UNIVERSIDADE DE SÃO PAULO
ESCOLA DE ENGENHARIA DE SÃO CARLOS

Eduardo Correia Gibara

Avaliação da Eficiência de Técnicas de Detecção de EGs em Ambientes Sujeitos a Ataques Cibernéticos FDI

São Carlos

2025

Ficha catalográfica elaborada pela Biblioteca Prof. Dr. Sérgio Rodrigues Fontes da EESC/USP com os dados inseridos pelo(a) autor(a).

Gibara, Eduardo
G437a Avaliação da eficiência de técnicas de detecção de EGs em ambientes sujeitos a ataques cibernéticos FDI / Eduardo Gibara; orientador João Bosco London Júnior. São Carlos, 2025.

Monografia (Graduação em Engenharia Elétrica com ênfase em Sistemas de Energia e Automação) -- Escola de Engenharia de São Carlos da Universidade de São Paulo, 2025.

1. Estimadores de Estado. 2. FDI. 3. Processamento de Erros Grosseiros. 4. Redes Inteligentes. 5. Cibersegurança. I. Título.

Eduardo Graziosi Silva - CRB - 8/8907

FOLHA DE APROVAÇÃO

Nome: Eduardo Correia Gibara

Título: "Avaliação da Eficiência de Técnicas de Detecção de EGs em Ambientes Sujeitos a Ataques Cibernáticos FDI"

Trabalho de Conclusão de Curso defendido e aprovado em 05/12/2025,

com NOTA 9,5 (nove, cinco), pela Comissão Julgadora:

Prof. Titular João Bosco Augusto London Júnior - Orientador SEL/EESC/USP

Mestre Gustavo da Silva Pinheiro Rondon - Doutorando EESC/USP

Dra. Etiane Oliveira Ponciano de Carvalho - Professora substituta - Universidade Federal de Mato Grosso (UFMT)

Coordenador da CoC-Engenharia Elétrica - EESC/USP:
Professor Associado José Carlos de Melo Vieira Júnior

AGRADECIMENTOS

Ao meu orientador o Professor Doutor João Auguto Bosco London Junior e à Gustavo da Silva Pinheiro Rondon pelas orientações, sugestões e ensinamentos que me acompanharam ao longo do caminho.

Aos meus pais e familiares, pelo suporte e confiança nos momentos difíceis.

Aos meus amigos por me proporcionarem momentos de felicidade e relaxamento.

RESUMO

GIBARA, E. C. 2025. 69p. Monografia (Trabalho de Conclusão de Curso) - Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2025.

O presente trabalho investiga os impactos de ataques de Injeção de Dados Falsos (*FDI*) no processo de Estimação de Estado em Sistemas Elétricos de Potência, considerando condições operacionais realistas, como a presença de ruído e Erros Grosseiros (EGs) nas medições. Foram avaliados o estimador WLS e dois métodos de detecção e tratamento de EGs: o teste do maior resíduo normalizado e a técnica de correção por erro composto, fundamentada no índice de não detecção (*UI*). Os resultados mostram que ataques *FDI* podem permanecer indetectáveis mesmo em cenários adversos, evidenciando a vulnerabilidade do processo tradicional de estimação de estado. Observou-se ainda que o erro composto apresenta alto desempenho em alguns casos, mas sua acurácia é prejudicada quando o ataque altera diretamente as medidas utilizadas no cálculo do erro composto, enquanto o teste do resíduo normalizado apresentou maior estabilidade em algumas situações. Por fim, discute-se a necessidade de investigar vetores de ataque mais esparsos e a possibilidade de utilizar a remoção de medidas orientada pelo erro composto como alternativas promissoras para aprimorar a detecção de ataques *FDI*.

Palavras-chave: Estimadores de Estado, *FDI*, Processamento de Erros Grosseiros, Redes Inteligentes, Cibersegurança.

ABSTRACT

GIBARA, E. C. . 2025. 69p. Monograph (Conclusion Course Paper) - Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2025.

ABSTRACT

This work investigates the impacts of False Data Injection (FDI) attacks on the State Estimation process in Electric Power Systems (EPS), considering realistic operating conditions such as measurement noise and Gross Errors (GEs). The study evaluates the Weighted Least Squares (WLS) estimator and two methods for detecting and handling GEs: the normalized residual test and the correction technique based on the composite error, derived from the Undetectability Index (UI). The results show that FDI attacks can remain undetectable even under adverse conditions, highlighting the vulnerability of conventional state estimation procedures. Furthermore, the composite error method demonstrated high accuracy in some scenarios, but its performance deteriorated when the attack directly affected the measurements used in its computation, whereas the normalized residual test exhibited more consistent behavior in specific cases. Finally, the findings suggest future investigations involving sparser attack vectors and the use of composite-error-based measurement removal as promising directions for enhancing FDI detection in modern EPS.

Keywords: State Estimation; FDI; Gross Errors Processing; Smart Grids; Cybersafety.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

SEP	Sistema Elétrico de Potência
EESEP	Estimação de Estado em Sistemas Elétricos de Potência
WLS	*Weighted Least Squares* (Mínimos Quadrados Ponderados)
EG	Erro Grosseiro
WLAV	*Weighted Least Absolute Value* (Mínimo Valor Absoluto Ponderado)
WLMS	*Weighted Least Median of Squares* (Mínima Mediana do Resíduo Ponderado ao Quadrado)
HTI	*Hypothesis Testing Identification* (Identificação por Teste de Hipótese)
UI	*Undetectability Index* (Índice de Não-Detecção)
FDI	*False Data Injection* (Ataque de injeção de dados falsos)
TCC	Trabalho de Conclusão de Curso
LACOSEP	Laboratório de Análise Computacional em Sistemas Elétricos de Potência
USP	Universidade de São Paulo
SCADA	*Supervisory Control and Data Acquisition* (Controle Supervisório e Aquisição de Dados)
P.U.	Por Unidade
EMA	Erro Médio Absoluto
EC	Erro Composto
V13	Tensão no barramento 13
P5	Injeção de potência ativa no barramento 5
P2	Injeção de potência ativa no barramento 2
Q5	Injeção de potência reativa no barramento 5
Q3	Injeção de potência reativa no barramento 3

SUMÁRIO

1 INTRODUÇÃO

Nos últimos séculos, a expansão da capacidade humana de transformar e transmitir energia permitiu mudanças radicais no estilo de vida das nações. A associação entre qualidade de energia elétrica e desenvolvimento econômico permanece até a atualidade, sendo que os países mais desenvolvidos são providos de fornecimento mais robusto de energia elétrica, apesar do seu alto consumo.

Todavia, a popularização de cargas eletrônicas na rede nas últimas décadas e o aumento da penetração de fontes renováveis de energia desafiam os operadores e pesquisadores da área. Equipamentos eletrônicos conectados à rede provocam alterações na qualidade da energia elétrica entregue ao consumidor, podendo ocasionar comportamentos imprevistos em motores e em outras cargas. Por outro lado, energias renováveis, como a solar e a eólica, contribuem para a redução dos custos de geração e das emissões de gases de efeito estufa, mas apresentam caráter intermitente e exigem o uso intensivo de dispositivos eletrônicos na rede.

Essas tecnologias emergentes requerem sistemas mais robustos, interconectados e autônomos, características associadas ao conceito de redes inteligentes (*smart grids*). Nesse cenário, informações confiáveis sobre as condições da rede elétrica tornam-se cada vez mais indispensáveis para que os operadores compreendam a situação atual do sistema e realizem estudos de estabilidade, segurança e expansão da rede.

Contudo, em Sistemas Elétricos de Potência (SEPs) há uma série de fatores que podem comprometer a qualidade das informações fornecidas aos operadores, como o ruído presente nos transdutores de medição, falhas nos sistemas de telecomunicação e até mesmo dados adulterados com o objetivo de interferir na operação. Para mitigar tais problemas, destacam-se os algoritmos de estimação de estado, que se destinam à obtenção, em tempo real, das variáveis de estado de um SEP (usualmente as tensões complexas nodais), através de um conjunto redundante[1] de medidas com ruído, constituído usualmente de: fluxo de potência ativa e reativa nas linhas, injeção de potência ativa e reativa e algumas magnitudes de tensão nos barramentos.

Desde o final da década de 1960, pesquisas sobre o processo de Estimação de Estado em Sistemas Elétricos de Potência (EESEP) consolidaram seu uso como ferramenta fundamental para a operação em tempo real. Nessa época, o professor Schweppe e colaboradores (SCHWEPPE; WILDES, 1970; SCHWEPPE; ROM, 1970) estudaram a natureza do problema e apresentaram conceitos que se tornaram a base da formula-

[1] Redundância refere-se ao excedente de medidas em relação ao número de variáveis de estado a serem estimadas.

