Cybersecurity of Distribution Networks Real-Time Monitoring: A Parameter Error Correction Model Against False Data Injection Attacks

Arturo Suman Bretas, Michel Caraballo, Nnamdi C Ejiofor, Newton G Bretas

Cybersecurity of Distribution Networks Real-Time Monitoring: A Parameter Error Correction Model Against False Data Injection Attacks

Arturo S. Bretas[1,2], Michel Caraballo[2], Nnamdi C. Ejiofor[2], Newton G. Bretas[3]*

[1]*Grid Security and Communications Department, Sandia National Laboratories, Albuquerque, NM, USA*
[2]*Univ. Grenoble Alpes, CNRS, Grenoble INP*, G2Elab, 38000 Grenoble, France*
[3]*Electrical and Computer Engineering Department, University of Sao Paulo, Sao Carlos, SP, Brazil*
** asbreta@sandia.gov*

Keywords: Cybersecurity, Distribution Networks, False Data Injection, Parameter Error, Measurement Error

Abstract

As Smart Grid technologies are deployed, the many advantages of new metering, controls, and analysis come with added technical challenges. Specifically, the digitalization of the power grid and the increasing dependence on communications systems makes the network real-time monitoring more vulnerable to cyber-attacks. Cyber-attacks, if not detected and accurately corrected, can lead to system operator misinformation. Current state-of-the-art models for real-time monitoring cybersecurity, hypothesizes that the measurement model is correct, without error. While this assumption might be acceptable for systems and devices not dependent on communication networks, this can be considered a strong hypothesis for power grids real-time monitoring. False data injection attacks on the measurement model are also possible. This work presents a parameter correction model against false data injection attacks. False data injection attacks on measurements and measurement models are simultaneously considered. A chi-squared hypothesis test is used for detection of cyberattacks, while a normalized composed measurement error test is used for cyberattack identification. Parameter correction model is then used if a modelling error is identified, otherwise a measurement correction model is used if a measurement error is identified. Easy-to-implement model, built of the classical quasi-static state estimator, without hard-to-design parameters, suggest potential for real-life applications.

1 Introduction

As distribution systems implement smart grid technologies, the many advantages of new metering, controls, and analysis come with added technical challenges. Specifically, the digitalization of the power grid and the increasing dependence on communications systems makes the network more vulnerable to cyber-attacks. Cyber-attacks, if not detected and accurately corrected, can lead to misinformation to system operators and potential collapse of the power system. While much research has been done to address this concern, science and technology for smart grids cybersecurity is still seldom. In any distribution system, real-time monitoring is a critical process for reliable operation. Currently, Power System State Estimation (PSSE) is the main tool for real-time system monitoring [1]. The Weighted Least Squares (WLS) measurement model is the most used for PSSE. The State Estimator (SE) uses sensor readings to provide information about the system condition. The results of the SE are used in many applications for distribution system operation. One of the most important applications of the PSSE is its gross error processing capability [2]. Measurements that are obviously incorrect or inconsistent are discarded in a pre-filtering step, still a post-processing step called bad data analysis is performed afterwards [3]. Classical PSSE uses the chi-squared test for bad data detection, and the normalized residual test for identification [1]. The WLS model fails though to consider the masked component of the error, which was corrected in [4]. Regarding False Data Injections (FDI) on measurements, [5] presents a correction model that is built on top of the classical WLS SE results. [6] otherwise presents proofs and properties of parameter model errors spreading out to the measurement function, while [7] presents a per-phase model for parameter error correction. [8] otherwise presents a parameter correction model for False Data Injections (FDI) in the measurement model. The fundamental limitation of [8], is that it does not consider the effect of the parameter error on the results of the two-step SE model in [9], during the measurement error correction. This will cause an increased necessary number of iterations and sometimes can lead to convergence to physically incorrect solutions. This effect is because, in [8], the parameter error correction model uses corrected measurements without considering the potential parameter error effect. Toward overcoming this limitation, this work presents a parameter correction model that incorporates the effect of the measurement error. Towards this effect modelling, the error is included in the measurement and parameter error correction model. The extended correction model is validated on a synthetic grid, with comparative test results in [8] considering different cyberattack scenarios. The remainder of this paper is

presented as follows. Section 2 presents a theoretical review on false data correction modelling. Section 3 presents the parameter correction model. A case study is presented in Section 4. Conclusions of this work are presented in Section 5.

