UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ENGENHARIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

JULIANA KLAS

ADVANCED APPLICATIONS FOR STATE ESTIMATORS IN SMART GRIDS: IDENTIFICATION, DETECTION AND CORRECTION OF SIMULTANEOUS MEASUREMENT, PARAMETER AND TOPOLOGY CYBER-ATTACKS

Porto Alegre
2018

JULIANA KLAS

ADVANCED APPLICATIONS FOR STATE ESTIMATORS IN SMART GRIDS: IDENTIFICATION, DETECTION AND CORRECTION OF SIMULTANEOUS MEASUREMENT, PARAMETER AND TOPOLOGY CYBER-ATTACKS

Thesis presented to Programa de Pós-Graduação em Engenharia Elétrica of Universidade Federal do Rio Grande do Sul in partial fulfillment of the requirements for the degree of Doctor in Electrical Engineering.
Area: Energy / Power Systems

ADVISOR: Prof. Dr. Arturo S. Bretas

Porto Alegre
2018

JULIANA KLAS

ADVANCED APPLICATIONS FOR STATE ESTIMATORS IN SMART GRIDS: IDENTIFICATION, DETECTION AND CORRECTION OF SIMULTANEOUS MEASUREMENT, PARAMETER AND TOPOLOGY CYBER-ATTACKS

This thesis was considered adequate for the awarding of the degree of Doctor in Electrical Engineering and approved in its final form by the Advisor and the Examination Committee.

Advisor: _____
Prof. Dr. Arturo S. Bretas , PPGEE UFRGS
Doutor pela (Virginia Polytechnic Institute and State University -Blacksburg, EUA)

Examination Committee:

Prof. Dr. Alexandre Sanfelici Bazanella , PPGEE - UFRGS
Doutor pela (UFSC – Florianopolis, Brasil)

Prof. Dr. Eduardo Nobuhiro Asada , PPGEE - EESC - USP
Doutor pela (UNICAMP – Campinas, Brasil)

Prof. Dr. Elizete Maria Lourenço , PPGEE - UFPR
Doutor pela (UFSC – Florianopolis, Brasil)

Prof. Dr. Flávio Antônio Becon Lemos , DELAE - UFRGS
Doutor pela (UFSC – Florianopolis, Brasil)

Prof. Dr. Roberto Chouhy Leborgne , PPGEE - UFRGS
Doutor pela (Chalmers University of Technology – Gothenburg, Suécia)

Coordinator of PPGEE: _____
Prof. Dr. Valner Joao Brusamarello

Porto Alegre, Junho 2018.

DEDICATÓRIA

"O erro da educação é o de ensinar as respostas que a filosofia e a ciência deram, sem deixar claro para os alunos quais eram as perguntas que as motivaram". (Moral e Ética: Dimensões Intelectuais e Afetivas, Yves de La Taille, pp.11).

Dedico este trabalho àqueles que me inspiram a buscar as perguntas.

AGRADECIMENTOS

À Olivia que no crescer diário me faz ver o mundo de outros ângulos.

Ao meu marido, Júlio pelo companheirismo e exemplo de empreendedorismo.

Aos meus pais Regina e Silvio pelo suporte e ajuda incondicional. Aos meus irmãos Leticia e Cristiano pelo carinho e sempre amizade. Aos cunhados e demais familiares pela torcida, agradecimento especial ao Lucas pela sabedoria compartilhada principalmente na reta final. E aos amigos que sempre estão ao meu lado me inspirando e alegrando na caminhada, casal Eliana e Scott meu muito obrigada pela ajuda na revisão final.

Ao Programa de Pós-Graduação em Engenharia Elétrica, PPGEE, pela oportunidade de realização de trabalhos em minha área de pesquisa e pela busca à excelência que inspira objetivos pessoais similares.

Ao meu orientador Prof. Dr. Arturo S. Bretas pelas ideias inovadoras e sempre apoio.

Aos colegas do PPGEE pelo auxílio e troca nas tarefas desenvolvidas durante o curso e aos colegas que conheci na PUCRS, por me acolherem na profissão que escolhi como missão de vida, em especial ao Prof. Dr. Marcos Tello pelo exemplo de profissional e professor na área de sistemas de potência.

À CAPES pela provisão da bolsa de doutorado.

ABSTRACT

Growing demand and concern over climate change are key drivers for renewable sources of electricity and grid modernization. Grid modernization, or the so called smart grid, not only enables renewable sources but also opens the door to new applications with far-reaching impacts such as preventing or restoring outages (self-healing capabilities), and enabling consumers to have greater control over their electricity consumption and to actively participate in the electricity market.

According to the Electric Power Research Institute (EPRI), one of the biggest challenges facing smart grid deployment is related to the cyber security of the systems.

The current cyber-security landscape is characterized by rapidly evolving threats and vulnerabilities that pose challenges for the reliability, security, and resilience of the electricity sector. Power system state estimators (PSSE) are critical tools for grid reliability, under a system observable scenario, they allow power flow optimization and detection of incorrect data.

In this work cyber-attacks are modeled as malicious data injections on system measurements, parameters and topology. The contributions of this work are twofold. First, a model for cyber-attack as a false data injection detection and identification is presented. The presented model considers the minimization of the composed measurement error while applying the Lagrangian relaxation. The presented contribution, enables false data injection attacks detection even if this belongs to the subspace spanned by the columns of the Jacobian matrix and in network areas with low measurement redundancy. Second, state-of-the-art solutions consider correction of parameters or topology when measurements are free of error. However, how may one correct measurements if parameters or topology might be simultaneously in error? To solve this problem, a relaxed model is presented and solved iteratively in a continuous manner. Once identified and detected, cyber-attacks in parameters, topology and measurements are corrected.

The proposed solution is based on a Taylor series relaxed, composed normalized error (CNE) hybrid approach with Lagrange multipliers. Validation is made on the IEEE-14 and IEEE-57 bus systems. Comparative results highlight the proposed methodology's contribution to the current state-of-the-art research on this subject. Providing mitigation, response and system recovery capabilities to the state estimator with reduced computational burden, the proposed model and methodology have strong potential to be integrated into SCADA state estimators for real-world applications.

Keywords: Power Systems, Cyber-security, Smart Grids, State Estimator.

RESUMO

APLICAÇÕES AVANÇADAS EM ESTIMADORES DE ESTADO DE REDES ELÉTRICAS INTELIGENTES: IDENTIFICAÇÃO, DETECÇÃO E CORREÇÃO DE SIMULTÂNEOS ATAQUES CIBERNÉTICOS EM MEDIDAS, PARÂMETROS E TOPOLOGIA.

O aumento da demanda e a preocupação com as mudanças climáticas são importantes motivadores para as fontes de energia renováveis e a modernização da rede elétrica. A modernização da rede elétrica inteligentes (REI) ou *smart grid*, não somente possibilita as fontes de energia renováveis mas também abre portas à novas aplicações de grande impacto como a prevenção e restauração automática de falhas e a possibilidade dos consumidores terem grande controle sobre o consumo de eletricidade e atuação participativa no mercado de energia.

De acordo com o Instituto Norte Americano de Pesquisas do Setor Elétrico, um dos principais desafios a ser enfrentado no desenvolvimento das REIs é relacionado a segurança cibernética dos sistemas.

O cenário da segurança cibernética atual é caracterizado pela rápida evolução dos riscos e vulnerabilidades que impõe desafios para a confiabilidade, segurança e resiliência do setor elétrico. Neste contexto, estimadores de estado do sistema de potência são ferramentas críticas para a confiabilidade da rede, sob um cenário de observabilidade do sistema eles possibilitam o fluxo de potência do sistema e a análise de dados incorretos.

Neste trabalho, ataques cibernéticos são modelados como injeção de dados incorretos em medidas, parâmetros e topologia do sistema. A metodologia proposta possibilita detecção de ataques mesmo se eles pertencerem ao subespaço ortogonal formado pelas colunas da matriz Jacobiana e em áreas do sistema com reduzida redundância de medidas. A solução proposta pelo estado da arte considera correções em parâmetros ou topologia quando medidas estão livres de erros.

Porém, como pode-se corrigir medidas se parâmetros ou a topologia estão simultaneamente com erros? Para resolver este problema um modelo relaxado é proposto e resolvido iterativamente. Assim que detectado e identificado, ataques cibernéticos em parâmetros, topologia e/ou medidas são corrigidos.

As contribuições específicas do trabalho são: cálculo do desvio padrão para pseudo-medidas (iguais à zero) e medidas de baixa magnitude baseado em medidas correlatas e propriedades da covariância; modelo baseado em relaxação lagrangiana e erro composto de medida para identificação e detecção de ataques cibernéticos; estratégia hibrida de relaxamento iterativo (EHRI) para correção de ataque cibernético em parâmetros da rede de modo contínuo e com reduzido esforço computacional e metodologia baseada em ciclo holístico de resiliência para estimadores de estado sob ataques cibernéticos simultâneos em parâmetros, topologia e medidas.

A validação é feita através dos sistemas de teste do IEEE de 14 e 57 barras, testes comparativos elucidam as contribuições da metodologia proposta ao estado da arte nesta área de pesquisa. Trazendo as capacidades de mitigação, resposta e recuperação ao estimador de estado com esforço computacional reduzido, o modelo e metodologia propostos tem grande potencial de ser integrado em SCADAs para aplicação em casos reais.

Palavras-chave: Sistemas de Potencia, Segurança Cibernética, Redes Inteligentes, Estimador de estado.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AB	Autonomous behavior
AC	Alternating current
ASV	Augmented state vector
AMS	Advanced metering system
CELM	Composing errors and Lagrange multipliers
CM	Countermeasures
CA	Cyber-attacks
CS	Cyber-security
DSE	Dynamic state estimator
DSSE	Distribution system state estimation
DER	Distributed energy resources
EPRI	Electric Power Research Institute
EMS	Energy management systems
FASE	Forecast-aided state estimation
FPCA	False parameter attack identification
GRL	Global redundancy level
HRC	Holistic resilience cycle
HIRA	Hybrid iterative relaxed approach
IC	Innovation concept
II	Innovation index
LASEP	Laboratório de Sistemas de Potência
LM	Lagrange multiplier
MASE	Multiarea state estimation
MGE	Measurement Gross Error
MLE	Maximum likelihood estimation
NE	Normal equation

NI	Numerical instabilities
NR	Normalized Residuals
NI	Numerical instability
NIST	National Institute of Standards and Technology
PCPT	Parameter correction process tolerance
PE	Parameter Error
PPGEE	Programa de Pós-Graduação em Engenharia Elétrica
PSSE	Power system state estimators
SCADA	Supervisory Control and Data Acquisition
SE	State estimation
TL	Transmission line
WLS	Weighted least square

LIST OF SYMBOLS

$\mathbf{z}$	measurement vector
$\mathbf{x}$	true state vector
$\mathbf{h}(\mathbf{x})$	nonlinear vector function relating measurements to states
N	number of unknown state variables to be estimated
$\mathbf{e}$	measurement error vector
$J(\mathbf{x})$	performance index
z_i	*i*th measurement
$h_i(x)$	nonlinear function relating the system state vector x to the *i*th measurement
σ_i	*i*th measurement's variance
R	covariance matrix of the measurements
$\mathbf{H}(\mathbf{x^k})$	Jacobian matrix of $\partial J\mathbf{x}/\partial\mathbf{x}$
$\hat{x}^k$	state estimate to be obtained
K	hat matrix
S	residual sensitivity matrix
$\Delta z(x^k)$	the measurement residuals equals to $z - h(x^k)$
$\Delta\hat{x}$	state estimate to be obtained $\Delta\hat{x}^k$
H	Jacobian matrix $\mathbf{H}(\mathbf{x^k})$
Δz	the measurement residuals equals to $\Delta z(x^k)$
W	inverse of the covariance matrix of the measurements R
II_i	innovation index
e_d	detectable component of the measurement error vector
e_u	undetectable component of the measurement error vector
CME	composed measurement error
CME^N	normalized form of CME
CNE	composed normalized error
$h(x, p')$	nonlinear function relating the measurements to the system states and network parameter

p'	assumed parameters
p_r	recorded parameters
λ	lagrange multiplier for parameter error constraints.
H_x	Jacobian matrix of $\frac{\partial h(x,p')}{\partial x}$
H_p	Jacobian matrix of $\frac{\partial h(x,p')}{\partial p_e}$
${\lambda_i}^N$	normalized λ element
λ_{CELM}	lagrange multiplier for the parameter error equality constraint
P_*	real power injection at bus *
g_{mn}	branch series conductance
θ_{mn}	voltage angles at terminal buses of branch m-n
b_{mn}	branch series susceptance
a_{mn}	transformer final turns ratio
Q_*	reactive power injection at bus *
b_{mn}^{sh}	branch shunt susceptance
b_*^{sh}	shunt susceptance (reactor) at bus *
P_{mn}	real power flow of branch m-n
Q_{mn}	reactive power flow of branch m-n

1 INTRODUCTION

Growing demand and concern over climate change are key drivers for renewable sources of electricity and grid modernization (BAKKEN et al., 2011). Grid modernization not only enables renewable sources but also opens the door to new applications with far-reaching impacts such as preventing or restoring outages (self-healing capabilities) and enabling consumers to have greater control over their electricity consumption and to actively participate in the electricity market (GIORDANO et al., 2013).

The basic components of the so called smart grid are information and communication technology with power system engineering. Several governmental entities have been concerned about the future standards and necessary technologies to implement the next generation of energy grid (GIORDANO et al., 2013; USA, 2014b; BRAZIL, 2012). In the last edition of the Smart Grid Framework and Roadmap for Interoperability Standards, the National Institute of Standards and Technology (NIST) defined nine priority areas: demand response and consumer energy efficiency; wide-area situational awareness; distributed energy resources (DER); energy storage; electric transportation; network communications; advanced metering infrastructure; distribution grid management and cyber-security.

According to the Electric Power Research Institute (EPRI), one of the biggest challenges facing smart grid deployment is related to the cyber security of the systems (YAN et al., 2012).

The current cyber-security landscape is characterized by rapidly evolving threats and vulnerabilities that poses challenges for the reliability, security, and resilience of the electricity sector (USA, 2017).

Cyber-attacks (CA) against measurements and the parameter database storage at SCADA (Supervisory Control and Data Acquisition) are recognized as possible and a high potential threat (FOVINO et al., 2011; TEN; LIU; MANIMARAN, 2008; HUG; GIAMPAPA, 2012). SCADA systems, in general, are exposed to a wide range of cyber threats (SUN; HAHN; LIU, 2018). The Repository of Industrial Security Incidents had 161 events listed in 2010 with about 10 new incidents being added each quarter, in 2013 this number reached 240 events (CHERDANTSEVA et al., 2016).

After the 2015 cyber-attack event which caused a six-hour blackout for hundreds of thousands of customers in Ukraine, several countries investigated the occurrence, trying to answer the question: could this happen in our power system?

Indeed, countries such as the U.S. are aware that critical infrastructure depends on electricity (USA, 2017) and that the growth and sustains of a workforce that is skilled in cyber-security and related fields is essential (USA, 2018). There have been no reported successful cases of cyber-terrorism in U.S. causing power outages (SULLIVAN; KAMENSKY, 2017), but data suggest that electricity system outages attributable to weather-related events can cost the U.S. economy an estimated $20 to $55 billion annually (USA, 2017).

One of Ukraine's hackers' successful strategy was their long-term exploration in order to learn the environment and execute a highly synchronized multi-level attack . Such attacks, very target and long-term, are called advanced persisted threats and normally are designed to satisfy international espionage or sabotage (SYMANTEC, 2011).

The threat environment is rapidly changing therefore the electric utilities face big challenges in securing their networks (information and operation). Efforts to understand, develop and evolve the emergency response capability to address ever-changing and evolving cyber threats are critical to the electrical power grid resilience (USA, 2017).

1.1 Objectives and Contributions

Data intrusion is the most common group of direct cyber attacks threatening the security of power systems. Data intrusion cyber attacks can happen as a false data injection (FDI) in measurements and remote terminal units (RTUs) such as: load bus injection and line power flow measurements; phasor measurement units and electrical vehicle charging stations. Further, they can happen in the SCADA database system and have impacts in energy management tools such as: optimal power flow; state estimators and security-constrained economic dispatch (MEHRDAD et al., 2018).

In order to address data intrusion cyber-attacks this work proposes enhancements to the state estimation tool in order to identify and detect simultaneous measurement, parameter and/or topology FDI cyber-attack.

(USA, 2014a) cites that one of the most important security solutions is to utilize and augment existing power system technologies, state estimators for example, to address new risks associated with the smart grid, which is done in the present work.

To address the complexity of the integrated cyber-physical power system the security of the power systems should be done in a holistic manner (MEHRDAD et al., 2018). The holistic resilience cycle (HRC), proposed by MEHRDAD et al. (2018), is composed by four stages: i) prevention and planning; ii) detection; iii) mitigation and response; iv) system recovery

Based in the HRC, this work presents a methodology to correct simultaneous measurement, parameter and/or topology FDI cyber-attack . This means to add the mitigation, response and system recovery capabilities to the state estimator, focusing in the development of countermeasures.

Also, in order to deal with resolution numerical instabilities due to pseudo and low/zero magnitude measurements, a standard deviation based on correlated measurements and covariance properties is proposed. Thus the specific contributions of this work are:

i) standard deviation for pseudo and low/zero magnitude measurements based on correlated measurements and covariance properties;

ii) Lagrange relaxation and composed measurement error based model for cyber attack detection and identification;

iii) hybrid iterative relaxed approach (HIRA) for parameter cyber-attacks detection and correction in a continuously manner and with reduced computational burden;

iv) holistic resilience cycle based methodology for state estimation under simultaneous parameter, topology and measurement cyber-attacks.

1.2 Thesis Organization

In order to present the measurement, topology and parameter cyber-attack detection, identification and correction methodology the following chapters are part of this document: Chapter 2 includes the literature review.

What is being used from existing methodologies and models and to what extent is described in chapter 3.

Chapter 4 details the main equations and the new formulation using composing error, Lagrange multiplier and Relaxed Taylor Series to identify, detect and correct measurement, topology and parameter cyber-attacks.

Chapter 5 explores the methodology capability of cyber-attack detection, identification and correction using two test cases, IEEE-14 and IEEE-57 bus systems and different cyber-attack scenarios and discusses the results and outlines comparisons with the state-of-the-art.

Finally, chapter 6 wraps-up the ideas and results with suggested extensions and refinements of the proposed methodology.

2 LITERATURE REVIEW

Although SE has been studied for several decades the new challenges and requirements that the smart grid imposes have recently brought new exploratory research in this area. Sections 2.1, 2.2, 2.3, 2.4 present the research, methodologies and findings in regards to SE and cyber security (CS). Section 2.5 presents a table that summarizes all subjects and researches related and presented in this review.

2.1 Cyber-security and State Estimators

In order to assist organizations as they craft a smart grid strategy, NIST developed the document entitled Guidelines for Smart Grid Cyber-security (USA, 2014a). This three-volume report presents an analytical framework to be used by companies to develop their own cyber-security strategies based on their particular changes towards smart grid-related characteristics. Organizations in the diverse community of energy management services and products need to recognize that the electric grid is changing from a relatively closed system to a complex, highly interconnected environment.

The document has two basic approaches: bottom-up, focusing on identifying vulnerability classes and top-down, focused on defining components/domains of the smart grid system and the logical interfaces between these components/domains. A logical reference model was defined as part of the top-down approach and presents smart grid domains, actors and interfaces.

Each logical interface can be allocated to a logical interface category as a means to simplify the identification of the appropriate security requirements. Logical Interface Category 1 can be defined as the interface between control systems and equipment with high availability and with computational and/or bandwidth constraints such as between transmission SCADA in support of state estimation and substation equipment for monitoring and controlling data using a high frequency mode.

Figure 1 presents the Category 1 logical reference model, where an actor is a device, computer system, software program, or the individual or organization that participates in the smart grid. The arrows on Figure 1 and their nomenclature (U) represent logical interfaces.

From the actors and interfaces in this category we expect low confidentiality, high integrity and high availability. A loss of integrity, which is unauthorized modification or destruction of information; or a loss of availability, which is the disruption of access to or use of information or an information system, can be critical in this category.

High integrity and availability are expectations of the transmission SCADA and its related interfaces. It is also expected that existing capabilities and software functions that exist on it and in other EMS are tailored or expanded to meet the security requirements.