ção clássica. O método mais tradicional, o estimador baseado no critério dos mínimos quadrados ponderados (WLS, *Weigthed Least Squares*), apresenta excelente desempenho na presença de ruídos gaussianos. Entretanto, erros de grande magnitude, definidos na literatura como Erros Grosseiros (EGs), podem ocorrer e precisam ser detectados e tratados por meio, por exemplo, da análise estatística dos resíduos do estimador de estado WLS (MONTICELLI, 2012; ABUR; EXPOSITO, 2004; BRETAS *et al.*, 2021). Além disso, a crescente complexidade dos sistemas modernos torna a ocorrência de inconsistências ainda mais provável.

Na ocorrência de EGs simples, isto é, quando apenas uma medida está corrompida, ou em casos particulares de EGs múltiplos não interativos[2], o estimador WLS, associado ao teste do maior resíduo normalizado, apresenta bom desempenho. Entretanto, essa abordagem pode falhar em três situações principais (ABUR; EXPÓSITO, 2004; BRETAS et al., 2021):

- EGs em medidas com baixa redundância;
- EGs múltiplos interativos;
- EGs em medidas altamente influentes, também chamadas de medidas ponto de alavancamento, capazes de atrair a convergência do processo de estimação.

Devido a essas limitações, diferentes estimadores robustos estatisticamente foram propostos. Um exemplo é o baseado no Mínimo Valor Absoluto Ponderado (*WLAV*, *Weigthed Least Absolute Value*) (IRVING; OWEN; STERLING, 1978; KOTIUGA; VIDYASAGAR, 2007), que apresentou maior robustez frente a EGs simples e múltiplos. Contudo, o *WLAV* também falha quando os EGs estão em medidas ponto de alavancamento (FALCẠO; ASSIS, 1988). Para superar esse problema, Mili, Phaniraj e Rousseeuw (2002) propuseram o estimador baseado no método da Mínima Mediana do Resíduo Ponderado ao Quadrado (*WLMS*, *Weighted Least Median of Squares*), considerado a primeira formulação robusta capaz de lidar com EGs em medidas de alavancagem. No entanto, por exigir uma busca combinatória, o *WLMS* torna-se inviável para aplicação em tempo real em SEPs de grande porte (FALCAO; ARIAS, 1994; MONTICELLI, 2012). Assim, apesar de seu apelo teórico, o *WLMS* permanece praticamente restrito ao uso acadêmico.

Em função da inviabilidade prática do *WLMS* e da simplicidade do estimador WLS, este último, associado ao teste do maior resíduo normalizado, consolidou-se como o mais utilizado na prática. Desde então, diversas pesquisas têm buscado aprimorar sua eficácia no processamento de EGs. Em Monticelli e Garcia (2007), por exemplo, o teste-$\hat{b}$ foi proposto em conjunto com o teste do maior resíduo normalizado para melhorar a identificação de

[2] Definições e conceitos pertinentes aos tipos de EGs em medidas, assim como, à análise de resíduos das medidas, serão detalhados no capítulo 2.

EGs pela análise dos resíduos. Já Cutsem, Ribbens-Pavella e Mili (1984) propuseram o processo de Identificação por Teste de Hipótese (*Hypothesis Testing Identification*, *HTI*), baseado em valores estimados de erro em medidas, em vez da análise direta dos resíduos. A eficiência do teste *HTI* depende da escolha de um conjunto suspeito de medidas, isto é, um subconjunto de medidas potencialmente corrompidas. Entretanto, essa seleção, geralmente feita com base nos maiores resíduos normalizados, pode ser comprometida quando medidas portadoras de EG apresentam resíduos baixos (ABUR; EXPOSITO, 2004; BRETAS *et al.*, 2021). Esse comportamento evidencia a necessidade de métricas capazes de capturar componentes do erro que não se manifestam no resíduo.

Buscando superar essa limitação, Benedito *et al.* (2014) propuseram o Índice de Não-Detecção (*UI*, *Undetectability Index*), uma métrica que classifica medidas segundo sua capacidade de refletir (ou mascarar) os erros introduzidos nos resíduos. Medidas com elevado *UI* têm maior probabilidade de esconder seus erros, dificultando a detecção por testes convencionais, como o do maior resíduo normalizado ou o teste-$\hat{b}$. Em simulações relatadas em Benedito (2011), observou-se que, em medidas com alto *UI*, o maior resíduo normalizado não correspondia à medida portadora de EG, evidenciando a falha dos métodos tradicionais e a utilidade do *UI* para avaliar a vulnerabilidade do processo de estimação.

Esse avanço é especialmente relevante porque, nos últimos anos, o interesse por técnicas mais robustas para detecção e identificação de EGs tem aumentado significativamente, em grande parte devido à possibilidade de ataques cibernéticos às informações utilizadas pelos estimadores de estado (ASHOK; GOVINDARASU; AJJARAPU, 2018; HUSNOO *et al.*, 2023; HABIB *et al.*, 2023). Inicialmente, acreditava-se que os métodos tradicionais de processamento de EGs seriam suficientes para detectar dados corrompidos por ataques. Contudo, Liu, Ning e Reiter (2011) demonstraram que um tipo específico de ataque, denominado ataque de injeção de dados falsos (*FDI*, *False Data Injection*), pode ser construído de modo a explorar o modelo matemático do estimador, permanecendo indetectável pelos métodos convencionais. Esse resultado revelou um novo patamar de vulnerabilidade nos SEPs, reforçando a importância de estudar técnicas de proteção e defesa cibernética aplicadas ao processo de estimação de estado. Esse resultado inaugurou uma nova linha de pesquisa em cibersegurança aplicada a SEPs, motivando o desenvolvimento de técnicas adicionais de análise de vulnerabilidade e mecanismos de defesa.

1.1 Objetivos

Este Trabalho de Conclusão de Curso (TCC) tem como objetivo principal analisar a vulnerabilidade do processo clássico de EESEP frente a ataques cibernéticos do tipo *FDI*.

Para alcançar este objetivo, os objetivos específicos são:

- Estudar e implementar o estimador de estado WLS e o teste do maior resíduo normalizado, técnicas amplamente utilizadas na indústria, para estimação de estado e processamento de EGs respectivamente;
- Estudar e implementar a técnica de processamento de EGs baseada no erro composto, desenvolvido com base no índice *UI* conforme proposto em Benedito *et al.* (2014). Ressalta-se que esta é a primeira aplicação conhecida desse método considerando a presença de ataques *FDI*;
- Estudar os conceitos de ataques cibernéticos do tipo *FDI* apresentados em Liu, Ning e Reiter (2011) para a geração de simulações computacionais;
- Realizar simulações no sistema de teste IEEE de 14 barras, considerando a presença de ruídos, EGs e ataques *FDI*, a fim de obter uma análise detalhada da vulnerabilidade do processo de EESEP;
- Avaliar a possibilidade de utilização do índice *UI* para a melhoria das estimativas na presença de ataques *FDI*.

As ferramentas computacionais a serem utilizadas incluem um estimador de estado desenvolvido por pesquisadores do Laboratório de Análise Computacional em Sistemas Elétricos de Potência (LACOSEP) da Universidade de São Paulo (USP) e o pacote de ferramentas MATPOWER para o software MATLAB, para o cálculo de fluxo de potência.

1.2 Organização do Trabalho

Este capítulo introduz o contexto atual dos SEPs e a relevância do estudo dos algoritmos para estimação de estado nesse cenário.

O Capítulo 2 aborda a formulação do estimador de estado WLS e do teste do maior resíduo normalizado. Em seguida, explora as limitações desses processos com a introdução e formulação matemática do índice *UI* e do erro composto.

O Capítulo 3 detalha a estrutura dos ataques *FDI*, que serve de base para as simulações.

O Capítulo 4 apresenta os resultados das simulações computacionais, destacando a congruência com os fundamentos teóricos e a discussão dos dados mais relevantes.

Finalmente, o Capítulo 5 reúne as conclusões do trabalho, apresentando sugestões para trabalhos futuros e uma síntese dos resultados das simulações computacionais.

2 ESTIMAÇÃO DE ESTADO EM SISTEMAS ELÉTRICOS DE POTÊNCIA

Este capítulo apresenta, inicialmente, as quatro etapas que compõem o processo tradicional de Estimação de Estado em Sistemas Elétricos de Potência. Essa abordagem baseia-se exclusivamente na disponibilidade de medidas provenientes do sistema *SCADA* (Controle Supervisório e Aquisição de Dados do inglês, *Supervisory Control and Data Acquisition*), na suposição de operação em regime permanente e equilibrado, e na premissa de que os parâmetros e topologia da rede estão corretos.

