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

Arturo S. Bretas, Newton G. Bretas, Breno E. B. Carvalho

***Abstract*— This paper presents further contributions to smart grids cyber-physical security as a malicious data attack. The contributions are twofold. First, a formal proof of how parameter errors spread out on the measurement function having a parameter with error. The largest composed measurement error property, in its normalized form, is then demonstrated for this case of error. Second, a methodology for smart grid cyber-physical malicious data injection correction is presented. Current state of the art solutions corrects simultaneous attacks assuming measurements or parameters without error. However, how may one correct a measurement if the parameter might be simultaneously in error or the other way around? In this paper, a relaxed model strategy for such is presented. Attacks are processed simultaneously and analyzed using only the framework of measurement gross error analysis. Cyber-attack detection is made through a Chi-square (χ^2) Hypothesis Testing (*HT*) applied to the normalized composed measurement error (*CME*^{N}). 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*) in a relaxed model strategy. The proposed solution works for malicious measurement and parameter data attacks. Still, the state estimation software does not need major changes. Validation is made on the IEEE 14-bus and 57-bus systems.**

***Index Terms*—Smart grid, cyber-physical security, malicious data injection, weighted least squares, innovation**

I. Introduction

POWER system state estimation (PSSE) is the process of estimating unknown state variables in a power grid based on the network's data (system topology and transmission lines parameters) and meter's remote measurements. Both network data and measurements are subject to noises and/or interferences. The output of state estimation, the state variables (buses complex voltages), is used in the contingency analysis, which will then be used to control the power grid components to maintain the reliable operation of the grid, even if some faults may occur.

However, due to the constant modernization of the power system with the installation of new electrical devices and structures, the research on power system vulnerabilities to cyber-attacks is crucial to keep the grid operation secure. Considering smart grids cyber-physical security, 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 Figure 1. The relevant literature, as presented in [2], [3] and [4], 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 attack) and development of countermeasures (improvement of bad data detection methods and communication systems).

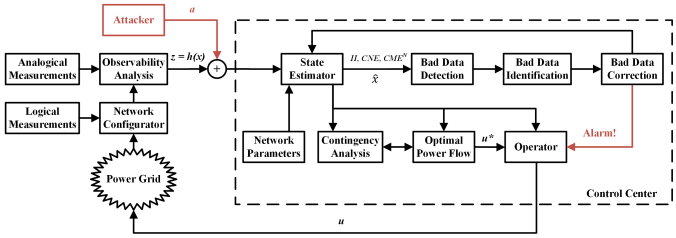

Figure 1. State estimator under a cyber-attack (adapted from [21]).

This work is intended as a contribution to the third category (development of countermeasures). The objective of this work is to implement methodologies to detect malicious data attacks and protect the power grid, by improving bad data detection schemes. In the following, a brief literature review on this subject will be presented.

In [5], it is demonstrated that it is possible to defend against

This work was supported by NSF grant CPS-1646229 and FAPESP grant 2015/15274-4.

A. S. Bretas is with the Department of Electrical & Computer Engineering, University of Florida, Gainesville, FL 32611-6200 USA.

N. G. Bretas and B. E. B. Carvalho are with the Department of Electrical & Computer Engineering, University of Sao Paulo, Sao Carlos, SP 13566-590 Brazil.

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 mechanism for detection of PMU data manipulation attacks. The proposed mechanism is based on continuously monitoring the equivalent impedances of transmission lines and classifying observed anomalies for detecting the presence and location of attacks. In [8] and [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], the authors propose data attack scenarios that combine data integrity and availability attacks on state estimation, also using cyber-physical models to propose security metrics and mitigation schemes. In [12], the authors developed methods to estimate the state of the power grid following a joint cyber and physical attack, and study the resilience of different topologies as well as the resilience to different kinds of attacks. The authors also present conditions on the structure of a grid, so the presented method is guaranteed to recover the state of the grid inside an attacked zone. Finally, in [13], the authors provide an overview of graphical methods for performing cyber-security analysis in power system state estimation. First, the method to model power networks in a graph is described. Then, the authors establish a graph-based characterization of state estimation security, and introduce representative graphical algorithms to solve security problems in state estimation.

The main question of all previous solutions is that they detect the malicious data attacks based on the measurement residual, which is just one component of the measurement error [16],[17], [25]. With this approach, any measurement having error and being close to the Jacobian range space will be hidden from the malicious data attack detection test. In our previous work [21], we have introduced the concept of Innovation for smart grids cyber-physical security. On such work, we have presented a new hypothesis testing for cyber-attack as a malicious data injection detection. The significance of the method is most important, since it considers the error component contained in the Jacobian range space, which is hidden from the classical SE methodology. Another novelty presented in [21] was the processing of simultaneous malicious cyber-attacks in measurements and parameters. Multiple cyber-attacks types, including cyber-attacks on system parameters, were investigated. Once cyber-attacks were detected, identification proposed in [21] was based on the error pattern analysis. Observations suggested pattern behavior and were used on [21] to design an identification solution. However, with respect to the later, no specific proofs of such observations were provided.