2 Theoretical Background

Consider a system with the following measurement model:

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

where $z \in \mathbb{R}^m$ is the measurement vector, $h(x) : \mathbb{R}^N \rightarrow \mathbb{R}^m$, $(m > N)$ is a continuously differentiable nonlinear algebraic function that relates the state to the measurement vector, $x \in \mathbb{R}^N$ is the state vector, $e \in \mathbb{R}^m$ is the measurement residual vector with a Gaussian probability function, zero mean, and known standard deviation σ, $N = 2n - 1$ is the number of state variables, and n is equal to the number of buses. One can solve (1) through the WLS model, as:

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

where R is the covariance matrix of the residuals, $J(x)$ is effectively a weighted L_2-norm in the measurement vector space $\mathbb{R}^m$. Regarding the solution of (2), it is obtained through the Newton-Raphson method. The linearization of (1) fives:

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

where H is the Jacobian matrix of h in the current estimated state variable vector $\hat{x}$, $\Delta z = z - h(\hat{x})$ is the correction of the measurement vector and $\Delta x = x - \hat{x}$ is the correction of the state vector. The WLS solution can be seen geometrically as the projection of Δz onto the Jacobian space by a linear projection matrix P, that is, $\Delta\hat{z} = P\Delta z$. The projection matrix P is the idempotent matrix that has the following expression:

$$P = H(H^T R^{-1} H)^{-1} H^T R^{-1} \tag{4}$$

The general problem of the previous equations is that they consider the measurement model to be correct, without errors. In [9], it is shown that in the gross error analysis process a two-step approach should be adopted. In the first step, all measurements should be weighted equally proportional to the magnitude of the measurement and the gross error analytic performed. After processing of gross error, in the second step, the meter precision can be restored and the state estimation executed. The fundamental limitation of this process is that it considers the model free of error. Toward solving this limitation, [8] presented a parameter correction mode. The conjugate of the complex power flow is expressed in (5).

$$S^*_{km} = E^*_k I_{km} = y_{km} V_k e^{-j\theta_k}(V_k e^{j\theta_k} - V_m e^{j\theta_m}) + j b^{sh}_{km} V_k^2 \tag{5}$$

From the real and imaginary components of the aforementioned equation, the expressions for active and reactive power flows can be derived as follows.

$$P_{km} = V_k^2 g_{km} - V_k V_m g_{km} cos(\theta_{km}) - V_k V_m b_{km} sin(\theta_{km}) \tag{6}$$

$$\begin{aligned} Q_{km} = &- V_k^2 (b_{km} + b^{sh}_{km}) + V_k V_m b_{km} cos(\theta_{km}) \\ &- V_k V_m g_{km} sin(\theta_{km}) \end{aligned} \tag{7}$$

Given that the active power loss is defined as the sum of the active power at both ends, it can be expressed as (8).

$$\begin{aligned} P_{km(loss)} &= P_{km} + P_{mk} \\ P_{km(loss)} &= g_{km}(V_k^2 + V_m^2 - 2V_k V_m cos(\theta_{km}) \end{aligned} \tag{8}$$

[8] arranged the aforementioned equation in a matrix format and applied a Taylor series expansion to relate the correction of an identified measurement to the error of the parameters, as shown in (9). This framework uses the output of the WLS estimation to define the state variables $V_k, V_m, \theta_k, \theta_m$. It is important to note that the measurements were assumed to be free of gross errors, despite the presence of Gaussian noise with zero mean coming from the current and potential transformers.