Em seguida, é detalhada a formulação matemática do estimador de estado baseado no método dos Mínimos Quadrados Ponderados (*WLS*, do inglês *Weigthed Least Squares*), bem como o teste do maior resíduo normalizado, utilizado para a detecção e identificação de medidas portadoras de EGs.

2.1 Etapas do Processo Tradicional de EESEP

O processo clássico de EESEP envolve quatro etapas principais (BRETAS *et al.*, 2021):

1. Obtenção da topologia – consiste em determinar a configuração do sistema no modelo barra-ramo, a partir de dados de status de chaves e disjuntores fornecidos pelo sistema *SCADA*, além da localização dos medidores.

2. Análise de observabilidade – verifica se o conjunto de medidas analógicas[1] disponíveis é suficiente para determinar todas as variáveis de estado. Caso não seja, pseudo-medidas[2] podem ser incluídas para assegurar a observabilidade.

3. Estimação de estado – realizada a partir das medidas analógicas e dos parâmetros do sistema armazenados no banco de dados[3]. O estimador pode ser estático ou dinâmico:

    - O estático representa uma "fotografia" do sistema em um instante de tempo, sendo baseado em equações algébricas não lineares.
    - O dinâmico considera a evolução temporal das variáveis, mas sua aplicação prática ainda é limitada devido à baixa taxa de amostragem e assincronismo das

[1] As medidas analógicas são aquelas realizadas continuamente e usualmente se constituem de fluxo de potência ativa e reativa nas linhas, injeção de potência ativa e reativa e magnitudes de tensão nas barras.

[2] Pseudo-medidas são dados de previsão de carga, previsão de geração, dados históricos, etc., que fazem parte do banco de dados dos centros de operação.

[3] Impedância de linhas de transmissão, posição de taps de transformadores, etc.

medidas *SCADA*. Com a crescente utilização das Unidades de Medição Fasorial (PMUs, *Phasor Measurement Units*), entretanto, espera-se maior aplicabilidade futura.

4. Tratamento de EGs – como as medidas analógicas estão sujeitas a ruídos e inconsistências, a estimação obtida nunca é exata. Como indicado no capítulo 1, para SEP o estimador *WLS* é o mais utilizado na prática e estudado na academia, eficaz frente a erros gaussianos, mas sensível a EGs. Tais erros podem ter diversas origens, como falhas na conversão analógico-digital, saturação de transformadores de instrumentação ou problemas de comunicação. Para lidar com EGs, o processo tradicional inclui uma etapa de detecção e identificação, na qual o método mais comum é o teste do maior resíduo normalizado. Caso um EG seja identificado, a etapa de estimação é repetida até que se obtenha um conjunto de variáveis de estado consistente.

Face ao exposto, o processo tradicional de EESEP busca garantir que, mesmo diante de medidas ruidosas ou corrompidas, seja possível obter uma representação confiável das variáveis de estado dos SEPs.

2.2 Estimador WLS

Conforme mencionado no capítulo 1, o estimador de estado mais utilizado em SEPs baseia-se no critério *WLS*. Isso se deve a algumas vantagens desse método como o custo computacional relativamente baixo e maior verossimilhança na presença de erros gaussianos (BRETAS *et al.*, 2021). Além disso, são comumente utilizados estimadores monofásicos com os componentes de sequência positiva do SEP devido a sua alta acurácia em sistemas de transmissão de alta tensão. Tal fato decorre do baixo nível de desbalanceamento entre as 3 fases dos sistemas elétricos, o que é típico desses sistemas, apesar de serem notáveis casos na literatura de sistemas de distribuição que requerem o uso de uma abordagem por fase para o EESEP (HANSEN; DEBS, 2002; ZHONG; ABUR, 2002; ALMEIDA; ASADA; GARCIA, 2006; STEFOPOULOS *et al.*, 2007). Ademais, utilizando outras hipóteses simplificadoras das equações de fluxo de potência em SEPs foram definidas outras variações do algoritmo *WLS* como os estimadores lineares, que linearizam as equações de fluxo de potência, e o algoritmo *WLS* desacoplado, que despreza alguns dos termos presentes nas equações (MONTICELLI, 2012; JONES; THORP; GARDNER, 2013).

2.2.1 Modelo de Medição

Conhecida a topologia e os parâmetros de um SEP, a determinação das variáveis de estado é realizada a partir de valores medidos, os quais estão sujeitos a imperfeições inerentes ao processo de medição, como imprecisão dos instrumentos, problemas nos canais de comunicação e efeitos da conversão analógico–digital. Dessa forma, as medidas

disponíveis em um SEP podem ser relacionadas aos erros de medição por meio do seguinte modelo:

$$z = z^v + e, \tag{2.1}$$

onde:

- z é o vetor das medidas analógicas aferidas, de dimensão $(m \times 1)$;
- z^v representa o vetor com os valores "verdadeiros" das medidas, também de dimensão $(m \times 1)$;
- e é o vetor aleatório associado aos erros de medição, de dimensão $(m \times 1)$.

Como os valores verdadeiros das variáveis de estado não são conhecidos, os valores verdadeiros das medidas também são desconhecidos. Para estimar o estado do sistema, é necessário assumir hipóteses estatísticas sobre o vetor de erros e. No processo convencional de EESEP, admite-se que e segue uma distribuição gaussiana de média zero, $E(e) = 0$, e matriz de covariância R, tal que $E(ee^T) = R$. Além disso, considera-se que os erros são não correlacionados. Assim, R é usualmente uma matriz diagonal, cujos elementos correspondem às variâncias dos erros de medição, valores normalmente determinados a partir da precisão e do fundo de escala dos instrumentos.

A partir dessas hipóteses, o modelo de medição tradicional (equação (2.1)) pode ser escrito de forma equivalente como:

$$z = h(x) + e, \tag{2.2}$$

onde:

- x é o vetor das variáveis de estado, de dimensão $(N \times 1)$, formado por $(n-1)$ ângulos de fase e n magnitudes de tensão nodais, para um SEP com n barras, considerando que uma barra é tomada como referência angular $(N = 2n - 1)$;
- $h(x)$ é o vetor das funções, lineares ou não lineares, que relacionam as quantidades medidas às variáveis de estado, possuindo dimensão $(m \times 1)$.

Conforme mencionado anteriormente, as medidas analógicas utilizadas no processo de EESEP são, em geral, fluxos de potência ativa e reativa (em linhas e transformadores), injeções de potência em barras e magnitudes de tensão nodal obtidas via *SCADA*. Com o surgimento das PMUs, novas pesquisas têm buscado incorporar ao processo de estimação as Medidas Fasoriais Sincronizadas (MFSs), que incluem fasores de tensão em barras e

fasores de corrente em ramos. A base de tempo utilizada pelas PMUs provém do sinal de sincronização do sistema GPS (Global Positioning System).

Além dessas informações oriundas de equipamentos de medição, informações provenientes de barras com injeção nula, as chamadas medidas virtuais, também podem ser utilizadas no processo de EESEP. Embora não correspondam a valores diretamente medidos, tais informações representam condições operativas válidas e podem ser incluídas como medidas de injeção com baixa variância ou tratadas como restrições de igualdade no modelo.

2.2.2 Formulação Matemática

O algoritmo estimador de estado *WLS* objetiva resolver o problema de encontrar o vetor das variáveis de estado x que torna mínimo o índice $J(x)$ na equação abaixo. Onde a matriz W se trata da matriz de ponderações que pondera a influência númerica de cada medida na equação.

$$J(\mathbf{x}) = \Big(\mathbf{z} - \mathbf{h}(\mathbf{x})\Big)^{\top} \mathbf{W} \Big(\mathbf{z} - \mathbf{h}(\mathbf{x})\Big), \tag{2.3}$$

onde $W = R^{-1}$ é a matriz de ponderações, definida como o inverso da matriz de covariância dos erros de medição. Quando os erros são independentes, R é diagonal e contém as variâncias associadas a cada medida.

A adoção de $W = R^{-1}$ garante que medidas mais precisas exerçam maior influência no processo de estimação, enquanto medidas mais imprecisas são naturalmente penalizadas.