This work presents further contributions to the smart grid cyber-security as a malicious data attack problem. First, a formal proof of how parameter errors spread out on the measurement function having a parameter with error is presented. The largest composed measurement error property, in its normalized form, is then demonstrated for this case of error. Second, simultaneous data attack types are considered in [21], assumptions are that the parameters attacks are to be corrected when measurements are without error. However, how may one correct measurements if parameters might be simultaneously in error [23], [24], or the other way around? This work presents a relaxed model strategy for simultaneous malicious data injection attacks. Attacks are processed simultaneously and analyzed using only the framework of measurement gross error analysis. Method validation is made on the IEEE 14-bus and 57-bus systems. Case study shows methodology reliability and robustness. Comparative test results highlight the 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 security. Still, test results show that the presented methodology is accurate even when of low magnitude cyber-attack vectors. Multiple and simultaneous cyber-attacks on measurements and parameters are detected and identified correctly in all of the simulated cases. Corrections of identified attacks are precise, independently of the intrusion type.

The remaining of this paper is organized as follows. Section II presents a summary of Innovation concept on the State Estimation Theory. Section III presents the theorem and proof of error spreading out on the measurements functions having the parameter in error. Section IV presents the methodology to defend from the malicious cyber-attack. Section V presents a case study and test results discussion. The conclusions of this work are presented on Section VI.

II. Innovation Concept in State Estimation Theory

The power system is modelled as a set of non-linear equations as described in the following:

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

with $z \in \mathbb{R}^m$ is the measurement vector, $x \in \mathbb{R}^N$ is the state variables vector. Also, $h: \mathbb{R}^N \rightarrow \mathbb{R}^m$, ($m$>$N$) 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).

OBS.: one should be aware that in fact the previous e is not the error but the residual, however not the optimal one. Wrongly, researchers from SE field call it as the measurement error vector. The error vector is in fact in the measurement z direction [22].

As it is very well known, the objective of the classical weighted least squares (WLS) state estimator is to find the best estimative for the N-dimensional state vector $\hat{x}$, which minimizes the cost function $J(x)$:

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

Geometrically, the $J(x)$ index is a norm in the measurements

vector space $\mathbb{R}^m$, 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 of (1), at a certain operating point x^*, implies:

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

where $H = \partial h/\partial x$ is the Jacobian matrix of h calculated at x^*, $\Delta z = z - h(x^*) = z - z^*$ 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, $\langle u, v\rangle = u^T R^{-1} v = 0$.

The SE as a projection formulation:

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 residual 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:

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

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 of $\Re(H)$ 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 e_D component is nothing else than the residual.

Two main differences between the *error* component and the *residual* will be enumerated:

i) The error has *m* degrees of freedom and the residual *m-n*;

ii) The error is a random variable by hypothesis of the SE formulation, having *m* components in a space of dimension *m* and the residual 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. In order to estimate the error one needs also to estimate the e_U error component. With that purpose, the *innovation* of a measurement, related to the other measurements of the measurement set, is defined. The *innovation* of a measurement is the information it contains, but not the others measurements of the measurement set [16],[17],[19],[25]. 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 the 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 be 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 *i*-th measurement:

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

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 [17]:

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

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. Using (11), (10) can be rewritten as:

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

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 *i*-th measurement and II_i is the innovation index of this same measurement, both known quantities. If instead we work with the normalized residual one obtains the *Composed Normalized Error* (*CNE*), given by:

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

where r_i^N is the normalized residual of the *i*-th measurement. Otherwise, if one normalizes the error one obtains:

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

where σ_i is *i*-th measurement standard deviation.

It has been proved that the measurement having error is the one with Largest CME^N and the measurement correction is through the corresponding *CNE* [16]. All the previous demonstrations were made only for the case of measurements having errors. For the case of parameter error in the h function related to the measurement z, corresponding demonstration is required and this is what will be presented in the following.

III. Largest Normalized Error Theorem for the Case of Parameter Error

THEOREM:

For the situation in which all the measurements are perfect (obtained for load flow) except the measurement z_i, that has a parameter error in h_i, then the largest error will be on this measurement equation.

PROOF:

Consider a situation in which all the measurements are perfect except the measurement z_i, having a parameter error b_i in his measurement equation. This equation can be written as:

$$z_i^{true} = H^{true}x^{true} + \Delta z_i u_i + e. \quad (16)$$

Where the term $\Delta z_i u_i$ models the error in the measurement caused by the parameter error b_i. Following, the measurement residual vector can be obtained as:

$$\hat{r} = z - \hat{z} = (I - HG^{-1}H^T R^{-1})z = R_{\hat{r}}R^{-1}z. \quad (17)$$

Where $G = H^T R^{-1} H$, $R_{\hat{r}}$ is the residual covariance matrix and H is the Jacobian matrix having the parameter error. Since the other measurements (not having parameter error) are assumed to be perfect, this yield:

$$\hat{r} = R_{\hat{r}}R^{-1}(\Delta z_i u_i) = \Delta z_i R^{-1} R_{\hat{r}} u_i. \quad (18)$$

