Electrical Power and Energy Systems 104 (2019) 43–51

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

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

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[a,*], Newton G. Bretas[b], Breno E.B. Carvalho[b]

[a] Department of Electrical & Computer Engineering, University of Florida, Gainesville, FL 32611-6200 USA
[b] Department of Electrical & Computer Engineering, University of Sao Paulo, Sao Carlos, SP 13566-590 Brazil

ARTICLE INFO

Keywords:
Smart grid
Cyber-physical security
Malicious data injection
Weighted least squares
Innovation

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.

1. 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 Fig. 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).

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 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

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

[*] Corresponding author.
E-mail address: arturo@ece.ufl.edu (A.S. Bretas).

https://doi.org/10.1016/j.ijepes.2018.06.039
Received 6 February 2018; Received in revised form 27 April 2018; Accepted 18 June 2018

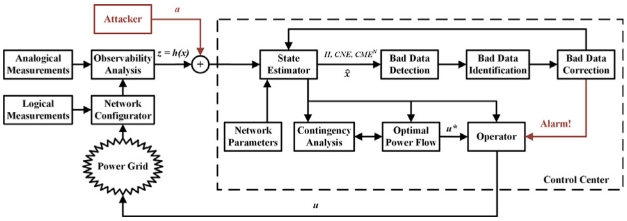

Fig. 1. State estimator under a cyber-attack (adapted from [21]).

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, including [14,15], 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.

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

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 $u, v = u^T R^{-1} v$, 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 subspace 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