first papers that modeled stealthy attack vectors in state estimation and showed that it is possible for an attacker to introduce malicious measurements in the state estimation process, as illustrated in Fig. 1. The relevant literature, as presented in [2,3], can be classified in three main topics: vulnerability analysis (weaknesses of the traditional state estimation bad data detection methods), impact analysis (consequences of an undetected malicious

[☆] This work was supported by NSF grant's ECCS-1129061, CPS-1646229 and CNS-1239274, and FAPESP grant 2015/15274-4.

[*] Corresponding author.

http://dx.doi.org/10.1016/j.epsr.2017.04.018
0378-7796/Published by Elsevier B.V.

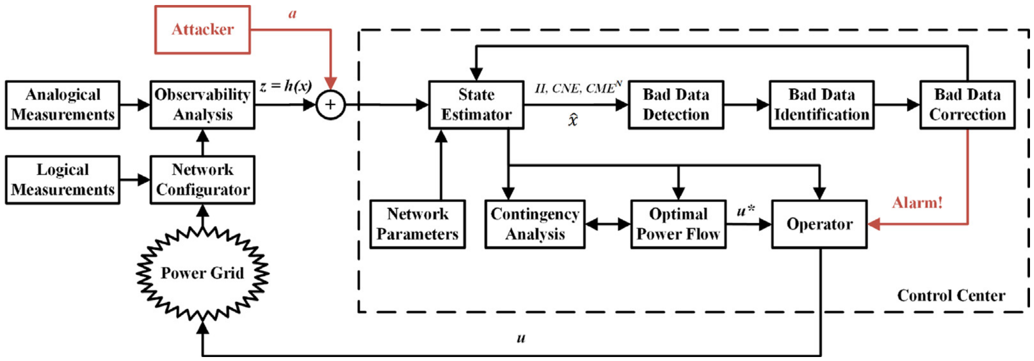

Fig. 1. State estimator under a cyber-attack.

Adapted from [4].

attack) and development of countermeasures (improvement of bad data detection methods and communication systems).

This paper presents an improved cyber-attack detection, identification and correction methodology and is intended as a contribution to the third category (development of countermeasures), so, a brief literature review will be presented. In [5], it is demonstrated that it is possible to defend against malicious data injection if a small subset of measurements can be made immune to the attacks. It is also proposed an algorithm to strategically allocate secure phasor measurement units (PMUs) at key buses in the network to defend against those attacks. This optimal PMU placement is also studied in [6]. In [7] the authors propose a security-oriented cyber-physical state estimator that utilizes information provided by systems that monitor the cyber infrastructure for abnormal activity and the output of a traditional state estimator. In [8,9], the authors propose multiple robust state estimators, such as the least trimmed squares estimator, to improve the overall cyber-security of power systems considering attacks on both the measurement vector and measurement function. In [10], the authors study the cyber-security of power systems from the perspective of the attacker, where different kind of attacks are considered, and the control center, where a generalized likelihood ratio (GLR) detector that incorporates historical data is proposed. In [11,12], a sequential detector based on the generalized likelihood ratio is proposed to detect false data injection attacks in wide-area smart grids. In that paper, a new cumulative sum type algorithm based on the GLR, for centralized and distributed cyber-attack detection, is applied for real-time system monitoring (considering, also, arbitrary load situations). An analysis on the state-of-the-art for smart grids cyber-physical security will show that these only address potential attacks on measurements and apply residual based approaches for cyber-attack detection. Still, as cited in [4], in general, a stealthy attack requires the corruption of more measurements than the targeted ones. This relates to the fact that a stealthy attack must have the attack vector “*a*” fitting the measurement model, which for the weighted linear case is equivalent to have an attack vector belonging to the subspace spanned by the columns of the Jacobian matrix of the electrical network. Cyber-attacks with such characteristics are hard to detect when applying the classical bad data approaches, where the residual is the objective function to be minimized, which may cause the cyber-attack to remain undetected [4].

This work, otherwise, presents a methodology where the objective function to be minimized is the error [13,14] and not the residual. Since the error is a random variable and consequently not correlated, any combination of measurement’s error is captured by the proposed methodology. In order to do that, it will be used the classical property, from linear algebra, which states that the error component of the linear state estimation formulation has a unique decomposition: one component that is orthogonal to the Jacobian range space and the other that belongs to that space. The first one is no more than the residual, the component considered in the classical SE. The other error component, the masked error component when the residual is the objective function to be minimized, must be estimated and then the error composed (*CME*). To estimate this masked error component, the Innovation concept for static formulations [13,14] will be used. Then the error is composed and a χ^2 Hypothesis Testing is applied to this error vector in order to detect a possible malicious data attack. To protect against this cyber-attack and to identify the measurements/parameters/topology which were maliciously changed, the Largest Normalized Error Test (LNET) theorem [14] is used. Once the measurements/parameters/topology subject to the Cyber-attack were identified and their errors’ magnitudes were estimated, they are corrected using the Composed Normalized Error (*CNE*), within a predefined reliability index. This correction step constitutes a big advantage when compared to the proposed solutions, because it does not delete any measurement avoiding possible network unobservable conditions. Cyber-attacks validation is made on the IEEE 14-bus and 57-bus systems. Case study shows methodology reliability and robustness. Comparative test results highlight the method’s precision, even when the cyber-attack vector belongs to the subspace spanned by the columns of the Jacobian matrix of the electrical network, presenting a clear contribution to the state-of-the-art of cyber-physical systems security. Test results show that the presented methodology is accurate even when of low magnitude cyber-attack vectors. Multiple and simultaneous cyber-attacks on measurements, parameters and topology are detected and identified correctly in all of the simulated cases. Corrections of identified attacks are precise, independently of the intrusion type.

The main paper contribution is to consider, for the first time, multiple and simultaneous cyber-attack presence in measurements, parameters and topology, highlighting the improved accuracy of the proposed method, while even further, allowing correction of cyber-attacks.

The remaining of this paper is organized as follows. Section 2 presents a summary of State Estimation Theory and the Innovation Concept. Section 3 presents the cyber-attacks models and the proposed methodology. Section 4 presents a case study and test results discussion. The conclusions of this work are presented on Section 5.

2. Classical state estimation theory and the innovation concept

The power system is modeled as a set of non-linear equations as described in the following [15]:

$$z = h(x) + e, \qquad (1)$$

with $z \in \mathbb{R}^m$ is the measurement vector, $x \in \mathbb{R}^N$ is the state variables vector. Also, $h : \mathbb{R}^N \to \mathbb{R}^m$, $(m > N)$ is a continuously nonlinear differentiable function, $e \in \mathbb{R}^m$ is the measurement error vector assumed having zero mean, standard deviation σ and Gaussian probability distribution and $N = 2n - 1$ is the number of unknown state variables to be estimated (n is the number of buses of the power system).