Where $R_{\hat{r}}u_i$ is the *ith* column of the residual covariance matrix, $R_{\hat{r}}$. The vector of normalized residuals is then given by:

$$r^n = (diag(R_{\hat{r}}))^{-1/2}\hat{r} = \Delta z_i R^{-1}(diag(R_{\hat{r}}))^{-1/2}R_{\hat{r}}u_i, \quad (19)$$

which can be rewritten as:

$$r^n = \Delta z_i R^{-1}\begin{bmatrix} \rho_{1i}^2\rho_{11}^{-1} \\ \vdots \\ \rho_{ii} \\ \vdots \\ \rho_{ji}^2\rho_{jj}^{-1} \\ \vdots \\ \rho_{mi}^2\rho_{mm}^{-1} \end{bmatrix}. \quad (20)$$

Where ${\rho_{ii}}^2$ are the variances of the residual vector i. The ratio of the magnitude of a normalized residual r_j^n, $j \neq i$ and the magnitude of the normalized residual associated with the measurement affected by bad parameter, r_i^n, is given by:

$$\frac{|r_j^n|}{|r_i^n|}\frac{|\rho_{ji}^2|}{\rho_{ii}\rho_{jj}} = \gamma_{ji} \leq 1. \quad (21)$$

As a consequence, $r_i^n \geq r_j^n$ for all j=1…, m. Another way of seeing the previous relation is: $|r_i^{N,new} - r_i^N| \geq |r_j^{N,new} - r_j^N|$, where the *new* refers to the situation with parameter error and before that the residuals will be, for all measurements, equal to zero, that is, measurements without parameter error. Transforming in error that relation will be: $|CME_i^{N,new} - CME_i^N| \geq |CME_j^{N,new} - CME_j^N|$, j=1…m, that is the large increment of error will be in the measurement to which parameter error has been added, since with the measurements without parameter error it will be zero.

q.e.d.

Generalization for the case of all measurements not being perfect measurements:

A natural consequence of the previous theorem is: assuming that all the measurements of a measurement set have limited parameter errors, smaller than a predefined value, then if a parameter error is added to one of them, one can assure that it will exist a minimum error magnitude to be added so that measurement will contain the largest error.

Obs.: (i) With the Largest Normalized Error Theorem as previously presented, one can assure, within an uncertainty degree, that once an error in the measurement set is detected, the measurement with the largest CME^N will have the error; (ii) The previous uncertainty degree is caused by the choice in the predefined value for which error is accepted as not existing. For example, if that predefined value is assumed as zero, then the measurement with error will have by sure the largest error for any magnitude of error.

A. How to Differentiate Between Measurement Error and Parameter Error

From the Largest Normalized Parameter Error Theorem, it is a direct conclusion that for all measurements in which the added parameter error appears, that error will be larger than any measurement that does not have parameter error. That means the parameter error will spread to the measurements where the parameter in error appears, what does not happen for the case of the other measurements of the measurement set.

B. Relaxed Model for Simultaneous Malicious Data Attack Processing: An Iterative based Solution

Current state of the art solutions for simultaneous multiple cyber-attack types processing consider the correction of parameters when measurements are free of error [21]. **However, how may one correct measurements if parameters might be simultaneously in error** [23], [24], **or the other way around?** For the solution of such problem, we present a relaxed model which is solved iteratively. Let's consider simultaneous parameter and measurement malicious data attacks. On such, we can consider initially that all measurements are free from errors. Then, one can estimate the system states, x^n, considering parameters p^n, through the iterative solution of $z^n = h(x^n)$. Of course, the measurements and parameters might be simultaneously in error, so a relaxation is proposed to find an estimate of the parameters. One considers that z^n is equal to $h(x^n, p^n) + \frac{dh(x^n,p^n)}{dp}\Delta p$. On such model, we do not decrease the degrees of freedom and have observability problems, since we relax the model by considering that measurements are correct. After convergence, a new parameter estimate, p^{n+1}, is obtained. We can now consider these parameters as without errors, and estimate new states, x^{n+1}, and then correct the measurements with the estimated *CNE*, obtaining z^{n+1}. This problem also relaxes the model by considering the parameters without error, and does not generate any observability problems or decreases the degrees of freedom of the original measurement model. These new states and corrected measurements are used again to estimate the new set of parameters, p^{n+2}, through the solution of $z^{n+1} = h(x^{n+1}, p^{n+1}) + \frac{dh(x^{n+1},p^{n+1})}{dp}\Delta p$. This iterative process is continued until a convergence criteria is reached.

Formally, if a correct measurement z_i has a parameter error p_i, that is:

$$z_i = h_i(x, p_i) + e_i \quad (22)$$

where p_i is the parameter in error.

Then developing function (22) in Taylor series one will have: $z_i = h_{i,0} + \frac{\partial h_i}{\partial p}(x_0, p_0)\Delta p_i$, then $\Delta p_i = \frac{z_i - h_{i,0}}{H_{p,o}}$, where all the quantities are known, allowing in this way computing the parameter error. If we divide Δp_i by the known p_i and multiply the results by one hundred, one will find the correction in percentage of the parameter p_i.

