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

Arturo Bretas[1,2] Michel Caraballo[1] Nnamdi Ejiofor[1] Newton Bretas[3]
Univ. Grenoble Alpes, CNRS, Grenoble INP, G2Elab, 38000 Grenoble, France* [1]
Electric Grid Security and Communications Department, Sandia National Laboratory, Albuquerque, NM, USA [2]
Department of Electrical and Computer Engineering, University of Sao Paulo, Sao Carlos, SP, Brazil [3]
asbreta@sandia.gov, {michel.caraballo-gomez, chinenye-nnamdi.ejiofor}@grenoble-inp.fr, ngbretas@sc.usp.br

2025 IEEE Kiel PowerTech | 979-8-3315-4397-6/25/$31.00 ©2025 IEEE | DOI: 10.1109/PowerTech59965.2025.11180321

***Abstract*—As smart grid technologies are deployed, the many advantages of new measurement, control, and analysis come with added technical challenges. Specifically, the digitalization of the power grid and the increasing dependence on communication systems makes network real-time monitoring more vulnerable to cyber-attacks. Cyber-attacks, if not detected and corrected accurately, can lead to misinformation to the system operator. Current state-of-the-art models for real-time cybersecurity monitoring hypothesize that the measurement model is correct, without error. Although this assumption might be acceptable for systems and devices that are not dependent on communication networks, this can be considered a strong hypothesis for real-time monitoring of power grids. 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 cyber-attacks, while a normalized composed measurement error test is used for cyber-attack identification. The parameter correction model is then used if a modeling error is identified; otherwise, a measurement correction model is used if a measurement error is identified. The easy-to-implement model, built of the classical quasi-static state estimator, without hard-to-design parameters, suggests potential for real-life applications.**

***Index Terms*—Cybersecurity, Distribution Networks, False Data Injection, Parameter Error, Measurement Error**

I. Introduction

As distribution systems implement smart grid technologies, the many advantages of new meters, controls, and analysis come with added technical challenges. In particular, the increasing digitalization of the power grid and its reliance on communications systems have heightened its vulnerability 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. Although considerable research has been done to address this concern, significant gaps remain, especially in real-time resilience and detection, as the science and technology for smart grid cybersecurity are still seldom.

One critical area affected by these vulnerabilities is Power System State Estimation (PSSE), which plays a central role in the reliable operation of distribution systems [1]. The Weighted Least Squares (WLS) measurement model is the most widely used method for PSSE, which depends on accurate sensor measurements and a robust State Estimator (SE) to provide reliable information about the system conditions. However, PSSE remains susceptible to False Data Injections (FDI) attacks and parameter model errors that can compromise system reliability. The results of the SE are used in many applications for distribution system operation, such as optimal power flow and contingency analysis. One of the most important applications of the PSSE is its gross error processing capability [2], where measurements that are obviously incorrect or inconsistent are discarded in a prefiltering step, followed by a post-processing bad data analysis phase [3]. Classical PSSE rely on chi-squared testing for bad data detection and the normalized residual test for identification [1]. Nevertheless, the WLS model fails to consider the masked component of the error, which was addressed in [4]. For False Data Injections (FDI), [5] developed a correction model built on top of the classical WLS-based SE.

Beyond measurement issues, parameter errors can also result from malicious modifications to the parameter model, whether through malware introduced via trusted software or through exploited vulnerabilities in third-party hardware, as noted in [6]. Furthermore, [7] presented analytical proofs and properties on how parameter model errors spread through the measurement function, and [8] proposed a per-phase model for parameter error correction. A complementary approach is found in [9], which suggested a correction model to mitigate the effects of unbalanced parameter errors on the measurement model. Although, a key limitation of the model in [9] is that it neglects the influence of parameter error during the two-step SE process described in [10]. As a result, the model may require an unnecessarily high number of iterations and, sometimes, can converge to physically incorrect solutions, since it performs correction without considering the potential parameter error effect.