As stated in the classical state estimation bibliography, for example [15,16], the objective of the classical WLS state estimator is to find the best estimative for the N-dimensional state vector $\hat{x}$, which minimizes the cost function $J(x)$ [15]:

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

Geometrically, the $J(x)$ index is a norm in the vector space $\mathbb{R}^m$ of the measurements, induced by the inner product $\langle u, v\rangle = u^T R^{-1} v$, where R is a positive definite symmetric matrix. Let $\hat{x}$ be the solution of this minimization problem, thus, the estimated measurements vector is given by $\hat{z} = h(\hat{x})$ and the residuals vector is defined as the difference between z and $\hat{z}$, i.e., $r = z - \hat{z}$. The linearization (through expansion in Taylor series) of Eq. (1), at a certain point x^*, implies [15]:

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

where $H = \partial h/\partial x$ is the Jacobian matrix of h calculated at x^*, $\Delta z = z - h(x^*) = z - z^*$ is the correction of the measurements vector and $\Delta x = x - x^*$ is the correction of the state vector. If the system represented by (3) is observable, then, the vector space $\mathbb{R}^m$ of the measurements can be decomposed in a direct sum of two vector sub-spaces, in the following way:

$$\mathbb{R}^m = \Re(H) \oplus [\Re(H)]^{\perp}, \tag{4}$$

so, the range space of H, given by $\Re(H)$, is a N-dimensional vector sub-space that belongs to $\mathbb{R}^m$ and $\Re(H)^{\perp}$ is its orthogonal complement, i.e., if $u \in \Re(H)$, and $v \in \Re(H)^{\perp}$, then, $\langle u, v\rangle = u^T R^{-1} v = 0$.

In the formulation of the linear state estimator, represented by (3), the solution can be interpreted as the projection of the correction of the measurements vector Δz in $\Re(H)$. Let P be the linear operator that projects the vector Δz in $\Re(H)$, i.e., $\Delta\hat{z} = P\Delta z$ and let $r = \Delta z - \Delta\hat{z}$ be the residuals vector. The operator P, that minimizes the norm $J(x)$, is the one that projects Δz orthogonally in $\Re(H)$, i.e., the vector $\Delta\hat{z} = H\Delta\hat{x}$ is orthogonal to the residuals vector. More precisely:

$$\Delta\hat{z}, r = (H\Delta\hat{x})^T R^{-1} (\Delta z - H\Delta\hat{x}) = 0. \tag{5}$$

Solving this equation for $\Delta\hat{x}$, one obtains:

$$\Delta\hat{x} = (H^T R^{-1} H)^{-1} H^T R^{-1} \Delta z. \tag{6}$$

Since $\Delta\hat{z} = H\Delta\hat{x}$, the projection matrix P will be the idempotent matrix:

$$P = H(H^T R^{-1} H)^{-1} H^T R^{-1}. \tag{7}$$

Therefore, geometrically, the classical WLS state estimator can be interpreted as a projection matrix P acting on the correction of the measurements vector Δz, but *using the residual as the correction*. Another way to visualize the state estimation is seeing the geometrical position of the measurement *error* related to the Jacobian range space $\Re(H)$. Then, decomposing the measurements' vector space into a direct sum between $\Re(H)$ and $\Re(H)^{\perp}$, it is possible to decompose the measurements error vector e into two components: undetectable (e_U) component and detectable (e_D) component, in the following way:

$$e = \underbrace{Pe}_{eU} + \underbrace{(I - P)e}_{eD}. \tag{8}$$

where $e_U \in \Re(H)$ and $e_D \in \Re(H)^{\perp}$. Therefore:

$$||e||^2_{R^{-1}} = ||e_U||^2_{R^{-1}} + ||e_D||^2_{R^{-1}}. \tag{9}$$

The difference between the two previous components is that they belong to different spaces, the first pertaining to the $\Re(H)$ and the other pertaining to the $\Re(H)^{\perp}$, consequently having different properties. Two main differences between the error component and the residual will be enumerated:

(i) Degrees of freedom m and $m - n$ respectively;
(ii) The first is a random variable by hypothesis of the SE formulation, having m residuals in a space of dimension m and the second is not a random variable (m residuals in a space of dimension $m - n$).

One should be aware that e_U is undetectable, at lights of the classical WLS, because it looks only for the error component which is orthogonal to the range space of the Jacobian, that is, e_D. That statement is because the WLS state estimation objective function minimizes the distance from the measurement z to the Jacobian range space. This error component turns out to be therefore, the measurement residual. In order to estimate the error one needs also to estimate the error component e_U. With that purpose, the *innovation* of a measurement, related to the other measurements, is defined as the information it contains, and not the others measurements of the measurement set [13]. This definition suggests that the innovation is contained in the portion of the measurement that is independent of the other measurements of the system, i.e., the portion that cannot be obtained from linear combinations of rows of the Jacobian matrix. Therefore, the new information of a measurement is its part that is orthogonal to the range space of the Jacobian matrix, i.e., belonging to $\Re(H)^{\perp}$. If a measurement has an error, its component orthogonal to the range space of the Jacobian matrix will show the error through its residual, the other component, however, will have its error completely masked. Thus, the vector of masked error, in the state estimation process, is the vector belonging to the range space of the Jacobian matrix. Since the residual e_D and the other error component e_U are orthogonal to each other, it is possible to compose the measurement error vector, that is, for the ith measurement:

$$||e^i||^2 = ||e^i_U||^2 + ||e^i_D||^2. \tag{10}$$

This error vector is called *Composed Measurement Error* (*CME*). In order to find the masked error and compose the measurement's total error, it is used the *II*, as proposed by [13]:

$$II_i = \frac{||e^i_D||}{||e^i_U||} = \frac{\sqrt{1 - P_{ii}}}{\sqrt{P_{ii}}}. \tag{11}$$

A measurement with low *Innovation Index (II)* indicates that a large component of its error is not reflected in its residual as obtained by the classical WLS estimator. Consequently, even when those measurements have gross errors, their residuals will be relatively small. Knowing that vector spaces $\Re(H)$ and $\Re(H)^{\perp}$ are orthogonal to each other, then it is possible to estimate the composed error of the ith measurement. Thus, (10) becomes:

$$||e^i||^2 = \left(1 + \frac{1}{II_i^2}\right) ||e^i_D||^2. \tag{12}$$

Since e_D is the residual, (12) becomes:

$$||e^i||^2 = \left(1 + \frac{1}{II_i^2}\right) r_i^2 \Rightarrow CME_i = r_i \sqrt{1 + \frac{1}{II_i^2}}, \tag{13}$$

where r_i is the residual of the ith measurement and II_i is the innovation index of this same measurement, both known quantities once an initial state is chosen. If instead we work with the normalized residual one obtains the *Composed Normalized Error* (*CNE*), given by:

$$CNE_i = r_i^N \sqrt{1 + \frac{1}{II_i^2}}, \quad (14)$$

where r_i^N is the normalized residual of the ith measurement. Otherwise, if one normalizes the error one obtains:

$$CME_i^N = \frac{CME_i}{\sigma_i} = \frac{r_i}{\sigma_i}\sqrt{1 + \frac{1}{II_i^2}}, \quad (15)$$

where σ_i is the standard deviation of ith measurement.