O problema consiste então em encontrar x tal que o gradiente de $J(x)$ seja nulo:

$$\frac{\partial J(x)}{\partial x} = 0 \tag{2.4}$$

Dessa forma:

$$H^{\top}(\hat{x})\, R^{-1} \Big[z - h(\hat{x})\Big] = 0 \tag{2.5}$$

Onde a matriz H na equação acima é conhecida como matriz jacobiana e seus valores são as primeiras derivadas dos valores do vetor z em relação aos valores de x para o vetor $\hat{x}$ estimado.

$$H(\hat{x}) = \left.\frac{\partial h(x)}{\partial x}\right|_{x=\hat{x}} \tag{2.6}$$

Como o índice $J(x)$, partindo do pressuposto que as equações de $h(x)$ são não lineares, não oferece uma solução algébrica direta (Schweppe; Handschin, 1974) opta-se por utilizar um método iterativo para encontrar $\hat{x}$. Destarte, o processo passa a ser corrigir sucessivamente o valor de x em cada iteração k até encontrar o valor que satisfaça o problema.

$$x^{k+1} = x^{k} + \Delta x^{k} \tag{2.7}$$

Além disso, partindo da definição da matriz Jacobiana o vetor de medidas em cada iteração também pode ser aproximado por:

$$h(x^{k+1}) \cong h(x^k) + H(x^k)\,\Delta x^k \tag{2.8}$$

Assim, para uma variação Δx o índice $J(x)$ se torna:

$$J(\Delta x) = \left[\Delta z(x^K) - H(x^K)\Delta x^K\right]^T W \left[\Delta z(x^K) - H(x^K)\Delta x^K\right] \tag{2.9}$$

onde

$$\Delta z(x^k) = z - h(x^k).$$

E o problema descrito pode ser reescrito como:

$$\frac{\partial J(\Delta x)}{\partial \Delta x} = H(x^K)^T W \left[\Delta z(x^K) - H(x^K)\Delta x^K\right] = 0 \tag{2.10}$$

A solução iterativa do problema passa a ser obtida pela seguinte equação:

$$\Delta x^K = \left[H(x^K)^T W H(x^K)\right]^{-1} H(x^K)^T W \Delta z(x^K) \tag{2.11}$$

Essa equação, denominada Equação Normal, é definida por uma multiplicação de matrizes que é definida como uma matriz ganho G que é calculada em cada iteração:

$$H(x^K)^T W H(x^K) = G(x^K) \tag{2.12}$$

E consequentemente a partir das Equaçãoes (2.12) e (2.11) pode-se obter:

$$\Delta \hat{x} = G(x^k)^{-1} H(x^K)^T W \Delta z(\hat{x}) \tag{2.13}$$

Outrossim, necessariamente por se tratar de um método recursivo para resolver um problema númerico um critério de para precisa ser adotado a partir da um tolerância ϵ estabelecida. Nesse caso, o critério utilizado é o valor máximo da variação de x em cada iteração:

$$\max|\Delta x^K| \leq \varepsilon \tag{2.14}$$

2.2.3 Matriz de Projeção (Matriz Chapéu)

A partir das equações do *WLS*, pode-se definir a matriz K, chamada de matriz de projeção ou matriz chapéu, como:

$$K = HG(\hat{x})^{-1} H(\hat{x})^T R^{-1}. \tag{2.15}$$

A estimativa das medidas é dada por:

$$\Delta\hat{z} = H(\hat{x})\Delta\hat{x} = K\Delta z. \tag{2.16}$$

A matriz K permite avaliar o grau de redundância do plano de medição e quantificar a influência relativa de cada medida no valor estimado. Diagonais próximas de 1 indicam medidas altamente influentes.

2.2.4 Etapas do Algoritmo do Estimador WLS

- **Passo 1:** Escolher uma solução inicial $x^K = x^0$;
- **Passo 2:** Calcular as matrizes $H(x^K)$ e $G(x^K)$ no ponto $x = x^K$;
- **Passo 3:** Obter a correção nas variáveis de estado através da equação normal e atualizar as variáveis:

$$\Delta x^K = G(x^K)^{-1} H(x^K)^T W \Delta z(x^K) \tag{2.17}$$

$$x^{K+1} = x^K + \Delta x^K \tag{2.18}$$

- **Passo 4:** Testar o critério de parada: se $\max|\Delta x^K| \leq \varepsilon$, o processo convergiu. Caso contrário, faça $\hat{x} = x^{(k+1)}$, $k = k + 1$ e retorne ao **Passo 2**.

Para execução do estimador de estado *WLS* é necessário estimar os desvios padrão das medidas para obtenção da matriz de ponderação W.

Assumindo erro gaussiano, o desvio padrão associado a cada medida $z[i]$ pode ser estimado por:

$$\hat{\sigma}[i] = \frac{\text{Precisão} \cdot |z[i]|}{3} \tag{2.19}$$

Essa definição decorre do fato de que, para variáveis aleatórias gaussianas, aproximadamente 99,72% dos valores encontram-se dentro do intervalo $\pm 3\sigma$. Assim, conhecendo o intervalo de precisão (Precisão) do medidor, é possível estimar o desvio padrão correspondente.

2.2.5 Processamento de Erros Grosseiros

Medidas portadoras de erro grosseiro no plano de medidas prejudicam a acurácia do processo de EESEP e consequentemente na literatura diversos métodos foram desenvolvidos para realizar a detecção, identificação e eliminação, ou, até mesmo, a correção de medidas portadoras de EGs. Um dos métodos mais utilizados é o chamado teste do maior resíduo normalizado (teste rN).

O vetor de resíduos é definido por:

$$r = z - h(\hat{x}) \tag{2.20}$$

Os resíduos normalizados são:

$$r_i^N = \frac{r_i}{\sqrt{\Omega_{ii}}}, \tag{2.21}$$

onde Ω é a matriz de covariância dos resíduos:

$$\Omega = R - H(\hat{x})\, G^{-1}(\hat{x})\, H^T(\hat{x}) \tag{2.22}$$

O teste consiste em:

- Se $\max |r_i^N| > \beta$, há suspeita de EG;
- Caso contrário, não há suspeita.

O valor escolhido para o limiar é geralmente de 3 (ABUR; EXPOSITO, 2004) e seu valor representa uma certa probabilidade do a_i da medida ser identificada incorretamente para uma distribuição normal padrão.

2.3 Considerações Finais

Neste capítulo foram apresentadas as principais etapas do processo tradicional de EESEP, cuja aplicação baseia-se em medidas fornecidas pelo sistema *SCADA*, na suposição de operação em regime permanente e equilibrado e na representação adequada da topologia e dos parâmetros do SEP.

Foram discutidos em detalhe o modelo de medição, a formulação matemática do estimador baseado no método *WLS* e as técnicas clássicas de detecção de EGs, com destaque para o teste do maior resíduo normalizado, amplamente utilizado na prática operacional.

O conteúdo apresentado consolida a base conceitual necessária para a compreensão do processo de estimação de estado convencional, incluindo a modelagem estatística dos erros, o procedimento iterativo de solução e os mecanismos tradicionalmente empregados para identificação de medidas inconsistentes.

A partir dessa estrutura, torna-se possível entender as limitações do estimador *WLS* diante de condições mais desafiadoras, especialmente quando erros não se manifestam de forma evidente nos resíduos, como ocorre em medidas altamente influentes ou em situações de ataque cibernético. Esses aspectos motivam o estudo de métodos complementares e métricas adicionais.

No capítulo seguinte, são introduzidos o Índice *UI* e o modelo de ataques *FDI*, que permitem avaliar de maneira mais aprofundada a vulnerabilidade do processo de EESEP e investigar cenários nos quais o processamento convencional de EGs pode falhar.

3 EMBASAMENTO TÉORICO

Este capítulo apresenta os fundamentos teóricos necessários para compreender as vulnerabilidades do processo de EESEP frente à ocorrência de ataques cibernéticos. A partir do conhecimento consolidado sobre o estimador baseado no método *WLS*, discutido no capítulo anterior, são agora introduzidas métricas e formulações que permitem aprofundar a análise de desempenho e segurança desse processo.

Inicialmente, são apresentados o *UI* e o erro composto, conceitos que possibilitam avaliar quantitativamente a sensibilidade do estimador *WLS* na presença de medidas portadoras de EGs. Essas métricas permitem identificar medidas potencialmente "críticas" no contexto de processamento de EGs, cujos erros podem ser mascarados pelo processo de estimação, comprometendo a eficácia dos métodos convencionais de detecção baseados na análise de resíduos.

Em seguida, é desenvolvida a formulação matemática de um tipo específico de ataque cibernético ao processo de EESEP, conhecido como *FDI*, que explora o modelo do estimador de estado para introduzir perturbações nas medições de forma deliberada e não detectável pelos testes tradicionais. Esse tipo de ataque representa uma ameaça crescente para sistemas elétricos modernos, especialmente em ambientes que fazem uso intensivo de monitoramento remoto e telecomunicação.

Por fim, é apresentado um exemplo didático que ilustra, por meio da aplicação do estimador *WLS* em suas versões linear e não linear, o comportamento do processo de estimação diante de EGs e ataques *FDI*. Esse exemplo tem como objetivo demonstrar, de forma prática, os conceitos teóricos abordados ao longo do capítulo e fornecer a base para as análises e simulações que serão realizadas nos capítulos seguintes.