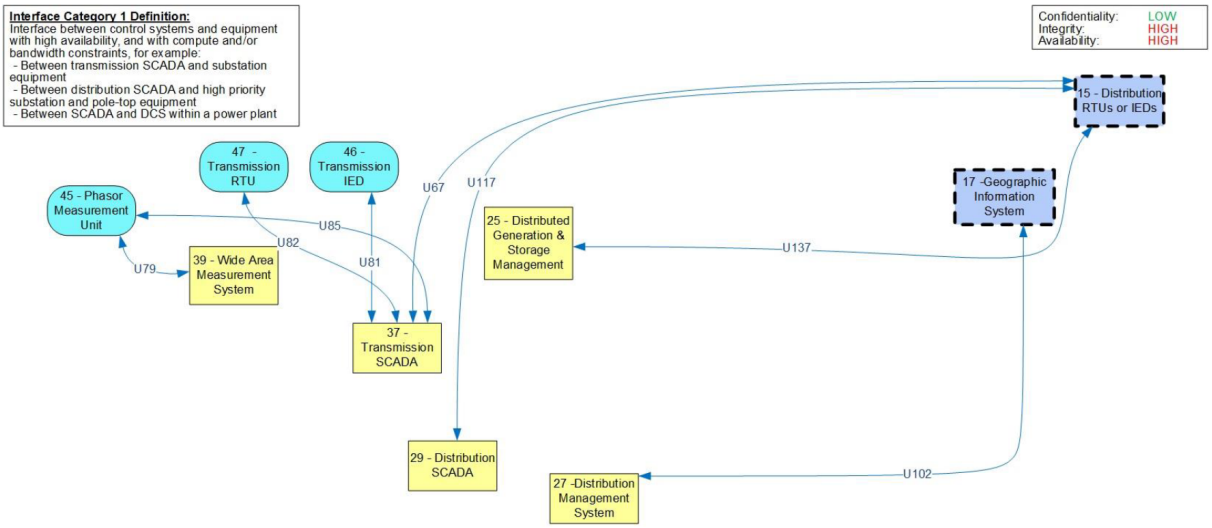

Figure 1: Logical Reference Model - Category 1 (USA, 2014a)

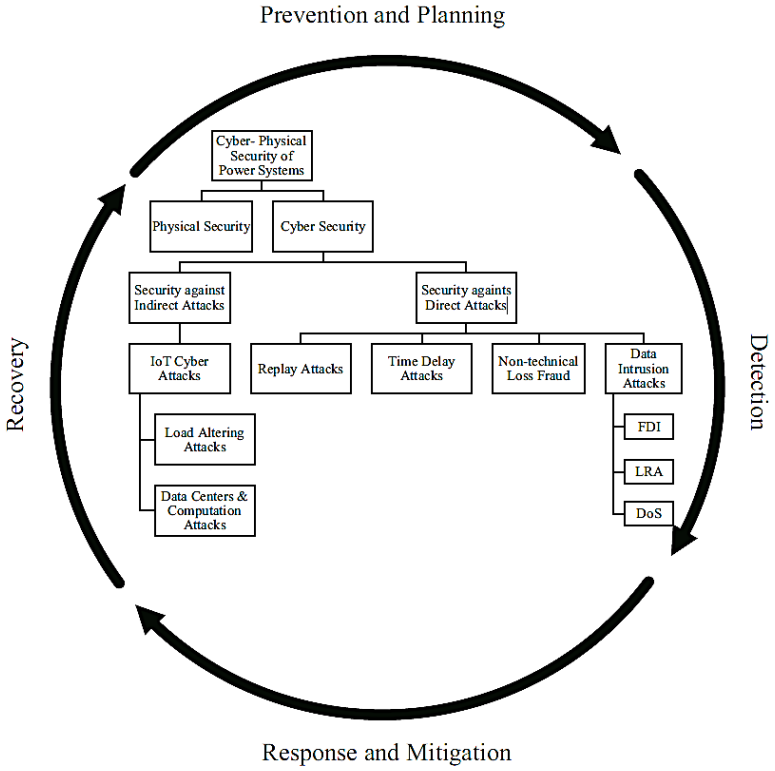

Figure 2: Holistic resiliency cycle (MEHRDAD et al., 2018)

PSSE is a software with functions that can be expanded towards this goal (USA, 2014a).

MEHRDAD et al. (2018) provides a systematic view to the security of the power systems and a framework to categorize the current bibliography in the field. The authors classify the bibliography by the phase (e.g. Detection) of the cyber-attack and by the format (e.g. against direct attacks) as figure 2 depicts, in a so called holistic resiliency cycle.

In regards to physical security MEHRDAD et al. (2018) states that the majority of studies is related to stages prevention and planing, detection and response and mitigation. As for cyber security, the majority of researches is related to planing, detection and

response.

Data intrusion is the most common group of direct cyber attacks threatening the security of power systems.

Data intrusion cyber attacks can happen in the SCADA database system and have impacts in energy management tools such as:

i) optimal power flow (MOUSAVIAN; VALENZUELA; WANG, 2013; VALENZUELA; WANG; BISSINGER, 2013);

ii) state estimators (BOBBA et al., 2010; DÁN; SANDBERG, 2010; KIM; POOR, 2011; HUG; GIAMPAPA, 2012; ZHAO et al., 2016; MOHAMMADPOURFARD; SAMI; SEIFI, 2017; BRETAS et al., 2017; HU et al., 2018);

iii) security-constrained economic dispatch (YUAN; LI; REN, 2011; XIANG et al., 2017).

Also, they can happen in measurements and remote terminal units (RTUs) such as:

i) load bus injection and line power flow measurements (YUAN; LI; REN, 2011; XIANG et al., 2017);

ii) phasor measurement units (MOUSAVIAN; VALENZUELA; WANG, 2015);

iii) electrical vehicle charging stations (MOUSAVIAN; EROL-KANTARCI; ORTMEYER, 2015).

Further, denial of service cyber attacks can happen using artificial loads (WANG et al., 2017).

Considering data intrusion cyber-attacks in state estimators it is possible to identify that most works consider stealthy attacks only in measurements and proceed with residual based solutions (HUG; GIAMPAPA, 2012; ZHAO et al., 2016; DÁN; SANDBERG, 2010; BOBBA et al., 2010). Residual based solutions methodology hardly will detect an attack vector a fitting the measurement model, which for the weighted linear case is equivalent to have it belonging to the subspace spanned by the columns of the Jacobian matrix of the electrical network (KIM; POOR, 2011; TEIXEIRA et al., 2010).

With regards to cyber-security and state estimators within SCADA systems the research can be classified into three categories (HUG; GIAMPAPA, 2012):

i) Research on vulnerability analysis of state estimation (LIU; NING; REITER, 2011; DÁN; SANDBERG, 2010; TEIXEIRA et al., 2010; SANDBERG; TEIXEIRA; JOHANSSON, 2010): inherent weaknesses of state estimators bad data detection investigation in order to identify malicious alterations to SCADA data i.e.: which SCADA measurements need to be altered and by how much in order to render the attack undetectable by bad data detection?

ii) Research on consequence or impact analysis (MOHAJERIN ESFAHANI et al., 2010; ESFAHANI et al., 2010): state estimation cyber-attack consequences on functions that rely on state estimation results such as power flow calculations, congestion analysis and management, and automatic generation control i.e.: what the resulting consequences on those functions would be if a false data attack were to remain undetected and how an attacker could take advantage of such a vulnerability?

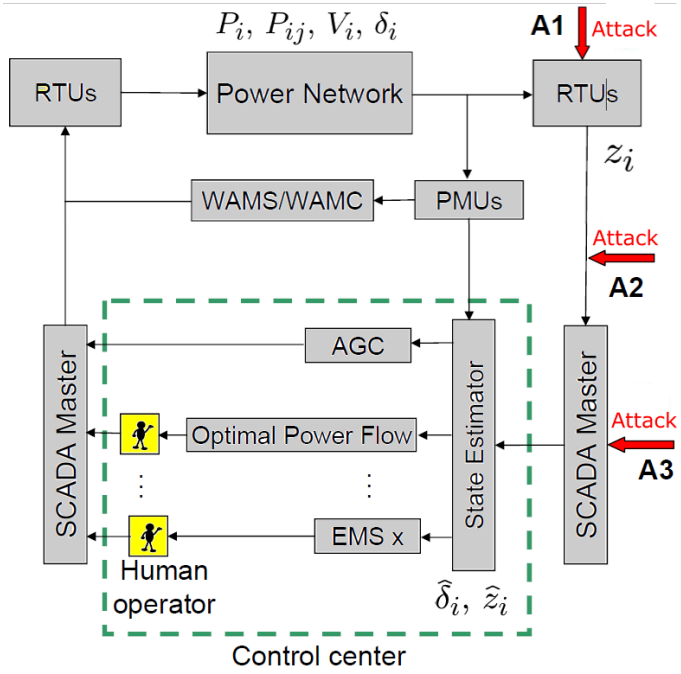

Figure 3: A state estimator under a cyber-attack adapted from (SANDBERG; TEIXEIRA; JOHANSSON, 2010)

iii) Research on the development of countermeasures: The key question of this research area is how to detect malicious attacks and protect the power system, focusing on improving bad data detection schemes or improving the security of the communication system (KOSUT et al., 2010; KIM; POOR, 2011; BOBBA et al., 2010).

The literature also shows that the current model for a stealthy deception attacker is to compromise the telemetered measurements available to the PSSE such that:

1) The PSSE algorithm still converges;

2) For the targeted set of measurements, the estimated values at convergence are close to the compromised ones introduced by the attacker;

3) The attack remains fully undetected by the bad data detection scheme. As a consequence of the attackers' stealthy action, the incorrect state estimates generated by the PSSE can have different effects on other power management functions. A state estimator under a cyber-attack is depicted on Figure 3

In (KOSUT et al., 2010) the problem of constructing malicious data attack of smart grid state estimation is considered together with countermeasures that detect the presence of such attacks. For the adversary, using a graph theoretic approach, an efficient algorithm with polynomial-time complexity is obtained to find the minimum size unobservable malicious data attacks. When the unobservable attack does not exist due to restrictions of meter access, attacks are constructed to minimize the residue energy of attack while guaranteeing a certain level of increase of mean square error. For the control center, a computationally efficient algorithm is derived to detect and localize attacks using the generalized likelihood ratio test regularized by an *L1* norm penalty on the strength of attack.

In (KIM; POOR, 2011) data injection attacks to manipulate system state estimators on power grids are considered. A unified formulation for the problem of constructing attacking vectors is developed for linearized measurement models. Based on this formulation, a new low-complexity attacking strategy is shown to significantly outperform naive l_1 relaxation. 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. However, selecting such subsets is a high-complexity combinatorial problem given the typically large size of electrical grids. To address the complexity issue, a fast greedy algorithm to select a subset of measurements to be protected is proposed. Another greedy algorithm that facilitates the placement of secure phasor measurement units to defend against data injection attacks is also developed. Simulations on the IEEE test systems demonstrate the benefits of the proposed algorithms.

Finally in (BOBBA et al., 2010) the detection of false data injection attacks of (LIU; NING; REITER, 2011) is explored by protecting a strategically selected set of sensor measurements and by having a way to independently verify or measure the values of a strategically selected set of state variables. Specifically, it is shown that it is necessary and sufficient to protect a set of basic measurements to detect such attacks.

Analyzing the contributions to cyber-physical security on the development of countermeasures (KOSUT et al., 2010; KIM; POOR, 2011; BOBBA et al., 2010) it is possible to identify that most works consider stealth attacks only on measurements and proceed with residual based solutions. Residual based solutions methodology hardly will detect an attack vector *a* fitting the measurement model, which for the weighted linear case is equivalent to have it belong to the subspace spanned by the columns of the Jacobian matrix of the electrical network (TEIXEIRA et al., 2010).

BRETAS et al. (2017) cover this issue presenting a methodology where the error is composed and analyzed and not the residual. BRETAS; BRETAS; PIERETI (2011); BRETAS et al. (2013) show that the error component of the linear state estimation formulation has an unique decomposition: one component that is orthogonal to the Jacobian range space and the other that belongs to that space. The former is the residual, the later the masked error component. To estimate this masked error component, the Innovation concept for static formulations is used.

2.2 State estimation and bad data process in balanced power systems

Initially transmission and bad data power networks had only supervisory control systems that monitored the status of circuit breakers and controlled the generators output. Eventually real-time system-wide data acquisition capabilities were added that led to the establishment of the first SCADA systems. However, the information provided by a SCADA system may not always be reliable due to errors in data and data acquisition and the collected set of measurements may not allow direct extraction of the corresponding alternating current (AC) operating state of the system. In order to cover these issues Fred Schweppe and J. Wildes in 1970 proposed the idea of state estimation in power systems (SCHWEPPE; WILDES, 1970).

The static-state estimator results from a combination of two big fields, load flow and statistical estimation theory (SCHWEPPE; WILDES, 1970). It is based on the nonlinear measurement model as described by equation (1) (SCHWEPPE; WILDES, 1970) where $\mathbf{z} \in \mathbb{R}^m$ is the measurement vector, $\mathbf{x} \in \mathbb{R}^N$ is the true state vector (N < m), $\mathbf{h}(\mathbf{x}) : \mathbb{R}^{\mathbf{N}} \rightarrow \mathbb{R}^{\mathbf{m}}$ is a nonlinear vector function relating measurements to states,

$N = 2n - 1$ is the number of unknown state variables to be estimated with n equals to the systems' buses and $\mathbf{e} \in \mathbb{R}^m$ is the measurement error vector.

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

The measurement errors are commonly assumed to have a Gaussian (normal) distribution (SCHWEPPE; WILDES, 1970) and the parameters for such a distribution are its mean (or expected value).

Regarding the statistical properties of the measurement errors the following assumptions are made (SCHWEPPE; WILDES, 1970):

1. The expected value $E(e_i)$ of the error e_i is zero for all $i = 1, ..., m$;
2. Measurement errors are independent, therefore the corresponding variance matrix $Cov(e)$ is called $R = diag({\sigma_1}^2, {\sigma_2}^2, ..., {\sigma_m}^2)$, where σ is the standard measurement deviation.

The static-state estimation exact model proposed by SCHWEPPE; WILDES (1970) using the matrix $\mathbf{Cov(e)} = \mathbf{R}$ is described by equation (2). The state estimate vector $\hat{\mathbf{x}}$ is defined to be the value of $\mathbf{x}$ which minimizes equation (2).

$$J(\mathbf{x}) = [\mathbf{z} - \mathbf{h}(\mathbf{x})]'\mathbf{R^{-1}}[\mathbf{z} - \mathbf{h}(\mathbf{x})] \tag{2}$$

To find the $\hat{\mathbf{x}}$ the first order optimal condition is applied and as $\mathbf{h(x)}$ is a nonlinear equation, the Newton Raphson method is used, resulting in the iterative procedure as described by equation (3) (MONTICELLI, 1999) and known as the WLS SE via the use of the normal equation (NE). $\mathbf{H(x^k)}$ is the Jacobian matrix of $\partial\mathbf{h(x)}/\partial\mathbf{x}$, $\hat{\mathbf{x}}^\mathbf{k}$ is the state estimate to be obtained and $\mathbf{\Delta z(x^k)}$ is the measurement residual equal to $\mathbf{z} - \mathbf{h(x^k)}$ and k is the iteration number.

$$\begin{aligned} &(\mathbf{H^t(x^k)R^{-1}H(x^k)})\mathbf{\Delta\hat{x}^k} = \mathbf{H^t(x^k)R^{-1}\Delta z(x^k)} \\ &\mathbf{x^{k+1}} = \mathbf{x^k} + \mathbf{\Delta\hat{x}^k} \end{aligned} \tag{3}$$

The foregoing is the most common implementation of an AC SE although alternative formulations have been proposed mainly to deal with resolution numerical instabilities (NI) (HOLTEN et al., 1988).

The state estimation problem using equality constraints was introduced in 1977 (ASCHMONEIT; PETERSON; ADRIAN, 1977), where equation $c(\mathbf{x}) = \mathbf{0}$ represents a set of nonlinear constraints such as zero power injections in buses.

This approach is used (LIU; WU; LUN, 1992) to improve the numerical robustness of estimation as no weights are assigned to the equality constraints. When zero power injections are used as pseudo-measurements, large weight factors are applied. For large weight factors the coefficient matrix $(\mathbf{H^t(x^k)R^{-1}H(x^k)})$ tends to be singular causing ill-conditioning problems (HOLTEN et al., 1988; MONTICELLI, 1999).

The constrained WLS state estimation problem can then be formulated as equation (4).

$$\begin{aligned} \underset{\mathbf{x}}{\text{minimize}} \quad & J(\mathbf{x}) = [\mathbf{z} - \mathbf{h(x)}]^\mathbf{t}\mathbf{R^{-1}}[\mathbf{z} - \mathbf{h(x)}] \\ \text{subject to} \quad & c(\mathbf{x}) = \mathbf{0} \end{aligned} \tag{4}$$

Extending this approach to regular measurements another formulation adding the residual equation as constraint was proposed (GJELSVIK; AAM; HOLTEN, 1985). In this formulation the Karush-Kunh-Tucker first order necessary conditions are expressed by an augmented coefficient matrix called Hachtel's matrix or tableau (WU; LIU; LUN, 1988).

In a general sense the SE serves as a large-scale filter between the remote measurements and the EMS in order to achieve an interconnected external network model as depicted in Figure 4. SE bad data processing entails error detection and identification functions that can filter non-Gaussian errors in the set of measurements, detect topology errors and improve values of suspicious network parameter, such as transformer taps.

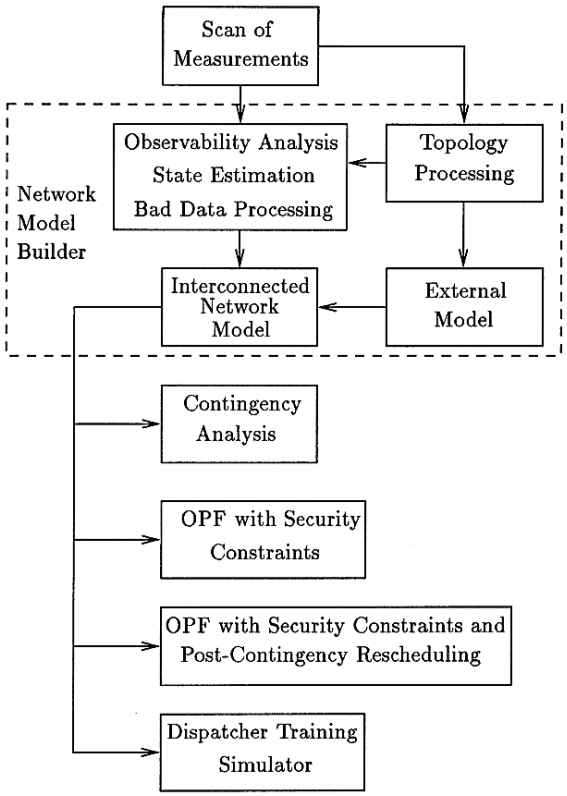

Figure 4: Network analysis functions (MONTICELLI, 1999)

It is also possible to find in the state estimation bibliography review a series of researches related to sensitivity analysis (MINGUEZ; CONEJO, 2007; CARO; CONEJO; MINGUEZ, 2009; CARO et al., 2010).

MINGUEZ; CONEJO (2007) provides expressions to compute sensitivities regarding measurement schemes, transmission line modeling, and other parameters variation against the quality of the state estimation solution.

In (CARO et al., 2010) the authors show that dependencies among measurements exist and they vary with the operating conditions of the substation. CARO; CONEJO; MINGUEZ (2009) proposes the use of measurement dependencies among substation measurements in the state estimation, contrary to the vastly used assumption that measurement errors are independent.

Finally, there is also an important field within SE in regards to observability (MONTICELLI; WU, 1985; LONDON; ALBERTO; BRETAS, 2007) and multi-area approach (GÓMEZ-EXPÓSITO et al., 2011).

In the multi-area approach, SE is solved locally within each measurement area, and data is exchanged between areas. Two devices architectures are used on this approach: hierarchical scheme, where a master processor distributes the work among slaves devices performing local area SE, and decentralized architecture, where there is no central computer; each local processor communicates only with those processors in charge of neighboring areas (GÓMEZ-EXPÓSITO et al., 2011).

Identification of observable islands are matrix based analysis that bring information on critical measurements and sets (MONTICELLI; WU, 1985; LONDON; ALBERTO; BRETAS, 2007).

2.2.1 Measurement Gross Error Detection, Identification and Correction

Historically bad data detection and identification were done after the WLS estimation by processing the measurement residuals based on the statistical properties of it, a process called the largest normalized residual test (WU; LIU; LUN, 1988; CARO; CONEJO; MINGUEZ, 2011). Detection refers to the determination of whether or not a set contains any bad data and identification finds out which specific item contains bad data. The test is composed of the following steps (ABUR; EXPOSITO, 2004):

1. Solve the WLS estimation and obtain the elements of the measurement residual vector: $\hat{r_i} = z_i - h_i(\hat{x}), i = 1, ..., m$
2. Compute the normalized residuals (NR): $r_i^N = |r_i|/\sqrt{\Omega_{ii}}, i = 1, ..., m$
3. Find k; such that r_k^N is the largest among all r_i^N, $i = 1, ..., m$
4. If $r_k^N >$ threshold (for instance 3.0) , then the k_{th} measurement will be suspected as bad data. Else, stop, no bad data will be suspected.
5. Eliminate the k_{th} measurement from the measurement set and go to step 1. Actual removal of the bad measurement may be avoided by subtracting the estimated error from the bad measurement.

Ω_{ii} is the diagonal element of the residual covariance matrix Ω. The sensitivity of the measurement residuals to the measurement errors, or residual sensitivity matrix S need to be defined in order to derive Ω_{ii}. From equation (3) it is possible to write equation (5) where $\Delta\hat{x}^k$ is equal to $\Delta\hat{x}$, $H(x^k)$ to H and $\Delta z(x^k)$ equal to Δz. The term $(H^t(x^k)R^{-1}H(x^k))$ is called gain matrix (G).

$$\begin{aligned} \Delta\hat{x} &= (H^t R^{-1} H)^{-1} H^t R^{-1} \Delta z \\ &= (G)^{-1} H^t R^{-1} \Delta z \end{aligned} \tag{5}$$

From the linearization of the objective function at the solution point it is possible to find the hat matrix K definition.

$$\begin{aligned} \Delta\hat{z} &= H\Delta\hat{x} = K\Delta z \\ K &= H(G)^{-1} H^t R^{-1} \end{aligned} \tag{6}$$

Considering that $(I - K)H = 0$

$$
\begin{aligned}
r &= \Delta z - \Delta \hat{z} \\
&= (I - K)\Delta z \\
&= (I - K)(H\Delta z + e) \\
&= (I - K)e \\
&= Se
\end{aligned} \tag{7}
$$

Using the linear relation $r = Se$, the mean, the covariance and the probability distribution of the measurement residuals can be obtained as follows:

1. $E(r) = E(Se) = SE(e)$ and as the expected value $E(e)$ of the error e is zero $E(r) = 0$

2. $Cov(r) = \Omega = E[rr^t] = SE[ee^t]S^t = SRS^t = SR$

The largest normalized residual approach is not robust in the presence of multiple interacting/conforming gross errors (ABUR; EXPOSITO, 2004; LIU; NING; REITER, 2011). To cover this issue instead of the classical normalized measurement residual, the corresponding normalized composed measurement error CME^N was proposed in the gross error detection and identification test. This approach acknowledges the existence of a masked effect of the measurement error not reflected in the state estimation residual that is recovered using the innovation index (II) (BRETAS; PIERRETI, 2010; BRETAS; BRETAS, 2018).