$$\begin{pmatrix} \Delta g_{km} \\ \Delta b_{km} \\ \Delta b^{sh}_{km} \end{pmatrix} = \tau^{-1} \begin{pmatrix} z_{P_{km(loss)}} - h^n_{P_{km(loss)}} \\ z_{P_{km}} - h^n_{P_{km}} \\ z_{Q_{km}} - h^n_{Q_{km}} \end{pmatrix} \tag{9}$$

where τ is given by (10).

$$\begin{pmatrix} V_k^2 + V_m^2 - 2V_k V_m \cos(\theta_{km}) & 0 & 0 \\ V_k^2 - V_k V_m \cos(\theta_{km}) & -V_k V_m \sin(\theta_{km}) & 0 \\ -V_k V_m \sin(\theta_{km}) & -V_k^2 + V_k V_m \cos(\theta_{km}) & -V_k^2 \end{pmatrix}^n \tag{10}$$

The deviations between the true values of the line parameters and those in their parameter model could be attacks made individually, an unbalanced parameter error, as reflected in (11).

$$\begin{aligned} g_{km} &= {g_{km}}^{\text{true}} + \Delta g_{km} \\ b_{km} &= {b_{km}}^{\text{true}} + \Delta b_{km} \\ b^{sh}_{km} &= {b^{sh}_{km}}^{\text{true}} + \Delta b^{sh}_{km} \end{aligned} \tag{11}$$

where g, b, and $b^{sh} \in \mathbb{R}^\rho$, and ρ equal to the number of parameters of the measurement model.

Although, it should be noted that the state variables are derived from estimated measurements without error. Toward solving this, the next section presents a parameter correction model which considers this effect.

3 Parameter Correction Model

The parameter correction model presented by [8] fails to model the effect of parameter error on measurements, which can cause multiple unnecessary iterations and/or convergence to a physically incorrect solution. (1) does not consider the parameter error effect, and thus will be modified as:

$$z = h(x) + e + e_\rho \tag{12}$$

where $e_\rho \in \mathbb{R}^\rho$ that is the residual vector of parameters with a Gaussian probability function, zero mean and known standard deviation σ_ρ.

Therefore, the error of the parameter is incorporated into the corresponding equation $h^n(\hat{x})$. The power flow equations (6)-(8) then become (13)-(15). Then, (13)-(15) are used in (9).

$$\begin{aligned} h^n_{P_{km}} =& V_k^2 g_{km} - V_k V_m g_{km} cos(\theta_{km}) \\ & - V_k V_m b_{km} sin(\theta_{km}) + e_{\rho_{P_{km}}} \end{aligned} \tag{13}$$

$$\begin{aligned} h^n_{Q_{km}} =& - V_k^2 (b_{km} + b^{sh}_{km}) + V_k V_m b_{km} cos(\theta_{km}) \\ & - V_k V_m g_{km} sin(\theta_{km}) + e_{\rho_{Q_{km}}} \end{aligned} \tag{14}$$

$$\begin{aligned} h^n_{P_{km(loss)}} =& g_{km}(V_k^2 + V_m^2 - 2V_k V_m cos(\theta_{km})) \\ & + e_{\rho_{P_{km}}} + e_{\rho_{P_{mk}}} \end{aligned} \tag{15}$$

Since the parameter error is propagated not only at both ends of the line but also to other measurements related to the involved buses, a single iteration may not be sufficient to fully correct the error upon its initial detection. To address this issue, the following procedure is proposed and in Fig. 1 the improvements of the current procedure and new blocks are highlighted in green.