3.1 Indíce UI

O indíce *UI* foi primeiro definido em Benedito (2011) a partir da interpretação geométrica do estimador de estado *WLS*. Conforme apresentado no capítulo anterior, o estimador *WLS* objetiva minimizar o indíce $J(x)$ (equação (3.2)), que pode ser interpretado como sendo a norma, no espaço vetorial das medidas R^m. Essa norma, por sua vez, vem da definição do produto interno nesse espaço vetorial: $\langle u, v\rangle = u^t \cdot R^{-1} \cdot v$. Assim, é possível reescrever o indíce $J(x)$ como na equação (3.2):

$$J(x) = \|(z - h(x))\|^2_{R^{-1}} = \langle z - h(x),\, z - h(x)\rangle \tag{3.1}$$

$$J(x) = (z - h(x))^t \, R^{-1} \, (z - h(x)) \tag{3.2}$$

Durante o processo de EESEP as equações são linearizadas utilizando a matriz Jacobiana apropriada em cada iteração. Destarte, partindo da equação (2.2) encontramos a seguinte equação:

$$\Delta z = H \cdot \Delta x + w \tag{3.3}$$

Considerando que $m > N$ devido à redundância típica de medidas em SEPs, e assumindo que o posto de H é igual a N (condição de observabilidade), é possível decompor o espaço vetorial das medidas como:

$$R^m = R(H) \oplus R(H)^{\perp}, \tag{3.4}$$

onde, a imagem de H é representada pelo subespaço vetorial $R(H)$ e o seu complemento ortogonal é o subespaço vetorial $R(H)^{\perp}$. Ou seja, se $u \in R(H)$ e $v \in R(H)^{\perp}$, então $\langle u, v \rangle = u^t \cdot R^{-1} \cdot v = 0$.

A equação (3.3) pode ser interpretada como uma projeção de vetor de correção em $R(H)$, de tal forma que ocorra a minimização do índice $J(x)$. Assim, a matriz chapéu K, discutida no capítulo anterior, pode ser reinterpretada como um operador linear que relaciona uma variação no vetor de medidas com uma variação no subespaço $R(H)$. Ademais, o vetor resíduo, definido no capítulo anterior, pode ser escrito de forma a definir uma nova matriz, a matriz S, chamada de matriz de sensbilidade dos resíduos, que projeta o vetor z em $R(H)^{\perp}$.

$$\begin{aligned} r &= \Delta \underline{z} - \Delta \hat{\underline{z}} = \Delta \underline{z} - K \cdot \Delta \underline{z} \\ &= (I - K) \cdot \Delta \underline{z} = S \cdot \Delta \underline{z} \end{aligned} \tag{3.5}$$

A partir das definições expostas até aqui o vetor de erro e pode ser decomposto em duas compenentes. Para isso,vamos escrever o vetor e em função das matrizes K e S:

$$e = K \cdot e + (I - K) \cdot e = K \cdot e + S \cdot e \tag{3.6}$$

Torna-se então possível a definição dos componentes detectável (e_D) e não detectável (e_U) do vetor e:

$$e_U = K \cdot e \tag{3.7}$$

$$e_D = S \cdot e \tag{3.8}$$

De acordo com a definição dos componentes do erro, pode-se calcular a norma do erro como previamente definida como soma das normas dos componentes do erro:

$$||e||^2_{R^{-1}} = ||e_D||^2_{R^{-1}} + ||e_U||^2_{R^{-1}} \tag{3.9}$$

Ao realizar a mesma decomposição nos componentes do erro ao resíduo, podemos reescrever o vetor de resíduos da seguinte maneira:

$$r = (I - K) \cdot \Delta z \tag{3.10}$$

$$r = (I - K) \cdot \Delta z_v + (I - K) \cdot \Delta e_U + (I - K) \cdot \Delta e_D \tag{3.11}$$

Entretanto, podemos simplificar essa equação já que $(I - K) \cdot \Delta z_v = 0$ e $(I - K) \cdot \Delta e_U = 0$, o que resulta na equação (3.12).

$$r = (I - K) \cdot \Delta e_D \tag{3.12}$$

Isso evidencia que o teste de resíduos responde apenas ao componente detectável do erro, sendo totalmente insensível ao componente não detectável. Essa é a motivação central para o uso do índice *UI*.

O índice *UI* para a medida i é definido como (BENEDITO et al., 2013):

$$UI_i = \frac{||e_U^i||_{R^{-1}}}{||e_D^i||_{R^{-1}}} = \frac{\sqrt{(e_U^i)^t * R^{-1} * (e_U^i)}}{\sqrt{(e_D^i)^t * R^{-1} * (e_D^i)}} \tag{3.13}$$

Em (BENEDITO, 2011) foi demonstrado também que o numerador e o denominador da equação (3.13) pode ser simplificado como nas equações

$$||e_U^i||_{R^{-1}} = b * \sigma_i^{-1} * \sqrt{K_i} \tag{3.14}$$

$$||e_D^i||_{R^{-1}} = b * \sigma_i^{-1} * \sqrt{1 - K_i} \tag{3.15}$$

onde b se trata da magnitude do erro da medida em questão. Consequentemente:

$$UI_i = \frac{b\,\sigma_i^{-1}\sqrt{K_{ii}}}{b\,\sigma_i^{-1}\sqrt{(1 - K_{ii})}} = \frac{\sqrt{K_{ii}}}{\sqrt{(1 - K_{ii})}} \tag{3.16}$$

A partir do que foi exposto até aqui é possível calcular uma estimativa do erro total, nomeado erro composto, em uma medida em função de seu *UI*, como proposto em Benedito *et al.* (2014):

$$ec_i = r_i \cdot \sqrt{(UI_i^2 + 1)} \tag{3.17}$$

Ou alternativamente, utilizando o vetor de resíduos normalizados, pode-se escrever o erro em sigmas da medida em função do resíduo normalizado:

$$ec_{\sigma_i} = r_i^N \cdot \sqrt{(UI_i^2 + 1)} \tag{3.18}$$

Com o objetivo de corrigir medidas portadoras de EGs, em Benedito (2011) foi proposto um algoritmo fazendo uso do erro composto:

- **Passo 1:** Determine o valor estimado das variáveis de estado ($\hat{x}$), através da solução iterativa da equação normal;

- **Passo 2:** Calcule as matrizes K e S considerando $\hat{x}$, ou calcule apenas os elementos da diagonal principal dessas matrizes;
- **Passo 3:** Calcule o resíduo normalizado r_i^N para cada medida i e o índice *UI*.
- **Passo 4:** Calcular o erro composto utilizando os valores de resíduo normalizado e *UI* do passo 3 para cada medida i utilizando a equação (3.18):
- **Passo 5:** Para a medida com o maior resíduo normalizado em módulo, verifique se o módulo de seu erro composto em desvio padrão é maior que o certo limiar de detecção pré-estabelecido β. Caso seja inferior ao limiar o processo de ESSEP é encerrado, caso contrário vá para o próximo passo:
- **Passo 6:** Corrija a medida i identificada como portadora de EG conforme esquação a seguir e retorne ao **Passo 1**:

$$z_i^{corrigido} = z_i - e_{\sigma_i} \cdot \sigma_i \tag{3.19}$$

3.2 Contextualização de ataques FDI

Hodiernamente, há uma crescente preocupação na literatura com a vulnerabilidade da rede elétrica a ataques de cibersegurança de diversos tipos (SUN; HAHN; LIU, 2018). Entre os possíveis meios de intervir no funcionamento de SEPs se destacam os ataques *FDI*, que consistem na modificação maliciosa do vetor de medidas. Esses ataques podem ser conduzidos tanto no nível físico (sensor, RTU) quanto no nível lógico (alteração de pacotes de comunicação), e têm como objetivo alterar decisões operativas sem levantar suspeitas.

Usualmente, o procedimento de EESEP padrão descrito anteriormente detectaria alterações nos valores das medidas e minimizaria seu impacto. Entretanto, em Liu, Ning e Reiter (2011) foi demonstrado como construir vetores de ataque não observáveis pelo procedimento tradicional de validação baseado em resíduos. Trabalhos subsequentes (KOSUT *et al.*, 2010) analisaram o impacto desses ataques, inclusive em processos de precificação em mercados de energia, onde o ataque poderia ser utilizado para aumentar o lucro pelos responsáveis por determinados geradores ao alterar a precificação em sua região. Outrossim, ataques FDI poderiam ocasionar em danos nas linhas de transmissão e transformadores ao ocultar a sua verdadeira condição de operação e induzir o operador a tomar decisões indevidas no controle do sistema.

Diversas nomenclaturas equivalentes aparecem na literatura: *load redistribution attacks*, *malicious data attacks*, *data integrity attacks*, *stealthy deception attacks*, entre outras.

Independentemente da nomenclatura, esses ataques requerem o conhecimento da matriz H, consequentemente, conhecimento dos parâmetros das linhas que compõem a

rede, que por sua vez é multiplicada por um vetor c, que define a alteração desejada nas variáveis de estado da rede, com o objetivo de encontrar o vetor das alterações necessárias no vetor de medida (a).