3. Cyber-attacks models and proposed methodology

The methodology for cyber-attacks security is proposed for detection, identification and to defend from the malicious data attack, for that purpose correcting the attack that was made. Next, we present the methodology proposed as well as the explanation for using them:

(i) To detect the attack, a χ^2 Hypothesis Testing (HT) is applied to the random variable Composed Measurement Error in its normalized form (CME^N). As described in [17], CME^N has m degrees of freedom (choosing a probability $1-\alpha$ of false alarm and being α the significance level of the test, a number C is obtained via Chi-square distribution table for $\chi^2_{m;1-\alpha}$ such that, in the presence of cyber-attacks, $J(\hat{x}) > C$);

(ii) To identify the measurement/parameter under cyber-attack the *Largest Normalized Error Test* [13,14] is used;

(iii) The most important point on defending from the cyber-attack is the correction of the malicious changes the attacker has performed and, for that purpose, the *CNE* is used. The reasons for this choice is because the CME^N were generated from the residuals to a space of larger dimension, generating in this way noises, but the *CNEs* were generated from the residuals, however they pertain to the residuals space and, as a consequence, not generating noises in the computation.

In this work, the hypothesis testing is based on the Gaussian behavior of the error and that the consequence of the malicious data attack will cause a non-Gaussian behavior to the error, thus, a smart grid cyber-attack is modeled as a bad data (e_i) of the ith equation. The bad data can occur due to three main reasons:

(1) A cyber-attack in the ith measurement;
(2) A cyber-attack in a transmission line (TL) parameter (series or shunt), related to the ith equation;
(3) A cyber-attack in system topology (inclusion or exclusion of TLs), also related to the ith equation.

The method proposed for cyber-attack identification analyses the characteristics of a specific attack, as described in the following:

(1) A measurement cyber-attack will cause a *Hypothesis Testing Error Detection* but with a high local CME^N. Mainly the affected measurement will present a *CNE* above a chosen threshold value β (this threshold can be chosen based on a desired level of detection sensitivity). In the state estimation literature, usually β is equal to three standard deviations of the corresponding measurement, i.e., $\beta = 3$ [13];
(2) A parameter cyber-attack in the line $i-j$ will spread out the error in all the equations in which this parameter is present, so, the respective active or reactive power flow $i-j$ and $j-i$ will present errors with high magnitude values as well as the injections on the limit buses. This attack is identified analyzing the firsts larger $CME^N s$ and the corresponding *CNE*s larger than three;
(3) The system topology cyber-attack can be considered as an extreme case of a parameter cyber-attack, also spreading out the error in the transmission line's neighborhood. In this case, however, considering that an exclusion topological error occurred, i.e., the operating line $i-j$ was configured as being offline, the respective active or reactive power flow $i-j$ and $j-i$ will not appear, since the line was excluded. On the other hand, the i and j power injections will present very high CME^N values (above 15 standard deviations, observed in the simulations), due the power unbalance generated by the exclusion of the transmission line.

Based on these cyber-attack characteristics, it is proposed an approach to detect, identify and correct malicious data attacks in measurements, line parameters and topology. In the proposed methodology, the cyber-attacks are processed iteratively. Initially, according to the χ^2 HT values, a cyber-attack is detected. Cyber-attack identification is made by analyzing the characteristics of a specific attack. Once identified the cyber-attack type, correction is made using measurement's CNE_i. The proposed method's algorithm is presented in the following:

(1) Read the input data. For a given measurements set and network configuration, perform the WLS state estimation;
(2) Compute the estimated state vector ($\hat{x}$), the normalized residual vector (r^N), the projection matrix (P), the innovation index vector (II) and the composed measurement error (CME^N) vector;
(3) Perform the gross error detection test, not using the r^N, but the CME^N instead. Then, build a descending list of measurements, according to their corresponding CME^N values;
(4) Based on the list of *Step 3*, verify if there are power injection measurements i and j with very high CME^N values (beyond 10 standard deviations) and no measurements $i-j$ and $j-i$ (active or reactive power flows) in the list. If this situation occurs, then the branch $i-j$ is suspicious of being under cyber-attack, i.e., a topological cyber-attack has occurred. Then, correct the system's topology. Return to *Step 1*. If this situation does not occur again, proceed to *Step 5*;
(5) Based on the list of *Step 3*, verify if there are measurements $i-j$ and $j-i$ (active or reactive power flows) and measurements i and j (active or reactive power injections) with CME^N above the threshold value in the list. If this situation occurs, then the branch $i-j$ is suspicious of having a cyber-attack. Then, perform the parameter correction using the CNE_i (related to the measurement with the largest CME^N), i.e., for series and shunt parameters, the correction is given by:

$$p_i^C = \frac{p_i^E}{1 + \frac{CNE_i}{100}}, \quad (16)$$

where p_i^C is the corrected parameter value and p_i^E is the erroneous parameter value. Return to *Step 1*. If this situation does not occur, proceed to *Step 6*;

Obs.: one should be aware that the correction component (16) is obtained making a Taylor series expansion of z_i around the operating point obtained using the erroneous parameter value and the correspondent *CNE*.

(6) Based on the list of *Step 3*, verify if there is an isolated measurement with the CME^N above the threshold value in the list. If this situation occurs, the error was caused by a measurement cyber-attack, then, perform the correction routine, by applying the following equation:

$$z_i^C = z_i^E - CNE_i\sigma_i, \tag{17}$$

where z_i^C is the corrected measurement value and z_i^E is the erroneous measurements value. Return to *Step 1*. If this situation does not occur, proceed to *Step 7*;

(7) End of the cyber-attack processing routine.