1. Read the data input, which includes the network parameters and the set of measurements.
2. Perform WLS estimation using the two-steps procedure proposed in [9], where the weight matrix is constructed with $\sigma_i = \frac{z_i}{100}$.
3. Perform the detection of gross error by applying the χ^2 test to the Composed Measurement Error in its normalized form CME^N defined in [1]. If the test is true, proceed to Step 4. Otherwise, proceed to Step 8.
4. Identify the gross error by constructing a descending list of the measurements based on $|CME^N|$. If an isolated measurement with the highest $|CME^N|$ exceeds the threshold value β, proceed to step 5. If a set of measurements with the same pair of buses and high $|CME^N|$ exceeding β is identified, proceed to step 6.
5. Correct the measurement error using (16) proposed in [9], where CNE_i is the Composed Normalized Error of the measurement i. Then, return to Step 2.

$$z_i^{new} = z_i^{old} - CNE_i \sigma_i \tag{16}$$

6. If a set of measurements with the same pair line is identified with a parameter error, a variable z_{wpe} is created and stored. $z_{wpe} \in R^m$ is the affected measurement with the highest $|CME^N|$. If z_{wpe} has an associated stored line and is in the descending $|CME^N|$ list, the procedure continues with this line until it has a value lower than β. In both cases, proceed to Step 7.
7. Using the state variable vector from the output of Step 2, perform the parameter correction in z_{wpe} using (9) while applying (13)-(15). Then, return to step 2.
8. Proceed to step two of the two-step procedure suggested by [9].

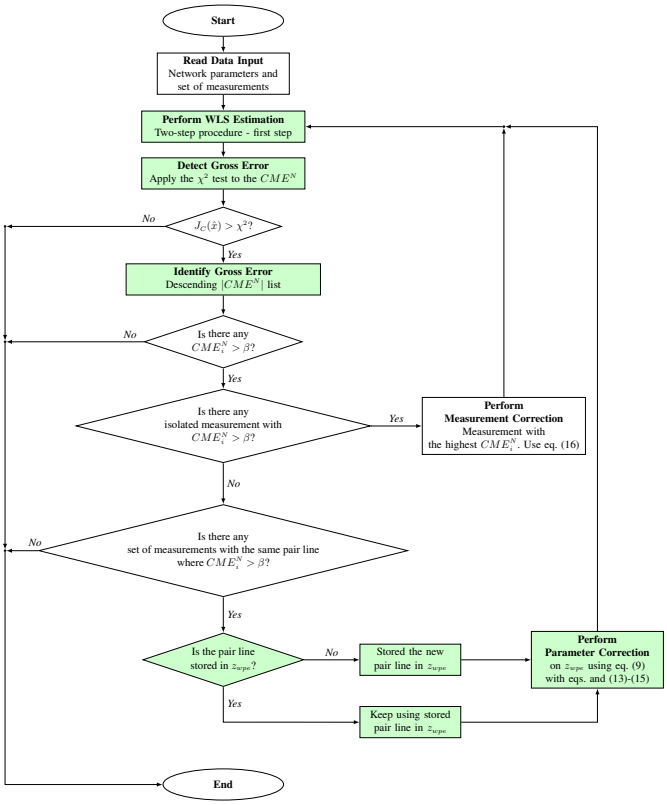

Fig. 1 Simultaneous FDI detection, identification, and correction flowchart.

4 Case Study

A 3-bus system was used to evaluate the proposed framework, as shown in Fig. 2. The test system consists of one generator as a slack machine with $|V_1| = 1.06$ p.u. and two PQ loads with power demands given by $P_1 = 0.076$ p.u., $Q_1 = 0.016$ p.u. and $P_2 = 0.216$ p.u., $Q_2 = 0.127$ p.u., respectively. Line parameters are defined in Table 1.

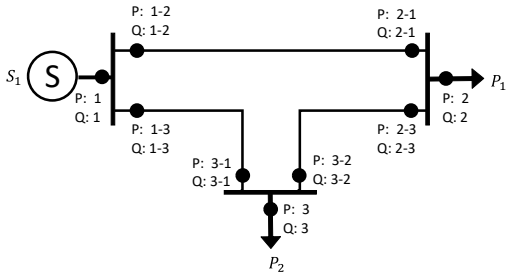

Fig. 2. 3-Bus Test System

Table 1 Line parameters in per unit (p.u.).

