Malicious data injection attacks: A relaxed physics model based strategy for real-time monitoring

Tierui Zou, Arturo Suman Bretas, Nader Aljohani
Department of Electrical and Computer Engineering
University of Florida
Gainesville, FL
tieruizou@ufl.edu, arturo@ece.ufl.edu, nzjohani@taibahu.edu.sa

Newton Geraldo Bretas
Department of Electrical and Computer Engineering
University of Sao Paulo
Sao Carlos, SP
ngbretas@sc.usp.br

***Abstract*—With the rapid advances in the infrastructure of power networks, modern power systems have become vulnerable to cyber-attacks. An attacker can mislead the operators in power system control centers by introducing malicious data that affect the outputs of the state estimator which turn disrupts in the operation and control functions of many power system applications. Hence, an accurate and fast algorithm for detecting, identifying and correcting malicious data injection attacks is crucial to prevent catastrophic failures in power systems. This paper presents further contributions to power system real-time monitoring in the presence of a malicious data injection attacks. State of the art solutions consider either measurement or parameter is free of error when estimating the state variables, such as complex voltages. However, malicious data in measurements and parameters can be injected simultaneously and such assumption does not provide an accurate solution. In this work, a relaxed model strategy is proposed to handle such simultaneous data attack. The framework of measurement gross error analysis is deployed in processing and analyzing attacks. Chi-square χ^2 Hypothesis Testing applied to the normalized composed measurement error (CME^N) is considered for detecting cyber-attacks. The property of largest normalized error test is used for identifying malicious data injection. The correction of cyber-attack considers the type of attack and the composed normalized error (CNE) in a relaxed model strategy that takes into account the effect of the measurement in error when correcting the attacked parameter. The proposed model is validated on IEEE 14-bus system.**

***Index Terms*—Smart grid, malicious data injection, state estimation, parameter error, weighted least square**

I. Introduction

The control and operation of modern power systems are becoming more complex due to the advancements in sensors and communication networks. The gradual developments in the power system's infrastructure enhances the automation level which in turn results in a reliable electricity supply. However, the underlying cyber-systems, which support the reliability of supplied power, need to have countermeasures against the pervasive application of information technologies in order to ensure the safety and economy of power system operations.

Cyber physical security of power systems has become a crucial concern for the future of real-time operation. State estimation in the control center is of utmost importance to be protected against cyber-attacks. In fact, an inaccurate state estimator solution cannot operate with the new cyber physical security demands for real-time system operation. Such estimator can lead to convergence issues which was considered as one of the several factors that lead to the catastrophic failures of the 2003 Northeast blackout in the U.S [1]. Therefore, continuous development of power systems state estimators is vital to keep the grid operation secure. This paper pertains to the development of state estimation in regards to a defense strategy against false data injection attacks.

In the paper by Liu [2] ,it is shown that it is possible for a hacker to inject malicious data in Weighted Least Squares (WLS) state estimation and not become detected by classical residual based gross analysis solutions. In [3], an algorithm is proposed to strategically allocate secure phasor measurement units (PMUs) at key buses in the network to defend against false data injection attacks on measurements. In [4], an algorithm which is based on monitoring variance in equivalent impedance of transmission line is developed to face the problem of how to detect and allocate manipulation attacks in PMU data. In [5], the cyber-attack tests from the perspective of the attackers is considered. A schematic explanation of how cyber-attack analysis works in power system state estimation and algorithm to solve security problems in state estimation are addressed in [6].

However, [7], [8] and the aforementioned papers considered only the manipulation data attacks through the measurement residual analytics which is only one component of the error as demonstrated in [9]–[11]. In previous work by Bretas [11], authors proposed the concept of Innovation Index and presented a new algorithm to test malicious injection data in measurements which have significant effects on state estimation. In this method, one can find the masked error, undetectable error, in the Jacobian range space which is not reflected through the residual. Malicious attacks on static data in topology, i.e. the network parameters, is another source of concern in state estimation. The work in [12], [13] investigated the presence of cyber-attacks in the topology of grid network. [13] presented a relaxed model to correct measurements and parameters that are being attacked simultaneously. One can see that parameter errors can be accurately corrected via the relaxed model in [13]

The research reported here was partially supported by the National Science Foundation under grant's ECCS 1646229 and 1809739

978-1-7281-0407-2/19/$31.00 ©2019 IEEE

if enough iterations are performed for the correction process.