IV. Cyber-Attacks Models And Proposed Methodology

In the following, it is present the proposed methodology to defend against the cyber-attack:

1. To detect the malicious attack, a χ^2 Hypothesis Testing (HT) is applied to Composed Measurement Error in its normalized form (CME^N). Choosing a probability *1-α* 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, $J(\hat{x}) > C$;
2. To identify the measurement/parameter under cyber-attack the *Largest Normalized Error Test* is used.
3. To defend from the cyber-attack, the correction of the malicious data is made using the measurement *CNE* and the relaxed model. As a reminder, the CME^N is generated from the residuals to a space of larger dimension, the measurement subspace, generating in this way noises; the *CNEs,* in contrary, 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, smart grid cyber-attack is modeled as a bad data (e_i) of the *i*-th equation, which can occur due to two main reasons:

1. A cyber-attack in the *i*-th measurement;
2. A cyber-attack in a transmission line (TL) parameter (series or shunt), related to the *i*-th equation.

The identification of the cyber-attack is by analysis of the consequences of the specific attack, as described in the following [21]:

1. A measurement cyber-attack will cause a *Hypothesis Testing Error Detection* with a high local CME^N (from the Largest Normalized Composed Error Theorem, LNCE). The affected measurement will present a CME^N above a chosen threshold value β (this threshold can be chosen based on a desired level of detection sensitivity). Usually β is equal to three standard deviations of the corresponding measurement, i.e., $\beta = 3$;
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, (previous theorem of LNCE, for parameter error case) so, the respective active or reactive power flows *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 creating a sequence of suspicious measurements having parameter error attack and analyzing the firsts larger than three CME^N*s*.

The proposed algorithm is presented in the following:

1. Read the input data. For a given measurements set and network configuration, perform the WLS state estimation [22];
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. 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 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:
$$z_i^C = z_i^E - CNE_i\sigma_i, \quad (23)$$
where z_i^C is the corrected measurement value and z_i^E is the erroneous measurements value, when in case of the measurement with error;
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 parameter cyber-attack. Then, perform the parameter and measurement correction through the relaxed model strategy using the CNE_i (related to the measurement with the largest CME^N), for measurement correction, and for series and shunt parameters, the correction is given by:
$$z_i = h_{i,0} + \frac{\partial h_i}{\partial p}(x_0, p_0)\Delta p_i$$
or,
$$\Delta p_i = \frac{z_i - h_{i,0}}{H_{p,o}} \quad ; \quad (24)$$
Obs.: one should be aware that the correction component (24) is obtained making a Taylor series expansion of z_i around the operating point obtained using the erroneous and known parameter value. Return to *Step 1*. If this situation does not occur, proceed to *Step 6*;
6. 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:
$$z_i^{noise} = z_i + k * noise * \sigma_i. \quad (25)$$

To generate the measurements, it was considered that all measurements have standard deviations calculated by:
$$\sigma_i = \frac{pr\left|z_i^{lf}\right|}{3}, \quad (26)$$

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. State-of-the-art methodologies consider, for each measurement type, a specific standard deviation value [18].

V. Case Study

The validation of the proposed methodology is made 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 (number of measurements divided by the number of state variables) *GRL = 3*, and for the IEEE 57-bus test system the measurement plan consists of 339 measurements, leading to the same *GRL*. Systems' topologies and parameters are found in [20].

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

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

1. Cyber-attack of magnitude 5σ added to measurement *P:07-09 = 0.2808 pu* (active power flow from bus 7 to bus 9);
2. Cyber-attack of 7% added to the series and shunt parameters of the line *03-04*.

The attack processing routine begins with the first attack detection at *Step 1*, where the "cost function" ($J(\hat{x}) = 153.26$) is higher than the *C* value for this measurement scenario ($\chi^2_{81;0.95} = 103.01$), as presented in Table I. Once the attack is detected, the CME^N descending list is built. By analyzing the list in Table I, one can see that the measurements of the line *03-04* and injection on those buses presented $CME^N s$ above the threshold β. 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 = 7.1775* (corresponding to the measurement with the largest CME^N) and the relaxed model strategy. The parameters' corrections are shown in Table II, presenting small approximation errors, demonstrating the efficiency of the parameter correction method. After the correction of the parameters of the line *03-04*, a new state estimation was performed.

After the re-estimation is performed, the χ^2 test was applied again, and a cyber-attack was detected, since $J(\hat{x}) > C$, as presented in Table III. Once the attack is detected, the CME^N descending list is built and the largest CME^N was identified in the measurement *P:07-09* (note that this was the only measurement with $CME^N > \beta$, since the parameters were already corrected in the previous step). Since it was not found any other adjacent measurement with the CME^N above the threshold β, a measurement cyber-attack is identified (as explained at the algorithm's *Step 4*). Then, this measurement was corrected by its corresponding *CNE = 5.4483*, obtaining a corrected value *P:07-09 = 0.2812* (approximation error *0.1425%*). This routine is summarized in Table III. After the re-estimation, no cyber-attack was detected ($J(\hat{x}) = 37.82 < 103.01$), then, the attack processing routine is finished and the state variables can be correctly estimated.