The implemented software reads automatically the database in *.txt* format, inserting a random noise to the measurements vector according to the user choice. To add measurement noise, a routine was developed so the standard deviation of each measurement is multiplied by a constant randomly generated. Thus, one can add to the measurements "*k*noise*" standard deviations. The "*noise*" variable has standard normal distribution with zero mean and unitary variance and the constant *k* is an integer defined by the user, so the measurements may vary up to *k* standard deviations, i.e., $\pm k\sigma_i$. Thus, the new value of the measurement is given by:

$$z_i^{noise} = z_i + k * noise * \sigma_i. \tag{18}$$

To generate the measurements, it was considered that all measurements have standard deviations calculated by:

$$\sigma_i = \frac{pr\left|z_i^{lf}\right|}{3}, \tag{19}$$

where *pr* is the meter's precision (considered 3% in the simulations) and z_i^{lf} is the value of the *i*th measurement obtained from a load flow solution, which is also used to build the measurements database. State-of-the-art methodologies consider, for each measurement type, a specific standard deviation value. In this work, since all the measurements are assumed possible of containing error, the measurement's standard deviation σ is assumed as a percentage (1%) of each measurement magnitude. In case of virtual measurements, or even measurements of low magnitudes, e.g., a no-generation and no-demand bus (with zero active and reactive power injections), a routine was developed. This routine identifies the null and near zero measurements and, then, associates a low, but non-zero, standard deviation for those measurements, so the weight matrix will not present numerical problems. Fig. 2 illustrates the flowchart of the proposed methodology.

4. Case study

The validation of the proposed methodology is done using the IEEE 14-bus and 57-bus systems. The measurement plan used for the 14-bus system consists of 81 measurements, leading to a global redundancy level *GRL* = 3, and for the IEEE 57-bus test system the measurement plan consists of 339 measurements, leading to *GRL* = 3. Systems' topologies and parameters can be found in [15].

In the following, three representative cyber-attack scenarios are analyzed:

(i) Attack Scenario I: Multiple measurements cyber-attacks in the IEEE 14-bus test system ($C = \chi^2_{81;0.95} = 103.01$)

(1) Cyber-attack of magnitude 9σ, added to measurement Q:08-07 = 0.1762 pu (reactive power flow from bus 8 to bus 7);

(2) Cyber-attack of magnitude 5σ, added to measurement P:01-02 = 1.5689 pu (active power flow from bus 1 to bus 2);

Cyber-attack of magnitude 4σ, added to measurement P:03 = −0.9420 pu (active power injection at bus 3).

The steps of the cyber-attack processing are described in Table 1, where the measurements cyber-attacks are corrected iteratively and the new estimation is performed after each correction.

Table 1
IEEE-14: processing of multiple measurement cyber-attacks.

Processing multiple measurement cyber-attacks	
Original measurements (pu)	Measurements with cyber-attack (pu)
Q:08-07 = 0.1762 P:01-02 = 1.5689 P:03 = −0.9420	(Q:08-07) + 9σ = 0.1963 (P:01-02) + 5σ = 1.6589 (P:03) + 4σ = −0.9021
Processing measurement cyber-attack step 1	
$J(\hat{x}) = 159.85 > C = \chi^2_{81;0.95} = 103.01 \Rightarrow$ **Attack Detected!**	
Meas. with $\left\|CME^N\right\| \geq 3.0$	CME^N
Q:08-07 = 0.1962	9.3760
Corrected measurement: *Q:08-07 – CNE*σ = 0.1760 pu* (approximation error = 0.1135%)	
Processing measurement cyber-attack step 2	
$J(\hat{x}) = 138.08 > C = \chi^2_{81;0.95} = 103.01 \Rightarrow$ **Attack Detected!**	
Meas. with $\left\|CME^N\right\| \geq 3.0$	CME^N
P:01-02 = 1.6466	4.7656
Corrected measurement: *P:01-02 – CNE*σ = 1.5663 pu* (approximation error = 0.1657%)	
Processing measurement cyber-attack step 3	
$J(\hat{x}) = 123.07 > C = \chi^2_{81;0.95} = 103.01 \Rightarrow$ **Attack Detected!**	
Meas. with $\left\|CME^N\right\| \geq 3.0$	CME^N
P:03 = -0.9033	3.9560
Corrected measurement: *P:03 – CNE*σ = -0.9418 pu* (approximation error = 0.0212%)	
Processing measurement cyber-attack step 4	
$J(\hat{x}) = 42.50 < C = \chi^2_{81;0.95} = 103.01 \Rightarrow$ **No Attack Detected!**	

The first process of the presented method is the cyber-attack detection. At *Step 1*, as one can see, the value for the "cost function" ($J(\hat{x}) = 159.85$) is greater than the *C* value for this measurement scenario ($\chi^2_{81;0.95} = 103.01$), therefore, the attack is successfully detected. After the detection, the attack is identified by analyzing the largest CME^N above the threshold value (β = 3), which turns out to be measurement *Q:08-07*. Since it was not found any other adjacent measurement with the CME^N above the threshold β for error detection, a measurement cyber-attack is identified. Then, the measurement value is corrected with its *CNE*, by applying Eq. (17). Note that the approximation error, i.e., the difference between the measurement's correct database value and the measurement's value corrected by the its *CNE* is very small (0.1135%), which means that the recovery of the original value is very accurate. After the correction, a new state estimation is performed.

At *Step 2*, another attack is detected, since the $J(\hat{x}) = 138.08$ is still greater than C ($\chi^2_{81;0.95} = 103.01$). After the detection, the attacked measurement was identified as being *P:01-02*, since it has the largest CME^N above the threshold value β. Then, the measurement value is corrected with its *CNE* (approximation error 0.1657%) and a new state estimation is performed.

At *Step 3*, the last attack is detected, since the $J(\hat{x}) = 123.07$ is greater than C ($\chi^2_{81;0.95} = 103.01$). Then, the attacked measurement was identified as being *P:03*, since it has the largest CME^N above the threshold value β. After, the measurement value is corrected with its *CNE* (approximation error 0.0212%) and another state estimation is performed.

At *Step 4*, there is no attack detection, since the $J(\hat{x}) = 42.50$ is smaller than C ($\chi^2_{81;0.95} = 103.01$). Finally, with no attacks detected, the presented method ends and the state variables can be correctly estimated.

Considering the IEEE 14-bus test system and its set of measurements, several simulations using the presented methodology and the established largest normalized residual test for malicious data attack detection were performed. Still,