3.2.1 Viabilidade de Ataques FDI

Grande parte da literatura inicial para tratamento de ataque *FDI* assumiu estimadores DC e a necessidade de conhecimento completo da matriz Jacobiana. Para estimadores AC, um ataque não detectável requer, em princípio, conhecimento mais detalhado das variáveis de estado e dos parâmetros da rede. Quando essas informações não estão disponíveis, o ataque ainda pode ser formulado de maneira aproximada usando o modelo DC, porém com limitações em sua magnitude (HUG; GIAMPAPA, 2012). Em Zhang *et al.* (2016), demonstrou-se que ataques pequenos em estimadores AC podem permanecer indetectáveis quando construídos com conhecimento local da rede. Como adquirir informações completas é difícil, ataques realistas tendem a ser baseados em medições locais e histórico de operação (RAHMAN; MOHSENIAN-RAD, 2012).

3.2.2 Métricas de vulnerabilidade

Em Sandberg, Teixeira e Johansson (2010), foram propostas as métricas α_i (mínima esparsidade) e β_i (mínima magnitude), que quantificam a dificuldade de adulterar uma medida mantendo o ataque oculto. Ambas as métricas foram definidas no contexto de modelos lineares, nos quais o vetor de medidas inclui apenas grandezas de potência ativa.

A métrica α_i mede quantas medidas precisam ser adulteradas para mascarar uma alteração na medida i, enquanto β_i quantifica a magnitude mínima necessária da adulteração.

3.2.3 Defesa contra ataques

Algumas estratégias propõem a proteção direta de medidas críticas (BI; ZHANG, 2014; KIM; POOR, 2011), porém não há metodologia prática que permita garantir essa proteção de forma sistemática em SEPs reais.

Métodos baseados em aprendizado de máquina também foram explorados (ALMASABI *et al.*, 2024; ALMASABI *et al.*, 2021; SONG *et al.*, 2019; MOUDOUD *et al.*, 2022), mas apresentam limitações:

- dependência de PMUs,
- necessidade de treinamento específico por SEP,
- incapacidade de identificar quais medidas foram adulteradas,
- dificuldade de generalização.

Métodos baseados na alteração dinâmica dos parâmetros da rede, embora promissores, exigem infraestrutura FACTS e podem comprometer a operação em tempo real (LIU *et al.*, 2018; DENG *et al.*, 2017; ZHANG *et al.*, 2022).

Diante dessas limitações, permanece o desafio de desenvolver métodos robustos e escaláveis de detecção e mitigação.

3.3 Formulação Matemática

Para estimadores lineares, define-se o vetor de ataque:

$$a = Hc, \tag{3.20}$$

onde, o vetor c corresponde a alteração dessejada no vetor das variáveis de estado. Em seguida, considere que o atacante injeta o vetor a nas medições e que a matriz E é a matriz que quando multiplicada pelo vetor de medidas resulta no vetor das variáveis de estado utilizando o estimador linear, a chamada matriz inversa da jacobiana :

$$\hat{x}_a = Ez_a = E(z + a) = Ez + EHc = \hat{x} + c \tag{3.21}$$

Para verificar a detectabilidade do ataque, avalia-se o módulo do resíduo das medidas. Então, devido à linearidade desse tipo de estimadores não se torna possível perceber uma alteração no módulo do resíduo:

$$\|r_a\|_2 = \|z_a - H\hat{x}_a\|_2 = \|(z+a) - H(\hat{x}+c)\|_2 = \|(z - H\hat{x}) + (a - Hc)\|_2 = \|z - H\hat{x}\|_2 = \|r\|_2 \tag{3.22}$$

Tal fato, compromete o funcionamento de testes tradicionais para identificar EGs que utilizam de variações no resíduo para detectar os erros. Esse tipo de ataque também pode ser generalizado para estimadores não lineares utilizando a seguinte relação entre o a e o vetor c.

$$a = h(\hat{x} + c) - h(\hat{x}) \tag{3.23}$$

O que de maneira análoga leva ao módulo do vetor dos resíduos ser igual antes e depois do ataque:

$$\|r_a\|_2 = \|z_a - h(\hat{x}_a)\|_2 = \|(z + a) - h(\hat{x} + c)\|_2 = \|z - h(\hat{x})\|_2 = \|r\|_2 \tag{3.24}$$

3.4 Considerações Finais

O desenvolvimento apresentado neste capítulo fornece as bases teóricas necessárias para avaliar a vulnerabilidade do processo de EESEP diante de EGs e ataques *FDI*. O

índice UI e o erro composto oferecem meios adicionais de análise que complementam o teste tradicional baseado em resíduos.

Esses conceitos permitem explorar, no capítulo seguinte, cenários de simulação que evidenciam tanto as limitações do estimador WLS quanto o potencial das métricas adicionais na identificação de medidas críticas e na detecção de ataques cibernéticos.

4 SIMULAÇÕES COMPUTACIONAIS E ANÁLISE DOS RESULTADOS

Neste capítulo, detalha-se a metodologia utilizada nos testes numéricos e apresentam-se os resultados obtidos, de modo a comparar diferentes formulações do processo de EESEP e investigar os efeitos de ataques *FDI* no sistema IEEE 14 barras, ilustrado na Figura 1. Os cenários de simulação foram organizados em três grupos de casos, com características semelhantes, para facilitar a análise comparativa. Na figura 1 está exposto um diagrama representativo da rede IEEE 14 barras, onde as medições de tensão são indicadas com a letra V seguida pelo número do barramento, as posições das medições de fluxo de potência ativa são indicadas por triângulos e as posições das medições de potências reativas são indicadas por quadrados.

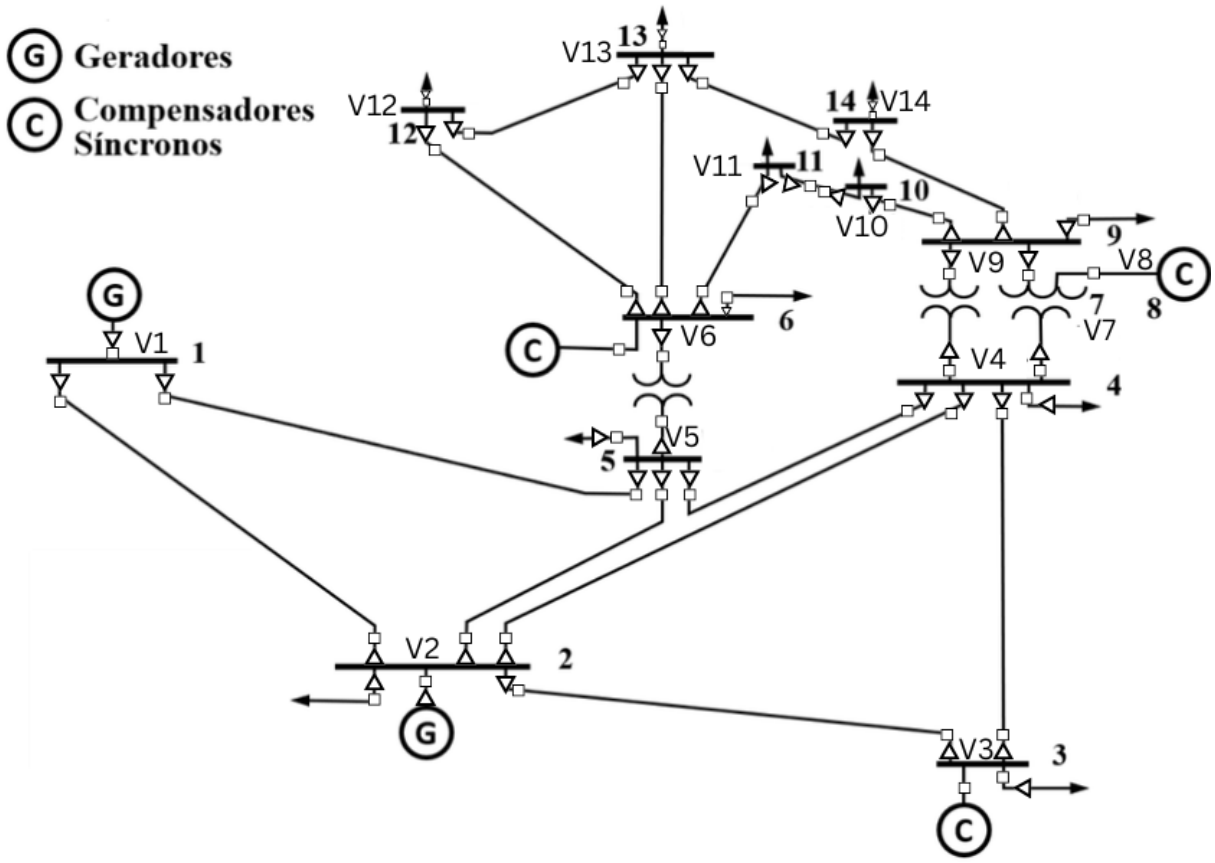


Figura 1 – Sistema IEEE 14 barras com as respectivas posições onde as medições são realizadas.