TABLE I - IEEE-14: Processing Cyber-attacks, First Step

Processing Measurement Cyber-Attack Step 1			
$J(\hat{x}) = 153.26 > C = \chi^2_{81;0.95} = 103.01 \Rightarrow$ **Attack Detected!**			
CME^N **Descending List**			
Measurement	***II***	CME^N	***CNE***
Q:04-03	2.8604	6.9641	7.1775
Q:04	0.4734	-4.1836	-9.7775
Q:03-04	2.4239	-4.1222	-4.4592
P:07-09	3.0523	4.1065	4.3212
P:03-04	1.8432	3.3369	3.7963
Q:03-02	0.7282	3.1446	4.0602

TABLE II - IEEE-14: Corrected Parameters

Parameters Correction				
Parameter	**Database Value**	**Erroneous Value**	**Corrected Value**	**Approximation Error**
g_{03-04}	1.9860	2.1250	1.9725	0.6798%
b_{03-04}	-5.0688	-5.4236	-5.0343	0.6806%
b^{shunt}_{03-04}	0.0064	0.0068	0.0063	1.5625%

TABLE III - IEEE-14: Processing Cyber-attacks, Second Step

Processing Measurement Cyber-Attack Step 2			
$J(\hat{x}) = 137.45 > C = \chi^2_{81;0.95} = 103.01 \Rightarrow$ **Attack Detected!**			
CME^N **Descending List**			
Meas. with $\|CME^N\| \geq 3$	***II***	CME^N	***CNE***
P:07-09 = 0.2972	3.0516	5.1774	5.4483
Corrected Measurement: P:07-09 – *CNE*$*\sigma$ = 0.2812 (Approximation Error = 0.1425%)			

In the following, a single transmission line parameter cyber-attack test case is simulated. 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 based method [18], the list of suspicious measurements is presented on Table IV.

TABLE IV - 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

Following this residual descending list, the 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 on Table V. One can see that the measurements of line *01-05* and the injections on those buses present $CME^N s$ above the threshold β. As explained in the *Step 5* of the algorithm, this situation characterizes a parameter cyber-attack. Then, the parameters on this line are corrected using the *CNE = -9.3212* (corresponding to the measurement with the largest CME^N) and the relaxed strategy. Corrections are presented on Table VI. The proposed methodology correctly detects, identify and corrects

the parameter cyber-attack, as seen on such Tables. After the parameters correction, no cyber-attack was detected ($J(\hat{x}) = 44.23 < 103.01$), then, the attack processing routine is finished and the state variables can be correctly estimated.

TABLE V - 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 VI - IEEE-14: Corrected Parameters

Parameters Correction				
Parameter	**Database Value**	**Erroneous Value**	**Corrected Value**	**Correction 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%

ii) Attack Scenario II: Simultaneous Measurement and Parameter Cyber-attacks in the IEEE 57-bus test system ($C = \chi^2_{339;0.95} = 382.93$)

1. Cyber-attack of magnitude -8σ added to measurement *P:45-44 = 0.3725 pu* (active power flow from bus 45 to bus 44);
2. Cyber-attack of 6% added to the series and shunt parameters of the line *12-13*.

The first step of the cyber-attack processing routine is the attack detection. Following Table VII, at *Step 1*, one can notice that the value for the "cost function" ($J(\hat{x}) = 696.34$) is greater than the *C* value for this measurement scenario ($\chi^2_{339;0.95} = 382.93$), therefore, the attack is successfully detected. After the detection, the attacked measurement is identified by searching the measurement with the largest *CME*^{N} above the threshold value ($\beta = 3$), which turns out to be the measurement *P:45-44*. Note that no other adjacent measurements presented a *CME*^{N} above the threshold value β, which characterize a measurement cyber-attack, as described in the *Step 4* of the algorithm. Then, the measurement value is corrected with its *CNE*, by applying the equation (23). Note that the approximation error, i.e., the difference between the measurement's correct database value and the measurement's value corrected by the *CNE*, is very small (0.0268%), which means that the recovery of the original value is very efficient. After the correction, another state estimation is performed.

After the re-estimation was performed, another cyber-attack was detected ($J(\hat{x}) > C$). By analyzing the *CME*^{N} descending list in Table VIII, several measurements of the line *12-13* presented *CME*^{N}s 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 = 5.8447* (related to the measurement with the largest *CME*^{N}) and the relaxed model strategy. The corrected parameters are shown in Table IX and, again, presented very small approximation errors, when compared to the correct database values.

After correcting the parameters of the line *12-13* and re-estimation, no cyber-attack was detected ($J(\hat{x}) = 87.04 < 382.93$), then, the attack processing routine is finished and the state variables can be correctly estimated.