Toward overcoming the mentioned limitation, this work presents a parameter correction model that explicitly incorporates the effect of the parameter error into the measurement model during the correction phase. The proposed model is

validated using the 9-bus IEEE test system and compared with results from the one presented in [9] under different cyber-attack scenarios. Results demostrate a significant reduction in the number of iterations required to converge and achieve statistically valid parameter estimations. The remainder of this paper is presented as follows: Section II presents a theoretical review on false-data correction modeling. Section III details the proposed parameter correction model. Section IV outlines the case study. Final conclusions are presented in Section V.

II. 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 R^m. The solution of (2) is typically obtained by using the Newton-Raphson method.

Linearizing (1) via a first-order Taylor series expansion gives the following:

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

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 [10], it was 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, [9] presented a parameter correction model.

The conjugate of the complex power flow (S_{km}) is expressed in (5).

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

where $k = 1, \ldots, n$ and n is the number of buses in the system, m is the bus adjacent to the bus k, y_{km} is the line admittance, b^{sh}_{km} is the shunt susceptance between buses k and m, and V and θ are the magnitude and angle of the voltage at a given bus.

From the real and imaginary components of the aforementioned equation, the expressions for active (P_{km}) and reactive (Q_{km}) power flows can be derived as follows.

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

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

where g_{km} and b_{km} are the conductance and the susceptance, respectively, between buses k and m.

The active power loss ($P_{km(loss)}$) is defined as the sum of the active power at both ends, it can be expressed as (8).

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

As presented in [9], the power flow equations can be arranged in matrix format and by applying a Taylor series expansion, the parameter correction model relates the identified measurement with error to the parameter errors, as shown in (9).

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

where τ is given by (10), and n represents the iteration at which the estimated values are used.

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

Deviations between the true values of the line parameters and those used in their parameter model may arise from intentional cyber-physical attacks or modeling inaccuracies. These discrepancies often appear as unbalanced parameter errors, as described 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.

It is important to emphasize, however, that the estimated state variables are derived from measurements without errors. Toward solving this, the next section presents a parameter correction model that explicitly accounts for the propagation of parameter errors within the measurement model.

III. Parameter Correction Model

The parameter correction model presented by [9] fails to model the effect of parameter errors within the measurement model. A critical consideration is that parameter errors do not only affect the set of measurements associated with the attacked line parameter. As highlighted in [10], the interconnected nature of power system equations causes such errors to propagate to other measurements that are functionally linked to the affected state variables. For instance, a conductance term g_{km} may be present in multiple measurement model equations. This propagation effect can significantly magnify the impact of the original error, potentially compromising the stability and accuracy of the state estimation process if not properly mitigated. As a result, the measurement model in (1) neglects the contribution of parameter errors and can lead to multiple unnecessary iterations and/or convergence to a physically incorrect solution. To overcome this limitation, the model is extended to include an additional error term, e_ρ, as shown in (12).

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

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.

Gross errors in measurements can be effectively identified using the *largest normalized error test* as demonstrated by [10]. When a gross error is added to a measurement z_i, such that $z_i^{new} = z_i + b_i\sigma_i$ (with b_i as the gross error scalar and σ_i the standard deviation), the Normalized Composed Measurement Error (CME^N) increases, clearly identifying the measurement with gross error. This result can be extended to include an additional unbalanced parameter error, e_ρ, giving $z_i^{new} = z_i + b_i\sigma_i + e_\rho$. Even in this case, CME^N remains effective in isolating the affected set of measurements.

Once an unbalanced parameter error and its corresponding affected set of measurements have been identified, a localized parameter correction strategy can be applied. Unlike previous methods that augment the state vector by introducing additional variables (i.e. $X = \{x\} \rightarrow X' = \{x, \rho\}$), the approach presented in this work retains the original dimensionality and focuses exclusively on correcting the line parameters associated with the measurements with the highest error in the descending CME^N list. Therefore, the parameter error is incorporated in the corresponding equation $h^n(\hat{x})$. Consequently, the power flow equations (6)-(8) are adjusted as shown in (13)-(15), and the updated equations are used in the correction step (9).

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

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

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

To ensure accurate and efficient correction of unbalanced parameter errors, it is essential to update the state variables after each correction step. As previously discussed, parameter errors can propagate across the system through the estimated state variables, affecting measurements beyond the initially compromised data. Therefore, rerunning the state estimator after every adjustment to the parameter model is critical for capturing the updated system dynamics. This iterative and localized correction process enhances the overall efficiency by concentrating on the specific measurements and line parameters most impacted by the error. As a result, it promotes faster convergence and yields more reliable state estimates. To systematically implement this approach, the procedure illustrated in Fig. 1 is proposed.