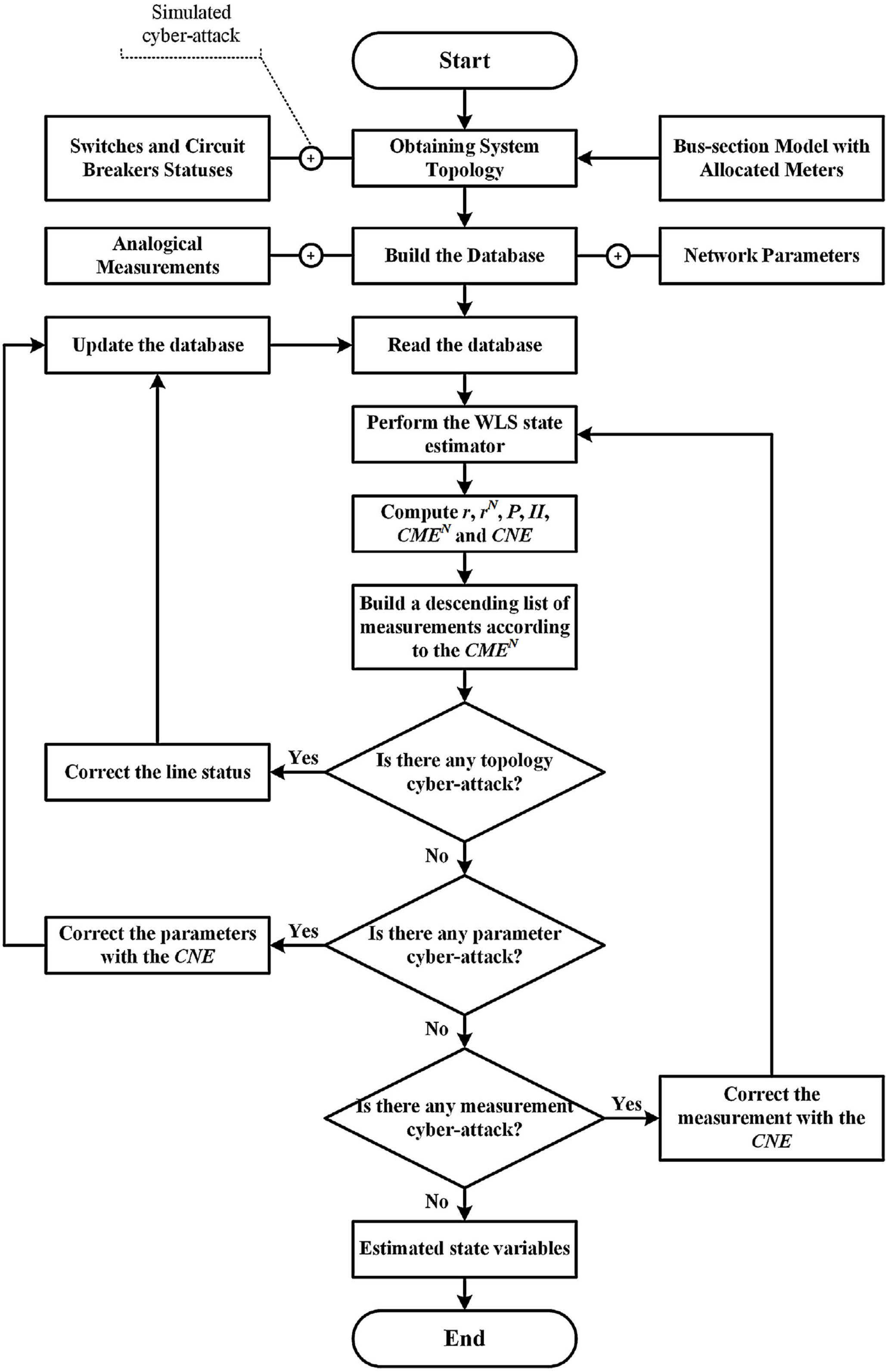
Simulated cyber-attack
Start
Switches and Circuit Breakers Statuses
Obtaining System Topology
Bus-section Model with Allocated Meters
Analogical Measurements
Build the Database
Network Parameters
Update the database
Read the database
Perform the WLS state estimator
Compute r, r^N, P, II, CME^N and CNE
Build a descending list of measurements according to the CME^N
Correct the line status
Yes
Is there any topology cyber-attack?
No
Correct the parameters with the CNE
Yes
Is there any parameter cyber-attack?
No
Is there any measurement cyber-attack?
Yes
Correct the measurement with the CNE
No
Estimated state variables
End

Fig. 2. Flowchart of the proposed methodology.

for all simulations, a random noise was added to the set of measurements (the noise was defined in such a way that the measurements vary up to $\pm 2\sigma_i$ from their original values).

To compare the performance of both approaches, with regard to single measurement cyber-attacks, a list of "*problematic*" measurements was created. "*Problematic*" measurements are defined as measurements with *low Innovation Index* (with magnitude values near or lower than 1) that, in case of gross errors, are hard to detect and identify correctly by the largest normalized residual test. For the IEEE 14-bus

Table 2
IEEE-14: measurements with low *II*.

Active		Reactive	
Measurement	II	Measurement	II
Power flow measurements			
P:09-10	1.1946	Q:2-3	0.9103
P:12-13	1.1361	Q:2-5	1.0179
P:10-09	1.1957	Q:5-1	0.8948
P:13-12	1.1401	Q:3-2	0.7137
Power injection measurements			
P:02	0.2999	Q:04	0.4713
P:05	0.1741	Q:05	0.2254
P:06	0.7729	Q:07	0.8958
P:07	0.4137	Q:11	0.7683
P:11	0.6727	Q:12	0.4981

system, the "*problematic*" measurements are listed in Table 2, considering the complete measurement plan composed by 122 measurements provided by [18].

For the first comparative test, a cyber-attack on the measurement with the lowest *II* was simulated, i.e., the active power injection at bus 5 (cyber-attack of -4σ in *P:05*). When applying the largest normalized residual test it failed for this and all other comparative test simulations. In these simulations, the absolute value for the r^N varied between 1.5125 (lowest of all) to 2.0472 (largest of all), but never exceeding the threshold value for gross error detection ($\beta = 3$). Thus, one can conclude that the largest normalized residual test fails to detect gross errors on measurements with low *II*.

On the other hand, when using the presented methodology, the procedure correctly detected, identified and corrected the measurements with cyber-attacks in all simulations. Table 3 shows the results of one simulation.

For the second comparative test, multiple and simultaneous measurement cyber-attacks were simulated: -6σ in *P:12-13*, -8σ in *Q:04* and 7σ in *Q:05-01*. In this case, the normalized residual test presented similar results to the single measurement cyber-attacks. The established largest normalized residual test correctly detected and identified the measurements cyber-attacks in *P:12-13* and *Q:05-01*, but failed to detect the third measurement cyber-attack, *Q:04*, due its low *II*.

Results for such cyber-attack case are presented in Table 4.

Otherwise, when applying the presented methodology, the three measurements cyber-attacks were correctly detected, identified and corrected. Test results for such case are presented in Table 5.

Table 3
IEEE-14: processing single measurement cyber-attack.

Single measurement cyber-attack processing			
Original measurement		Measurement with cyber-attack	
P:05 = –0.0757		(P:05) – 4σ = –0.0788	
Processing measurement cyber-attack step 1			
$J(\hat{x}) = 147.47 > C = \chi^2_{81;0.95} = 103.01 \Rightarrow$ Attack Detected!			
Meas. with $\lvert CME^N \rvert \geq 3.0$	*II*	CME^N	*CNE*
P:05 = –0.0789	0.2004	–3.5790	–3.9032
Corrected measurement: P:*05 – CNE*σ = -0.0758 pu* (approximation error = 0.1321%)			
Processing measurement cyber-attack step 2			
$J(\hat{x}) = 35.80 < C = \chi^2_{81;0.95} = 103.01 \Rightarrow$ No Attack Detected!			