In this paper, a new contribution to the relaxed model proposed in [13] is presented. Specifically, the relaxed model in [13] does not consider the effect of the measurement in error when correcting the attacked parameter. This may lead to necessary high iterations number for convergence. The presented model incorporates such effect. Since the relaxed model is an iterative based solution, the number of operations for correcting the errors in measurements and/or parameters can be thus greatly reduced. In the power system industry, the process of state estimation usually takes 3 to 10 seconds to converge. Further, state estimation is reported to run as fast as every 10 seconds. Thus, if one would consider simultaneous malicious data attacks, the necessary time for convergence would logically increase, creating an upper bound limit for state estimation runs. Therefore, a faster solution is vital for cyber secure real-time monitoring. Validation is carried out using the IEEE 14-bus system. The case study shows that by using the presented model, one can reach the accurate solution faster than the state of the art [13].

The remainder of this paper is organized as follows. Section II presents a summary of the state estimation with Innovation Index. Section III presents the relaxed model strategy for correcting simultaneous attacks on measurements and parameters. A case study and test results discussion are presented in section IV. The conclusion of this work is presented in Section V.

II. State estimation with Innovation Index

The power system with n buses and m measurements is modeled as a set of non-linear algebraic equations as follow [14]:

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

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

Weighted least squares is a classical state estimator that search for the best estimates of the states x of the well-known problem that minimizes the cost function as follow:

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

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

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

where $H = \frac{\partial h}{\partial x}$ is the Jacobian matrix of h calculated at the point x^*. $\triangle z = z - h(x^*) = z - z^*$ and $\triangle x = x - x^*$ are the correction of measurement and state vector respectively. Under observability condition for the system in (3), i.e $rank(H) = N$, the vector space of measurements can be decomposed into two sub-spaces that are orthogonal to each other as follow:

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

where $\Re(H)$ is the range space of H and it is a N dimensional sub-space vector that belongs to $\mathbb{R}^m$ while $\Re(H)^{\perp}$ is the orthogonal complement.

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

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

Solving (5) for $\triangle \hat{x}$, one can obtain the following:

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

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

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

The geometrical position of the measurement error in relation to the range space of H provides another way of interpreting the state estimation. Hence, as the measurements' vector can be decomposed into two subspaces as in (4), it is possible to decompose the measurement error vector into two components as follow:

$$e = \underbrace{Ke}_{e_U} + \underbrace{(I - K)e}_{e_D} \tag{8}$$

The component e_D is the detectable error which is the residual in the classical model while the component e_U is the undetectable error. e_D is in the orthogonal space to the range space of Jacobian whereas e_U is hidden in the Jacobian space.

$$\|e\|^2 = \|e_D\|^2 + \|e_U\|^2 \tag{9}$$

The error vector in (9) is called Composed Measurement Error (CME). In order to quantify the undetectable error, the Innovation Index (II) is introduced [10] and is presented in the following:

$$II_i = \frac{\left\|e^i_D\right\|}{\left\|e^i_U\right\|} = \frac{\sqrt{1 - k_{ii}}}{\sqrt{k_{ii}}} \tag{10}$$

Low Innovation index means there is a large component of error that is not reflected from residual. Therefore, the residual will be very small even if there is a gross error. By using (9) and (10), the composed measurement error can be expressed in terms of the residual and the innovation index as follow:

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

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

$$CNE_i = r_i^N \left(\sqrt{1 + \frac{1}{{II_i}^2}} \right) \tag{12}$$

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

$$CME_i^N = \frac{r_i}{\sigma_i} \left(\sqrt{1 + \frac{1}{{II_i}^2}} \right) \tag{13}$$

where σ_i is the standard deviation for measurement i.