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 [10], 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 CME^N. 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 [10], 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 [10].

IV. Case Study

The 9-bus test system available in [11] was used to evaluate both the framework proposed by [9] and the one presented in this paper under the presence of single and simultaneous FDI. In the case of single FDI, an unbalanced parameter error was introduced in one of the lines. For the simultaneous FDI, an unbalanced parameter error and a measurement error were applied to different elements of the system. Finally, a value of 3.0 was used as threshold (β).

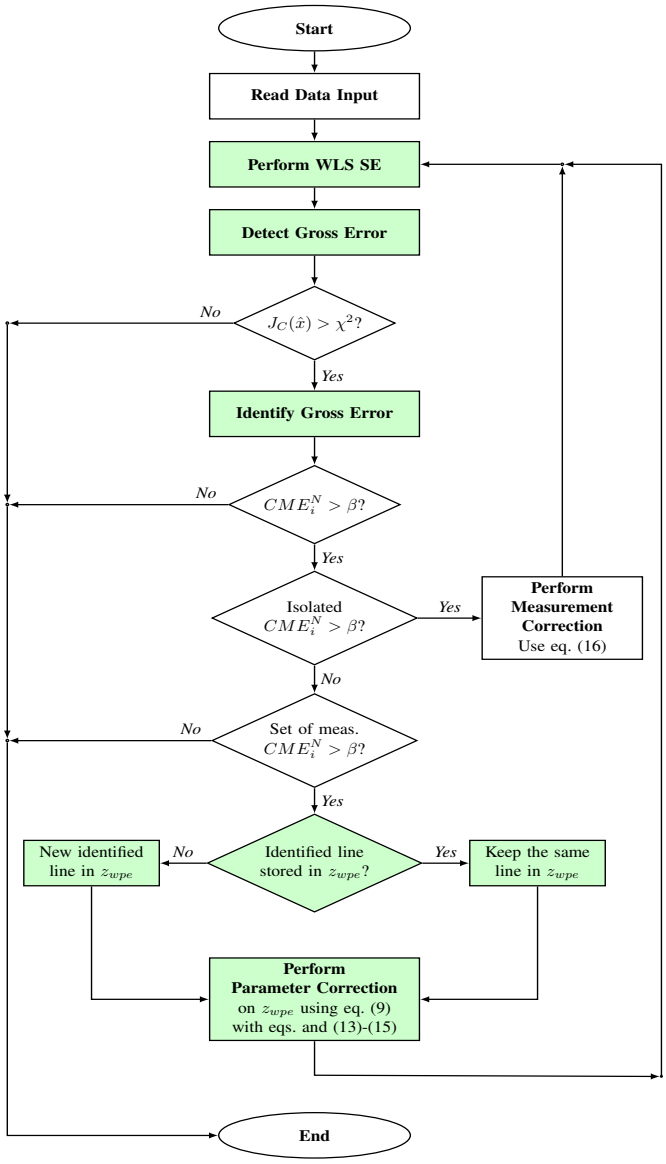

Fig. 1. Simultaneous FDI detection, identification, and correction flowchart.

In the case of a single FDI, the element under attack was $Line_{46}$, with the following unbalanced parameter error of: g decreased by 5.3%, while b and b^{sh} increased by 7.0% and 6.8%, respectively. Table I presents the results obtained from the detection and identification analysis of the first WLS results. As expected, an attack was detected after applying the χ^2 test; moreover, in the descending $|CME^N|$ list, two measurements associated with the attacked element are identified with the highest value. Notably, the error in parameter b significantly influenced the estimated measurement Q_{64}.

The performance of [9] is shown in Fig. 2, where it does not converge. As discussed previously, neglecting the measurement errors $e_{\rho P_{km}}$ and $e_{\rho Q_{km}}$ in the correction procedure can lead to suboptimal performance and (9) may not always yield accurate results.