Table 4
IEEE-14: processing multiple measurement cyber-attacks with the classical largest normalized residual test [16].

Step	Measurement under cyber-attacks	r^N
1	P:12-13	4.5068
2	Q:05-01	3.8392
3	No cyber-attacks detected	

Table 5
IEEE-14: processing multiple measurement cyber-attacks with proposed analytical methodology.

Multiple measurement cyber-attacks processing			
Original measurement		Measurement under cyber-attacks	
P:12-13 = 0.0161		(P:12-13) – 6σ = 0.0151	
Q:04 = 0.0389		(Q:04) – 8σ = 0.0358	
Q:05-01 = 0.0221		(Q:05-01) + 7σ = 0.0237	
Processing measurement cyber-attack step 1			
$J(\hat{x}) = 330.59 > C = \chi^2_{81;0.95} = 103.01 \Rightarrow$ Attack Detected!			
Meas. with $\lvert CME^N \rvert \geq 3.0$	*II*	CME^N	*CNE*
Q:05-01 = 0.0237	0.9594	5.2774	7.8230
Corrected Measurement: *Q:05-01 – CNE*σ = 0.0217 pu* (approximation error = 1.4018%)			
Processing measurement cyber-attack step 2			
$J(\hat{x}) = 270.62 > C = \chi^2_{81;0.95} = 103.01 \Rightarrow$ Attack Detected!			
Meas. with $\lvert CME^N \rvert \geq 3.0$	*II*	CME^N	*CNE*
P:12-13 = 0.0152	1.0681	–4.3150	–5.9110
Corrected measurement: *P:12-13 – CNE*σ = 0.0162 pu* (approximation error = 0.6211%)			
Processing measurement cyber-attack step 3			
$J(\hat{x}) = 173.73 > C = \chi^2_{81;0.95} = 103.01 \Rightarrow$ Attack Detected!			
Meas. with $\lvert CME^N \rvert \geq 3.0$	*II*	CME^N	*CNE*
Q:04 = 0.0359	0.4323	–3.3983	–8.5640
Corrected measurement: *Q:04 – CNE*σ = 0.0390 pu* (approximation error = 0.2571%)			
Processing Measurement Cyber-attack Step 4			
$J(\hat{x}) = 54.36 < C = \chi^2_{81;0.95} = 103.01 \Rightarrow$ No Attack Detected!			

In this attack scenario, one can notice the analytical methodology's efficiency for processing multiple and simultaneous measurement cyber-attacks. The errors between the measurement values corrected by the method and the correct values presented very small approximation errors.

In the following, a simultaneous attack scenario on measurements and network parameters is presented.

(ii) Attack Scenario II: Simultaneous Measurement and Parameter Cyber-attacks in the IEEE 14-bus test system ($C = \chi^2_{81;0.95} = 103.01$)

(3) Cyber-attack of magnitude -6σ added to measurement P:04-09 = 0.1609 pu (active flow from bus 4 to bus 9);

(4) Cyber-attack of 6% added to the 06-12 line parameters.

The presented method initially detects the first attack since the "cost function" ($J(\hat{x}) = 158.62$) is greater than the C value for this measurement scenario ($\chi^2_{81;0.95} = 103.01$). Once the attack is detected, the CME^N descending list is built and the largest CME^N was identified in the measurement *P:04-09*. Since it was not found any other adjacent measurement with the CME^N above the threshold β for error detection, a measurement cyber-attack is identified (as explained at the algorithm's *Step 6*). Then, this measurement was corrected by its corresponding *CNE* = –6.2053, obtaining a corrected value *P:04-09* = 0.1602 (approximation error 0.4351%). This process is summarized in Table 6. After the measurement correction, a new state estimation was performed.

After the new estimation is performed, the χ^2 test was applied to the error and, again, an attack was detected, since $J(\hat{x}) > C$. However, by analyzing the CME^N descending list, one may notice that several measurements of the line *06–12*

Table 6
IEEE-14: processing cyber-attacks, first step.

Processing measurement cyber-attack step 1			
$J(\hat{x}) = 158.62 > C = \chi^2_{81;0.95} = 103.01 \Rightarrow$ Attack Detected!			
CME^N descending list			
Measurement	*II*	CME^N	*CNE*
P:04-09	2.9654	−5.8800	−6.2053
Q:12	0.4989	−5.8059	−13.0046
P:12-06	2.0719	4.7710	5.2976
Q:12-06	1.9688	4.0204	4.5093
Q:06-12	2.0766	−3.9147	−4.3450
Q:13	0.9701	−3.0646	−4.4012
Meas. with $\lvert CME^N \rvert \geq 3$	*II*	CME^N	*CNE*
P:04-09 = 0.1509	2.9654	−5.8800	−6.2053
Corrected measurement: P:04-09 – *CNE***σ* = 0.1602 (approximation error = 0.4351%)			

Table 7
IEEE-14: processing cyber-attacks, second step.

Processing measurement cyber-attack step 2			
$J(\hat{x}) = 121.97 > C = \chi^2_{81;0.95} = 103.01 \Rightarrow$ Attack Detected!			
CME^N descending list			
Measurement	*II*	CME^N	*CNE*
P:12-06	2.0691	5.4585	6.0626
Q:12	0.4989	−5.0717	−11.3601
Q:12-06	1.9688	4.2039	4.7151
Q:06-12	2.0765	−2.7853	−3.0915
Q:13	0.9701	−2.6720	−3.8375
P:13-12	1.0450	1.9677	2.7235

presented CME^Ns above the threshold β, as presented in Table 7. As explained in the *Step 5* of the algorithm, this situation characterizes a parameter cyber-attack. Then, the parameters of this line were corrected using the *CNE* = 6.0626 (corresponding to the measurement with the largest CME^N) applied to Eq. (16). The parameters' corrections are shown in Table 8, and have very small approximation errors, demonstrating the efficiency of the parameter correction method. After the correction of the parameters of the line *06–12* and a new estimation, no cyber-attack was detected ($J(\hat{x}) = 64.79 < 103.01$).

In the following, a single transmission line parameter cyber-attack test case is presented. Comparative test results with the established largest normalized residual test for parameter error processing are also investigated. Considering the IEEE 14-bus test system and its set of measurements, a −10% cyber-attack was added to the series and shunt parameters of the TL *01-05*. When applying the residual method, the list of suspicious measurements obtained is presented in Table 9.