III. Relaxed Model Strategy

It is believed that an attacker can introduce data in the state estimator through measurements or network parameters. Meanwhile, malicious data can be injected simultaneously in measurements as well as the parameters of the grid model. The work in [13] proposed a methodology to deal with such attack. The method relaxes the model of the simultaneous attacks to measurements and parameters by considering initially that measurements are without errors. Then, one can estimate the system state, x^n, considering p^n, through the iterative solution of the the model $z^n = h(x^n)$. After convergence, an estimate of the corrected parameters p^{n+1} are obtained through the Taylor series expansion of the model $z^n = h(x^n, p^n)$.The obtained estimated parameters, p^{n+1}, which are considered to be without errors, are used in the state estimation to estimate the new states x^{n+1}, and then a new measurements z^{n+1} are obtained through the correction of the measurements in errors using their CNE. From the new measurements, z^{n+1}, and the new states x^{n+1}, a new set of parameters p^{n+2} can be estimated through the Taylor series expansion of the model $z^{n+1} = h(x^{n+1}, p^{n+1})$. The process continues until a convergence is achieved.

Since the relaxed model is solved iteratively, normally it takes several iterations to correct the parameter in error to reach an accurate value (1% approximation error). However, an extra step in correcting the parameter will cost several iterations to reach convergence. Therefore, a faster solution will be reached if the effect of the parameters in error to the estimated measurement values is considered in the correction process of attacked parameters. Hence, the extended relaxed model in this paper considers such effect in which the number of operations for correcting parameters is reduced. To illustrate the effect of parameter errors in the measurement correction, consider the residual vector in its normalized form to be as follow:

$$r^N = \frac{r}{\sqrt{SR}} \tag{14}$$

where S is the sensitivity matrix and is given by the following expression:

$$S = I - K \tag{15}$$

where K is the projection matrix as in (7). By substituting (15) for measurement i into (14), and using the result of the substitution with the equation (10) into (12), one can write the composed normalized error for measurement i to be as follow:

$$CNE_i = \frac{r_i}{(1 - k_{ii})\sigma_i} = \frac{z_i - h_i(x, p)}{(1 - k_{ii})\sigma_i} \tag{16}$$

By expanding the model $z_i = h_i(x, p)$ using Taylor series expansion, one can get the following:

$$z_i = h_{i,0} + \frac{\partial h_i(x, p)}{\partial p} \triangle p \tag{17}$$

where $\triangle p$ is the parameter error. From (17), the parameter error can be calculated to be as follow:

$$\triangle p = \frac{z_i - h_{i,0}}{H_{p,0}} \tag{18}$$

where $H_{p,0}$ is the Jacobian of parameters. It is important to note that the quantities in (18) are all known. By using the model in (17) for the residual into (16), the composed normalized error for measurement i can be written in the following form:

$$CNE_i = \frac{z_i - [h_i(x) + \frac{\partial h_i(x,p)}{\partial p} \triangle p]}{(1 - k_{ii})\sigma_i} \tag{19}$$

where $\triangle p$ is the parameter error calculated through Taylor series. Since CNE is used for correcting measurements in error, one can see through (19) that the total effect of the parameter on measurement is:

$$\text{Total Effect} = \frac{\frac{\partial h_i(x,p)}{\partial p} \triangle p}{(1 - k_{ii})\sigma_i} \tag{20}$$

If Total Effect in (20) is normalized, then one can get the coefficient of masked error in the parameter correction to be:

$$\text{Coefficient of masked error} = \frac{(\frac{-k_{ii}}{1-k_{ii}})}{(\frac{1}{1-k_{ii}})} = -k_{ii} \tag{21}$$

Through this coefficient and (8), (10) and (12), one can get the deviation of h caused by the parameter in error to be as follow:

$$\triangle h = \frac{(\triangle p)\sigma_i}{-k_{ii}} \tag{22}$$

Then, one can calculate the masked parameter error through the projection from $\triangle h$ to $\triangle p$ by using (17):

$$\triangle \triangle p = \frac{\triangle p \sigma}{-k_{ii} H_{p,0}} \tag{23}$$

Therefore, the total correction is:

$$CPE = \triangle \triangle p + \triangle p \tag{24}$$

where CPE is Composed Parameter Error. Therefore, if the attacked parameters are corrected considering CPE in (24) rather than $\triangle p$ alone [13], a faster solution can be reached.