The innovation approach (BRETAS et al., 2017) has clear improvements compared to solutions which minimize the residual, however real-world assumptions with regards to the presence of pseudo and low/zero magnitude measurements e.g., a no-generation and no-demand bus (with zero active and reactive power injections) are not considered or investigated. For these types of measurements BRETAS et al. (2017) have an arbitrary low standard deviation that result in high weights that can lead to ill-conditioning of the gain matrix (MONTICELLI, 1999; ABUR; EXPOSITO, 2004).

A two step approach for the power system state estimation was proposed using the II (BRETAS; BRETAS, 2015) where the first step is the gross error detection test when all the measurements are assumed as possible of having errors. With that assumption, a rule for the measurement's weights as being the inverse of a constant percentage of the measurement's magnitudes was proposed. Then, using the error as the objective function of the state estimation process to be minimized, the gross error analysis is performed.

In case a gross error is detected, the Composed Measurement Error (CME), in its normalized form CME^N, is used to identify the measurement(s) with error(s). The measurement(s) with error(s) is corrected using the Composed Normalized Error CNE. In the second step, the state estimation is again performed, but using as the weight for each measurement the inverse of the measurement's standard deviation as proposed in the classical estimators. (BRETAS; BRETAS, 2015).

Another proposed strategy is to make use of a correlation coefficient (CARO; CONEJO; MINGUEZ, 2009) to remove from the correlated measurements the dispersed multiple gross error (CARO et al., 2011).

These new techniques (CARO et al., 2011; BRETAS; BRETAS, 2015) avoid the removal of the inconsistent data, as it was done in previous works (WU; LIU; LUN, 1988).

2.2.2 Parameter Error Detection, Identification and Correction

State estimation methods, as all EMS applications, make use of the network model in the mathematical formulation of their problem. Inconsistencies detected during the estimation process will be blamed on analogue measurement errors, while errors in the network model may be due to topology and/or parameter errors (ZHU; ABUR, 2006).

The most common source of network parameter (branch impedance or tap changer position) errors are inaccurate manufacturing data, miscalibration, tap changer being locally modified without knowledge of the control center, etc (ZARCO; GOMEZ EXPOSITO, 2000; LIU; WU; LUN, 1992).

Another not so trivial, but possible, source is a cyber-attack against the parameter database storage in SCADA systems. Potential cyber threats to SCADA systems, ranging from computer system to power system aspects, are recognized as possible (TEN; LIU; MANIMARAN, 2008).

Network parameter errors may produce (ZARCO; GOMEZ EXPOSITO, 2000):

1. a significant degradation of the results provided by the SE and, therefore, of the conclusions arrived at by other applications, like security assessment;

2. acceptable measurements being detected as bad data owing to its lack of consistency with network parameters;

3. a loss of confidence in the SE by the operator.

Traditionally, in the bibliography, two classifications of parameter error identification methods are found: one based on residual sensitivity analysis (LIU; WU; LUN, 1992) and one based on augmenting the state vector (ZARCO; GOMEZ EXPOSITO, 2000).

An alternative to these methods is the use of the Lagrange multipliers (LM). This approach is used to identify parameter errors where there is no need to apriori specify a suspect parameter set (ZHU; ABUR, 2006; ZHANG; ABUR, 2013; LIN; ABUR, 2016). This is an advantage, especially with regards to process time, although the method relies on the NR test and there are cases where this test is incapable of identifying multiple interacting errors .

A method that does not rely on the normalized residual test was proposed (BRETAS; CARVALHO; ALBERTINI, 2015) using the CME^N. The approach verifies if there are measurements with CME^N larger than the threshold value (equals to three standard deviations of the corresponding measurement), if those measurements are associated with the same branch $i-j$ of a transmission line and have similar values for their CME^N. If so, a parameter is suspected of having an error, otherwise, it is a case of simple or even multiple gross errors.

The parameter cyber-attack identification proposed by (BRETAS et al., 2017) relies on power flow measurement in both directions and assumes that a parameter cyber-attack in the line $i-j$ will spread out the error in all of the equations in which this parameter is present, so the respective active or reactive power flow $i-j$ and $j-i$ will present errors with high magnitude values as well as the injections on the sending and receiving end buses. Attacks would not be identified though if the stealthy deception attacker compromises individual parameters or parameters in lines without flow measurements in both directions, a common condition in systems with a low global measurement redundancy level (GRL).

Two approaches of parameter correction are found in the bibliography. In the first, corrections to be made in the line parameter are given by the corresponding composed normalized error CNE_i multiplied by the correction factor based on the II. The methodology

was tested with good results, however no individual values are able to be corrected or other network parameters, such as taps values.

The second proposed solution to correct parameters uses the augmented state vector (ASV) strategy (DEBS, 1974; MONTICELLI, 1999; ZHU; ABUR, 2006).

It is based on the augmented state vector that is formed by the usual state variables and the parameters to be estimated. Although this solution enables the correction of any network parameter, the inherent assumption is a necessary measurement redundancy level due to the increment of the state vector size, thus the detection test decreases its efficiency, since the measurement model degrees of freedom also decreases.

2.2.2.1 Topology Error Detection and Identification

Network topology (e.g. breaker positions), within parameters category, is another resource used by the state estimator that can contain gross errors. Early approaches of using state estimation results for topology error detection were based in the residual test analysis (LUGTU et al., 1980; CLEMENTS; KRUMPHOLZ; DAVIS, 1981; WU; LIU, 1989).

As an extension of the normalized residuals method, CLEMENTS; COSTA (1998) proposed the use of Lagrange multipliers, computed as by-products in the sparse tableau formulation (GJELSVIK; AAM; HOLTEN, 1985) for least-squares state estimation. Built in this approach LOURENCO; COSTA; CLEMENTS (2004) devised a more efficient topology error identification method using hypothesis test based on Bayesian statistics.

2.3 State Estimation and bad data process in non balanced power systems

A natural extension of the methodology described in section 2.2 is to consider non balanced distribution power systems. Moving the state estimator to distribution forces the use of pseudo-measurements to achieve the necessary measurement redundancy (BRETAS et al., 2017; LEFEBVRE; PREVOST; LENOIR, 2014; FANTIN, 2016).

State estimation programs are formulated as overdetermined systems of non-linear equations and solved as weighted least-squares (WLS) problems, therefore, for their good operation a higher number of measurements (i.e. 3 times) than the states to estimate is needed. As telemetry exists in abundance on transmission systems, state estimators have worked well for balanced power systems for many years.

In networks where telemetry does not exist in abundance the use of pseudo-measurements is necessary. Pseudo-measurements are those that are based on load prediction and generation schedulings or that are related to values that are equal to zero (e.g. power injection measurement in a bus that does not have generation or load).

The quality of pseudo measurements on non balanced distribution power systems is recognized as variable, but their use is necessary to make the distribution system observable (LEFEBVRE; PREVOST; LENOIR, 2014).The problem of pseudo-measurements is that they are based on a load profile considered relatively constant over a period. Load profiles are not expected to be constant on power systems with high variable generation (VG) penetration and under a transactive energy scenario (DENHOLM et al., 2015; CHEN; LIU, 2017).

Figure 5 presents the net load chart published in 2013 by California Independent System Operator (CAISO). In the chart, each line represents the net load, equal to the normal load minus wind and PV generation. The net load variation and its slope in this

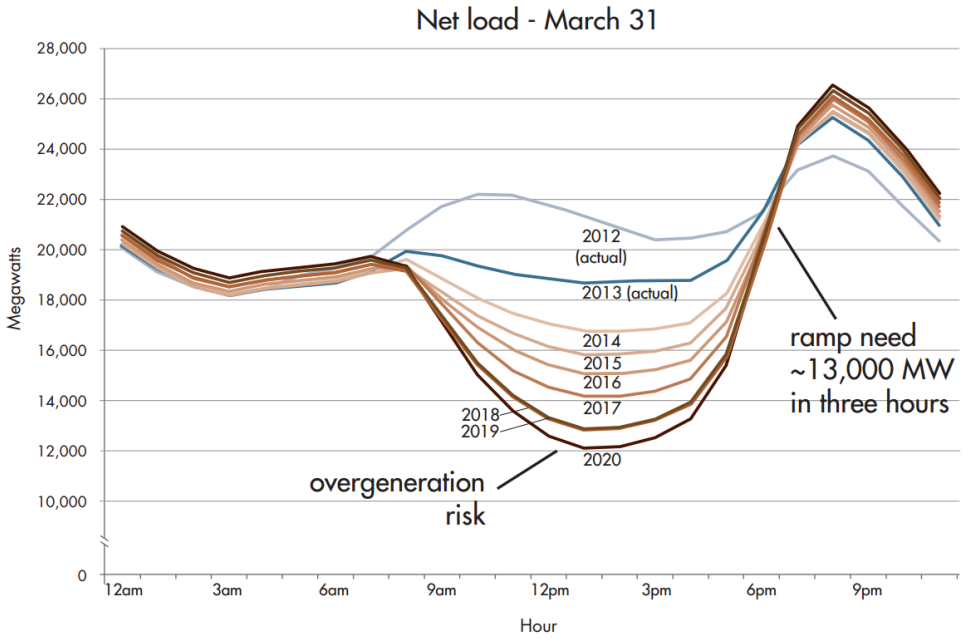

Figure 5: The CAISO duck chart (DENHOLM et al., 2015)

chart illustrate the general challenges of accommodating solar energy and the potential for over-generation and solar curtailment (DENHOLM et al., 2015). This variation is also a general challenge for state estimators that use predictive data as pseudo-measurements.

Transactive energy involves an automated communication and control system connecting energy providers and users, exchanging information about price and availability of power. The Pacific Northwest Smart Grid Demonstration project carried out a simulation on transactive energy which concluded that if nearly one third of the region's loads were responsive to the transactive system, the peak load could be cut by about eight percent (CHEN; LIU, 2017).

The use of different weights to differentiate between the quality of real-time and pseudo-measurements is a proposed approach (DZAFIC et al., 2017) to solve the aforementioned problem of variance of pseudo-measurements. Unfortunately this solution can lead to state estimation numerical instabilities.

2.4 Simultaneous bad data process

The Lagrange multiplier approach proposed by CLEMENTS; COSTA (1998); ZHU; ABUR (2006); GOMEZ-EXPOSITO et al. (2011) relies on the assumption that measurements are without error (BRETAS; BRETAS, 2017; LIN; ABUR, 2017). Only in the absence of gross measurement errors the Lagrange multipliers are zero mean random variables whose variances can be efficiently computed directly from the sparse tableau coefficient matrix factors (CLEMENTS; COSTA, 1998).

In LOURENCO; COELHO; PAL (2015) the authors acknowledge that detection and identification of bad data in state estimation when they comprise of both topology and measurement errors is a real challenge.

To overcame this challenge the authors use geometric tests based on the geometric interpretation of the Lagrange multiplier vector to detect and identify simultaneous topology and measurement bad data.

The proposed method is capable of processing modeling error without making previous assumption about the network topology or the analog measurements. In the proposed formulation circuit breakers are modeled as zero impedance branches and structural and operational constraints are used LOURENCO; COELHO; PAL (2015).

The methodologies proposed in (ZHU; ABUR, 2006; GOMEZ-EXPOSITO et al., 2011) observe network parameter other than topology but are limited in parameter cyber-attack detection and correction, while they consider that in such analysis, measurements or parameters are free of errors

As simultaneous cyber-attacks against parameters, measurements and topology at the SCADA database storage are recognized as possible, the identification and correction of multiple simultaneous measurement and parameter cyber-attacks is a contribution of (BRETAS et al., 2017). This is done using an heuristic based on the analysis of the CME^N and II and correction is done based on the use of the CNE as depicted in Figure 6.

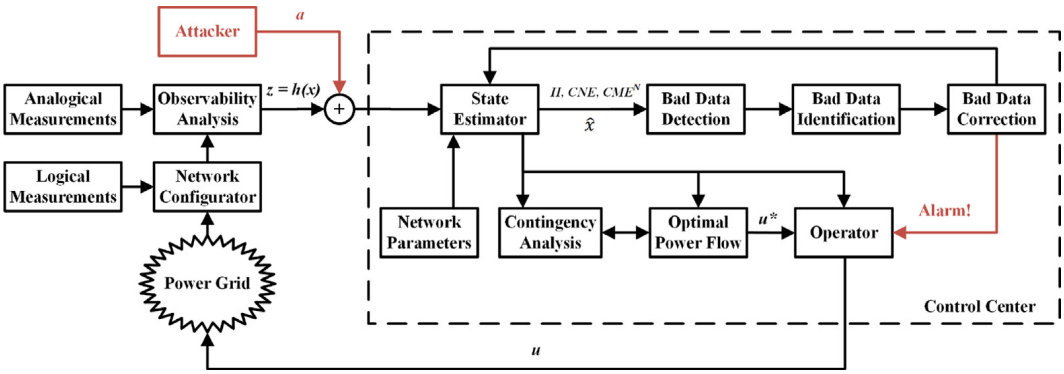

Figure 6: Cyber-attack analysis (BRETAS et al., 2017)

The heuristic proposed by (BRETAS et al., 2017) relies on power flow measurement in both directions and bus injections, therefore it will fail in the absence of some measurement. Moreover the correction based on composed normalized error CNE_i is done exclusively on branch resistance r and branch reactance x, as if the attack would always happen on both parameters.

Parameter cyber-attack identification is an intricate task especially in meshed systems due to parallel flows. In case of parameter cyber-attacks, the value alteration would significantly impact power flows which would make the LM approach ineffective. This situation is exemplified on a simple three bus system as depicted by Figures 7 and 8. Figure 8 has the same network configuration as Figure 7, apart from a 10% increase (or cyber-attack) on $1-2$ branch parameters, which lead to a change of 12% on branch $2-3$ power flow, 4% on branch $1-2$ and 5% on branch $1-3$.

2.5 Summary

Table 1 provides an overview of the bibliography researched.

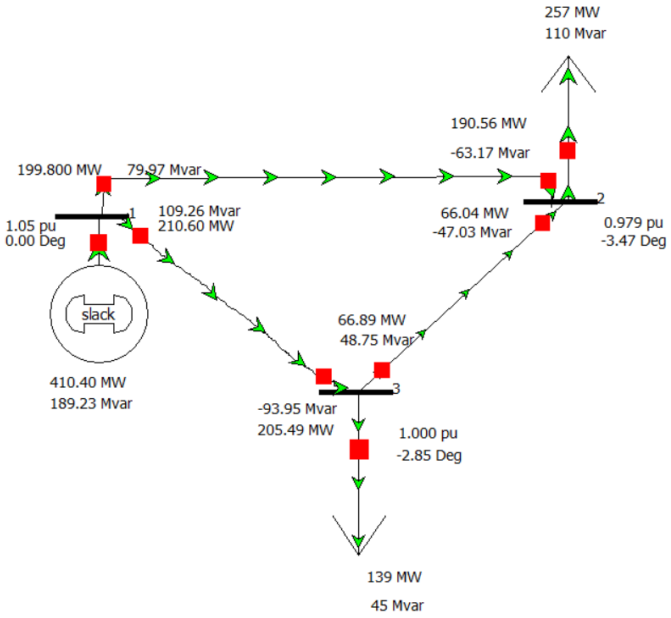

Figure 7: Meshed three bus system

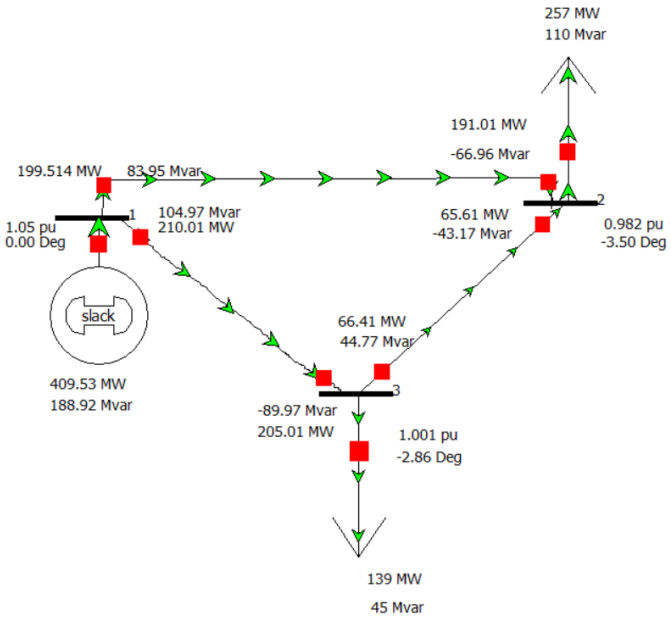

Figure 8: Meshed three bus system - $1-2$ modified branch parameters

Table 1: Literature Review Summary

	General	AB	CME^N based	NR based	Data Elimination	LM based	ASV	CNE	Constrains to solve NI	Weight to solve NI
CS	USA (2014a); YAN et al. (2012); TEN; LIU; MANIMARAN (2008); USA (2018); CHERDANTSEVA et al. (2016); SULLIVAN; KAMENSKY (2017); FOVINO et al. (2011); SUN; HAHN; LIU (2018); MEHRDAD et al. (2018)									
CS SE Vulnerability analysis	LIU; NING; REITER (2011), DÁN; SANDBERG (2010), TEIXEIRA et al. (2010), SANDBERG; TEIXEIRA; JOHANSSON (2010)									
CS SE impact analysis	MOHAJERIN ESFAHANI et al. (2010), ESFAHANI et al. (2010), MOUSAVIAN; VALENZUELA; WANG (2013); VALENZUELA; WANG; BISSINGER (2013), BOBBA et al. (2010); DÁN; SANDBERG (2010); KIM; POOR (2011); HUG; GIAMPAPA (2012); ZHAO et al. (2016); MOHAMMADPOURFARD; SAMI; SEIFI (2017); BRETAS et al. (2017); HU et al. (2018), YUAN; LI; REN (2011); XIANG et al. (2017)									
CS SE Countermeasures (CM)	KOSUT et al. (2010), KIM; POOR (2011), HUG; GIAMPAPA (2012), ASHOK; GOVINDARASU; AJARAPU (2016)									
CS SE CM CA modeled as MGE - detection and identification	BOBBA et al. (2010)		BRETAS et al. (2017)	HUG; GIAMPAPA (2012)						BRETAS et al. (2017)
CS SE CM CA modeled as PE - detection and identification			BRETAS et al. (2017)							BRETAS et al. (2017)
CS SE CM CA correction								BRETAS et al. (2017)		
SE	ABUR; EXPOSITO (2004); ZARCO; GOMEZ EXPOSITO (2000); MONTICELLI (1999); ASCHMONEIT; PETERSON; ADRIAN (1977); SCHWEPPE; WILDES (1970); GOMEZ-EXPOSITO et al. (2011); LIU; NING; REITER (2011); MINGUEZ; CONEJO (2007); CARO; CONEJO; MINGUEZ (2009); CARO et al. (2010); MONTICELLI; WU (1985); LONDON; ALBERTO; BRETAS (2007); GÓMEZ-EXPÓSITO et al. (2011)		BRETAS; BRETAS (2018)	CLEMENTS; COSTA (1998), GOMEZ-EXPOSITO et al. (2011), TEIXEIRA et al. (2010)		CLEMENTS; COSTA (1998)		BRETAS; BRETAS (2018)	ZHU; ABUR (2006), GJELSVIK; AAM; HOLTEN (1985), ASCHMONEIT; PETERSON; ADRIAN (1977)	BRETAS; CARVALHO; ALBERTINI (2015)
			BRETAS; BRETAS; PIERETI (2011), BRETAS; CARVALHO; ALBERTINI (2015), BRETAS; PIERRETI (2010), BRETAS; BRETAS (2015), BRETAS et al. (2013)	ZHU; ABUR (2006), ZHANG; ABUR (2013)						
SE MGE Correction					ZHU; ABUR (2006)			BRETAS; CARVALHO; ALBERTINI (2015), BRETAS; BRETAS (2015), BRETAS et al. (2013)		
SE PE Detection and Identification			BRETAS; CARVALHO; ALBERTINI (2015)			ZHU; ABUR (2006); LIN; ABUR (2016), ZHANG; ABUR (2013)				
SE PE Correction							ZHU; ABUR (2006)	BRETAS; CARVALHO; ALBERTINI (2015)		
SE Simultaneous Errors Detection and Identification	LOURENCO; COELHO; PAL (2015)			ZHANG; ABUR (2013)		ZHANG; ABUR (2013); LOURENCO; COELHO; PAL (2015)				
Smart Grid	BAKKEN et al. (2011), GIORDANO et al. (2013), USA (2014b), BRAZIL (2012), GOMEZ-EXPOSITO et al. (2011), USA (2017), RAPOSO; RODRIGUES; SILVA (2017)	KARIM; CURRIE; LIE (2018), ELKALASHY et al. (2016), HASSAN; ABIDO (2014)								

3 CURRENT MODEL AND METHODOLOGY

State estimation has been discussed for more than 20 years, specially in regards to general problem formulation. Based in the bibliography review, the author believes that the most suitable state estimation formulation is the composed measurement error approach as it minimizes the error and not the residual. The current model and methodology is implemented and tested in Matlab Software R2015a (MATLAB, 2015).