TABLE I
SE WITH SINGLE FDI. FIRST STEP - $GRL = 2.8$

Type of error:	**Parameter error**		
Element:	$Line_{46}$		
Error:	$g = -5.3\%$	$b = +7.0\%$	$b^{sh} = +6.8\%$
Detection			
χ^2 test:	$J_C(\hat{x}) = 458.3 > \chi^2 = 70.2$ Attack detected!		
Identification			
Measurement with $\lvert CME^N \rvert > 3.0$	II	CME^N	CNE
Q_{64}	3.52	12.89	6.69
Q_{46}	0.07	11.34	79.96
Q_{75}	0.51	7.21	7.90
Q_6	2.40	5.43	2.94
Q_{69}	1.08	4.61	3.15

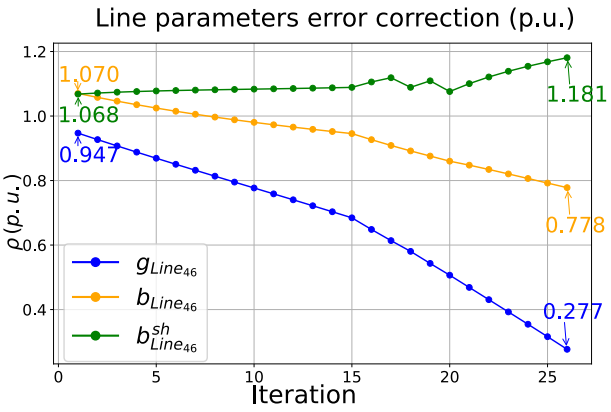

Fig. 2. Performance of the parameter error correction using [9] framework.

When the proposed framework is applied, convergence is achieved after nine iterations with a maximum error of 2.9% in $g_{\text{Line}_{46}}$, as shown in Fig.3. In each iteration, Step 2 of the framework updates the state variables, and the χ^2 test is subsequently applied to evaluate whether the cost function $J_C(\hat{x})$ falls below β. Once this condition is satisfied, the convergence criterion is satisfied. The corresponding results are summarized in Table II. Afterward, the algorithm proceeds to Step 8 using the most recently updated line parameters.

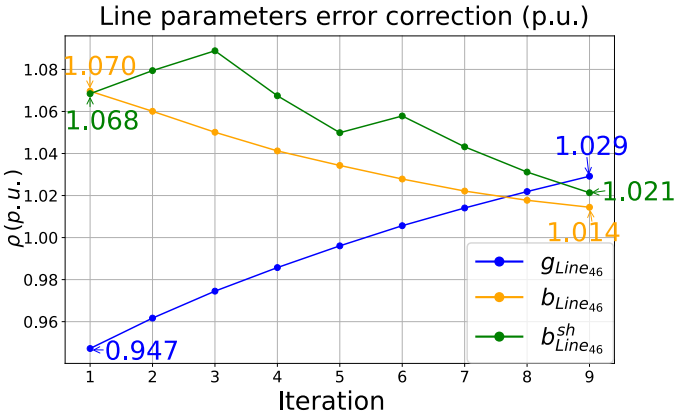

Fig. 3. Performance of the parameter error correction by using framework proposed during a single FDI.

TABLE II
SE WITH SINGLE FDI AFTER CORRECTION. FIRST STEP - $GRL = 2.8$

Type of error:	**Parameter error**
Element:	$Line_{46}$
Error:	$g = -5.3\%$ $b = +7.0\%$ $b^{sh} = +6.8\%$
Detection	
χ^2 test:	$J_C(\hat{x}) = 33.2 < \chi^2 = 70.2$ No attack detected

For a simultaneous FDI involving both parameter and measurement errors, Table III illustrates the errors introduced in $Line_{46}$ and measurement P_{93}, as well as how the detection step flags a gross error in the estimated state variables through CME^N. Consequently, the first two measurements in the descending list were identified as related to line $Line_{46}$. Based on this, the parameter error correction, corresponding to Step 6 of the prorposed framework, is performed.