Errors can be injected into measurements and/or parameters. In the case of a measurement cyber-attack, the correction of

the erroneous measurement value is performed by applying the following equation:

$$z_i^C = z_i^E - CNE_i\sigma_i \tag{25}$$

where z_i^C is the corrected measurement, z_i^E is the measurement with error, CNE_i is the one that is obtained using (12), and σ_i is the standard deviation of the measurement. However, if the attack is characterized as a parameter attack, then the affected parameter is corrected first using equation (18) and then a second correction is performed using equation (24) in order to take into account the effect of the attacked parameters on measurements. If measurements and parameters are free of errors, then no attack is present. Hence, the detection routine will not flag. The flowchart of the presented algorithm is shown in Fig. 1.

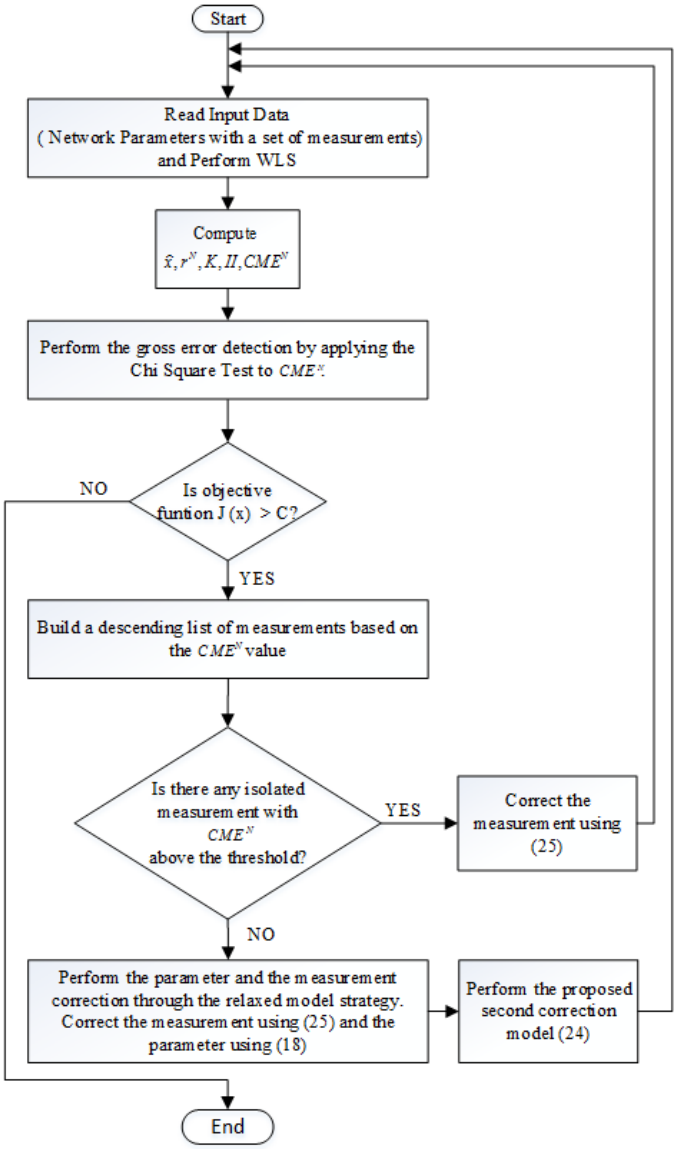

Fig. 1. The flowchart of the algorithm

IV. Case Study

The proposed methodology is validated using the IEEE 14-bus system. In this paper, a set of 107 measurements obtained from MATPOWER [15] are considered, which lead to the GRL (Global Redundancy Level) of 3.96. The system topology and parameters are found in [16]. For the next tables, the following nomenclature is used: $P:a$, $Q:a$ are real and reactive power injection at bus a respectively; $P:a-b$, $Q:a-b$ are real and reactive power flow from bus a to bus b respectively; g_{a-b} the series conductance of the line between bus a and bus b; b_{a-b} and b_{a-b}^{sh} are the series and shunt susceptance of the line between bus a and bus b respectively. In the following, two scenarios of malicious data attacks are presented.