3.1 Normal equations SE and the Innovation approach

A state estimator is based on the nonlinear measurement model as described in equation (1) (SCHWEPPE; WILDES, 1970). What is being used from this formulation and to what extent is described in this chapter With the conventional WLS approach, the goal is to find the N-vector that minimizes $J(\mathbf{x})$ resulting on the formulation described on equation (2).

In BRETAS; CARVALHO; ALBERTINI (2015) the authors considered that all meters have standard deviations calculated by $\sigma_i = p_r|z_i^{lf}|/3$ where p_r is the meter's precision (considered 3%) and z_i^{lf} is the value of the $i-th$ measurement obtained from an exact load flow solution.

This approach is used since the measurements are not equal in magnitude, so their standard deviations should be proportional to their respective magnitudes.

In case of pseudomeasurements, or even measurements of low magnitudes, e.g., a no-generation and no demand bus (with zero active and reactive power injections), BRETAS; CARVALHO; ALBERTINI (2015) identify the null and near zero measurements, and then associates a low, but non-zero, standard deviation for those measurements. This latest procedure can lead to numerical problems therefore a new approach for this specific task is proposed in 4.1.

Based on equation (6) it is possible to interpret the SE solution as a projection of the measurements vector mismatch Δz onto the subspace spanned by the columns of the Jacobian matrix $\Re(H)$. The residual vector, that is orthogonal to $\Re(H)$, is defined by:

$$r = \Delta z - \Delta\hat{z} = \Delta z - K\Delta z = (I - K)\Delta z \tag{8}$$

.

The geometrical interpretation of operator K acting on vector Δz is depicted in Figure 9.

In BRETAS; BRETAS; PIERETI (2011); BRETAS et al. (2013); BRETAS; BRETAS (2018) demonstrated the existence of an undetectable component of the error $e_u \in \Re(H)$, which together with the detectable one $e_d \in \Re(H)^{\perp}$ form the measurement composing error $e = e_d + e_u$ and $||e||^2 = ||e_d||^2 + ||e_u||^2$. They proved that the undetectable part of

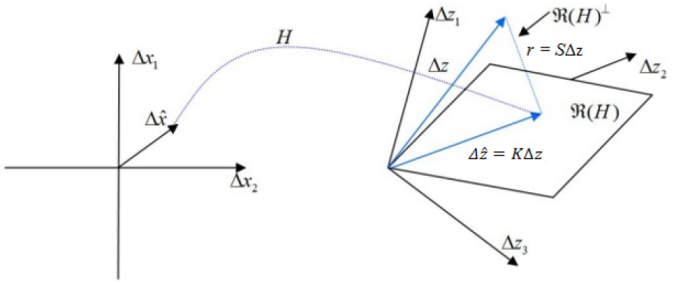

Figure 9: $\Delta z(x)$ projected on $\Re(H)$ and $\Re(H_p)$ (BRETAS; CARVALHO; ALBERTINI, 2015)

the error does not contribute to the residual vector, and thus, that small residual does not necessarily mean small error and vice-versa. The detectable component of the measurement error is the residual r.

A natural consequence of the previous is that the minimization, in x, of $J(x)$ in equation (2), will be reasonable, for state estimation purposes, only for the cases where the vector e_u, is equal or close to zero. In the engineering world however, the measurements and parameters may have large errors or even be modified by intruders and, as a consequence, before performing the SE those measurements and parameters need to be evaluated.

In order to address this issue BRETAS; BRETAS (2015) proposed a new objective function (9) which minimizes the measurement composing errors instead of the residual.

$$\min_x \sum (z_i - h_i(x))^2 \Big(1 + \frac{1}{II_i^2}\Big) W_{ii} \tag{9}$$

II_i is presented in (9) as the measurement innovation index, and is used to estimate the measurement errors based on the geometrical interpretation of state estimation, and $W_{ii} = R_{ii}^{-1} = 1/{\sigma_i}^2$ is the weight value. A measurement innovation index is defined as the new information related to other measurements; that suggests that it is the part of a measurement which is independent of those measurements and it is calculated by equation (10).

$$II_i = \frac{\sqrt{1 - K_{ii}}}{\sqrt{K_{ii}}} \tag{10}$$

Equation (10) supports the computation of the composed measurement error (CME) as described in (11). CME_i represents the values which results from the addition of the detectable and non-detectable error vector components (BRETAS et al., 2013), where r is the residual vector equal to $z - h(\hat{x})$. From (11) it is also possible to derive D which is defined as (12).

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

$$D_i = \Big(1 + \frac{1}{{II_i}^2}\Big)^{1/2} \tag{12}$$

${CME_i}^N$ is defined in equation (13).

$${CME_i}^N = D_i \frac{r_i}{\sigma_i} \tag{13}$$

Using (12) and (13) it is possible to rewrite equation (9) as follows:

$$\underset{x}{\text{minimize}} \quad J(\mathbf{x}) = {CME^N}^t CME^N \tag{14}$$

. This equation is solved applying the first order optimal condition, the Newton Raphson method is used, resulting in an iterative procedure that calculates x until the difference of $x^{k+1} - x^k$ is less than the tolerance of $1e-6$.

Instead of the measurement elimination (ZHU; ABUR, 2006), a countermeasure is proposed, with the measurement error correction using the composed normalized error CNE_i, as equation (15) and (16), where ${r_i}^N$ is the normalized residual, z_{ic} the corrected measurement and z_{ie} the measurement in error.

$$CNE_i = D_i {r_i}^N \tag{15}$$

$$z_{ic} = z_{ie} - CNE_i \sigma_i \tag{16}$$

3.2 Cyber-attack model

Data intrusion is the most common group of direct cyber attacks threatening the security of power systems. Cyber-attacks can be modeled as malicious data inserted to measurements and/or parameters and topology. Malicious data attacks will cause a non-Gaussian behavior of the error, equivalent to bad data, that can occur individually or combined mainly due to the following reasons:

1) A cyber-attack in measurement(s);

2) A cyber-attack in a transmission line (TL) parameter (series, shunt or tap);

3) A cyber-attack in system topology (inclusion or exclusion of TLs).

Only one type of topological cyber-attack model is used, that is setting the operation status to offline and have the power flow measurements values defined as zero.

4 PROPOSED MODEL AND METHODOLOGY

The rationale behind the improved methodology is the intelligent use of relaxations together with error analyses in a state estimator to attain high performance cyber-attack detection, identification and correction considering a reduced measurement's redundancy scenario and an evolving cyber-attack learning behavior.

There are two main relaxations in the problem to solve. First the use of a parameter error constraint together with an error minimization objective function. This combination provides important and accurate information with regards to a parameter cyber-attack through the analyses of the Lagrange multiplier, that is a relaxation of the parameter error condition. The second is needed in order to calculate the correct parameter in case of a cyber-attack. The augmented vector approach is inefficient under a low redundancy measurement level.

The proposed model and methodology is implemented and tested in Matlab Software R2015a (MATLAB, 2015).

In section 4.1 the deduction of a standard deviation for pseudo and low/zero magnitudes measurements is presented based on correlated variables and covariance properties. This approach solves numerical problems without having to use power injection constrains in the optimization model. The use of power injection constrains imposes the calculation of partial derivatives on each Newton Raphson loop. This is not necessary with the proposed approach.

Cyber-attack identification, detection and correction contemplating the evolving cyber-attack learning behavior is possible due to two aspects of the proposed methodology. One related to the use of mathematical tools that brings more accuracy in regards to multiple cyber-attacks as presented in section 4.2 and the other related to the process continuous flow as presented in section 4.4. A cyber-attack learning behavior would target vulnerable areas with reduced GRL, for example, that the current state-of-the-art methodologies are not covering.

In section 4.2 a Lagrange relaxation and composed normalized error (CNE) based model for cyber-attacks as a malicious data attack detection and identification method is detailed. Lagrange relaxation together with composed normalized error has never been used to detect and identify cyber-attacks. Due to the continuous process flow the LM assumption that no measurement gross errors exist is not necessary.

Section 4.3 presents the hybrid iterative relaxed strategy for parameter cyber-attack correction. This process calculates parameters with states being considered correct; then calculates states with parameters being considered correct; in a continuous manner using convergence tolerance as a way to explore the range of possible answers. The continuous flow is a way to achive a HRC within the state estimator as depicted in Figure 4.2.

4.1 Standard deviation for pseudo and low/zero magnitude measurements

For a set of pseudomeasurements, or even measurements of low magnitudes, e.g., a no-generation and no demand bus (with zero active and reactive power injections) it is proposed a weight value calculation based on correlated variables and covariance properties based in the formulation below.

For two variables, the covariance is related to the variance by equation (17) (KYLE, 2017).

$$var(x+y) = var(x) + var(y) + 2.cov(x,y) \tag{17}$$

Then using $cor(x,y) = cov(x,y)/(std(x).std(y))$ it possible to rewrite (18) as

$$var(x+y) = var(x) + var(y) + 2.cor(x,y).std(x).std(y). \tag{18}$$

By using the definition $std(x) = sqrt(var(x))$ or the equivalent $var(x) = std(x)^2$ and (18), (19) is defined.

$$std(x+y) = \sqrt{std(x)^2 + std(y)^2 + 2.cor(x,y).std(x).std(y)} \tag{19}$$

Considering power injection at bus i, P_i, as the sum of all power flow measurements arriving to bus i, $P_{i\Omega}$, with Ω being all adjacent buses to i. All $P_{i\Omega}$ can be considered as close to independent variables so the correlation between them can be considered as null (COTILLA-SANCHEZ et al., 2012). If so, and considering equation (19), it is possible to infer that the standard deviation of power injection at bus i is equal to the square root of the power flow measurement's standard deviation arriving to bus i sum as described by equation (20) with Ω being all adjacent buses.

$$std(P_i) = \sqrt{\sum_{j=1}^{\Omega} std(P_{ij})^2} \tag{20}$$

4.2 Lagrange relaxation and composed measurement error based model

The calculation of a Lagrange multiplier related to each network parameter is feasible if an equality constraint for parameters is considered. Initially, one can consider that all parameters have no errors, that is the parameter errors are all zeros, and this assumption will be confirmed or not based on the LM analysis. Let us further assume that the measurements are without errors. Under such conditions, the parameters are equal to the true value, p_r. Let us call $p' = p - p_r$

The WLS-SE problem with parameter constraints is then formulated as (21) where $W = R^{-1} = Cov(e)^{-1} = diag({\sigma_1}^2, {\sigma_2}^2, ..., {\sigma_m}^2)^{-1}$ and $h(x,p)$ is the nonlinear function relating the measurements to the system states and network parameters.

$$\begin{aligned} \underset{x,p'}{\text{minimize}} \quad & J(x) = \frac{1}{2} CME^t \, W \, CME \\ \text{subject to} \quad & p = p_r \end{aligned} \tag{21}$$

ZHU; ABUR (2006) has proven that the problem in (2) is entirely equivalent to the problem in (21), considering the residual instead of the composed measurement error. The question is how to generalize the paper proof (ZHU; ABUR, 2006) to any condition. For

that purpose, considering the Implicit Function Theorem, if a property is valid for this initial condition, and there is no bifurcation going from it to another one, then that property is valid for any other condition. Thus, at the solution of (21), this property should also be valid if no bifurcation exists. Using Lagrange relaxation it is possible to write equation (21) as (22) where λ_{CELM} are the LMs for the equality constraint in (22). Another more detailed form of (22) is described in (24) using (23). It is important to highlight that this formulation is different than the proposed in previously researches, as the error, not the residual, is used to derive LM, therefore the LM is renamed LMI (Lagrange Multiplier Innovation based)

$$\underset{x,p'}{\text{minimize}} \quad L = \frac{1}{2} CME^t \, W \, CME - \lambda_{CELM} p' \tag{22}$$

$$CME = D(z - h(x, p')) \tag{23}$$

$$\underset{x,p'}{\text{minimize}} \quad L = \frac{1}{2} (D(z - h(x, p')))^t \, W \, D(z - h(x, p')) - \lambda_{CELM} p' \tag{24}$$

The first order optimal condition is applied resulting in the following equations:

$$\frac{\partial L}{\partial x} = -(D \, H_x)^t \, W \, CME = 0 \tag{25}$$

$$\frac{\partial L}{\partial p'} = -(DH'_p)^t \, W \, CME - \lambda_{CELM} = 0 \tag{26}$$

$$\frac{\partial L}{\partial \lambda_{CELM}} = -p' = 0 \tag{27}$$

Where H_x is the Jacobian matrix of $\partial h(x, p')/\partial x$ and H_p the Jacobian matrix of $\partial h(x, p')/\partial p'$. The corresponding Jacobian matrix elements are described in appendix A.

Using equation (26), λ_{CELM} is expressed in terms of CME as described by (28) where S is the parameter sensitivity matrix defined by (29).

$$\lambda_{CELM} = S \, CME \tag{28}$$

$$S = -(DH'_p)^t \, W \tag{29}$$

If the measurement errors are zero mean random variables with covariance matrix $Cov(e) = R$ then λ_{CELM} is a zero mean random vector with covariance matrix V. As a consequence, under these conditions, λ^N_{CELMi} is a zero mean random variable with unity variance and it is possible to compare it with a statistically reasonable threshold and to evaluate its significance and parameters errors.

$$\lambda^N_{CELMi} = \frac{\lambda_{CELMi}}{\sqrt{V_{ii}}} \tag{30}$$

It is possible to define V as $V = cov(\lambda_{CELM}) = S(cov(CME))S^t$, the covariance of CME is equal to $Cov(e) = R$, so $V = cov(\lambda_{CELM}) = S \, R \, S^t$. Parameter cyber-attack detection and identification is made when λ^N_{CELMi} value is above the defined threshold of three, considering a confidence level of 97%.

4.3 Hybrid iterative relaxed approach

How to correct a measurement error if the parameter may be simultaneously in error, and the other way around? State-of-the-art solutions make strong assumptions as the corrections of the parameters are made when measurements have no error, or the opposite. In real-world engineering applications such assumptions are far from reality, since attacks are evolving and may occur on both simultaneously.

To solve this problem a hybrid iterative relaxed strategy is presented. Consider a simultaneous measurement and parameter cyber-attack. Ponder still that the parameter attack is identified first, considering the error pattern approach proposed previously.

After a parameter cyber-attack detection and identification it is necessary to correct it. Assuming the attacked parameter name p_c, $p(n)$ the new parameter to be estimate, n being the iteration number.

As an example $p(1)$ equals to the current value storage in p_c when the hybrid iterative relaxed approach code is run for the first time. Using the system states already calculated through the solution of (14), the equation (32) is solved in a continuous manner with a new parameter $p(n)$ being calculated by the addition of Δp to $p(n-1)$ until Δp is smaller than the parameter correction process tolerance (PCPT).

The first PCPT assumed value is quite big (e.g. 10^3) and after the first convergence the state estimation runs estimating new states, which means an iteration of L5 loop.

In the process, the PCPT value is reduced by one fifth in every iteration of L5 loop. (32) is continuously solved followed by a conventional state estimation until the PCPT reaches a pre defined small value. This process is carried out iteratively as describes algorithm (1).

As the approach is iterative and relaxed even with a simultaneous measurement cyber-attack the algorithm converges and continue to L4 loop, which means, a better estimated parameter value is found, enabling the detection and identification of further cyber-attacks or the correct state estimation.

After convergence the parameters are considered as without errors, following to loop L4, new states are estimated, $x(k+1)$. If it is the case, measurements cyber-attacks will be corrected with the estimated CNE (BRETAS et al., 2017), obtaining $z(n+1)$ and following to loop L2.

This problem relaxes the model by considering the parameters without error, and does not generate any observability problems or decrease the degrees of freedom of the original measurement model. These new states and corrected measurements are used again to estimate the new set of parameters, $p(n+2)$, through the solution of (31). An iterative process is built based on such decomposition.

As such, it is considered initially that all measurements are free from errors. Then one can estimate the system states, $x(n)$, considering parameters $p(n)$, through the iterative solution of $z(n) = h(x(n))$.As the measurements and parameters might be simultaneously in error, thus the iterative process is proposed. One considers that $z(n)$ is equal to

$$z(n) = h(x(n), p(n)) + \frac{\partial h(x(n), p(n))}{\partial p} \Delta p \tag{31}$$

In such a model the degrees of freedom are not decreased reducing observability problems, since in the relaxed model it is considered that the measurements are correct.

To solve equation (32), where H_{pc} is the Jacobian matrix of $\partial h(x, p_c)/\partial p_c$, W_{pc}, the inverse of the covariance matrix of the parameter estimate needs to be calculated using equation (33) as proposed by (MONTICELLI, 1999).

$$\Delta p = (H'_{pc} W_{pc} H_{pc} + W_{pc})^{-1} (H'_{pc} W_{pc} \Delta z + W_{pc}(p(n) - p(n-1))) \tag{32}$$

$$W_{pc} = H'_{pc} W H_{pc} + W_{pc} - H'_{pc} W H_x (H'_x W H_x)^{-1} H'_x W H_{pc} \tag{33}$$

Algorithm 1 HIRA algorithm

while $iter < 500$ and $PCPT > 1e-6$ **do**
looppar:
Calculate Δp using 32
$p(n-1) \leftarrow p(n)$
$p(n) = p(n) + \Delta p$
$tol_{dp} = abs(\Delta p)$
Calculate W_{pc} using 33
if $tol_{dp} < tolvalue_{dp}$ **then**
    goto *loopstates*
if $tolvalue_{dp} > 1e-6$ **then**
    $tolvalue_{dp} = \dfrac{tolvalue_{dp}}{5}$
    $PCPT = tolvalue_{dp}$
    goto *looppar*
loopstates:
States calculated through the solution of (14) while $tol = x^{k+1} - x^k > 1e-6$
$iter = iter + 1$
goto *looppar*

4.4 Holistic resilience cycle based methodology

Figure 10 illustrates the cyber-attacks by author's view. Proposed improved methodology process are represented in gray and are dealing with cyber-attacks as illustrated in Figures 11 and 12 in a continuous flow going through the HRC stages.

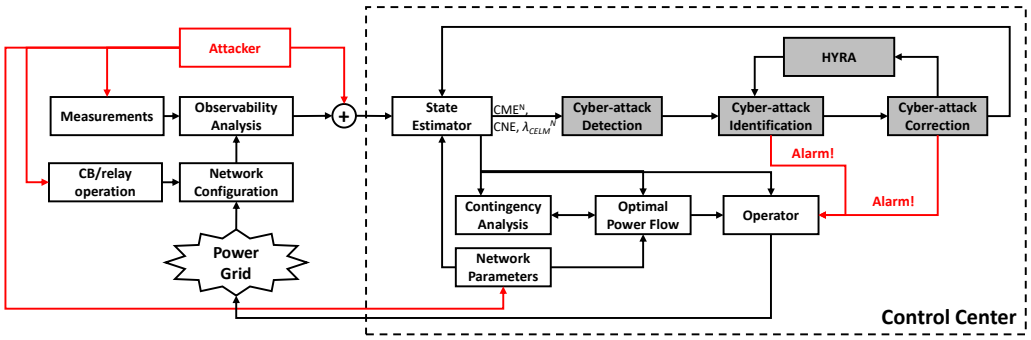

Figure 10: Cyber-attack by author's view

Figure 11 illustrates the methodology cyber-attack detection process and Figure 12 presents processes with regards to measurement, parameter and topological cyber-attacks identification and correction.

In Figure 11 a cyber attack detection is made by analysis of the CME^N and λ_{CELM} after a state estimation error minimizing process. Identification of cyber attack in parameters is made first considering ${\lambda_{CELM}}^N > 3$. Parameter Cyber-attack correction is made considering the hybrid iterative relaxed strategy. A measurement cyber-attack is identified and corrected if: i) CME_i^N value is > 3 and ii) all ${\lambda_{CELM}}^N$ are < 3 or a topology cyber-attack is identified as true and corrected if: i) CME_i^N value is > 3 in adjacent nodes and ii) all ${\lambda_{CELM}}^N$ are < 3. In the presented solution, states are estimated after measurement, parameter or topology cyber-attack correction.

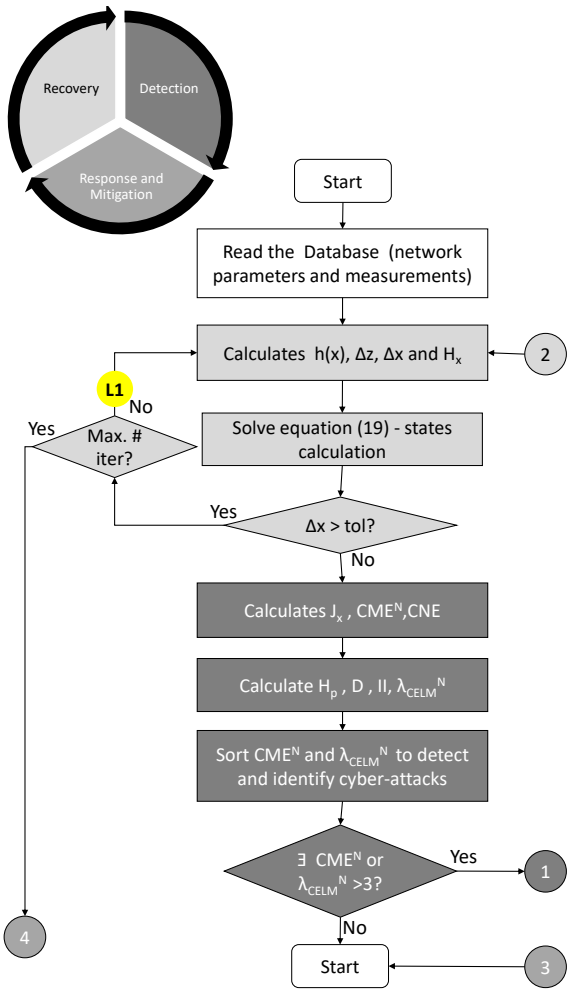

Figure 11: Proposed methodology flowchart - Part 1

Most important processes are described in the following.