TABLE III
SE WITH SIMULTANEOUS FDIS. FIRST STEP - $GRL = 2.8$

Type of error:	**Parameter & Measurement error**		
Parameter error			
Element:	$Line_{46}$		
Error:	$g = +7.1\%$	$b = +8.7\%$	$b^{sh} = +6.7\%$
Measurement error			
Element:	P_{93}		
Error:	$k_{ge} = 9\sigma_{93}$		
Detection			
χ^2 test:	$J_C(\hat{x}) = 552.86 > \chi^2 = 70.12$ Attack detected!		
Identification			
Measurement with $\lvert CME^N \rvert > 3.0$	II	CME^N	CNE
Q_{64}	3.53	12.74	6.61
Q_{46}	0.07	12.17	85.72
P_{93}	1.42	7.37	4.72
Q_{75}	0.51	7.02	7.72
Q_6	2.40	5.99	3.24

On one hand, Fig. 4 illustrates the performance of the framework proposed by [9], which continues to exhibit convergence issues. On the other hand, in Fig. 5 can be seen a smooth parameter error correction, with the final parameters converging within a range of $\pm 1.45\%$ after eight iterations.

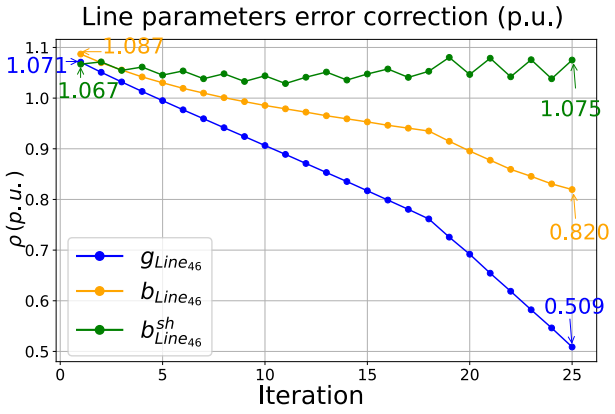

Fig. 4. Performance of the parameter error correction using [9] framework while a simultaneous FDI.

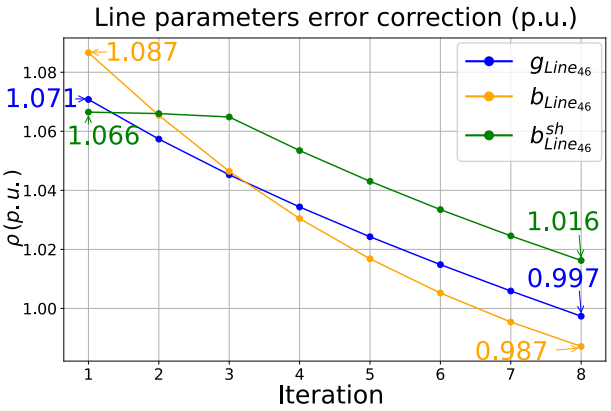

Fig. 5. Performance of the parameter error correction by using framework proposed while a simultaneous FDI.

After the parameter error correction, the χ^2 test is applied, followed by the creation of a new descending $|CME|^N$ list. As shown in Table IV, measurements related to $Line_{46}$ no longer have CME^N values exceeding β. However, in this updated list, the CME^N value of measurement P_{93} surpasses the threshold as an isolated case. Consequently, Step 5 of the framework proposed is performed.

TABLE IV
SE WITH SIMULTANEOUS FDIS AFTER PARAMETER ERROR CORRECTION. FIRST STEP - $GRL = 2.8$

Type of error:	**Parameter & Measurement error**		
Parameter error			
Element:	$Line_{46}$		
Error:	$g = +7.1\%$	$b = +8.7\%$	$b^{sh} = +6.7\%$
Measurement error			
Element:	P_{93}		
Error:	$k_{ge} = 9\sigma_{93}$		
Detection			
χ^2 test:	$J_C(\hat{x}) = 104.82 > \chi^2 = 70.12$ Attack detected!		
Identification			
Measurement with $\lvert CME^N \rvert > 3.0$	II	CME^N	CNE
P_{93}	1.42	7.40	4.73
P_{39}	1.52	3.74	2.23
P_3	1.52	3.46	2.07

Finally, the same stopping procedure is applied, in which another χ^2 test is performed. The results, shown in Table V, indicate that the value of $J_C(\hat{x})$ falls below the expected threshold. Once this condition is satisfied, the framework proceeds to Step 8, using the last updated parameters.