Line	g (p.u.)	b (p.u.)	b^{sh} (p.u.)
L_{12}	2.499	-7.632	0.013
L_{13}	1.026	-4.235	0.025
L_{23}	1.701	-5.194	0.017

To evaluate the framework, two different tests were conducted. For the first test, a measurement error was added to P_{13} with a value of $k_{ge} = 5\sigma$, resulting in $P_{13}^{new} = P_{13}^{old} + k_{ge}$. The results of the first detection and identification steps are displayed in Table 2, where the measurement error was accurately detected and identified.

Table 2 Measurement Cyber-attack: First step - $GRL = 3.6$.

Type of error:	**Measurement error**		
Element:	P_{13}		
Error:	$k_{ge} = 5\sigma$		
Detection			
χ^2 test:	$J_C(\hat{x}) = 59.6 > \chi^2 = 32.35$ Attack detected!		
Identification			
Measurement with $\lvert CME^N \rvert > 3.0$	II	CME^N	CNE
P_{15}	1.193	4.596	0.989
P_{51}	0.832	4.564	1.189

In Table 3, the chi-square test shows that the measurement error was successfully corrected by using (16). The procedure then proceeds to step 9 of the proposed framework.

Table 3 Measurement Cyber-attack - After correction.

Detection	
χ^2 test:	$J_C(\hat{x}) = 26.04 < \chi^2 = 32.35$ No attack detected

For the second test, an unbalanced parameter error was applied to $line_{13}$ with the following adjustments: g decreased by 3%, b increased by 6%, and b^{sh} decreased by 8%. Table 4 highlights the significant impact of this unbalanced error on the detection step. Furthermore, the descending CME^N list emphasizes the influence of the error in the parameter b on the estimated measurement of Q_{13}. In this first approach, the [8] framework is tested.

Table 4 Parameter Cyber-attack: First step - $GRL = 3.6$.

Type of error:	**Measurement error**		
Element:	$Line_{13}$		
Error:	$g = +3\%$ $b = +6\%$ $b^{sh} = +8\%$		
Detection			
χ^2 test:	$J_C(\hat{x}) = 756.29 > \chi^2 = 32.35$ Attack detected!		
Identification			
Measurement with $\lvert CME^N \rvert > 3.0$	II	CME^N	CNE
Q_{13}	0.855	15.772	12.127
Q_{23}	2.512	11.132	5.990
Q_{12}	2.266	7.174	3.931
P_{12}	2.812	6.802	3.599
P_{21}	2.818	6.099	3.235
P_{31}	2.286	4.669	2.557
P_{13}	2.291	3.571	1.947

Using the framework proposed in [8], the correction does not converge, as shown in Figures 3 and 4. As previously described, neglecting the measurement errors used to estimate state variables results in the correction procedure converging only to a point of uncertainty.