1) Variables calculation: Lagrange multiplier vector ${\lambda_{CELM}}^N$ as equations (30) and ${CME_i}^N$ as equation (13), and other ancillary values are calculated;

2) Cyber-attack identification and detection: Cyber-attacks on measurements will cause a Hypothesis Testing Error Detection characterized with a high local CME^N. The attacked measurement will present a CME^N above a chosen threshold value (usually equal to three standard deviations of the corresponding measurement (BRETAS et al., 2013)). Lagrange multiplier vector ${\lambda_{CELM}}^N$ is sorted and the largest with value above threshold (3.0) is used to detect and identify a cyber-attack modeled as parameter's

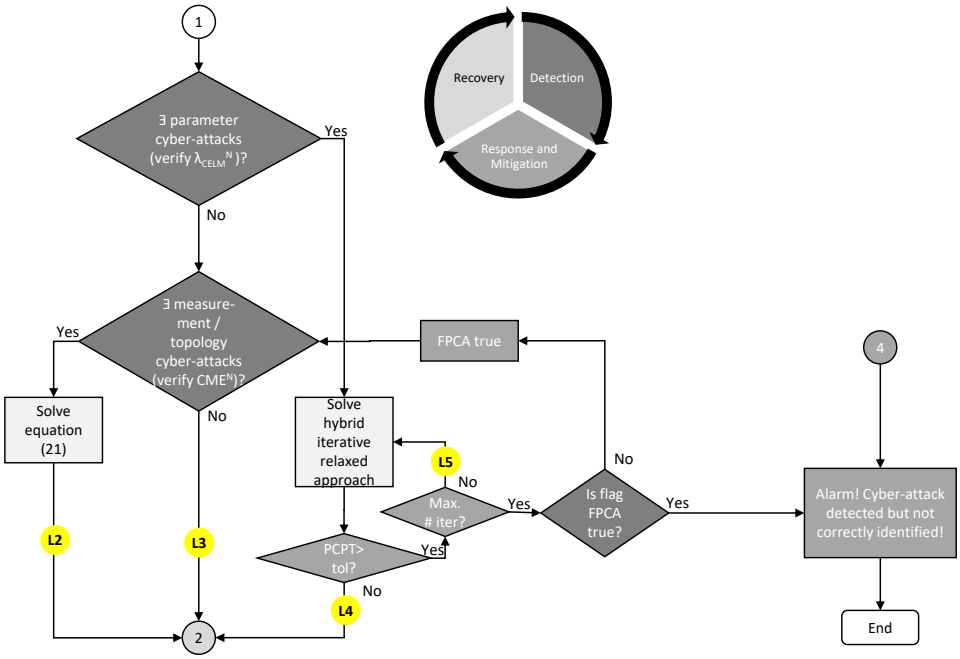

Figure 12: Proposed methodology flowchart - Part 2

errors (threshold selection is a consequence of the χ^2 Hypothesis Testing application to the normalized Lagrange multiplier. The chosen reliability index is 97%);

3) Cyber-attack correction: Following the process of detection and identification the countermeasure approach proposed of correcting the attacked measurement/topology or parameter using CNE and the Hybrid iterative relaxed approach 4.3 is carried out.

In the presented flowchart, on all software loops L1, L2, L3, L4 and L5 the states are recalculated. Moreover based on a number of software iterations during the HIRA process a two step procedure is applied:

1) Test if this could be a false parameter attack identification (FPCA) - go to position 5 of the flowchart, which means testing only measurements cyber-attacks by verifying CME_i^N and correcting it.

2) Cyber-attack detected but incorrect identified, alarm set.

4.5 Overview

The proposed methodology contributions as described in chapter 4 can be divided into two streams, one related to mathematical models and other to process flow.

In both streams the core idea is to use efficient strategies to deal with evolving cyber-attack learning behavior. Targeting vulnerable areas with reduced GRL or simultaneous attacks are possible learning behavior.

A cyber-attack on remote terminal units, communication channels and SCADA Master database or A1, A2 and A3 as represented on Figure 3 is a possible situation and the presented methodology has to deal with such attacks. Chapter 5 presents case studies and results to prove this ability.

5 CASE STUDY AND RESULTS

The presented methodology was tested using the IEEE 14-bus and 57-bus systems where cyber-attacks composed of malicious injected data to measurements and/or parameters/topology were investigated.

Two different measurement sets or GRLs were analyzed. One considering voltage measurements on the slack bus, active and reactive power injections and flows on all buses, with a GRL of 3 for both 14-bus and 57-bus. Another, considering a smaller and more realistic GRL of 2.8, where power flow meters are not found in all system lines branches (RAPOSO; RODRIGUES; SILVA, 2017).

As described in 3.2 there are different types of cyber-attacks.

5.1 IEEE 14-bus Test System

The IEEE 14 Bus Test Case represents a portion of the American Electric Power System (in the Midwestern US) as of February, 1962. It has balanced loads and transposed lines and is often used in papers related to state estimation (ZHU; ABUR, 2006; BRETAS; CARVALHO; ALBERTINI, 2015; BRETAS; BRETAS, 2015; BRETAS et al., 2017; LIU; NING; REITER, 2011; DÁN; SANDBERG, 2010; KOSUT et al., 2010; BOBBA et al., 2010). Figure 13 illustrates the IEEE 14-bus Test System. All measurements used were generated through power flow with a fixed random noise added. Measurement values without error are found in appendix B.

5.1.1 Multiple measurement cyber-attack scenario

Cyber-attacks on measurements are those that can occur on position A1, A2 or A3 as depicted in Figure 3. They are detected by hypothesis testing error, which is indicated with a high local CME^N. The affected measurement will present a CME^N above a chosen threshold value (based on a desired level of detection sensitivity). In the state estimation literature, usually it is equal to three standard deviations of the corresponding measurement, i.e.$\beta = 3$ (BRETAS et al., 2017). Considering GRL above 3, if the conditions stated below are all true, the measurement cyber-attack is recognized as true and corrected using the CNE as described in the methodology.

i) CME_i^N value is > 3.

ii) all ${\lambda_{CELM}}^N$ are < 3.

Supposing the measurement cyber-attack as described:

1) Cyber-attack of magnitude 9σ added to measurement $Q : 08-07 = 0.1762pu$ (reactive power flow from bus 8 to bus 7)

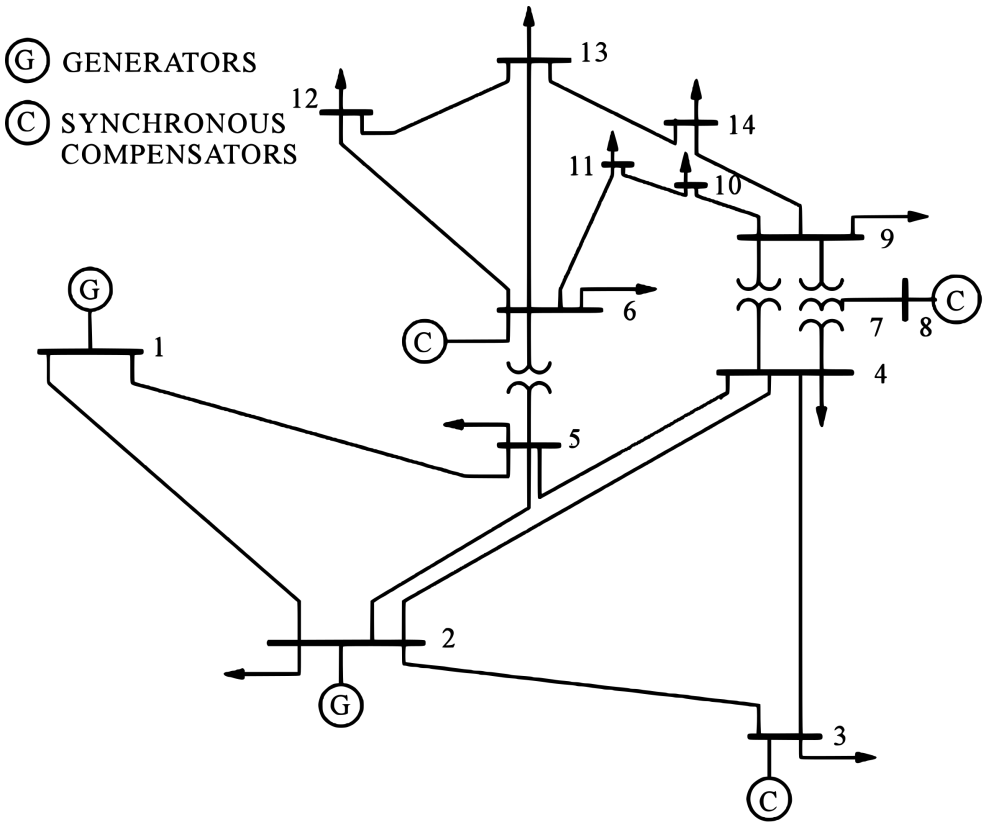

Figure 13: IEEE 14-bus Test System

2) Cyber-attack of magnitude 5σ added to measurement $P : 01 - 02 = 1.5683pu$ (active power flow from bus 1 to bus 2)

3) Cyber-attack of magnitude 4σ added to measurement $P : 03 = -0.9420pu$ (active power injection at bus 3).

The following results are found in Tables 2, 3 and 4. Each Table presents the values found until L2 loop as described in Figure 12.

Table 2: 14-bus - multiple measurement cyber-attack - 1^{st} loop - CME^N

CME^N descending list		
Measurement	CME^N	CNE
$Q : 07 - 08$	6.715	8.914
$Q : 8$	5.607	8.075
$P : 01 - 02$	4.056	4.128
$P : 3$	3.931	4.029
$P : 7$	2.312	2.383
Corrected Measurement:		
$Q : 07 - 08$	0.1726	

Table 5 indicates the most significant variances of state values just before and after the states are recalculated after all measurements are corrected. Decrease in the difference between estimated states and the real ones (generated by the original system load flow) is

Table 3: 14-bus - multiple measurement cyber-attack -2^{nd} loop - CME^N

CME^N descending list		
Measurement	CME^N	CNE
$P:01-02$	4.060	4.132
$P:2$	3.931	4.029
$P:03-04$	1.164	1.335
$P:2$	0.870	3.559
$Q:03-04$	0.868	0.959
Corrected Measurement:		
$P:01-02$	1.5714	

Table 4: 14-bus - multiple measurement cyber-attack -3^{rd} loop - CME^N

CME^N descending list		
Measurement	CME^N	CNE
$P:03$	4.020	4.120
$P:03-04$	1.085	1.244
$Q:03-04$	0.787	0.870
$P:04-05$	0.683	0.713
$P:12-06$	0.561	0.608
Corrected Measurement:		
$P:03$	-0.9432	

considered as an answer improvement. It is possible to notice a comparative improvement of at least 20% in all of the states. After these three L2 loops the largest CME^N value was

Table 5: States (phase in degrees and voltage in kV) variation and answer improvement for measurement cyber-attack

$State_{Bus}$	IEEE values	Before Correction	%	After Correction	%	Improvement %
$Angle_{13}$	-15.169	-15.136	0.22	-15.142	0.17	20
$Angle_{8}$	-13.368	-13.347	0.16	-13.351	0.13	20
$Angle_{14}$	-16.036	-16.011	0.16	-16.018	0.11	29
$Voltage_{13}$	105.000	105.162	0.15	105.113	0.11	30
$Angle_{12}$	-15.077	-15.054	0.15	-15.061	0.11	28

equal to 0.6284, below the threshold value of 3. The Lagrange multipliers were checked in all loops and no value above threshold was found.

5.1.2 Multiple measurement and parameter cyber-attack scenario

Cyber-attacks on parameters are those that can occur on position A3 as depicted in Figure 3. They are detect through the hypothesis testing error, which is indicated with a high λ^N_{CELM}. The affected parameter will present the corresponding λ^N_{CELM} above a chosen threshold value equal to three standard deviations. Individual (reactance or resistance) parameter cyber-attacks are not possible to be observed by local CME^N_i as the

following results prove. Malicious data to measurements and parameters were added in order to test this cyber-attack scenario. The first multiple simultaneous measurement and parameter set of attack using the IEEE 14-bus is described as follows:

1) Cyber-attack of magnitude 9σ added to measurement $Q : 08-07 = 0.1762pu$ (reactive power flow from bus 8 to bus 7)

2) Cyber-attack of magnitude 5σ added to measurement $P : 01 - 02 = 1.5683pu$ (active power flow from bus 1 to bus 2)

3) Cyber-attack of 6% added to the 02-03 line parameter $r_{02-03} = 0.04699pu$ resistance only.

Note in Table 6 that although CME^N has values above threshold, according to the heuristic proposed by (BRETAS et al., 2017) it is not possible to detect or identify a parameter cyber-attack, but the ${\lambda_{CELM}}^N$ value above three as indicated in Table 7 provides the correct parameter cyber-attack indication.

The Hybrid Iterative relaxed approach is run adjusting the r_{02-03} parameter value and states in a continuous manner until the pre-defined tolerance is reached after 350 iterations. Table 9 indicates the states variation and answer improvement before and after the HIRA process.

The corrected value as indicated in Table 7 is 2.33% different than the true value. As a manner to understand why the correction was not precise, the same cyber-attack was tested without measurement cyber-attack, and the corrected value was only 0.22% different after 87 iterations. On the second loop the LM was still above threshold as indicated in Table 8 and the HIRA process was run again. After two loops with similar LMs values the parameter reached its correct value as the LM value indicated, present in Table 10.

Table 6: 14-bus - multiple measurements and parameters cyber-attacks -1^{st} loop - CME^N

CME^N descending list	
Measurement	CME^N
Q:03-02	20.575
Q:02-05	15.256
Q:04-03	14.515
Q:03-04	13.830
Q:02-03	10.272

After the parameter correction, states were recalculated and the methodology continuous process verified again CME^N and ${\lambda_{CELM}}^N$. As expected with the corrected parameter no ${\lambda_{CELM}}^N$ was above three. As cyber-attacks happened simultaneously on parameters and measurements, there were CME^N values above threshold as presented in Table 11. The largest CME^N value was used for cyber-attack identification. The measurement value was corrected using CNE. The continuous process was run until no more CME^N or ${\lambda_{CELM}}^N$ was above threshold.

In order to further test the algorithm another multiple measurement and parameter cyber-attack simulation was tested as follows:

1) Cyber-attack of magnitude 6σ added to measurement $P : 04 - 09 = 0.1609pu$ (active flow from bus 4 to bus 9)

Table 7: 14-bus - multiple measurements and parameters cyber-attacks -1^{st} loop - ${\lambda_{CELM}}^N$

${\lambda_{CELM}}^N$ descending list	
Parameter	${\lambda_{CELM}}^N$
r_{02-03}	23.258
x_{02-03}	20.586
x_{03-04}	20.176
r_{03-04}	16.600
Corrected Parameter:	
r_{02-03}	0.0481

Table 8: 14-bus - multiple measurement and parameter cyber-attack - 2^{nd} HIRA loop - ${\lambda_{CELM}}^N$

${\lambda_{CELM}}^N$ descending list	
Parameter	${\lambda_{CELM}}^N$
r_{02-03}	8.895
x_{02-03}	8.156
x_{03-04}	8.009
r_{03-04}	6.154

Table 9: States (phase in degrees and voltage in kV) variation and answer improvement for measurement and parameter cyber-attack - 1^{st} loop

$State_{Bus}$	IEEE values	Before Correction	%	After Correction	%	Improvement %
$Angle_8$	-13.368	-11.441	14.42	-11.521	13.82	4
$Angle_4$	-10.324	-10.153	1.66	-10.254	0.68	59
$Angle_{13}$	-15.169	-14.928	1.59	-15.054	0.76	52
$Angle_5$	-8.783	-8.644	1.58	-8.725	0.66	58
$Angle_6$	-14.223	-14.006	1.53	-14.124	0.69	55

Table 10: 14-bus - multiple measurement and parameter cyber-attack - 4^{th} HIRA loop - ${\lambda_{CELM}}^N$

${\lambda_{CELM}}^N$ descending list	
Parameter	${\lambda_{CELM}}^N$
r_{02-03}	1.875
r_{03-04}	1.619
x_{02-04}	1.590
x_{01-02}	1.504
Corrected Parameter:	
r_{02-03}	0.0468

Table 11: 14-bus - multiple measurement and parameter cyber-attack -5^{th} loop - CME^N

CME^N descending list		
Measurement	CME^N	CNE
Q:08-07	6.643	8.820492
Q:08	5.538	7.97039
P:01-02	4.956	5.042223
Q:03-04	2.299	2.370401
Q:02-03	1.633	2.836861

2) Cyber-attack of 6% added to the 06-12 line parameter $x_{06-12} = 0.25581pu$ (06-12 line reactance) only.

A similar cyber-attack scenario is suggested by (BRETAS et al., 2017) with one difference, cyber-attacks in parameters data happen simultaneously on all line's parameters: branch resistance r and branch reactance x.

In this case though, the Lagrange multiplier ${\lambda_{CELM}}^N$ for the parameter constraint is calculated with values and respective parameters indicated in Table 12. The Table also compares ${\lambda_{CELM}}^N$ and the λ^N as described by (ZHU; ABUR, 2006). Using ${\lambda_{CELM}}^N$ above threshold value of 3, parameter error was correctly detected and identified. Using the HIRA parameter and states were corrected. As one can see, in such a scenario the methodology proposed by ZHU; ABUR (2006) would not be able to detect such a parameter attack. Table 12 presents the ${\lambda_{CELM}}^N$ largest values and the corrected parameter value.

Table 12: 14-bus - multiple measurements and parameters cyber-attacks case two -1^{st} loop - ${\lambda_{CELM}}^N$

${\lambda_{CELM}}^N$ descending list		
Parameter	${\lambda_{CELM}}^N$	λ^N
x_{06-12}	3.082	2.885
r_{06-12}	2.981	2.760
r_{06-13}	2.347	2.118
x_{13-14}	2.036	1.687
Corrected Parameter:		
x_{06-12}: 0.25846		

Through the analysis of Table 13, which presents the second loop process, it is possible to observe that the measurement attack was detected as the threshold defined value of the highest CME^N was above three and in an isolated measurement. The cyber-attack was corrected using the CNE and equations (24) and (14) were calculated again. The continuous process iterated until no more CME^N value were above three.

Having information of power flow in both directions is an acceptable assumption in meshed transmission systems, however in a scenario where these measurements are not present, methodologies based on this assumption may fail to detect and identify parameter cyber-attacks. Cyber-attacks are an evolving phenomena. This premise is analyzed in this cyber-attack scenario, where attacks may happen in parts of the power system where there is not such a high measurement density, exploring the Lagrange multiplier as a complementary tool to the innovation approach.

Table 13: 14-bus - multiple measurement and parameter cyber-attack case two -1^{st} loop - CME^N

CME^N descending list		
Measurement	CME^N	CNE
$Q:07-08$	6.715	8.914
$Q:8$	5.607	8.075
$P:01-02$	4.056	4.128
$P:3$	3.931	4.029
$P:7$	2.312	2.383
Corrected Measurement:		
$Q:07-08$	0.1726	

The same attack scenario was tested with some measurements of power flow missing, those related to the parameters' branch which had the cyber-attack. The original set encompassed 82 measurements with a GRL of 3.04 and the new set 77 with a GRL of 2.85.

The fist loop process presents ${\lambda_{CELM}}^N$ with values and respective parameters indicated in table 14. Using ${\lambda_{CELM}}^N$ above threshold value of 3, parameter error was correctly detected and identified. Using the Hybrid iterative relaxed approach, parameter and states were corrected. As previously explained, measurement attack was detected as the highest CME^N value was above three.The continuous process was run until no more CME^N or ${\lambda_{CELM}}^N$ was above 3.

Table 14: 14-bus - multiple measurements and parameters cyber-attacks -1^{st} loop - ${\lambda_{CELM}}^N$ - GRL 2.8

Parameter	${\lambda_{CELM}}^N$
x_{06-12}	5.949
r_{12-13}	4.172
r_{01-05}	3.990
x_{04-05}	3.707
Corrected Parameter:	
x_{06-12}: 0.256	

5.1.3 Multiple measurement, parameter and topological cyber-attack scenario

A cyber-attack in system topology (inclusion or exclusion of TLs) is the equivalent of setting the operational line status as offline, which means to set the active and reactive power flow measurements to zero. This cyber-attack, in addition to measurement and parameter, is tested in this scenario as described as follows:

1) Cyber-attack of magnitude 6σ added to measurement $P:09=-0.29533$ (active power injection on bus 9)

2) Cyber-attack of 6% added to the 02-05 line parameter $x^{sh}_{02-05}=0.0346pu$

3) Topological cyber-attack at line 13-14, setting the operational line status as offline.

Table 15: 14-bus - multiple measurement, topology and parameter cyber-attack -1^{st} loop - CME^N

CME^N descending list	
Measurement	CME^N
$Q:02-05$	5.700
$P:09$	4.771
$Q:05$	4.657
$Q:04-09$	3.638
$Q:05-01$	3.075

Table 16: 14-bus - multiple measurement, topology and parameter cyber-attack -1^{st} loop - λ^N_{CELM}

${\lambda_{CELM}}^N$ descending list	
Parameter	λ^N
x^{sh}_{02-05}	6.422
r_{02-05}	6.346
x_{01-05}	4.840
r_{04-05}	4.709

The first loop values for CME^N and λ^N_{CELM} are presented in Tables 15 and 16 respectively.