TABLE VII - IEEE-57: Processing Cyber-attacks, First Step

Processing Measurement Cyber-Attack Step 1			
$J(\hat{x}) = 696.34 > C = \chi^2_{339;0.95} = 382.93 \Rightarrow$ **Attack Detected!**			
***CME*^{N} Descending List**			
Measurement	***II***	***CME*^{N}**	***CNE***
P:45-44	5.4704	-8.2857	-8.4229
Q:13-12	8.4988	6.1264	6.1687
Q:12-13	7.7278	-4.5339	-4.5717
P:13-12	1.1785	-3.9295	-4.6688
Q:13	1.1361	-3.0015	-4.8407
P:45	0.4767	2.9295	6.8768
Meas. with $\lvert CME^N \rvert \geq 3$	***II***	***CME*^{N}**	***CNE***
P:45-44 = 0.3437	5.4704	-8.2857	-8.4229
Corrected Measurement: P:45-44 – *CNE**σ = 0.3726 (Approximation Error = 0.0268%)			

TABLE VIII - IEEE-57: Processing Cyber-attacks, Second Step

Processing Measurement Cyber-Attack Step 2			
$J(\hat{x}) = 930.09 > C = \chi^2_{339;0.95} = 382.93 \Rightarrow$ **Attack Detected!**			
***CME*^{N} Descending List**			
Measurement	***II***	***CME*^{N}**	***CNE***
Q:13-12	8.4977	5.8046	5.8447
Q:12-13	7.7260	-5.7973	-5.8457
P:13-12	1.1785	-3.7040	-4.6954
Q:13	1.1361	-3.5514	-3.8034
Q:45-15	0.4275	-3.0749	-4.7343

TABLE IX - IEEE-57: Corrected Parameters

Parameters Correction				
Parameter	**Database Value**	**Erroneous Value**	**Corrected Value**	**Approximation Error**
g_{12-13}	4.8359	5.1260	4.8264	0.1964%
b_{12-13}	-15.7573	-16.7027	15.7265	0.1955%
b^{shunt}_{12-13}	0.0302	0.0321	0.0301	0.3311%

iii) Attack Scenario III: Simultaneous Measurements and Parameter Cyber-attacks in the IEEE 57-bus test system ($C = \chi^2_{339;0.95} = 382.93$)

1. Cyber-attack of -7% added to the series and shunt parameters of the line *38-48*;
2. Cyber-attack of magnitude -8σ added to the measurement *Q:16-01 = 0.0706 pu* (measurement far from the attacked line);
3. Cyber-attack of magnitude 6σ added to the measurement *P:47 = -0.2948* (measurement adjacent to the attacked line);
4. Cyber-attack of magnitude 5σ added to the measurement *Q:38-48 = -0.1935* (measurement belonging to the attacked line)

This scenario was simulated with measurements chosen accordingly to their location, related to the attacked transmission line, to verify the robustness of the algorithm.

In the first step of the attack detection routine, it was obtained $J(\hat{x}) = 571.25 > C = \chi^2_{339;0.95} = 382.93$, thus an attack was

detected. Then, the list of descending CME^N was built, as presented in Table X. By analyzing this table, it was identified the attack in the measurement *Q:16-01*, since it is an isolated measurement with CME^N above the threshold. After the attack identification, the measurement was corrected by its corresponding *CNE = -7.5732* and a new estimation was performed.

TABLE X - IEEE-57: Processing Cyber-attacks, First Step

Processing Measurement Cyber-Attack Step 1			
$J(\hat{x}) = 571.25 > C = \chi^2_{339;0.95} = 382.93 \Rightarrow$ **Attack Detected!**			
CME^N **Descending List**			
Measurement	***II***	CME^N	***CNE***
Q:16-01	2.4920	-7.0285	-7.5732
Q:48-38	3.4559	6.3743	6.6358
P:47	1.8864	4.7324	5.3562
P:48-38	2.3756	4.2930	4.6578
P:38-48	2.3708	-4.2100	-4.5692
Q:16	0.3575	2.8415	8.4126
Meas. with $\|CME^N\| \geq 3$	***II***	CME^N	***CNE***
Q:16-01 = 0.0652	2.4920	-7.0285	-7.5732
Corrected Measurement: Q:16-01 – *CNE*$*\sigma$ = 0.0705 (Approximation Error = 0.1416%)			

After the correction of the measurement *Q:16-01* and a re-estimation, in the second step of the routine, it was obtained $J(\hat{x}) = 479.02 > C = \chi^2_{339;0.95} = 382.93$, thus, another attack was detected. By analyzing the CME^N descending list, presented in Table XI, one notices the presence of several measurements that belong and measurements adjacent to the line *38-48* with the CME^N above the threshold, which characterizes a parameter attack. Then, the parameters of this line are corrected using the relaxed model strategy, with results presented in Table XII.