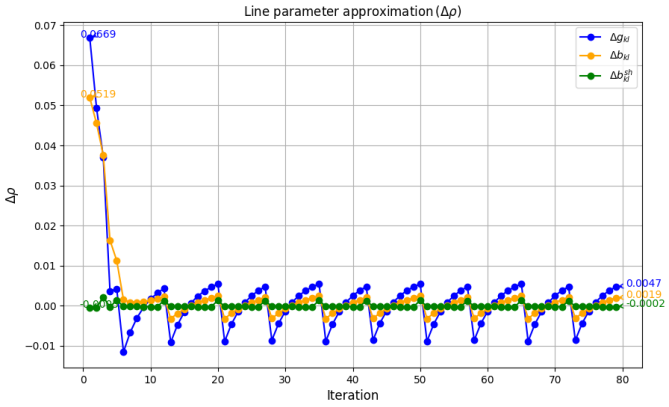

Fig. 3. Convergence of $\Delta\rho$ - [8] framework

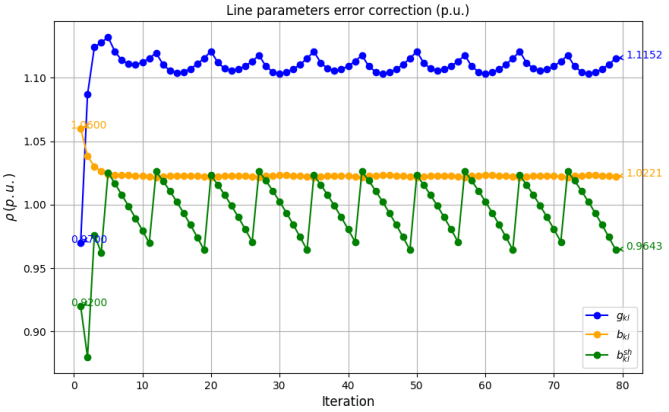

Fig. 4. Performance of Parameter Correction - [8] framework

The results of the proposed framework's implementation are presented. Table 5 provides the updated values of the descending CME^N list, reflecting the effects of Gaussian noise added to each measurement in each simulation.

Table 5 Parameter Cyber-attack: First step - $GRL = 3.6$.

Type of error:	**Measurement error**		
Element:	$Line_{13}$		
Error:	$g = +3\%$ $b = +6\%$ $b^{sh} = +8\%$		
Detection			
χ^2 test:	$J_C(\hat{x}) = 743.32 > \chi^2 = 32.35$ Attack detected!		
Identification			
Measurement with $\lvert CME^N \rvert > 3.0$	II	CME^N	CNE
Q_{13}	0.855	15.859	12.203
Q_{23}	2.511	11.246	6.060
Q_{12}	2.267	7.248	3.973
P_{21}	2.817	6.104	3.235
P_{12}	2.799	5.959	3.165
P_{13}	2.296	3.892	2.120
P_{21}	2.289	3.726	2.031

Fig. 5 illustrates the convergence of the parameter correction $\Delta\rho$ to a value below 10^{-2}. Fig. 6 shows the performance of the line parameter correction, which required 9 iterations to achieve an error of 1.99% for g and 0.21% for both b and b^{sh}. Table 6 presents the results of the parameter correction in the detection step, which is successfully below the chi-square threshold value.