A. Attack Scenario I

In this scenario, a cyber-attack is simulated by adding (-10%) to the series and shunt parameter of the line $06-13$. The data base values of g_{06-13}, b_{06-13} and b_{06-13}^{sh} are 3.0989, -6.1028 and 0 respectively. The results are presented in TABLE I. From TABLE I, one can see that the objective function $J(x)$ is 567.3243 ,which is higher than C ,the value that is obtained from χ^2 distribution using $df = m = 107$ and confidence probability level of 0.95. Therefore, the attack is detected through the Chi square test. For identification, the list of the composed measurement error in normalized form, i.e. CME^N, for all measurements is obtained in a descending order based on their absolute values. Considering space limitations, only part of the CME^N list is presented, which is the part of interest. One can see from the list that the CME^N absolute value of Q_{13} is above the threshold value (β=3) and is the largest among other suspicious measurements. At the same time, the other measurements related to the line $06-13$, i.e $P_{13}, P_{06-13}, Q_{06-13}$ and P_{06}, are also above the threshold value β. Therefore, this situation characterizes a parameter cyber-attack in the line $06-13$ since the error is spread out on the function $h(x)$. For the correction process, the suspicious parameters of this line were corrected in two ways :

1) Using $\triangle p$ in relaxed model strategy [13].
2) Using CPE as presented in (24).

For comparison purposes, the corrected values of the parameters in error using the relaxed model strategy in [13], named as (method 1) for reference, are presented in TABLE II while TABLE III presents the corrected values using the presented model, named as (method 2). By inspecting the corrected values of the suspicious parameters in each time step of the correction process, the presented model, method 2, obtained more accurate correction than the one obtained from method 1. In other words, method 2 resulted in a 0.0540% approximation error, after second correction, while method 1 obtained 0.1258% approximation error in the third correction step. One can conclude that a faster and at the same time more accurate solution is obtained using the presented model in this paper.

TABLE I
PROCESSING CYBER-ATTACKS

Processing Measurement Cyber-Attack Step 1			
J(x) = 567.3243 > C = 132.14 Attack Detected!			
CME^N Descending List			
Measurement	**II**	**CME^N**	**CNE**
$Q:13$	0.8397	10.2908	16.0026
$P:06$	1.2717	9.0702	15.0637
$Q:06-13$	3.8199	8.1708	8.4461
$P:06-13$	3.7055	7.8430	8.1236
$P:05$	0.1791	5.0185	28.4605
$P:13$	1.7892	4.1095	4.7079
$P:06-12$	2.7976	-3.0920	-3.2836

TABLE II
CORRECTED PARAMETERS USING THE MODEL IN [13]

Parameter	**Parameter correction**		
	First correction (Approx. error %)	***Second correction (Approx. error %)***	***Third correction (Approx. error %)***
g_{06-13}	3.0277 (2.2975 %)	3.0820 (0.5456 %)	3.0950 (0.1258 %)
b_{06-13}	-5.9625 (2.2975 %)	-6.0695 (0.5456 %)	-6.0951 (0.1258 %)
b^{sh}_{06-13}	0	0	0

TABLE III
CORRECTED PARAMETERS USING THE PRESENTED MODEL

Parameter	**Parameter correction**		
	First correction (Approx. error %)	***Second correction (Approx. error %)***	***Third correction (Approx. error %)***
g_{06-13}	3.1369 (1.2256 %)	3.0937 (0.0540 %)	3.0993 (0.0098 %)
b_{06-13}	-6.0341 (1.2256 %)	-6.0995 (0.0540 %)	-6.1034 (0.0098 %)
b^{sh}_{06-13}	0	0	0