Following this r^N descending list, the largest normalized residual test would assign the measurement Q:06 as under a cyber-attack, which is not the case. When applying the proposed methodology, the list of suspicious measurements is presented in Table 10 and the software corrections are presented in Table 11. In this case, the proposed methodology would correctly detect, identify and correct the parameter cyber-attack. Still, as one can see, after the parameters correction, no cyber-attack was detected ($J(\hat{x}) = 44.23 < 103.01$).

Table 8
IEEE-14: corrected parameters.

Parameters correction				
Parameter	Database value	Erroneous value	Corrected value	Approximation error
g_{06-12}	1.5260	1.6175	1.5250	0.0655%
b_{06-12}	−3.1760	−3.3665	−3.1741	0.0598%
b^{shunt}_{06-12}	0.0000	0.0000	0.0000	0.0000%

Table 9
IEEE-14: processing errors with normalized residual test.

r^N Descending list	
Measurement	r^N
Q:06	8.0702
P:05-01	−6.1616
P:01-05	6.1059
P:02-05	−5.3493
P:05-02	5.2887
Q:05-01	4.9895

Table 10
IEEE-14: processing errors with the proposed method.

Processing measurement cyber-attack step 1			
$J(\hat{x}) = 562.99 > C = \chi^2_{81;0.95} = 103.01 \Rightarrow$ Attack Detected!			
CME^N descending list			
Measurement	*II*	CME^N	*CNE*
P:05-01	7.2836	−9.2346	−9.3212
P:01-05	7.2267	9.2052	9.2929
Q:01-05	1.4835	8.8972	10.7297
Q:05-01	0.9848	8.6642	12.3483
P:02	0.2932	8.3714	29.7577
P:05	0.1708	8.0859	48.0152

Table 11
IEEE-14: corrected parameters.

Parameters correction				
Parameter	Database value	Erroneous value	Corrected value	Approximation error
g_{01-05}	1.0259	0.9233	1.0182	0.7506%
b_{01-05}	−4.2350	−3.8115	−4.2033	0.7485%
b^{shunt}_{01-05}	0.0246	0.0221	0.0244	0.8130%

In this attack scenario, the methodology proved to be successful to process parameter cyber-attacks as well as when of simultaneous measurement attacks. After the parameter value correction, the approximation errors are also very small. Still, the comparative test showed the proposed method's efficiency in a case where the established largest normalized residual test failed to process a parameter cyber-attack. In the following, *Scenario III*, the methodology is tested on a different test system for processing simultaneous measurement, parameter and topology cyber-attacks.

(iii) Attack Scenario III: Simultaneous measurement, parameter and topological Cyber-attacks in the IEEE 57-bus test system ($C = \chi^2_{339;0.95} = 535.23$)
   (5) Measurement cyber-attack of magnitude -6σ added to Q:50 = −0.1059 pu (reactive power injection at bus 50);
   (6) Parameter cyber-attack of 6% added to the parameters of the line 41–42;
   (7) Topology cyber-attack at line 19–20, setting the operational line status as offline.

On step 1 the presented analytical methodology detects the cyber-attack since the "cost function" ($J(\hat{x}) = 4414.8$) is greater than the *C* value for this measurement scenario ($\chi^2_{339;0.95} = 535.23$). Initially, the topological cyber-attack was identified, as it presents the characteristics described in the *Step 4* of the algorithm, such as very high values for the CME^N in the power injection

Table 12
IEEE-57: processing cyber-attacks, first step.

Processing measurement cyber-attack step 1			
$J(\hat{x}) = 4414.8 > C = \chi^2_{339;0.95} = 535.23 \Rightarrow$ Attack Detected!			
CME^N descending list			
Measurement	*II*	CME^N	*CNE*
P:20	2.9705	−49.3456	−52.0667
P:19	1.0596	26.0095	35.7626
P:21-20	1.1135	−15.3537	−20.6363
P:18-19	1.6759	14.5674	16.9638
P:20-21	1.1135	14.5040	19.4942
P:19-18	1.7107	−14.4779	−16.7701

Table 13
IEEE-57: processing cyber-attacks, second step.

Processing measurement cyber-attack step 1			
$J(\hat{x}) = 1227.8 > C = \chi^2_{339;0.95} = 535.23 \Rightarrow$ Attack Detected!			
CME^N descending list			
Measurement	*II*	CME^N	*CNE*
Q:50	2.5606	−8.6905	−9.3297
P:42-41	2.9901	5.1040	5.3819
P:41-42	2.9355	−4.8095	−5.0810
Q:41-42	2.0209	−4.6181	−5.1526
Q:41	0.8001	4.1885	6.7043
Q:42-41	1.8409	3.1513	3.5863
Meas. with $\left\|CME^N\right\| \geq 3$	*II*	CME^N	*CNE*
Q:50 = −0.1166	2.5606	−8.6905	−9.3297
Corrected measurement: Q:50 – *CNE**σ = −0.1057 (approximation error = 0.1888%)			

Table 14
IEEE-57: processing cyber-attacks, third step.

Processing measurement cyber-attack step 1			
$J(\hat{x}) = 1149.5 > C = \chi^2_{339;0.95} = 535.23 \Rightarrow$ Attack Detected!			
CME^N descending list			
Measurement	*II*	CME^N	*CNE*
P:41-42	3.2685	6.0375	6.3138
Q:41-42	2.2076	4.2419	4.6568
P:42-41	3.3315	−4.2251	−4.4113
Q:41	0.7669	−3.8609	−6.3444
Q42-41	2.0208	−3.8529	−4.2988

Table 15
IEEE-57: corrected parameters.

Parameters correction				
Parameter	Database value	Erroneous value	Corrected value	Approximation error
g_{41-42}	1.2414	1.3158	1.2327	0.7008%
b_{41-42}	−2.1109	−2.2376	−2.0963	0.6916%
b^{shunt}_{41-42}	0.0000	0.0000	0.0000	0.0000%

After correcting the parameters of the line *41–42* and a new estimation, no cyber-attack was detected ($J(\hat{x}) = 75.40 < 535.23$).

measurements in the limit buses of the affected area and the absence of measurements incident to the specific line in the CME^N descending list, i.e., power flows from bus 19 to 20 and vice versa. This last characteristic helps to distinguish between a topological error and a parameter error, since the latter will spread the error to the measurements incident to the affected line. Analyzing Table 12, one can verify that the power injections of the limit buses (19 and 20) present very high CME^N and, since there are no measurements incident to the line *19–20*, a topological cyber-attack is identified. Then, this topological error was corrected, i.e., the status of the line *19–20* was set as online and a new estimation was performed.

In the second step, another cyber-attack was detected, since $J(\hat{x}) > C$. In this case, by analyzing the CME^N descending list in Table 13, one can notice that the measurement *Q:50* presented the largest CME^N and no other adjacent measurements presented a CME^N above the threshold value β, which characterizes a measurement cyber-attack.