Three L4 loops presented λ^N_{CELM} values above threshold and the parameters were corrected with the following values: 0.03694, 0.036392, 0.03589. Finally on the forth loop there were no more λ^N_{CELM} above three. Still, with a measurement and topology cyber-attack, the CME^N had values above three as indicated in Table 18. Measurement $P:09$ was corrected using CNE and the process proceeded to L2. After the states correction no more CME^N values above threshold were found, so no topological cyber-attack was detected. Nevertheless the calculated states are very close to the correct ones as presented in Table 19, which indicates a cyber-attack without stability consequences.

Table 17: 14-bus - multiple measurement, topology and parameter cyber-attack -4^{th} loop - λ^N_{CELM}

${\lambda_{CELM}}^N$ descending list	
Parameter	λ^N
x^{sh}_{02-05}	2.984
r_{09-10}	2.972
r_{02-05}	2.960
x_{09-10}	2.179
Corrected Parameter:	
x^{sh}_{02-05}	0.035540814

Table 18: 14-bus - multiple measurement, topology and parameter cyber-attack -5^{th} loop - CME^N

CME^N descending list		
Measurement	CME^N	CNE
P:09	5.018	6.08379
P:10-09	3.225	15.70697
Q:02-05	2.848	9.727092
P:07-09	2.121	2.586903
Q:05	2.093	21.11171
Corrected Measurement:		
P:09	-0.2952	

Table 19: 14-bus - States (phase in degrees and voltage in kV) variation of measurement, topology and parameter cyber-attack

$State_{Bus}$	IEEE values	After Correction	%
$Angle_2$	-4.981	-4.992	0.23%
$Angle_3$	-12.718	-12.738	0.16%
$Angle_4$	-10.324	-10.351	0.26%
$Angle_5$	-8.783	-8.802	0.23%
$Angle_6$	-14.223	-14.245	0.15%
$Angle_7$	-13.368	-13.381	0.10%
$Angle_8$	-13.368	-13.337	0.23%
$Angle_9$	-14.947	-14.964	0.12%
$Angle_{10}$	-15.104	-15.122	0.12%
$Angle_{11}$	-14.795	-14.816	0.14%
$Angle_{12}$	-15.077	-15.101	0.16%
$Angle_{13}$	-15.169	-15.183	0.09%
$Angle_{14}$	-16.036	-16.057	0.13%
$Voltage_1$	106.000	105.971	0.03%
$Voltage_2$	104.500	104.476	0.02%
$Voltage_3$	101.000	100.970	0.03%
$Voltage_4$	101.900	101.821	0.08%
$Voltage_5$	102.000	101.994	0.01%
$Voltage_6$	107.000	106.953	0.04%
$Voltage_7$	106.200	106.155	0.04%
$Voltage_8$	109.000	108.948	0.05%
$Voltage_9$	105.600	105.587	0.01%
$Voltage_{10}$	105.100	105.086	0.01%
$Voltage_{11}$	105.700	105.664	0.03%
$Voltage_{12}$	105.500	105.472	0.03%
$Voltage_{13}$	105.000	104.992	0.01%
$Voltage_{14}$	103.600	103.539	0.06%

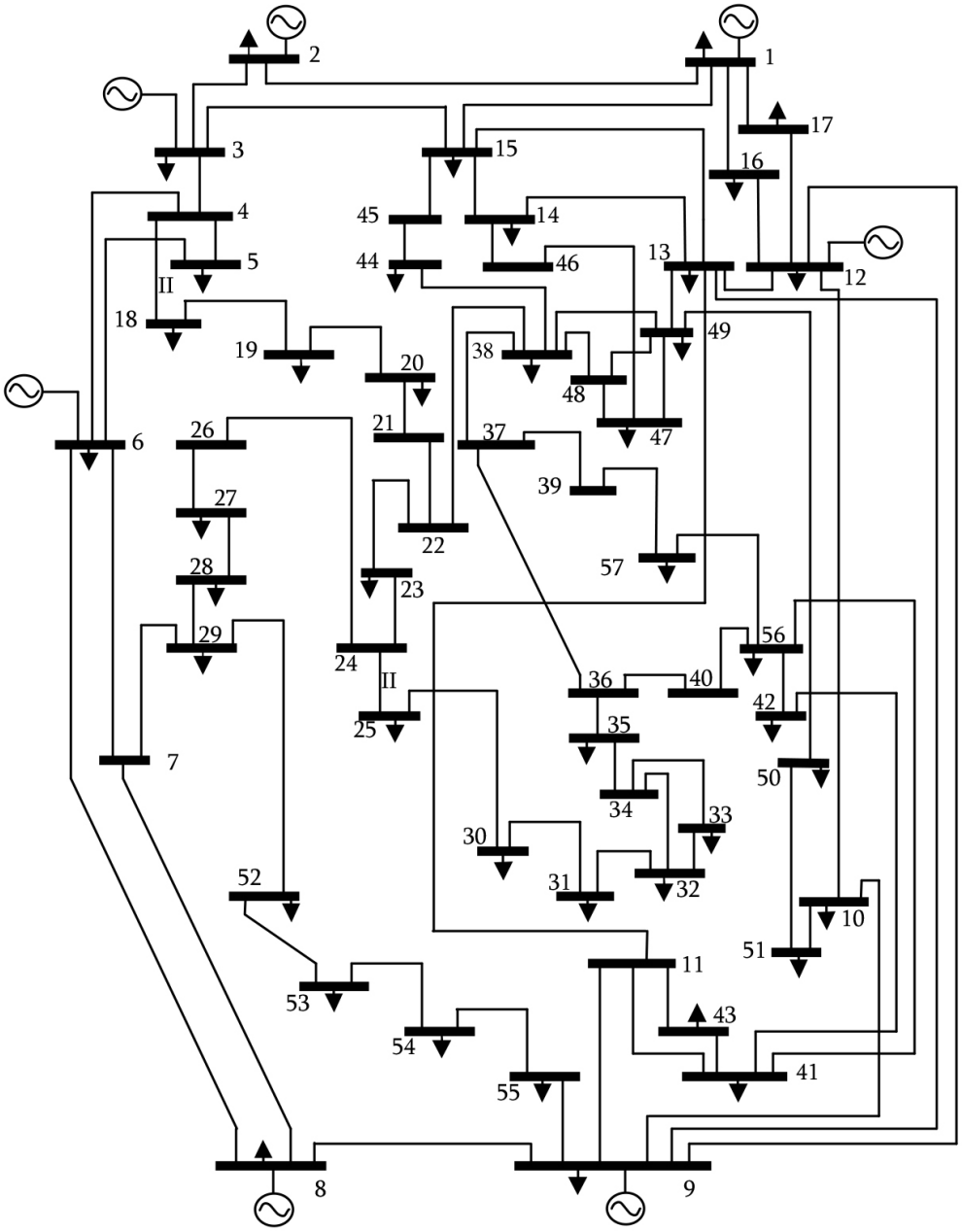

Figure 14: IEEE 57-bus Test System

5.2 IEEE 57-bus Test System

The standard IEEE 57-bus system consists of 80 transmission lines; seven generators at buses 1, 2, 3, 6, 8, 9, 12; and 15 transformers. The IEEE 57-Bus Test Case represents a portion of the American Electric Power System (in the Midwestern US) as it was in the early 1960's. It has balanced loads and transposed lines and together with 14-bus and 30-bus are often found in works related to state estimation (ZHU; ABUR, 2006; BRETAS et al., 2017; LIU; NING; REITER, 2011; BOBBA et al., 2010).

5.2.1 Multiple measurement cyber-attack scenario

The innovation approach used in this work should correctly deal with multiple interacting and conforming bad data. In order to find which measurements cyber-attack may lead to this situation an analysis of the II as suggested by (BRETAS et al., 2017) was carried out. Table 20 brings the measurements with low Innovation Index, that in case of gross errors, are hard to detect and identify correctly by the largest normalized residual test.

Table 20: 57-bus - Measurements with low II

II Ascending list			
Active Measurement	II	Reactive Measurement	II
Power Flow			
$P: 37-39$	0.248	$Q: 52-53$	0.1796
$P: 56-42$	0.458	$Q: 1-16$	0.1863
$P: 12-13$	0.470	$Q: 31-32$	0.2219
$P: 57-56$	0.656	$Q: 17-1$	0.2844
$P: 34-35$	0.660	$Q: 15-45$	0.3762
Power Injection			
$P: 07$	0.007	$P: 36$	0.0265
$P: 04$	0.008	$P: 37$	0.0273
$P: 37$	0.008	$P: 40$	0.0461
$P: 11$	0.012	$P: 13$	0.0486
$P: 03$	0.020	$P: 7$	0.0567

Based on the analysis of Table 20 the first multiple simultaneous measurements set of attacks using the IEEE 57-bus is described as follows:

1) Cyber-attack of magnitude 8σ added to measurement $P: 12-13 = -0.00606pu$ (active power flow from bus 12 to bus 13)

2) Cyber-attack of magnitude 6σ added to measurement $P: 09 = -1.2079pu$ (active power injection on bus 9)

As presented in table 21 and 22 the measurements cyber-attacks were detected and corrected, also no ${\lambda_{CELM}}^N$ were above threshold.

Table 21: 57-bus - multiple measurement cyber-attack -1^{st} loop - CME^N

CME^N descending list		
Measurement	CME^N	CNE
$P: 09$	5.581	5.974
$P: 12-13$	2.638	6.526
$P: 13-12$	2.538	2.789
$P: 55$	1.087	3.073
$P: 07$	0.960	135.835
Corrected Measurement:		
$P: 09$	-1.2076	

Table 22: 57-bus - multiple measurement cyber-attack -2^{nd} loop -CME^N

CME^N descending list		
Measurement	CME^N	CNE
$P:12-13$	3.012	7.573
$P:13-12$	3.008	3.296
$P:22$	0.691	2.698
$Q:32-33$	0.676	0.880
$Q:50-51$	0.651	0.795
Corrected Measurement:		
$P:12-13$	-0.0060	

If a the cyber-attack magnitude to measurement $P:09$ is increased to a value equal or higher to 10σ a false parameter cyber-attack identification (FPCA) was verified, as there were ${\lambda_{CELM}}^N$ values above threshold. If the cyber-attack magnitude to measurement $P:12-13$ is increased to a value higher to 12σ FPCA was also noticed. Either way as presented by the methodology flowchart depicted in Figures 12 and **??** FPCAs are expected and correctly threated.

5.2.2 Multiple measurement and parameter cyber-attack scenario

Multiple simultaneous measurement and parameter cyber-attack using the IEEE 57-bus is described as follows:

1) Cyber-attack of 9% subtracted to the 04-06 line parameter $r_{04-06} = 0.043pu$ (04-06 line resistance) only.

2) Cyber-attack of 10% added to the 13-14 line parameter $x_{13-14} = 0.0434pu$ (13-14 line reactance) only.

3) Cyber-attack of magnitude 6σ added to measurement $P:34-35 = -0.07412pu$ (reactive power injection at bus 50)

4) Cyber-attack of magnitude 8σ added to measurement $Q:1-16 = 0.18633pu$ (reactive power injection at bus 50)

The fist loop Tables 23 and 24 present both ${\lambda_{CELM}}^N$ and CME^N largest values. Once more CME^N could not be used to identify a parameter cyber-attack but ${\lambda_{CELM}}^N$ correctly identified and the methodology proceeded to the HIRA in order to correct parameters values. Note that in this case where there are also measurements cyber-attacks the parameter correction is not done in the first HIRA process, having to go through L4 more three times. Also the first HIRA number of iteration were close to 300. As a matter of comparison, the same cyber-attack scenario was tested without measurements cyber-attack . If the cyber-attacks happened only in parameters, i.e. r_{04-06} or x_{13-14} the HIRA process uses less than 40 iterations to find in the first loop the correct parameter value.

After r_{13-14} correction there were still ${\lambda_{CELM}}^N$ above threshold as presented in Table 25. Using the largest ${\lambda_{CELM}}^N$ for parameter cyber-attack detection and identification r_{4-6} was corrected and the process continued.

Fifth loop had no ${\lambda_{CELM}}^N$ above threshold therefore only CME^N Table is presented. The methodology corrected measurements using CNE as Table 26 indicates, with a measurement difference to the correct value of 0.4%.

Table 23: 57-bus - multiple measurement and parameter cyber-attack -1^{st} loop - λ^N_{CELM}

${\lambda_{CELM}}^N$ descending list	
Parameter	λ^N
x_{13-14}	5.744
x_{12-13}	5.700
r_{9-13}	5.694
x^{sh}_{11-13}	5.665
Corrected Parameter:	
x_{13-14}	0.043405722

Table 24: 57-bus - multiple measurement and parameter cyber-attack -1^{st} loop - CME^N

CME^N descending list	
Measurement	CME^N
$P:6-4$	8.728
$P:5-4$	7.527
$P:13$	7.521
$Q:15-13$	6.691
$Q:14-15$	5.962

Table 25: 57-bus - multiple measurement and parameter cyber-attack -4^{th} loop - λ^N_{CELM}

${\lambda_{CELM}}^N$ descending list	
Parameter	λ^N
r_{4-6}	3.947
r_{5-6}	3.422
r_{6-8}	3.416
r_{6-8}	3.414
Corrected Parameter:	
r_{4-6}	0.042894373

Table 26: 57-bus - multiple measurement and parameter cyber-attack -5^{th} loop - CME^N

CME^N descending list		
Measurement	CME^N	CNE
$P:34-35$	3.532	6.131
$P:35-0$	3.382	8.271
$P:36$	3.064	65.003
$P:37-0$	2.925	360.870
$P:37-39$	2.841	11.929
Corrected Measurement:		
$P:34-35$	-0.0744	

The last cyber-attack was not detected by the proposed methodology (CME^N<3). Comparative tests were done, the normalized residue (r^N) was calculated as presented by Table 27 and no detection was also made using this method.

Table 27: 57-bus - multiple measuremens and parametes cyber-attack -6^{th} loop - CME^N

CME^N descending list			
Measurement	CME^N	CNE	r^N
$Q: 1-16$	1.814	10.872	0.626
$Q: 16$	1.234	2.715	0.917
$P: 37$	1.181	144.665	0.463
$Q: 23-24$	1.026	1.551	0.040
$P: 16$	0.759	0.885	2.630

In order to verify the impact of this negative cyber-attack detection the calculated final states are compared to IEEE values as presented by Table 28.

5.2.3 Multiple Measurement, parameter and topological cyber-attack scenario

The set of attack using the IEEE 57-bus is described as follows.

1) Cyber-attack of magnitude 6σ added to measurement $Q: 50 = -0.1059pu$ (reactive power injection at bus 50)

2) Cyber-attack of 6% added to the 41-42 line parameter $r_{41-42} = 0.207pu$ (41-42 line reactance) only.

3) Topological cyber-attack at line 19-20, setting the operational line status as offline.

The Lagrange multiplier ${\lambda_{CELM}}^N$ for line parameter r_{41-42} presented value equal to 4.8, above threshold, therefore the cyber-attack in only this parameter was detected and identified. Necessary corrections on both parameter and states were done using the Hybrid iterative relaxed approach. Another loop process was run and the largest Lagrange multiplier ${\lambda_{CELM}}^N$ was below threshold.

Table 29 exemplifies for bus 12 the state values estimated considering the use or not of HIRA.

Following the methodology, as presented in Table 30, CME^N was above the threshold thus a cyber-attack was detected. The heuristic proposed by (BRETAS et al., 2017) was used and as there were high values of CME^N in power injection of bus 19 and 20, this indicated a topological cyber-attack.

After the detection and identification, the topological cyber-attack was corrected and the process continued. In the third loop identification was based on the analysis of CME^N as presented in Table 31, where was an isolated high CME^N value for measurement $Q: 50$. This indicated a measurement cyber-attack. The value was corrected and once more the process was run.

Finally no more CME^N or ${\lambda_{CELM}}^N$ values above threshold were found, as expected, no other cyber-attack detection was made.

Table 28: 57-bus - States (phase in degrees and voltage in kV) variation for multiple measurement and parameter cyber-attack

Bus Phase	IEEE values	After Correction	%	Bus Voltage	IEEE values	After Correction	%
2	-1.189	-1.180	0.75	1	143.520	143.504	0.01
3	-5.993	-5.974	0.32	2	139.380	139.357	0.02
4	-7.293	-7.324	0.42	3	135.930	135.905	0.02
5	-8.544	-8.524	0.23	4	135.005	135.354	0.26
6	-8.690	-8.654	0.41	5	134.647	134.665	0.01
7	-7.588	-7.586	0.03	6	135.240	135.216	0.02
8	-4.498	-4.456	0.94	7	135.502	135.767	0.20
9	-9.617	-9.566	0.53	8	138.690	138.662	0.02
10	-11.488	-11.437	0.45	9	135.240	135.212	0.02
11	-10.215	-10.177	0.38	10	136.027	136.035	0.01
12	-10.501	-10.467	0.32	11	134.302	134.384	0.06
13	-9.820	-9.797	0.24	12	140.070	140.041	0.02
14	-9.360	-9.336	0.25	13	134.950	135.074	0.09
15	-7.195	-7.185	0.13	14	133.694	133.832	0.10
16	-8.880	-8.861	0.22	15	136.220	136.319	0.07
17	-5.407	-5.391	0.30	16	139.835	139.765	0.05
18	-11.750	-11.715	0.30	17	140.401	140.329	0.05
19	-13.361	-13.208	1.14	18	134.564	138.114	2.64
20	-13.610	-13.418	1.41	19	131.307	133.832	1.92
21	-12.883	-12.899	0.13	20	131.059	133.003	1.48
22	-12.833	-12.850	0.13	21	138.055	139.075	0.74
23	-12.882	-12.919	0.29	22	138.400	139.351	0.69
24	-12.953	-13.259	2.36	23	138.138	139.075	0.68
25	-18.006	-18.143	0.76	24	135.820	137.833	1.48
26	-12.643	-12.959	2.50	25	129.416	135.483	4.69
27	-11.387	-11.486	0.88	26	130.451	132.314	1.43
28	-10.426	-10.456	0.29	27	134.233	135.492	0.94
29	-9.764	-9.756	0.07	28	136.565	137.563	0.73
30	-18.663	-18.696	0.17	29	138.593	139.356	0.55
31	-19.530	-19.357	0.89	30	126.974	132.719	4.52
32	-18.828	-18.474	1.88	31	124.186	129.130	3.98
33	-18.870	-18.514	1.89	32	127.774	130.929	2.47
34	-14.083	-14.113	0.22	33	127.457	130.653	2.51
35	-13.863	-13.872	0.07	34	130.976	132.309	1.02
36	-13.612	-13.602	0.08	35	132.135	133.274	0.86
37	-13.432	-13.421	0.08	36	133.612	134.656	0.78
38	-12.726	-12.720	0.05	37	134.936	135.899	0.71
39	-13.479	-13.471	0.06	38	138.980	139.764	0.56
40	-13.642	-13.632	0.07	39	134.660	135.623	0.71
41	-14.124	-14.060	0.45	40	133.211	134.242	0.77
42	-15.559	-15.511	0.31	41	137.144	137.425	0.20
43	-11.382	-11.337	0.39	42	132.908	133.284	0.28
44	-11.858	-11.869	0.09	43	139.145	139.352	0.15
45	-9.294	-9.257	0.39	44	139.670	140.318	0.46
46	-11.145	-11.898	6.76	45	142.609	142.941	0.23
47	-12.540	-12.499	0.33	46	145.866	144.866	0.69
48	-12.628	-12.599	0.23	47	142.030	142.521	0.35
49	-12.975	-12.929	0.35	48	141.160	141.694	0.38
50	-13.459	-13.398	0.46	49	142.526	142.938	0.29
51	-12.584	-12.527	0.46	50	140.857	141.147	0.21
52	-11.219	-11.476	2.30	51	145.079	145.144	0.04
53	-11.828	-12.237	3.46	52	133.529	135.216	1.26
54	-11.542	-11.699	1.36	53	131.735	133.973	1.70
55	-10.853	-10.788	0.60	54	136.151	137.418	0.93
56	-16.065	-16.051	0.08	55	141.809	142.248	0.31
57	-16.576	-16.572	0.02	56	133.046	133.556	0.38
				57	132.480	133.140	0.50

Table 29: 57-bus - States of bus 12 variation on measurement, topology and parameter cyber-attack

State_Bus	IEEE values	Without HIRA	With HIRA	%
Voltage_12 (kV)	145.59	145.684	145.656	2.81%
Angle_12 (degrees)	-15.07	-15.095	-15.063	3.20%

Table 30: 57-bus - multiple measurement, topology and parameter cyber-attack -2^{nd} loop - CME^N

CME^N descending list		
Measurement	CME^N	CNE
$Q:19$	21.165	40.249
$Q:20$	15.686	19.970
$P:19$	11.353	15.646
$Q:20$	6.008	8.335
$Q:50$	5.284	6.334

Table 31: 57-bus - multiple measurement, topology and parameter cyber-attack -3^{rd} loop - CME^N

CME^N descending list		
Measurement	CME^N	CNE
$Q:50$	13.399	16.537
$Q:49-50$	9.662	15.715
$Q:50-51$	5.022	6.042
$P:56-42$	4.616	11.215
$Q:51$	3.397	9.382
Corrected Measurement:		
$Q:50$	-0.1065	

5.3 Discussion

In order to proceed with the case study results discussion the Table 32 summaries all types of tests carried out.

Tables 5, 9, 19, 28 presented states variation and comparisons during tests.

The presented results highlight the core contributions of the proposed methodology. During all tests the state estimation never failed to converge, indicating that the proposed standard deviation for pseudo and low/zero magnitudes measurements based on correlated measurements and covariance properties works well, not bringing any addition calculation effort to the Newton Raphson process.