B. Attack Scenario II

For this scenario, a cyber-attack is simulated by adding (-20%) to the series and shunt parameter of Line $03-04$.A cyber-attack of magnitude 5 σ is added to the measurement of the real power flow between bus 7 and bus 8, i.e, $P: 07-09 = 0.2808$. The data base values of g_{03-04}, b_{03-04} and b^{sh}_{03-04} are 1.9860, -5.0688 and 0.0064 respectively. The result of this case is shown in TABLE IV. For attack detection, one can see that objective function $J(x)$ is 918.7029, which is higher than the threshold value C. Thus, a data attack in the system is detected. For identification, a descending list of the CME^N for all measurements is tabulated. Several measurements related to line $03-04$ have an absolute value of CME^N above the threshold value β, which again characterizes a parameter cyber-attack. In the correction stage, the parameters of the suspicious line are corrected using the same methods as presented in scenario I.

For comparison, the results using method 1 is presented in TABLE V whereas the ones using method 2 is shown in TABLE VI. A 20% error is a very high-value parameter cyber-attack. However, the purpose is to show the advantage of the presented method. From TABLE V, the error in the parameter after three operations of correction which means 30 iterations is still 1.1501%. However, the presented model, which obtained the results in TABLE VI, requires only 2 operations of correction to get nearly the same results as method 1. If the proposed method is extended for 3 times correction as method 1 by changing the convergence criteria, the approximation would be below 0.01%.

TABLE IV
PROCESSING CYBER-ATTACKS

Processing Measurement Cyber-Attack Step 1			
J(x) = 918.7029 > C = 132.14 Attack Detected!			
CME^N Descending List			
Measurement	**II**	**CME^N**	**CNE**
$P:03-04$	1.6150	12.4870	14.6870
$Q:03-04$	2.1491	12.2349	13.4836
$P:04-03$	2.0175	8.8496	9.8770
$Q:02-03$	0.9564	6.7753	9.8025
$Q:04$	0.4162	-6.6930	-17.4168
$Q:04-03$	3.2032	-4.2339	-4.4354
$P:07-09$	1.7252	4.4202	5.1091
$P:04$	1.2461	4.0893	5.2432

TABLE V
CORRECTED PARAMETERS USING THE MODEL IN [13]

Parameter	**Parameter correction**		
	First correction (Approx. error %)	***Second correction (Approx. error %)***	***Third correction (Approx. error %)***
g_{03-04}	2.1452 (8.0196 %)	2.0470 (3.0717 %)	2.0088 (1.1501 %)
b_{03-04}	-5.4753 (8.0196 %)	-5.2245 (3.0717 %)	-5.1271 (1.1501 %)
b^{sh}_{03-04}	0.0069 (7.8125 %)	0.0066 (3.1250 %)	0.0065 (1.5625 %)

TABLE VI
CORRECTED PARAMETERS USING THE PRESENTED MODEL

Parameter	**Parameter correction**		
	First correction (Approx. error %)	***Second correction (Approx. error %)***	***Third correction (Approx. error %)***
g_{03-04}	2.1008 (5.7804 %)	2.0149 (1.4551 %)	1.9928 (0.0100 %)
b_{03-04}	-5.3619 (5.7804 %)	-5.1426 (1.4551 %)	-5.0862 (0.0100 %)
b^{sh}_{03-04}	0.0067 (4.6875 %)	0.0065 (1.5625 %)	0.0064 (0 %)

After correcting the parameter in attack using method 2 and re-running the state estimator, another cyber-attack is detected. The result is shown in TABLE VII. As seen, the only CME^N value (absolute value) above the threshold is the real power flow of the line $07-09$. Therefore, the measurement P_{07-09} is in error. The correction of measurements as shown in the flowchart is performed using their CNE values. The approx-

TABLE VII
PROCESSING CYBER-ATTACKS, FIRST STEP.

Processing Measurement Cyber-Attack Step 1			
J(x) = 145.6037 $>$ C = 132.14 Attack Detected!			
CME^N Descending List			
Measurement	**II**	**CME^N**	**CNE**
$P: 07-09$	1.668	4.3327	5.0081

imate error after correction is found to be 0.0769%. After re-running the state estimator again, no CME^N value is found to be above the threshold. Therefore, both the measurement and the parameter in error are corrected.