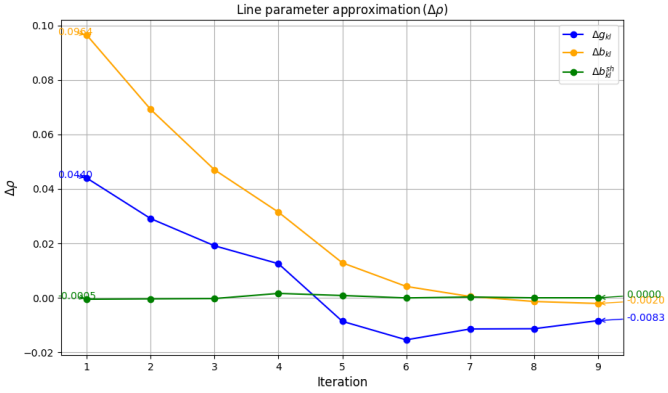

Fig. 5. Convergence of $\Delta\rho$ - proposed framework

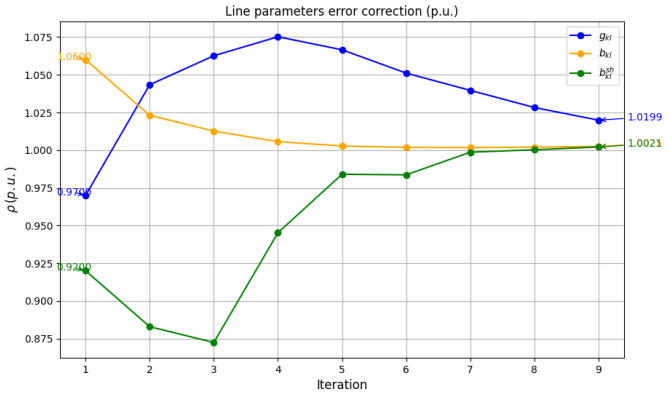

Fig. 6 Performance Parameter Correction - proposed framework

Table 6 Parameter Cyber-attack - After correction.

Detection
χ^2 test: $J_C(\hat{x}) = 17.59 < \chi^2 = 32.35$ No attack detected

5 Conclusion

This work presents a parameter correction model for distribution networks real-time monitoring. Current parameter error correction state-of-the-art models do not consider the effect of the parameter error on measurements. This will cause an increased necessary number of iterations and can sometimes lead to convergence to physically incorrect solutions. The parameter correction model presented in this work considers this effect by modelling the error in the measurement functions. A case study considering a synthetic 3-Bus system is further presented, highlighting the mitigated modelling error effect the parameter error correction model has. Easy-to-implement model, without hard-to-design parameters, built on the classical WLS solution, highlights potential aspects for real-life applications.

6 Acknowledgements

The authors would like to thank Université Grenoble Alpes and CNRS for their financial support through the project *Vers une transition énergétique sécurisée des modèles distribués pour une observabilité, une contrôlarité et une cybersécurité améliorées*.

7 References

[1] Arturo Bretas, Newton Bretas, Joao BA London Jr, and Breno Carvalho. *Cyber-physical power systems state estimation*. Elsevier, 2021.

[2] Rodrigo D Trevizan, Cody Ruben, Aquiles Rossoni, Surya C Dhulipala, Arturo Bretas, and Newton G Bretas. μ pmu-based temporal decoupling of parameter and measurement gross error processing in dsse. *electricity*, 2(4):423–438, 2021.

[3] Tierui Zou, Nader Aljohani, Pan Wang, Arturo S Bretas, and Newton G Bretas. Distributed nonlinear state estimation using adaptive penalty parameters with load characteristics in the electricity reliability council of texas. *Journal of Industrial Information Integration*, 24:100223, 2021.

[4] Newton G Bretas and Arturo S Bretas. The extension of the gauss approach for the solution of an overdetermined set of algebraic non linear equations. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 65(9):1269–1273, 2018.

[5] Arturo S Bretas, Newton G Bretas, Breno Carvalho, Enrique Baeyens, and Pramod P Khargonekar. Smart grids cyber-physical security as a malicious data attack: An innovation approach. *Electric Power Systems Research*, 149:210–219, 2017.

[6] Arturo S Bretas, Newton G Bretas, and Breno EB Carvalho. Further contributions to smart grids cyber-physical security as a malicious data attack: Proof and properties of the parameter error spreading out to the measurements and a relaxed correction model. *International Journal of Electrical Power & Energy Systems*, 104:43–51, 2019.

[7] Arturo Suman Bretas, Newton Geraldo Bretas, SH Braunstein, A Rossoni, and Rodrigo Daniel Trevizan. Multiple gross errors detection, identification and correction in three-phase distribution systems wls state estimation: A per-phase measurement error approach. *Electric Power Systems Research*, 151:174–185, 2017.

[8] Tierui Zou, Arturo S Bretas, Cody Ruben, Surya C Dhulipala, and Newton Bretas. Smart grids cyber-physical security: Parameter correction model against unbalanced false data injection attacks. *Electric power systems research*, 187:106490, 2020.

[9] Newton G Bretas and Arturo S Bretas. A two steps procedure in state estimation gross error detection, identification, and correction. *International Journal of Electrical Power & Energy Systems*, 73:484–490, 2015.