TABLE XI - IEEE-57: Processing Cyber-attacks, Second Step

Processing Measurement Cyber-Attack Step 2			
$J(\hat{x}) = 479.02 > C = \chi^2_{339;0.95} = 382.93 \Rightarrow$ **Attack Detected!**			
CME^N **Descending List**			
Measurement	***II***	CME^N	***CNE***
Q:48-38	3.4901	7.2657	7.5581
P:38-48	2.3919	-4.4770	-4.8525
P:48-38	2.3967	4.3814	4.7474
P:48	0.5702	-4.2771	-8.6345
Q:38	0.5691	3.3398	6.7522
P:47	1.8847	3.2802	3.7133

TABLE XII - IEEE-57: Corrected Parameters

Parameters Correction				
Parameter	**Database Value**	**Erroneous Value**	**Corrected Value**	**Approximation Error**
g_{38-48}	9.4641	8.8016	9.4641	0%
b_{38-48}	-14.6208	-13.5973	-14.4754	0.9944%
b_{38-48}^{shunt}	0	0	0	0%

In the third step, after the correction of the parameters, it was obtained $J(\hat{x}) = 458.57 > C = \chi^2_{339;0.95} = 382.93$, thus, another attack was detected. Then, the CME^N descending list was built, as presented in Table XIII, and the attack was identified in the measurement *P:47*. After the identification, this measurement was corrected by its corresponding *CNE = 5.3265*.

TABLE XIII - IEEE-57: Processing Cyber-attacks, Third Step

Processing Measurement Cyber-Attack Step 3			
$J(\hat{x}) = 458.57 > C = \chi^2_{339;0.95} = 382.93 \Rightarrow$ **Attack Detected!**			
CME^N **Descending List**			
Measurement	***II***	CME^N	***CNE***
P:47	1.8977	4.7123	5.3265
Q:38-48	3.2656	3.8757	4.0534
Q:21	1.5574	2.9321	3.4845
Q:46	0.6535	2.5156	4.5985
P:46	0.3581	2.4642	7.3091
Q:11	2.6327	2.3148	2.4762
Meas. with $\|CME^N\| \geq 3$	***II***	CME^N	***CNE***
P:47 = -0.2792	1.8977	4.7123	5.3265
Corrected Measurement: P:47 – *CNE*$*\sigma$ = -0.2949 (Approximation Error = 0.0339%)			

After the correction of the measurement *P:47*, a new estimation was performed and it was obtained $J(\hat{x}) = 427.62 > C = \chi^2_{339;0.95} = 382.93$, thus, another attack was detected. By analyzing the CME^N descending list, the attack was identified in the measurement *Q:38-48*, as presented in the Table XIV, and its value was corrected by its corresponding *CNE = 4.8325*.

TABLE XIV - IEEE-57: Processing Cyber-attacks, Fourth Step

Processing Measurement Cyber-Attack Step 4			
$J(\hat{x}) = 427.62 > C = \chi^2_{339;0.95} = 382.93 \Rightarrow$ **Attack Detected!**			
CME^N **Descending List**			
Measurement	***II***	CME^N	***CNE***
Q:38-48	3.2652	4.6207	4.8325
P:13-12	0.1846	-2.0146	-8.0987
Q:07	1.3844	2.0027	2.4706
Q:22	1.5885	1.8727	2.2129
Q:45	3.8018	1.8457	1.9085
Q:11	2.6327	1.8051	1.9309
Meas. with $\|CME^N\| \geq 3$	***II***	CME^N	***CNE***
Q:38-48 = -0.1842	3.2652	4.6207	4.8325
Corrected Measurement: Q:38-48 – *CNE*$*\sigma$ = -0.1937 (Approximation Error = 0.1033%)			

After the correction of the measurement *Q:38-*48, a new estimation was performed and it was obtained $J(\hat{x}) = 198.06 < C = \chi^2_{339;0.95} = 382.93$, thus, no attack was detected. As a conclusion, in this attack scenario, one could verify that the proposed methodology obtained good results, even in a case with simultaneous measurement and parameter attack. An observation can be made regarding the initial approximation error (0.9944%) between the estimated value and the true value for the parameter b_{38-48}. One may notice an approximation error larger than the ones obtained in other scenarios, which is justified by the presence of two attacked measurements in the neighborhood of the affected line. Still, the correction of the attacked measurements, a final parameter estimation was performed, as proposed on the relaxed model strategy, with results presented in Table XV.

TABLE XV - IEEE-57: Corrected Parameters

Parameters Correction				
Parameter	**Database Value**	**Erroneous Value**	**Corrected Value**	**Approximation Error**
g_{38-48}	9.4641	8.8016	9.4641	0%
b_{38-48}	-14.6208	-13.5973	-14.6106	0.0698%
b_{38-48}^{shunt}	0	0	0	0%

The approximation error was greatly reduced (smaller than 0.1%), which demonstrates the accuracy of the proposed solution.

VI. Conclusion

This paper has presented a formal proof of how parameter errors spread out to the measurements functions containing the parameter in error. After, an analytical methodology for smart grid cyber-physical security as a malicious data attack was introduced. The proposed method uses an innovation approach for cyber-attacks detection, identification and correction. Cyber-attacks are modeled as bad data. The methodology considers, during equation derivation, potential cyber-attacks on measurements and parameters. The detection test is based on a composed measurement error analysis. Cyber-attacks identification is based on the Generalized Largest Normalized Error test, in this paper developed. Correction of cyber-attacks is made using the composed normalized error and a relaxed model strategy. Simultaneous cyber-attacks are considered, even when the measurements belong to the image of the Jacobian, presenting clear contributions to the malicious data injection attack state-of-the-art. A big advantage of the proposition 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 or parameters, since the error is estimated and then the altered quantity is corrected. Still, the SE software does not require major changes for the implementation of the paper ideas.