Measurement and topological cyber-attacks identification, detection and correction were done correctly in almost all cases with different GRL scenarios contemplating the evolving cyber-attack learning behavior. The unidentified cases are related to measurements with very low II as those presented in Table 20. These cases were tested with the normalized residue test and no identification, detection and correction was neither possible.

Parameters cyber-attack detection and identification on cases of individual line parame-

Table 32: Case studies summary

Cyber-attack	GRL	IEEE 14-bus	IEEE 57-bus
Simultaneous measurements	3.1	Subsection 5.1.1	Subsection 5.2.1
Simultaneous measurements and parameters	2.8	Subsection 5.1.2	
Simultaneous measurements and parameters	3.1	Subsection 5.1.2	Subsection 5.2.2
Simultaneous measurements , topology and parameters	3.1	Subsections 5.1.3	Subsections 5.2.3

ter had 100% better results that the methodologies using CME^N only (BRETAS et al., 2017) or using LM with the normalized residue test (ZHU; ABUR, 2006), nevertheless depending the branch position and the system meshed configuration there are parameter cyber-attacks not detected or identified by any of the methodologies.

In order to minimize false parameter cyber-attack identification the authors proposed methodology suggests that number of iterations should be part of the identification process, specially on the HIRA processes that uses two types of relaxations while correcting parameter values and states at the same time. Moreover the HIRA process uses variable tolerances in order to verify convergence, so the non convergence fact can be used as a good indicator of incorrect cyber-attack identification.

The methodology arrived at an autonomous behavior with attacked measurement, topology or parameters and the system states correction. The countermeasure could bring the state estimator back to an operating mode. Also correction is an important part to the identification process. On cases such a false parameter cyber-attack happens, after trying to correct it, the methodology considers other types of cyber-attack, and the right correction and consequent convergence of the system helps the process to be more autonomous. The proposed methodology behavior under a cyber-attack is found on Figure 10.

The HIRA performance compared to the bibliography (BRETAS et al., 2017; ZHU; ABUR, 2006) is quite unique. Let us consider a single parameter (such as line reactance or resistance) cyber-attack on IEEE 14 bus system. (BRETAS et al., 2017) suggested methodology to correct parameter does not work as it is based on the CNE applied to both resistance and reactance parameters. Correction using the augmented vector need more than 400 iteration in order to converge. The same parameter cyber-attack need no more than 40 iteration to be corrected using the HIRA.

The augment process has known numerical issues (MONTICELLI, 1999), when a parameter is added to the state vector an arbitrary weight value must be used. This value normally is very different than the values used on measurements leading to numerical instabilities. Moreover this methodology forces the increase of the number of available measurements in order to maintain the same degrees of freedom, as the state vector increases.

Finally Tables 5, 9, 19, 28 indicated that the methodology states correction improves results. On cases that the cyber-attack was not detected it is also possible to noticed minor degradation on final states values.

5.4 Overview

Chapter 5 explored the proposed methodology under several cyber-attacks, that could simultaneously happen on measurements, topology and parameters. Two IEEE test cases were used as presented by 5.1 and 5.2. Observations over each program loop and HIRA iterations were made and presented through Tables containing CME^N, CNE, ${\lambda_{CELM}}^N$, corrected measurements and parameters.

Analysis over states values were also presented through Tables in order to identify improvements in final estimated states values.

Results were discussed in section 5.3 where core findings of the proposed approach as described in Chapter 4 could be highlighted. With methodology and results presented and discussed Chapter 6 brings the conclusion, possible refinements and extensions of this work.

6 CONCLUSION

This work presented and explored advanced applications for state estimators in smart grids with the capability to identify, detect and correct measurements, parameters and topology cyber-attacks in an HRC way, enabling self-protection and in case of cyber-attacks of even cyber-errors, self-correction of data and parameters.

The methodology is firmly supported by state estimators based on the normal equations with a standard deviation for pseudo and low/zero magnitudes measurements based on correlated measurements and covariance properties that avoid NI issues.

This work extends the innovation approach to the Lagrange multiplier calculation. Parameter cyber-attack identification, detection and correction is done contemplating the evolving cyber-attack learning behavior that will target vulnerable areas with reduced GRL.

The case studies as presented in chapter 5 were conducted on different cyber-attack scenarios. The proposed methodology could identify and correct simultaneous measurement, topology and parameter cyber attacks considering measurements' availability restrictions. The results demonstrate the robustness of the presented methodology.

A key finding of this work is that relaxations and continuous process flow can be used to solve the critical mathematical problem raised in the bibliography review (BRETAS; BRETAS, 2017; LIN; ABUR, 2017): Is it possible to correct parameters with measurement error and the other way around? The mathematical relaxation in several layers of this classical optimization problem lead to the hybrid iterative relaxed approach in order to identify and correct cyber-attacked parameters and measurements.

Providing mitigation, response and system recovery capabilities to the state estimator with reduced computational burden, the proposed model and methodology have strong potential to be integrated into SCADA state estimators for real-world applications.

6.1 Future Work

In the current implementation the system admittance matrix, $Ybus$, is reconstructed from scratch each time during the HIRA process. This could be improved as the HIRA process changes only one network parameter a time.

The software structure is strongly based on functions. They are used for data collection, to build the system admittance matrix, to calculate the Parameters Jacobian (for both LM and HIRA process) and to calculate main methodology variables such as CME^N, CNE and ${\lambda_{CELM}}^{i^N}$. Still, there are parts of on the main program that could be set into functions such as the states Jacobian and the $h(x)$ vector.

Only one type of topological cyber-attack model was tested, that is setting the operation status to offline and have the power flow measurements value defined as zero. The inclusion

of transmission lines should also be verified as a possible cyber-attack and even alternative network modeling where circuit breakers (CB) are explicitly represented (LOURENCO; COELHO; PAL, 2015) could also be verified.

A possible way to extend this work is to explore, in the light of Lagrange relaxation and composed measurement error and HIRA, the multiarea SE and identification of observable islands.

REFERENCES

ABUR, A.; EXPOSITO, A. G. **Power system state estimation**: theory and implementation. New York: CRC Press, 2004.

ASCHMONEIT, F.; PETERSON, N.; ADRIAN, E. State estimation with equality constraints. In: POWER INDUSTRY COMPUTER APPLICATION CONFERENCE,10., 1977, Toronto. **Proceedings...** New York: IEEE, 1977. p.427–430.

ASHOK, A.; GOVINDARASU, M.; AJJARAPU, V. Online Detection of Stealthy False Data Injection Attacks in Power System State Estimation. **IEEE Transactions on Smart Grid**, New York, v.PP, n.99, p.1, 2016.

BAKKEN, D. et al. GRIP-Grids with intelligent periphery: control architectures for grid2050π. In: IEEE INTERNATIONAL CONFERENCE ON SMART GRID COMMUNICATIONS (SMARTGRIDCOMM),2., 2011, Brussels. **Proceedings...** New York: IEEE, 2011. p.7–12.

BOBBA, R. B. et al. Detecting false data injection attacks on dc state estimation. In: WORKSHOP ON SECURE CONTROL SYSTEMS (SCS),1., 2010, Stockholm. **Proceedings...** Berkeley:TRUST, 2010. p.1–9.

BRAZIL. Manual do programa de pesquisa e desenvolvimento tecnologico do setor de energia eletrica. **Agencia Nacional de Energia Eletrica (ANEEL).**, Brasília,DF, 2012.

BRETAS, A. et al. 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**, Amsterdam, v.151, p.174 – 185, 2017.

BRETAS, A. S. et al. Smart grids cyber-physical security as a malicious data attack: an innovation approach. **Electric Power Systems Research**, Amsterdam, v.149, p.210 – 219, 2017.

BRETAS, N.; CARVALHO, B.; ALBERTINI, M. The innovation concept applied to the processing of measurements and parameters errors in power systems state estimation. In: POWERTECH IEEE EINDHOVEN, 2015, Eindhove. **Proceedings...** New York: IEEE, 2015. p.1–6.

BRETAS, N. G.; BRETAS, A. S. A two steps procedure in state estimation gross error detection, identification, and correction. **International Journal of Electrical Power and Energy Systems**, Amsterdam, v.73, p.484 – 490, 2015.

BRETAS, N. G.; BRETAS, A. S. Discussion on "A New Framework for Detection and Identification of Network Parameter Errors". **IEEE Transactions on Smart Grid**, New York, v.8, n.2, p.1028–1028, 2017.

BRETAS, N. G.; BRETAS, A. S. 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**, New York, v.65, n.9, p.1269–1273, Sept. 2018.

BRETAS, N. G.; BRETAS, A. S.; PIERETI, S. A. Innovation concept for measurement gross error detection and identification in power system state estimation. **IET Generation, Transmission Distribution**, Stevenage, v.5, n.6, p.603–608, June 2011.

BRETAS, N. G. et al. A Geometrical View for Multiple Gross Errors Detection, Identification, and Correction in Power System State Estimation. **IEEE Transactions on Power Systems**, New York, v.28, n.3, p.2128–2135, Aug. 2013.

BRETAS, N.; PIERRETI, S. The innovation concept in bad data analysis using the composed measurements errors for power system state estimation. In: POWER AND ENERGY SOCIETY GENERAL MEETING, 2010, Minneapolis. **Proceedings...** New York: IEEE, 2010. p.1–6.

CARO, E.; CONEJO, A. J.; MINGUEZ, R. Power System State Estimation Considering Measurement Dependencies. **IEEE Transactions on Power Systems**, New York, v.24, n.4, p.1875–1885, Nov. 2009.

CARO, E.; CONEJO, A. J.; MINGUEZ, R. Decentralized State Estimation and Bad Measurement Identification: an efficient lagrangian relaxation approach. **IEEE Transactions on Power Systems**, New York, v.26, n.4, p.2500–2508, Nov. 2011.

CARO, E. et al. Calculation of Measurement Correlations Using Point Estimate. **IEEE Transactions on Power Delivery**, New York, v.25, n.4, p.2095–2103, Oct. 2010.

CARO, E. et al. Multiple Bad Data Identification Considering Measurement Dependencies. **IEEE Transactions on Power Systems**, New York, v.26, n.4, p.1953–1961, Nov. 2011.

CHEN, S.; LIU, C.-C. From demand response to transactive energy: state of the art. **Journal of Modern Power Systems and Clean Energy**, Heidelberg, v.5, n.1, p.10–19, Jan. 2017.

CHERDANTSEVA, Y. et al. A review of cyber security risk assessment methods for SCADA systems. **Computers & Security**, Amsterdam, v.56, p.1 – 27, 2016.

CLEMENTS, K. A.; KRUMPHOLZ, G. R.; DAVIS, P. W. Power System State Estimation Residual Analysis: an algorithm using network topology. **IEEE Transactions on Power Apparatus and Systems**, New York, v.PAS-100, n.4, p.1779–1787, April 1981.

CLEMENTS, K.; COSTA, A. Topology error identification using normalized Lagrange multipliers. **IEEE Transactions on Power Systems**, New York, v.13, n.2, p.347–353, May 1998.

COTILLA-SANCHEZ, E. et al. Comparing the Topological and Electrical Structure of the North American Electric Power Infrastructure. **IEEE Systems Journal**, New York, v.6, n.4, p.616–626, Dec. 2012.

DÁN, G.; SANDBERG, H. Stealth attacks and protection schemes for state estimators in power systems. In: IEEE INTERNATIONAL CONFERENCE ON SMART GRID COMMUNICATIONS (SMARTGRIDCOMM),1., 2010, Gaithersburg. **Proceedings...** New York: IEEE, 2010. p.214–219.

DEBS, A. S. Estimation of Steady-State Power System Model Parameters. **IEEE Transactions on Power Apparatus and Systems**, New York, v.PAS-93, n.5, p.1260–1268, Sept. 1974.

DENHOLM, P. et al. **Overgeneration from Solar Energy in California. A Field Guide to the Duck Chart**. [S.l.]: National Renewable Energy Lab.(NREL), 2015.

DZAFIC, I. et al. Multi-Phase State Estimation Featuring Industrial-Grade Distribution Network Models. **IEEE Transactions on Smart Grid**, New York, v.8, n.2, p.609–618, March 2017.

ELKALASHY, N. I. et al. Transient selectivity for enhancing autonomous fault management in unearthed distribution networks with DFIG-based distributed generations. **Electric Power Systems Research**, Amsterdam, v.140, p.568 – 579, 2016.

ESFAHANI, P. M. et al. A robust policy for automatic generation control cyber attack in two area power network. In: IEEE CONFERENCE ON DECISION AND CONTROL (CDC),49., 2010, Atlanta. **Proceedings...** New York: IEEE, 2010. p.5973–5978.

FANTIN, C. d. A. **Metodologia para estimação de estado trifásica em sistemas de distribuição incorporando medidas SCADA, virtuais, pseudo-medidas e medidas fasoriais sincronizadas**. 2016. 98 p. Thesis (Doutorado em Sistemas de Potência — Universidade de São Paulo, São Paulo, 2016.

FOVINO, I. N. et al. Cyber security assessment of a power plant. **Electric Power Systems Research**, Amsterdam, v.81, n.2, p.518 – 526, 2011.

GIORDANO, V. et al. Smart grid projects in Europe. **Joint Research Centre**, Luxembourg, v.8, p.138, 2013.

GJELSVIK, A.; AAM, S.; HOLTEN, L. Hachtel's Augmented Matrix Method - A Rapid Method Improving Numerical Stability in Power System Static State Estimation. **IEEE Transactions on Power Apparatus and Systems**, New York, v.PAS-104, n.11, p.2987–2993, Nov. 1985.

GÓMEZ-EXPÓSITO, A. et al. A taxonomy of multi-area state estimation methods. **Electric Power Systems Research**, Amsterdam, v.81, n.4, p.1060–1069, 2011.

GOMEZ-EXPOSITO, A. et al. A multilevel state estimation paradigm for smart grids. **Proceedings of the IEEE**, New York, v.99, n.6, p.952–976, 2011.

HASSAN, M.; ABIDO, M. Real time implementation and optimal design of autonomous microgrids. **Electric Power Systems Research**, Amsterdam, v.109, p.118 – 127, 2014.

HOLTEN, L. et al. Comparison of different methods for state estimation. **IEEE Transactions on Power Systems**, New York, v.3, n.4, p.1798–1806, Nov. 1988.

HU, Q. et al. Secure State Estimation and Control for Cyber Security of the Nonlinear Power Systems. **IEEE Transactions on Control of Network Systems**, New York, v.5, n.3, p.1310–1321, Sept. 2018.

HUG, G.; GIAMPAPA, J. A. Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks. **IEEE Transactions on Smart Grid**, New York, v.3, n.3, p.1362–1370, Sept. 2012.

KARIM, M. A.; CURRIE, J.; LIE, T.-T. A machine learning based optimized energy dispatching scheme for restoring a hybrid microgrid. **Electric Power Systems Research**, Amsterdam, v.155, p.206 – 215, 2018.

KIM, T. T.; POOR, H. V. Strategic protection against data injection attacks on power grids. **IEEE Transactions on Smart Grid**, New York, v.2, n.2, p.326–333, 2011.

KOSUT, O. et al. Malicious data attacks on smart grid state estimation: attack strategies and countermeasures. In: IEEE INTERNATIONAL CONFERENCE ON SMART GRID COMMUNICATIONS (SMARTGRIDCOMM),1., 2010, Gaithersburg. **Proceedings...** New York: IEEE, 2010. p.220–225.

KYLE, S. **Random - Probability, Mathematical Statistics, Stochastic Processes**. Acesso em/Accessed: 30-August-2017, Disponível em/Available: <http://www.math.uah.edu/stat/expect/Covariance.html>.

LEFEBVRE, S.; PREVOST, J.; LENOIR, L. Distribution State Estimation: a necessary requirement for the smart grid. In: POWER AND ENERGY SOCIETY GENERAL MEETING (PES), 2014, National Harbor. **Proceedings...** New York: IEEE, 2014. p.1–5.

LIN, Y.; ABUR, A. A New Framework for Detection and Identification of Network Parameter Errors. **IEEE Transactions on Smart Grid**, New York, v.PP, n.99, p.1, 2016.

LIN, Y.; ABUR, A. Closure to Discussion on "A New Framework for Detection and Identification of Network Parameter Errors.";. **IEEE Transactions on Smart Grid**, New York, v.8, n.2, p.1029–1030, March 2017.

LIU, W. . E.; WU, F. F.; LUN, S. . Estimation of parameter errors from measurement residuals in state estimation (power systems). **IEEE Transactions on Power Systems**, New York, v.7, n.1, p.81–89, Feb. 1992.

LIU, Y.; NING, P.; REITER, M. K. False data injection attacks against state estimation in electric power grids. **ACM Transactions on Information and System Security (TISSEC)**, New York, v.14, n.1, p.13, 2011.

LONDON, J. B. A.; ALBERTO, L. F. C.; BRETAS, N. G. Analysis of measurement-set qualitative characteristics for state-estimation purposes. **IET Generation, Transmission Distribution**, Stevenage, v.1, n.1, p.39–45, Jan. 2007.

LOURENCO, E. M.; COELHO, E. P. R.; PAL, B. C. Topology Error and Bad Data Processing in Generalized State Estimation. **IEEE Transactions on Power Systems**, New York, v.30, n.6, p.3190–3200, Nov. 2015.

LOURENCO, E. M.; COSTA, A. S.; CLEMENTS, K. A. Bayesian-based hypothesis testing for topology error identification in generalized state estimation. **IEEE Transactions on Power Systems**, New York, v.19, n.2, p.1206–1215, May 2004.

LUGTU, R. L. et al. Power System State Estimation: detection of topological errors. **IEEE Transactions on Power Apparatus and Systems**, New York, v.PAS-99, n.6, p.2406–2412, Nov. 1980.

MATLAB. **version 8.5.0 (R2015a)**. Natick, Massachusetts: The MathWorks Inc., 2015.

MEHRDAD, S. et al. Cyber-Physical Resilience of Electrical Power Systems Against Malicious Attacks: a review. **Current Sustainable Renewable Energy Reports**, Philadelphia, v.5, n.1, p.14–22, 2018.

MINGUEZ, R.; CONEJO, A. J. State Estimation Sensitivity Analysis. **IEEE Transactions on Power Systems**, New York, v.22, n.3, p.1080–1091, Aug. 2007.

MOHAJERIN ESFAHANI, P. et al. Cyber attack in a two-area power system: impact identification using reachability. In: AMERICAN CONTROL CONFERENCE (ACC), 2010, Baltimore. **Proceedings...** New York:IEEE, 2010. p.962–967.

MOHAMMADPOURFARD, M.; SAMI, A.; SEIFI, A. R. A statistical unsupervised method against false data injection attacks: a visualization-based approach. **Expert Systems with Applications**, Amsterdam, v.84, p.242 – 261, 2017.

MONTICELLI, A. **State estimation in electric power systems**: a generalized approach. New York: Springer Science & Business Media, 1999.

MONTICELLI, A.; WU, F. F. Network Observability: identification of observable islands and measurement placement. **IEEE Transactions on Power Apparatus and Systems**, New York, v.PAS-104, n.5, p.1035–1041, May 1985.

MOUSAVIAN, S.; EROL-KANTARCI, M.; ORTMEYER, T. Cyber Attack Protection for a Resilient Electric Vehicle Infrastructure. In: IEEE GLOBECOM WORKSHOPS (GC WKSHPS), 2015, San Diego. **Proceedings...** New York: IEEE, 2015. p.1–6.

MOUSAVIAN, S.; VALENZUELA, J.; WANG, J. Real-time data reassurance in electrical power systems based on artificial neural networks. **Electric Power Systems Research**, Amsterdam, v.96, p.285 – 295, 2013.

MOUSAVIAN, S.; VALENZUELA, J.; WANG, J. A Probabilistic Risk Mitigation Model for Cyber-Attacks to PMU Networks. **IEEE Transactions on Power Systems**, New York, v.30, n.1, p.156–165, 2015.

RAPOSO, A.; RODRIGUES, A. B.; SILVA, M. da Guia da. Optimal meter placement algorithm for state estimation in power distribution networks. **Electric Power Systems Research**, Amsterdam, v.147, p.22 – 30, 2017.

SANDBERG, H.; TEIXEIRA, A.; JOHANSSON, K. H. On security indices for state estimators in power networks. In: WORKSHOP ON SECURE CONTROL SYSTEMS (SCS),1., 2010, Stockholm. **Proceedings...** Berkeley: TRUST, 2010. p.10–16.

SCHWEPPE, F.; WILDES, J. Power System Static-State Estimation, Part I: exact model. **IEEE Transactions on Power Apparatus and Systems**, New York, v.PAS-89, n.1, p.120–125, Jan. 1970.

SULLIVAN, J. E.; KAMENSKY, D. How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. **The Electricity Journal**, Amsterdam, v.30, n.3, p.30 – 35, 2017.

SUN, C.-C.; HAHN, A.; LIU, C.-C. Cyber security of a power grid: state-of-the-art. **International Journal of Electrical Power** & **Energy Systems**, Amsterdam, v.99, p.45 – 56, 2018.

SYMANTEC, W. Advanced Persistent Threats: a symantec perspective. **Symantec World Headquarters**, Mountain View, 2011.

TEIXEIRA, A. et al. Cyber security analysis of state estimators in electric power systems. In: IEEE CONFERENCE ON DECISION AND CONTROL (CDC),49., 2010, Atlanta. **Proceedings...** New York: IEEE, 2010. p.5991–5998.

TEN, C.-W.; LIU, C.-C.; MANIMARAN, G. Vulnerability assessment of cybersecurity for SCADA systems. **IEEE Transactions on Power Systems**, New York, v.23, n.4, p.1836–1846, 2008.