Fonte: Elaboração Própria. Esquemático original do IEEE 14 barras oriundo de Zellagui e Boudour (2014).

4.1 Metodologia Utilizada

Ao longo deste capítulo são apresentados os resultados do processo de estimação utilizando o estimador *WLS* não linear, associado a duas estratégias de processamento de EGs: (i) a eliminação de medidas com base no teste do maior resíduo normalizado (teste rN) e (ii) o método de correção de medidas a partir do erro composto (método EC).

Para comparar objetivamente a performance de diferentes métodos de detecção e tratamento de EGs, é necessário definir uma métrica de acurácia dos estimadores. Uma das métricas mais utilizadas nesse contexto é o erro médio absoluto (EMA), definido para uma variável de estado por:

$$EMA_i = \frac{1}{n_A} \sum_{j=1}^{n_A} \left| x_i^{Ref} - \hat{x}_{i,j} \right| \tag{4.1}$$

em que:

- n_A — número de amostras;
- x_i^{Ref} — valor de referência (considerado verdadeiro obtido a partir de um estudo de fluxo de potência) da variável de estado x_i;
- $\hat{x}_{i,j}$ — corresponde à i-ésima variável de estado estimada na j-ésima amostra.

Nos casos em que há apenas uma amostra, o EMA reduz-se ao desvio absoluto entre o valor estimado e o valor de referência da magnitude de tensão ou do ângulo em um determinado barramento.

Torna-se necessário, ainda, explicitar o processo de inserção de ruído e de EGs nos valores das medidas utilizadas neste trabalho. As medidas contaminadas com EGs são obtidas a partir da seguinte expressão:

$$Zeg[i] = Zverdadeiro[i] + 10 * \sigma[i] \tag{4.2}$$

onde:

- Zeg - vetor das medidas contaminado com erros grosseiros.
- i - índice da medida contaminada no vetor.
- Zverdadeiro - vetor dos valores verdadeiros das medidas (ou de referênciqa obtidos através de umm fluxo de potência).
- σ - vetor dos desvios padrões das medidas.

Para simulação das medidas σ_i de cada medida é calculado através da seguinte equação:

$$\sigma[i] = \frac{\text{Precisão} \cdot |Zverdadeiro[i]|}{3} \tag{4.3}$$

Optou-se por fixar a magnitude e o sinal do EG em 10σ para facilitar a comparação entre diferentes amostras, garantindo que todas apresentem o mesmo desvio introduzido nas medidas selecionadas.

Nos casos em que ocorre a presença de um ataque *FDI*, o vetor de ataque a é calculado a partir de um vetor c que representa uma alteração nas variáveis de estado (magnitude e ângulo de tensão) de apenas um barramento, de forma análoga ao exemplo didático apresentado no capítulo de embasamento teórico. Para representar um ataque *FDI* de grande impacto, adotou-se c correspondente a uma alteração de 100σ nas variáveis de estado do barramento atacado. Foram registrados os vetores a obtidos, bem como seus valores em número de desvios padrão, e os *outliers* associados diretamente ao *FDI* foram removidos dos gráficos de boxplot.

Ademais, o procedimento utilizado para obter os valores de referência das medidas consiste no seguinte: primeiro, é utilizada a biblioteca MATPOWER do MATLAB para realizar o fluxo de potência com o método Newton-Raphson para a rede IEEE 14 barras, em seguida, com as tensões complexas obtidas pelo fluxo de potência pode-se gerar um vetor com todas as medidas do sistemas. Depois, esse vetor de medidas alimenta um estimador de estado utilizando uma matriz de ponderação identidade, cujo equacionamento matemático é equivalente ao fluxo de potência baseado no Newton-Raphson utilizado anteriormente, para então gerar a partir do estado obtido pelo estimador o vetor de medidas de referência. Esse procedimento é utilizado para retirar possíveis erros de precisão dos cálculos ou pequenas diferenças nos parâmetros da rede, que podem levar a pequenas variações nos resultados obtidos usando o estimador de estado e o fluxo de potência.

4.2 Casos sem ruído

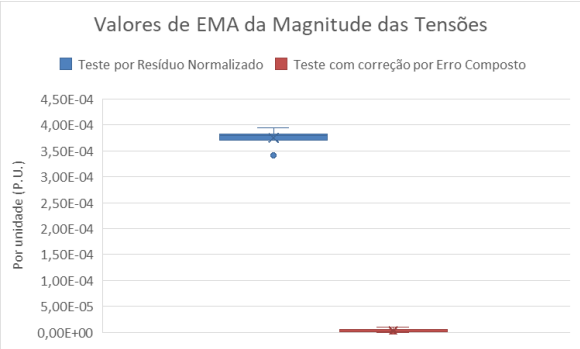
Com a metodologia descrita, foram obtidos os valores de referência das medidas do sistema IEEE 14 barras, que serviram de base para a inserção de ruído e de EGs em todos os casos estudados. Esses valores encontram-se listados no Apêndice 1

4.2.1 Caso 1 - Apenas Erros Grosseiros

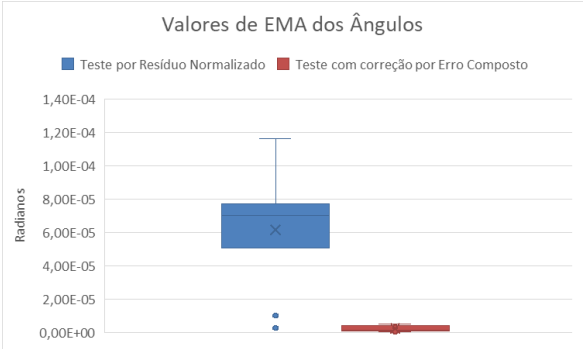
Inicialmente, foram selecionadas duas medidas com valores de *UI* bem distintos, com o objetivo de avaliar a influência de EGs e de ataques *FDI* nessas medidas. A medida de baixo *UI* escolhida foi a magnitude de tensão no barramento 13 (V13, com *UI* igual a

0,142924), enquanto a medida de alto *UI* foi a injeção de potência ativa no barramento 5 (P5, com *UI* igual a 5,548558).

Ao aplicar o teste do maior resíduo normalizado, apenas o EG em V13 foi identificado. Já o critério baseado no erro composto conseguiu detectar EGs em ambas as medidas. Como esperado, a correção via erro composto melhorou a acurácia das estimativas obtidas. Nas Figuras 2.a e 2.b são apresentados os valores de EMA para cada um das técnicas de processamento de EGs consideradas.



(a) Gráfico Boxplot do EMA das tensões não afetadas diretamente pelo *FDI*.



(b) Gráfico Boxplot do EMA dos ângulos não afetados diretamente pelo *FDI*.

Figura 2 – Resultados da estimação de estado utilizando a eliminação de medidas com o teste de resíduo normalizado e a correção por erro composto para o Caso 1.

Fonte: Elaboração própria.

4.2.2 Caso 2 - Apenas Ataques FDI

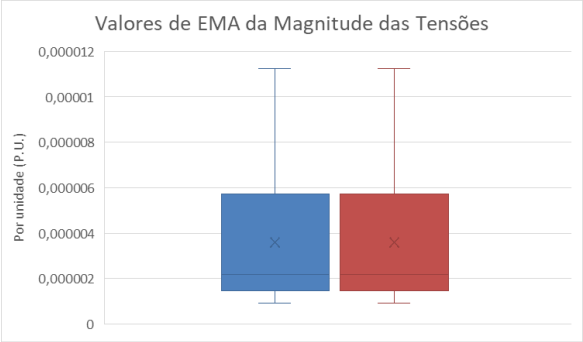
Em seguida, foram realizados testes para avaliar a acurácia do processo de estimação na presença de ataques *FDI* sem ruído adicional. Os ataques foram construídos de modo que, no Caso 2.a, nem V13 nem P5 fossem diretamente afetadas; no Caso 2.b, apenas V13 fosse alterada; e, no Caso 2.c, apenas P5 sofresse o ataque.

Como os ataques foram projetados para provocar alterações de grande magnitude no barramento alvo, os valores de EMA das variáveis diretamente atacadas foram descritos no texto e omitidos dos gráficos de boxplot. A análise mostra que, partindo de um estimador não linear e de um plano de medidas já contendo dois EGs, é possível construir um ataque *FDI* bem-sucedido. Além disso, o critério baseado no erro composto não apresentou desempenho superior ao teste do resíduo normalizado na detecção das medidas afetadas por um *FDI*.