After the measurement correction, a new estimation was performed and another cyber-attack was detected ($J(\hat{x}) > C$). By analyzing the CME^N descending list in Table 14, several measurements of the line *41–42* presented CME^Ns above the threshold β, which characterizes a parameter cyber-attack, as explained in the *Step 5* of the algorithm. After the cyber-attack identification, the parameters of this line were corrected using the *CNE* = 6.3138 (related to the measurement with the largest CME^N) and Eq. (16). The corrected parameters are shown in Table 15 and, again, presented very small approximation errors from the correct database values.

5. Discussion

The findings of this study clearly show that successful countermeasures can be implemented to mitigate the consequences of malicious data attacks in smart grids. The presented methodology was efficient in different attack scenarios where the established largest normalized residual test failed. An explanation for this is that the residual is not always a good estimate for the error caused by a cyber-attack, since the error can be masked depending on the position of the affected measurement to the image of the Jacobian [13].

The results further show that the presented method was successful in all simulated scenarios, correcting the attacked measurements, parameters and topology while obtaining very small approximation errors. Comparative test results with the established largest normalized residual test also highlight the presented method's improved accuracy. For example, in the *Attack Scenario I*, considering the list of problematic measurements, the residual test failed in 100% of the simulations performed. On the other hand, the proposed method was successful in 100% of the simulations realized.

6. Conclusion

This paper has presented an analytical methodology for smart grids cyber-physical security. The presented method is able to detect, identify and correct malicious data attacks in smart grids. The presented method is built on the classical WLS state estimation, associated with an innovation approach for processing malicious data attacks. The methodology considers, during equation derivation, potential cyber-attacks on measurements, parameters and topology. Malicious data attacks are modeled as bad data. The detection, identification and correction of the attacks are performed with new indexes proposed, instead of the established largest normalized residual. Simultaneous cyber-attacks are considered, even malicious data attacks on measurements that belong to the image of the Jacobian. Test results, considering multiple and simultaneous cyber-attacks highlight the improved accuracy of the proposed method, while further allowing correction of the attacks, presenting a clear contribution to the state-of-the-art. Another important advantage of the method is it does not require a previous knowledge of how the attack was performed, as far as it is restricted to a change of measurements, parameters or topology, since the error is estimated and then the affected quantity is corrected. The error correction allows a significant advantage of not creating any unobservable condition, since no measurement of the measurement set is deleted. Comparative tests have been realized, demonstrating the increased accuracy of the proposed method in cases where the established method had failed.

References

[1] Y. Liu, M.K. Reiter, P. Ning, False data injection attacks against state estimation in electric power grids, in: Proc. 16th ACM Conference on Computer and Communications Security, 2009.

[2] G. Hug, J.A. Giampapa, Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks, IEEE Trans. Smart Grid 3 (September (3)) (2012) 1362–1370.

[3] A. Ashok, M. Govindarasu, V. Ajjarapu, Online detection of stealthy false data injection attacks in power system state estimation, IEEE Trans. Smart Grid PP (99) (2016) 1–11.

[4] A. Teixeira, S. Amin, H. Sandberg, K.H. Johansson, S.S. Sastry, Cyber security analysis of state estimators in electric power systems, in: Proc. 49th IEEE Conf. Decision Control, 2010, pp. 5991–5998.

[5] T. Kim, H. Poor, Strategic protection against data injection attacks on power grids, IEEE Trans. Smart Grid 2 (June (2)) (2011) 326–333.

[6] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, K. Poolla, Smart grid data integrity attacks, IEEE Trans. Smart Grid 4 (September (3)) (2013) 1244–1253.

[7] S. Zonouz, K.M. Rogers, R. Berthier, R.B. Bobba, W.H. Sanders, T.J. Overbye, SCPSE: security-oriented cyber-physical state estimation for power grid critical infrastructures, IEEE Trans. Smart Grid 3 (December (4)) (2012) 1790–1799.

[8] Y. Chakhchoukh, H. Ishii, Coordinated cyber-attacks on the measurement function in hybrid state estimation, IEEE Trans. Power Syst. 30 (September (5)) (2015) 2487–2497.

[9] Y. Chakhchoukh, H. Ishii, Enhancing robustness to cyber-attacks in power systems through multiple least trimmed squares state estimations, IEEE Trans. Power Syst. PP (99) (2016) 1–11.

[10] O. Kosut, L. Jia, R. Thomas, L. Tong, Malicious data attacks on the smart grid, IEEE Trans. Smart Grid 2 (December (4)) (2011) 645–658.

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

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

[13] 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 (February (3)) (2013) 2128–2135.

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

[15] A. Monticelli, State Estimation in Electric Power Systems: A Generalized Approach, Massachusetts, USA, Kluwer Academic Publishers, 1999.

[16] N.G. Bretas, A.S. Bretas, A two steps procedure in state estimation gross error detection, identification, and correction, Int. J. Electr. Power Energy Syst. 73 (December) (2015) 484–490.

[17] R. Christie, "Power Systems Test Case Archive," Available on: https://www.ee.washington.edu/research/pstca/.

[18] P. Fairley, Upgrade Coming to Grid Cybersecurity in U.S., IEEE Spectr.: Technol. Eng. Sci. News (2016), Available on: http://spectrum.ieee.org/energy/the-smarter-grid/upgrade-coming-to-grid-cybersecurity-in-us?bt_alias=eyj1c2vyswqioiaimmnjzjayndytmdlkos00mzliltlizmqtnzm0yze0zwjjzjlkin0=.

[19] D. Volz, U.S. Government Concludes Cyber-Attack Caused Ukraine Power Outage, Reuters, 2016, Available on: http://www.reuters.com/article/us-ukraine-cybersecurity-iduskcn0vy30k.

[20] S. Morgan, Major Cyber Attack On U.S. Power Grid Is Likely, Forbes, 2016, Available on: http://www.forbes.com/sites/stevemorgan/2016/02/07/campaign-2016-major-cyber-attack-on-u-s-power-grid-is-likely/#131b743a610f.

[21] E. Perez, U.S. Investigators Find Proof of Cyberattack on Ukraine Power Grid, CNN, 2016, Available on: http://www.cnn.com/2016/02/03/politics/cyberattack-ukraine-power-grid/.

[22] Industrial Control Systems Cyber Emergency Response Team, Alert (IR-ALERT-H-16-056-01), in: Cyber-Attack Against Ukrainian Critical Infrastructure, 2016, Available on: https://ics-cert.us-cert.gov/alerts/ir-alert-h-16-056-01.

[23] http://www.usatoday.com/story/tech/news/2016/12/30/report-russia-penetrated-us-electrical-grid/96022986/.

[24] K. Zetter, An Unprecedented Look at Stuxnet, the World's First Digital Weapon. *Wired.com*, 2014, Available on: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[25] U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, 2004.