VII. References

[1] Y. Liu, M. K. Reiter and 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 and J. A. Giampapa, "Vulnerability Assessment of AC State Estimation with Respect to False Data Injection Cyber-attacks," in *IEEE* Transactions on Smart Grid, vol.3, no.3, pp.1362-1370, 2012.

[3] A. Ashok; M. Govindarasu; V. Ajjarapu, "Online Detection of Stealthy False Data Injection Attacks in Power System State Estimation," in *IEEE Transactions on Smart Grid*, (accepted for publication) 2018.

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

[5] T. Kim and H. Poor, “Strategic protection against data injection attacks on power grids,” in *IEEE* Transactions on Smart Grid, vol. 2, no. 2, pp. 326-333, 2011.

[6] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, “Smart grid data integrity attacks,” in *IEEE* Transactions on Smart Grid, vol. 4, no. 3, pp. 1244-1253, 2013.

[7] S. Zonouz, K. M. Rogers, R. Berthier, R. B. Bobba, W. H. Sanders and T. J. Overbye, "SCPSE: Security-Oriented Cyber-Physical State Estimation for Power Grid Critical Infrastructures," in *IEEE* Transactions on Smart Grid, vol. 3, no. 4, pp. 1790-1799, 2012.

[8] Y. Chakhchoukh and H. Ishii, "Coordinated Cyber-attacks on the Measurement Function in Hybrid State Estimation," in *IEEE* Transactions on Power Systems, vol. 30, no. 5, pp. 2487-2497, 2015.

[9] Y. Chakhchoukh; H. Ishii, "Enhancing Robustness to Cyber-attacks in Power Systems Through Multiple Least Trimmed Squares State Estimations," in *IEEE* Transactions on Power Systems, vol. 31, no.6, pp.4395-4405, 2016.

[10] O. Kosut, L. Jia, R. Thomas, and L. Tong, “Malicious data attacks on the smart grid,” in *IEEE* Transactions on Smart Grid, vol. 2, no. 4, pp. 645-658, 2011.

[11] K. Pan, A. M. H. Teixeira, M. Cvetkovic and P. Palensky, "Combined data integrity and availability attacks on state estimation in cyber-physical power grids," *2016 IEEE* International Conference on Smart Grid Communications (SmartGridComm), Sydney, NSW, pp. 271-277, 2016.

[12] S. Soltan; M. Yannakakis; G. Zussman, "Power Grid State Estimation Following a Joint Cyber and Physical Attack," in *IEEE* Transactions on Control of Network Systems, (accepted for publication) 2018.

[13] S. Bi and Y. J. A. Zhang, "Graph-based Cyber Security Analysis of State Estimation in Smart Power Grid," in *IEEE* Communications Magazine, vol. 55, no. 4, pp. 176-183, 2017.

[14] S. Li, Y. Yılmaz and X. Wang, "Quickest Detection of False Data Injection Attack in Wide-Area Smart Grids," in *IEEE* Transactions on Smart Grid, vol. 6, no. 6, pp. 2725-2735, 2015.

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

[16] N. G. Bretas, S. A. Piereti, A. S. Bretas and A. C. Martins, “A geometrical view for multiple gross errors detection, identification, and correction in power system state estimation,” in *IEEE* Transactions on Power Systems, vol. 28, no. 3, pp. 2128-2135, 2013.

[17] N. G. Bretas, A. S. Bretas and S. A. Piereti, "Innovation concept for measurement gross error detection and identification in power system state estimation," in IET Generation, Transmission & Distribution, vol.5, no.6, pp.603-608, 2011.

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

[19] N. G. Bretas, A. S. Bretas, “A two steps procedure in state estimation gross error detection, identification, and correction,” in International Journal of Electrical Power & Energy Systems, vol. 73, pp. 484-490, 2015.

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

[21] A. S. Bretas, N. G. Bretas, B. E. B. Carvalho, E. Bayens, P. P. Khargonekar, “Smart grids cyber-physical security as a malicious data attack: An Innovation approach”, in Electric Power Systems Research, vol. 149, pp. 210-219, 2017.

[22] N. G. Bretas, A. S. Bretas, “The Extension of the Gauss Approach for the Solution of an Overdetermined Set of Algebraic Non-Linear Equations”, in IEEE Transactions of Circuits and Systems II: Express Briefs, (accepted for publication) 2018.

[23] N. G. Bretas, A. S. Bretas, Discussion on “a new framework for detection and identification of network parameter errors”, in *IEEE* Transactions on Smart Grid, vol 8, no 2, pp. 1028–1028, 2017.

[24] Y. Lin, A. Abur, Closure to discussion on “a new framework for detection and identification of network parameter errors”, in *IEEE* Transactions on Smart Grid, vol 8, no 2, pp. 1029–1030, 2017.

[25] N. G. Bretas, A. S. Bretas, A. C. P. Martins, “Convergence property of the measurement gross error correction in power system state estimation, using the geometrical background’, in IEEE Transactions on Power Systems, vol 28, no 4, pp. 3729–3736, 2013.