TABLE V
SE WITH SIMULTANEOUS FDIS AFTER MEASUREMENT ERROR CORRECTION. FIRST STEP - $GRL = 2.8$

Type of error:	**Parameter & Measurement error**		
Parameter error			
Element:	$Line_{46}$		
Error:	$g = +7.1\%$	$b = +8.7\%$	$b^{sh} = +6.7\%$
Measurement error			
Element:	P_{93}		
Error:	$k_{ge} = 9\sigma_{93}$		
Detection			
χ^2 test:	$J_C(\hat{x}) = 40.83 < \chi^2 = 70.12$ No attack detected		

The tests of the presented framework, shown in Fig. 1, were successful in effectively detecting, identifying, and correcting simultaneous FDI when simultaneous attacks were introduced. The most significant improvement comes from the incorporation of the parameter error effect, $e_{\rho P_{km}}$, during the correction process, using the state variable vector obtained from the WLS estimation. With this enhancement, the framework achieves faster convergence in fewer iterations, whereas the approach proposed by [9] fails to achieve accurate results under the same conditions. This is evident in the corresponding figures and the χ^2 test, where the corrections made by the proposed framework result in a $J_C(\hat{x})$ value below the expected threshold.

Although the proposed framework demonstrates strong performance, a notable limitation remains: it relies on sequential correction. This was observed in the simultaneous attack scenario, where the unbalanced parameter error was corrected first, followed by the measurement error. Future research should explore optimization strategies to avoid sequential executions of the state estimator during corrections, thereby improving computational efficiency. Furthermore, under real-world conditions, on-field testing using medium-voltage radial networks is recommended to assess the accuracy and robustness of the proposed framework. Such testing would not only validate its practical applicability, but would also reveal potential areas for further refinement.

V. Conclusion

This work presents a novel framework and model for parameter correction in real-time monitoring in distribution networks. Unlike current state-of-the-art approaches, which do not consider the impact of parameter errors on the measurement model, the proposed model explicitly incorporates this effect. Neglecting it can lead to an increased number of iterations and, in some cases, convergence to physically incorrect solutions. By embedding the parameter error within the measurement model, the proposed framework enhances both the robustness and accuracy of the correction process. A case study considering the 9-bus test system is further presented, highlighting the mitigated modeling error effect the parameter error correction model has. Easy-to-implement model, without hard-to-design parameters, built on the classical WLS solution, highlight potential aspects for real-life applications, particularly in medium-voltage radial networks. Future works will focus on developing a simultaneous optimization strategy to jointly address measurement and unbalanced parameter errors.

Acknowledgment

The authors appreciate the support from the US Department of Energy (DoE), Office of Cybersecurity, Energy Security, and Emergency Response (DOE-CESER), and Sandia National Laboratories for funding part of this research. Sandia National Laboratories is a multimission laboratory managed and operated by National Technology Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

References

[1] Arturo S. Bretas, Newton G. Bretas, Joao B.A. London, and Breno E.B. Carvalho. Chapter 7 - the innovation methodology for error analysis in power systems. In Arturo S. Bretas, Newton G. Bretas, Joao B.A. London, and Breno E.B. Carvalho, editors, *Cyber-Physical Power Systems State Estimation*, pages 183–210. Elsevier, 2021.

[2] Rodrigo D. Trevizan, Cody Ruben, Aquiles Rossoni, Surya C. Dhulipala, Arturo Bretas, and Newton G. Bretas. 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] Milad Beikbabaei, Ali Mehrizi-Sani, and Chen-Ching Liu. State-of-the-art of cybersecurity in the power system: Simulation, detection, mitigation, and research gaps. *IET Generation, Transmission & Distribution*, 19(1):e70006, 2025.

[7] Arturo S. Bretas, Newton G. Bretas, and Breno E.B. 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.

[8] A.S. Bretas, N.G. Bretas, S.H. Braunstein, A. Rossoni, and R.D. 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.

[9] 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.

[10] 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.

[11] Vijay Vittal, James D McCalley, Paul M Anderson, and AA Fouad. *Power system control and stability*. John Wiley & Sons, 2019.