USA. Guidelines for Smart Grid Cybersecurity Rev. 1. **The National Institute of Standards and Technology (NIST) Interagency Report**, Gaithersburg, v.7628, p.668, 2014.

USA. Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. **The National Institute of Standards and Technology (NIST) Special Publication**, Gaithersburg, v.1108, p.246, 2014.

USA. **Transforming the Nation's Electricity System**. Washington, DC: Department of Energy, 2017. (Quadrennial Energy Review–Full Report 2).

USA. **Building the Foundation for a More Secure American Future**. Washington, DC: Department of Commerce, Department of Homeland Security, 2018. (Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce).

VALENZUELA, J.; WANG, J.; BISSINGER, N. Real-time intrusion detection in power system operations. **IEEE Transactions on Power Systems**, New York, v.28, n.2, p.1052–1062, 2013.

WANG, K. et al. Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid. **IEEE Transactions on Smart Grid**, New York, v.8, n.5, p.2474–2482, 2017.

WU, F. F.; LIU, W. . E. Detection of topology errors by state estimation (power systems). **IEEE Transactions on Power Systems**, New York, v.4, n.1, p.176–183, Feb. 1989.

WU, F. F.; LIU, W. . E.; LUN, S. . Observability analysis and bad data processing for state estimation with equality constraints. **IEEE Transactions on Power Systems**, New York, v.3, n.2, p.541–548, May 1988.

XIANG, Y. et al. Power System Reliability Evaluation Considering Load Redistribution Attacks. **IEEE Transactions on Smart Grid**, New York, v.8, n.2, p.889–901, 2017.

YAN, Y. et al. A Survey on Cyber Security for Smart Grid Communications. **IEEE Communications Surveys Tutorials**, New York, v.14, n.4, p.998–1010, 2012.

YUAN, Y.; LI, Z.; REN, K. Modeling Load Redistribution Attacks in Power Systems. **IEEE Transactions on Smart Grid**, New York, v.2, n.2, p.382–390, 2011.

ZARCO, P.; GOMEZ EXPOSITO, A. Power system parameter estimation: a survey. **IEEE Transactions on Power Systems**, New York, v.15, n.1, p.216–222, 2000.

ZHANG, L.; ABUR, A. Identifying Parameter Errors via Multiple Measurement Scans. **IEEE Transactions on Power Systems**, New York, v.28, n.4, p.3916–3923, Nov 2013.

ZHAO, J. et al. Forecasting-Aided Imperfect False Data Injection Attacks Against Power System Nonlinear State Estimation. **IEEE Transactions on Smart Grid**, New York, v.7, n.1, p.6–8, 2016.

ZHU, J.; ABUR, A. Identification of network parameter errors. **IEEE Transactions on Power Systems**, New York, v.21, n.2, p.586–592, 2006.

APPENDIX A JACOBIAN MATRIX ELEMENTS - LM

The corresponding Jacobian matrix elements would be the following, where P_* is real power injection at bus, g_{mn} the branch series conductance,θ_{mn} the voltage angles at terminal buses of branch m-n, b_{mn} the branch series susceptance, a_{mn} the transformer final turns ratio, Q_* is reactive power injection at bus, b^{sh}_{mn} the branch shunt susceptance, b^{sh}_* the bus shunt susceptance (reactor), P_{mn} the real power flow of branch m-n and Q_{mn} the reactive power flow of branch m-n.

Flow measurements:

$$\frac{\partial P_{mn}}{\partial g_{mn}} = -V_m V_n a_{mn} cos\theta_{mn} + V_m^2 a_{mn}^2 \tag{34}$$

$$\frac{\partial P_{mn}}{\partial b_{mn}} = -V_m V_n a_{mn} sin\theta_{mn} \tag{35}$$

$$\frac{\partial P_{mn}}{\partial a_{mn}} = -V_m V_n (g_{mn} cos\theta_{mn} + b_{mn} sin\theta_{mn}) + 2V_m^2 a_{mn} g_{mn} \tag{36}$$

$$\frac{\partial Q_{mn}}{\partial g_{mn}} = -V_m V_n a_{mn} sin\theta_{mn} \tag{37}$$

$$\frac{\partial Q_{mn}}{\partial b_{mn}} = +V_m V_n a_{mn} cos\theta_{mn} - V_m^2 a_{mn}^2 \tag{38}$$

$$\frac{\partial Q_{mn}}{\partial b^{sh}_{mn}} = -V_m^2 a_{mn}^2 \tag{39}$$

$$\frac{\partial Q_{mn}}{\partial a_{mn}} = -V_m V_n (g_{mn} sin\theta_{mn} - b_{mn} cos\theta_{mn}) - 2V_m^2 a_{mn} (b_{mn} + b^{sh}_{mn}) \tag{40}$$

Bus injection measurements:

$$\frac{\partial P_m}{\partial g_{mn}} = -V_m V_n a_{mn} cos\theta_{mn} + V_m^2 a_{mn}^2 \tag{41}$$

$$\frac{\partial P_n}{\partial g_{mn}} = -V_m V_n a_{mn} cos\theta_{mn} + V_m^2 \tag{42}$$

$$\frac{\partial P_m}{\partial b_{mn}} = \frac{\partial P_n}{\partial b_{mn}} = -V_m V_n a_{mn} sin\theta_{mn} \tag{43}$$

$$\frac{\partial P_m}{\partial a_{mn}} = -V_m V_n (g_{mn} cos\theta_{mn} + b_{mn} sin\theta_{mn}) + 2V_m^2 a_{mn} g_{mn} \tag{44}$$

$$\frac{\partial P_n}{\partial a_{mn}} = -V_m V_n (g_{mn} cos\theta_{mn} + b_{mn} sin\theta_{mn}) \tag{45}$$

$$\frac{\partial Q_m}{\partial g_{mn}} = \frac{\partial Q_n}{\partial g_{mn}} = -V_m V_n a_{mn} sin\theta_{mn} \tag{46}$$

$$\frac{\partial Q_m}{\partial b_{mn}} = V_m V_n a_{mn} cos\theta_{mn} - V_m^2 a_{mn}^2 \tag{47}$$

$$\frac{\partial P_n}{\partial g_{mn}} = V_m V_n a_{mn} cos\theta_{mn} - V_m^2 \tag{48}$$

$$\frac{\partial Q_m}{\partial b_{mn}^{sh}} = \frac{\partial Q_n}{\partial b_{mn}^{sh}} = -V_m^2 \tag{49}$$

$$\frac{\partial Q_m}{\partial a_{mn}} = -V_m V_n (g_{mn} sin\theta_{mn} - b_{mn} cos\theta_{mn}) - 2V_m^2 a_{mn} b_{mn} \tag{50}$$

$$\frac{\partial Q_n}{\partial a_{mn}} = -V_m V_n (g_{mn} sin\theta_{mn} - b_{mn} cos\theta_{mn}) \tag{51}$$

$$\frac{\partial Q_m}{\partial b_m^{sh}} = -V_m^2 \tag{52}$$

$$\tag{53}$$

APPENDIX B MEASUREMENT VALUES IEEE14-BUS AND 57-BUS

This appendix presents the calculated measurement values, where measurements type 1 is voltage, 2 active power injection, 3 reactive power injection, 4 active power flow and 5 is reactive power flow.

Table 33: Measurement Values IEEE14-bus

z	Type	Value (p.u.)	From	To	z	Type	Value (p.u.)	From	To
1	1	1.0600	1	0	42	4	-0.1754	13	6
2	2	2.3238	1	0	43	4	0.0000	7	8
3	2	0.1830	2	0	44	4	0.2809	7	9
4	2	-0.9420	3	0	45	4	-0.2809	9	7
5	2	-0.0755	5	0	46	4	-0.0522	10	9
6	2	-0.1119	6	0	47	4	0.0941	9	14
7	2	0.0000	7	0	48	4	-0.0930	14	9
8	2	-0.2953	9	0	49	4	-0.0378	10	11
9	2	-0.0349	11	0	50	4	0.0162	12	13
10	2	-0.1354	13	0	51	4	-0.0161	13	12
11	2	-0.1486	14	0	52	4	-0.0556	14	13
12	3	-0.1691	1	0	53	5	-0.2039	1	2
13	3	0.0552	3	0	54	5	0.0349	1	5
14	3	0.0568	4	0	55	5	0.0260	5	1
15	3	-0.0078	5	0	56	5	0.0158	3	2
16	3	0.0016	7	0	57	5	0.0356	2	3
17	3	0.1733	8	0	58	5	0.0356	4	2
18	3	-0.1672	9	0	59	5	0.0071	2	5
19	3	-0.0177	11	0	60	5	0.0393	3	4
20	3	-0.0160	12	0	61	5	-0.0430	4	3
21	3	-0.0584	13	0	62	5	-0.1457	5	4
22	4	1.5683	1	2	63	5	-0.0946	4	7
23	4	-1.5254	2	1	64	5	0.1067	7	4
24	4	0.7555	1	5	65	5	-0.0032	4	9
25	4	0.7319	2	3	66	5	0.1284	5	6
26	4	-0.7087	3	2	67	5	-0.0731	6	5
27	4	0.0778	6	12	68	5	-0.0335	11	6
28	4	0.4151	2	5	69	5	0.0250	6	12
29	4	-0.4061	5	2	70	5	-0.0235	12	6
30	4	-0.2333	3	4	71	5	0.0720	6	13
31	4	0.2370	4	3	72	5	-0.1688	7	8
32	4	-0.6126	4	5	73	5	0.1733	8	7
33	4	0.6178	5	4	74	5	-0.0509	9	7
34	4	-0.2687	7	4	75	5	0.0429	9	10
35	4	0.1609	4	9	76	5	-0.0425	10	9
36	4	-0.1511	9	4	77	5	0.0366	9	14
37	4	0.4406	5	6	78	5	-0.0155	10	11
38	4	0.0734	6	11	79	5	0.0158	11	10
39	4	-0.0728	11	6	80	5	-0.0074	13	12
40	4	-0.0771	12	6	81	5	0.0169	13	14
41	4	0.1775	6	13	82	5	-0.0158	14	13

Table 34: Measurement Values IEEE57-bus - Part 1

z	Type	Value (p.u.)	From bus	To bus	z	Type	Value (p.u.)	From bus	To bus
1	1	1.04	1	0	41	2	-0.00131	40	0
2	2	4.22864	1	0	42	2	-0.06258	41	0
3	2	-0.02698	2	0	43	2	-0.07104	42	0
4	2	-0.00696	3	0	44	2	-0.02	43	0
5	2	0.002017	4	0	45	2	-0.12894	44	0
6	2	-0.13353	5	0	46	2	0.004018	45	0
7	2	-0.74678	6	0	47	2	-0.45789	46	0
8	2	-0.00306	7	0	48	2	-0.04957	47	0
9	2	3.003364	8	0	49	2	-0.00877	48	0
10	2	-1.20792	9	0	50	2	-0.18196	49	0
11	2	-0.04841	10	0	51	2	-0.20914	50	0
12	2	0.001423	11	0	52	2	-0.18203	51	0
13	2	-0.66987	12	0	53	2	-0.05051	52	0
14	2	-0.18129	13	0	54	2	-0.19758	53	0
15	2	0.106539	14	0	55	2	-0.04311	54	0
16	2	-0.22568	15	0	56	2	-0.06734	55	0
17	2	-0.43095	16	0	57	2	-0.07725	56	0
18	2	-0.42084	17	0	58	2	-0.06623	57	0
19	2	-0.27179	18	0	59	3	1.12656	1	0
20	2	-0.0338	19	0	60	3	-0.88863	2	0
21	2	-0.02252	20	0	61	3	-0.22551	3	0
22	2	-0.00232	21	0	62	3	0.011365	4	0
23	2	0.029284	22	0	63	3	-0.0512	5	0
24	2	-0.08545	23	0	64	3	-0.00452	6	0
25	2	0.00434	24	0	65	3	-0.00393	7	0
26	2	-0.06241	25	0	66	3	0.403392	8	0
27	2	-0.00432	26	0	67	3	-0.23898	9	0
28	2	-0.09158	27	0	68	3	1.053461	12	0
29	2	-0.04055	28	0	69	3	-0.00888	13	0
30	2	-0.17606	29	0	70	3	0.085814	14	0
31	2	-0.03721	30	0	71	3	-0.04922	15	0
32	2	-0.05684	31	0	72	3	-0.03627	16	0
33	2	-0.02014	32	0	73	3	-0.08672	17	0
34	2	-0.03418	33	0	74	3	-0.09702	18	0
35	2	0.000346	34	0	75	3	-0.007	19	0
36	2	-0.06358	35	0	76	3	-0.00871	20	0
37	2	0.007875	36	0	77	3	-0.00583	21	0
38	2	-0.00143	37	0	78	3	0.028764	22	0
39	2	-0.13151	38	0	79	3	-0.0456	23	0
40	2	-0.00072	39	0	80	3	-0.00789	24	0

Table 35: Measurement Values IEEE57-bus - Part2

z	Type	Value (p.u.)	From bus	To bus	z	Type	Value (p.u.)	From bus	To bus
81	3	-0.03207	25	0	121	4	1.781363	8	9
82	3	0.007553	26	0	122	4	0.172447	9	10
83	3	-0.00347	27	0	123	4	0.12917	9	11
84	3	-0.01922	28	0	124	4	0.026248	9	12
85	3	-0.03025	29	0	125	4	0.02405	9	13
86	3	-0.01925	30	0	126	4	-0.10408	13	14
87	3	-0.02723	31	0	127	4	-0.48792	13	15
88	3	-0.01317	32	0	128	4	1.487916	1	15
89	3	-0.01539	33	0	129	4	0.791808	1	16
90	3	0.000514	34	0	130	4	0.932975	1	17
91	3	-0.03423	35	0	131	4	0.340174	3	15
92	3	0.00211	36	0	132	4	0.178736	4	18
93	3	-0.00256	37	0	133	4	0.178736	4	18
94	3	-0.06271	38	0	134	4	0.004239	5	6
95	3	0.002172	39	0	135	4	-0.78122	7	8
96	3	0.001812	40	0	136	4	-0.17529	10	12
97	3	-0.03101	41	0	137	4	-0.09752	11	13
98	3	-0.04521	42	0	138	4	-0.00606	12	13
99	3	-0.00579	43	0	139	4	-0.3324	12	16
100	3	-0.01162	44	0	140	4	-0.48336	12	17
101	3	-0.00246	45	0	141	4	-0.68616	14	15
102	3	-0.19758	46	0	142	4	0.046573	18	19
103	3	-0.05526	47	0	143	4	0.011683	19	20
104	3	-0.01065	48	0	144	4	0.010886	21	20
105	3	-0.08653	49	0	145	4	-0.01321	21	22
106	3	-0.1059	50	0	146	4	0.118254	22	23
107	3	-0.05237	51	0	147	4	0.032641	23	24
108	3	-0.0258	52	0	148	4	0.067849	24	25
109	3	-0.09618	53	0	149	4	0.067849	24	25
110	3	-0.01628	54	0	150	4	-0.10168	24	26
111	3	-0.03068	55	0	151	4	-0.106	26	27
112	3	-0.02352	56	0	152	4	-0.19965	27	28
113	3	-0.01858	57	0	153	4	-0.24278	28	29
114	4	1.015941	1	2	154	4	0.600549	7	29
115	4	0.97587	2	3	155	4	0.076048	25	30
116	4	0.60092	3	4	156	4	0.037727	30	31
117	4	0.139074	4	5	157	4	-0.01985	31	32
118	4	0.141281	4	6	158	4	0.034243	32	33
119	4	-0.17695	6	7	159	4	0.074462	34	32

Table 36: Measurement Values IEEE57-bus - Part3

z	Type	Value (p.u.)	From bus	To bus	z	Type	Value (p.u.)	From bus	To bus
160	4	-0.07412	34	35	200	4	-0.17112	10	9
161	4	-0.20949	37	38	201	4	-0.1287	11	9
162	4	0.039408	37	39	202	4	-0.0252	12	9
163	4	0.036143	36	40	203	4	-0.02402	13	9
164	4	-0.10219	22	38	204	4	-1.44896	15	1
165	4	0.091772	11	41	205	4	-0.76547	16	1
166	4	0.088867	41	42	206	4	-0.91374	17	1
167	4	-0.11587	41	43	207	4	-0.33784	15	3
168	4	-0.23673	38	44	208	4	-0.17096	18	4
169	4	0.371534	15	45	209	4	-0.17096	18	4
170	4	0.687708	14	46	210	4	-0.00411	6	5
171	4	0.229823	46	47	211	4	0.790177	8	7
172	4	0.178435	47	48	212	4	0.177158	12	10
173	4	0.000895	48	49	213	4	0.09778	13	11
174	4	0.096247	49	50	214	4	0.012987	13	12
175	4	-0.11373	50	51	215	4	0.33452	16	12
176	4	0.297994	10	51	216	4	0.492905	17	12
177	4	0.32396	13	49	217	4	0.694872	15	14
178	4	0.179137	29	52	218	4	-0.04548	19	18
179	4	0.123988	52	53	219	4	-0.01163	20	19
180	4	-0.07481	53	54	220	4	-0.01184	20	21
181	4	-0.11942	54	55	221	4	0.013224	22	21
182	4	0.135872	11	43	222	4	-0.11809	23	22
183	4	-0.36733	44	45	223	5	0.751324	1	2
184	4	0.034739	40	56	224	5	-0.04591	2	3
185	4	-0.05442	56	41	225	5	-0.08734	3	4
186	4	-0.01584	56	42	226	5	-0.03951	4	5
187	4	0.038632	39	57	227	5	-0.04941	4	6
188	4	-0.0276	57	56	228	5	-0.01534	6	7
189	4	-0.04484	38	49	229	5	-0.06555	6	8
190	4	-0.16606	38	48	230	5	0.198146	8	9
191	4	0.189922	9	55	231	5	-0.09098	9	10
192	4	-1.00285	2	1	232	5	0.02021	9	11
193	4	-0.94805	3	2	233	5	-0.15869	9	12
194	4	-0.5967	4	3	234	5	-0.02057	9	13
195	4	-0.13777	5	4	235	5	0.230108	13	14
196	4	-0.14034	6	4	236	5	0.050168	13	15
197	4	0.177607	7	6	237	5	0.338355	1	15
198	4	0.431823	8	6	238	5	-0.00684	1	16
199	4	-1.74976	9	8	239	5	0.043717	1	17

Table 37: Measurement Values IEEE57-bus - Part4

z	Type	Value (p.u.)	From bus	To bus	z	Type	Value (p.u.)	From bus	To bus
240	5	-0.18203	3	15	290	5	-0.00553	52	53
241	5	0.011674	4	18	291	5	-0.04389	53	54
242	5	0.011674	4	18	292	5	-0.06201	54	55
243	5	-0.06877	5	6	293	5	0.045907	11	43
244	5	-0.12638	7	8	294	5	0.035702	44	45
245	5	-0.20291	10	12	295	5	0.041239	40	56
246	5	-0.04545	11	13	296	5	0.006511	56	41
247	5	0.601919	12	13	297	5	0.015092	56	42
248	5	0.09243	12	16	298	5	0.029221	39	57
249	5	0.093906	12	17	299	5	0.007483	57	56
250	5	-0.09932	14	15	300	5	-0.104	38	49
251	5	0.014436	18	19	301	5	-0.1867	38	48
252	5	0.005806	19	20	302	5	0.101979	9	55
253	5	0.003089	21	20	303	5	-0.84271	2	1
254	5	-0.00892	21	22	304	5	0.043864	3	2
255	5	0.055924	22	23	305	5	0.064426	4	3
256	5	0.010073	23	24	306	5	0.017565	5	4
257	5	0.016698	24	25	307	5	0.019192	6	4
258	5	0.016698	24	25	308	5	-0.00795	7	6
259	5	-0.02375	24	26	309	5	0.052167	8	6
260	5	-0.01676	26	27	310	5	-0.03946	11	9
261	5	-0.02341	27	28	311	5	0.086609	12	9
262	5	-0.04663	28	29	312	5	-0.01829	13	9
263	5	0.130408	7	29	313	5	-0.23755	14	13
264	5	0.046619	25	30	314	5	-0.05049	15	13
265	5	0.0257	30	31	315	5	-0.24083	15	1
266	5	-0.00265	31	32	316	5	0.068801	16	1
267	5	0.015442	32	33	317	5	0.013291	17	1
268	5	0.038535	34	32	318	5	0.136731	15	3
269	5	-0.03802	34	35	319	5	0.001949	18	4
270	5	-0.06987	35	36	320	5	0.001949	18	4
271	5	-0.10719	36	37	321	5	0.178597	12	10
272	5	-0.13841	37	38	322	5	0.028361	13	11
273	5	0.027138	37	39	323	5	-0.63941	13	12
274	5	0.039567	36	40	324	5	-0.10507	16	12
275	5	-0.03611	22	38	325	5	-0.10001	17	12
276	5	0.035646	11	41	326	5	0.113002	15	14
277	5	0.033502	41	42	327	5	-0.01281	19	18
278	5	-0.03109	41	43	328	5	-0.00573	20	19
279	5	0.048598	38	44	329	5	-0.00324	20	21
280	5	-0.00763	15	45	330	5	0.00895	22	21
281	5	0.42269	14	46	331	5	-0.05567	23	22
282	5	0.183876	46	47	332	5	-0.01821	24	23
283	5	0.1267	47	48	333	5	-0.01068	25	24
284	5	-0.07462	48	49	334	5	-0.01068	25	24
285	5	0.045268	49	50	335	5	0.026448	26	24
286	5	-0.06263	50	51	336	5	0.01994	27	26
287	5	0.125162	10	51	337	5	0.027411	28	27
288	5	0.340184	13	49	338	5	0.050244	29	28
289	5	0.02628	29	52					