From scenario I and scenario II, one can see that the presented method is able to detect, identify and correct simultaneous cyber-attacks associated with measurements and parameters. Besides, an accurate correction of errors and faster solution were obtained by using CPE for correcting the parameter in error. In addition to the cases in I and II, several scenarios were simulated and the presented model in this paper, i.e., method 2, on average saves $1/5$ to $1/3$ of operation time compared to the model presented in [13]. In TABLE VIII, statistics for other cases are presented for comparison purposes between the model in [13], method 1, and the presented model in this paper, method 2. As one can see, correcting parameters using CPE in (24) rather than $\triangle p$ in (18) alone requires less operations than the model in [13] while providing a best estimate. For instance, when 20% error is added to the parameters of the line $06-11$, method 2 outperformed method 1, since the approximation error is found to be less than 1% after two operations.

TABLE VIII
OTHER CASES FOR COMPARISON

Line	**Method**	**Parameter Correction**		
		First correction	***Second correction***	***Third correction***
		Approx. error in %	***Approx. error in %***	***Approx. error in %***
$06-11$ (20% error added)	1	5.0707	1.2017	0.2784
	2	3.2119	0.3859	-
$09-10$ (-20% error added)	1	6.6567	2.4427	0.9203
	2	3.5888	0.9194	-
$09-14$ (-20% error added)	1	4.1002	1.1006	0.2277
	2	2.4264	0.4291	-

V. CONCLUSIONS

This paper presented a methodology for malicious data injection attacks detection, identification and correction. It presents a model to the masked parameter error via the effect of parameter error on the measurement. Second time correction equation, i.e equation (24), is proposed to efficiently deal with a malicious cyber-attack on a parameter. In this method, detection for error is based on chi square test of the composed measurement error, identification is based on Generalized Largest Normalized error test, correction of measurement is implemented using composed normalized error, and correction of parameter is based on the relaxed strategy using CPE presented in this paper. The major advantage of the proposed method is that one can save on average $1/5$ to $1/3$ of the time to process the correction stage for parameter in error.

REFERENCES

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

[2] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[3] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326–333, 2011.

[4] S. A. Zonouz, K. M. Rogers, R. Berthier, R. Bobba, W. H. Sanders, and T. J. Overbye, "Scpse: Security-oriented cyber-physical state estimation for power grid critical infrastructures." *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1790–1799, 2012.

[5] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645–658, 2011.

[6] S. Bi and Y. J. A. Zhang, "Graph-based cyber security analysis of state estimation in smart power grid," *IEEE Communications Magazine*, no. 99, pp. 2–9, 2017.

[7] S. Li, Y. Yılmaz, and X. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 2725–2735, 2015.

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

[9] 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," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 2128–2135, 2013.

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

[11] N. G. Bretas and A. 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*, 2018.

[12] A. S. Bretas, N. G. Bretas, B. Carvalho, E. Baeyens, and P. P. Khargonekar, "Smart grids cyber-physical security as a malicious data attack: An innovation approach," *Electric Power Systems Research*, vol. 149, pp. 210–219, 2017.

[13] A. S. Bretas, N. G. Bretas, and B. E. Carvalho, "Further contributions to smart grids cyber-physical security as a malicious data attack: Proof and properties of the parameter error spreading out to the measurements and a relaxed correction model," *International Journal of Electrical Power & Energy Systems*, vol. 104, pp. 43–51, 2019.

[14] A. Monticelli, *State estimation in electric power systems: a generalized approach*. Springer Science & Business Media, 2012.

[15] R. D. Zimmerman, C. E. Murillo-Sánchez, and D. Gan, "Matpower: A matlab power system simulation package," *Manual, Power Systems Engineering Research Center, Ithaca NY*, vol. 1, 1997.

[16] R. Christie, "Power systems test case archive," *Electrical Engineering dept., University of Washington*, 2000.