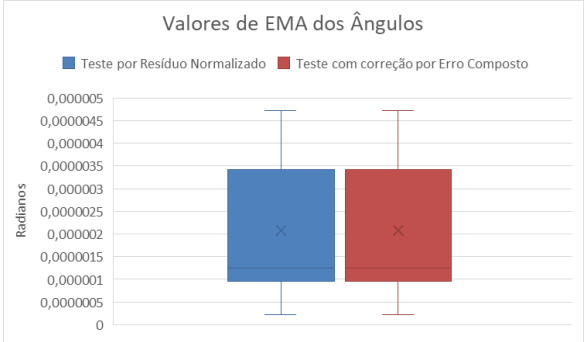
4.2.2.1 Caso 2.a

Nesse caso, o teste por resíduo normalizado obteve um EMA de 0,021057495 p.u. na tensão do barramento atacado e 0,050805799 radianos em seu ângulo.

Como nenhuma medida contaminada pelo *FDI* foi detectada por nenhum dos critérios, não houve diferença na acurácia obtida com o teste rN e com o método EC. Nas Figuras 3.a e 3.b são apresentados os valores de EMA para cada um das técnicas de processamento de EGs consideradas. O barramento alvo do ataque foi o barramento 11.



(a) Gráfico Boxplot do EMA das tensões.



(b) Gráfico Boxplot do EMA dos ângulos.

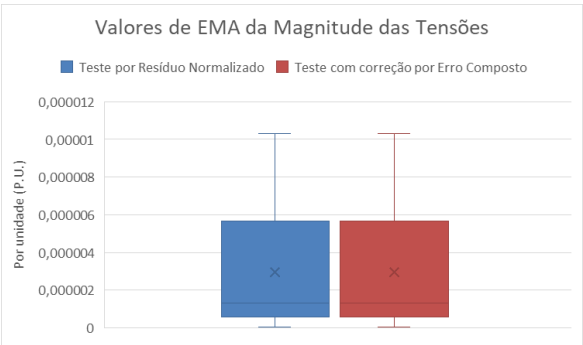
Figura 3 – Resultados da estimação de estado utilizando eliminação por resíduo normalizado e a correção das medidas com o erro composto para o Caso 2.a .

Fonte: Elaboração própria.

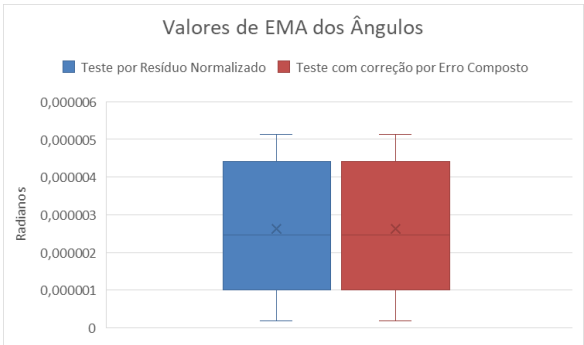
4.2.2.2 Caso 2.b

Nesse caso, o teste por resíduo normalizado obteve um EMA de 0,023308703 p.u. na tensão do barramento atacado e 0,051711711 radianos.

Novamente, nenhuma medida afetada pelo *FDI* foi detectada, resultando em desempenho equivalente entre o teste rN e o método EC. Nas Figuras 4.a e 4.b são apresentados os valores de EMA para cada um das técnicas de processamento de EGs consideradas. O barramento alvo do ataque foi o barramento 13.



(a) Gráfico Boxplot do EMA das tensões.



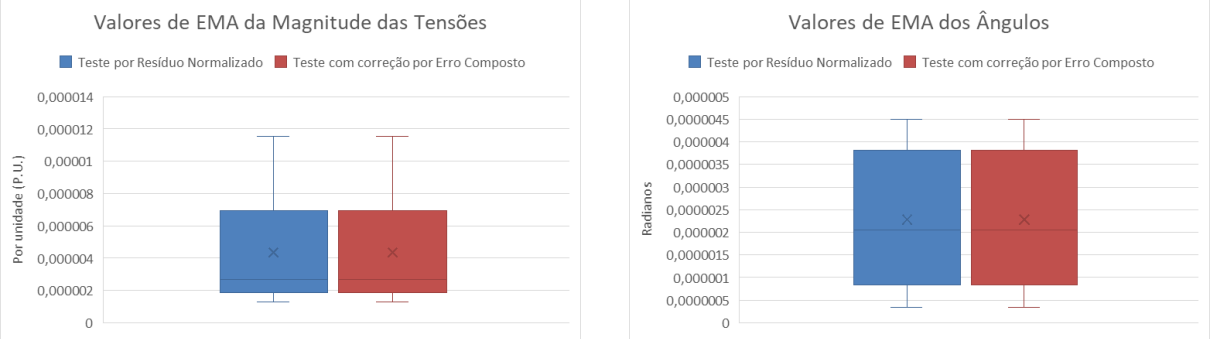
(b) Gráfico Boxplot do EMA dos ângulos.

Figura 4 – Resultados da estimação de estado utilizando eliminação por resíduo normalizado e a correção das medidas com o erro composto para o Caso 2.b .

Fonte: Elaboração própria.

4.2.2.3 Caso 2.c

Nesse caso, o teste por resíduo normalizado obteve um EMA de 0,02010912 p.u. na tensão do barramento atacado e 0,049555868 radianos em seu ângulo. Tal como nos casos anteriores, a ausência de detecção das medidas sob ataque levou a resultados idênticos para os dois critérios. O barramento alvo do ataque foi o barramento 4.



(a) Gráfico Boxplot do EMA das tensões. (b) Gráfico Boxplot do EMA dos ângulos.

Figura 5 – Resultados da estimação de estado utilizando eliminação por resíduo normalizado e a correção das medidas com o erro composto para o Caso 2.c .

Fonte: Elaboração própria.

4.2.3 Caso 3 - Ataques FDI com Erros Grosseiros

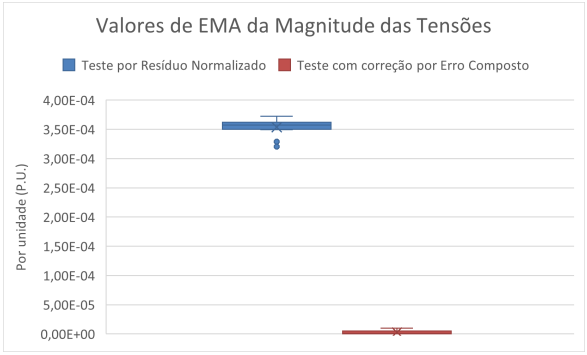
Nos casos do Grupo 3 foram combinados os ataques *FDI* com os EGs do Caso 1. A construção dos ataques segue a mesma lógica do Grupo 2: no Caso 3.a, o *FDI* não atua sobre V13 nem P5; no Caso 3.b, o *FDI* atua sobre V13; e no Caso 3.c, sobre P5.

Nos gráficos de EMA, as variáveis diretamente afetadas pelos ataques foram omitidas.

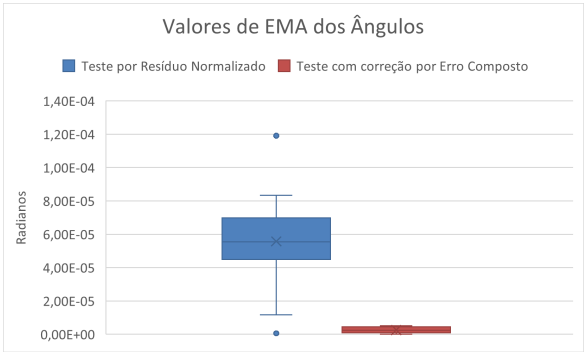
4.2.3.1 Caso 3.a

Para esse caso, observou-se que, exceto pela tensão e pelo ângulo do barramento atacado pelo *FDI*, os resultados foram muito semelhantes aos do Caso 1. Isso indica que o método EC manteve a capacidade de corrigir as duas medidas com EGs.

Os valores de EMA no barramento atacado pelo *FDI* foram de 0,0224382 p.u. para a tensão e 0,051675882 radianos para o ângulo com o teste rN, e de 0,022072698 p.u. e 0,051573256 radianos com o método EC. As medidas P5 e V13 (não diretamente associadas ao *FDI*) foram detectadas como portadoras de EG pelo erro composto, mas o teste do maior resíduo normalizado foi capaz de detectar apenas a medidas V13. Nas Figuras 6.a e 6.b são apresentados os valores de EMA para cada um das técnicas de processamento de EGs consideradas. O barramento alvo do ataque foi o barramento 11.



(a) Gráfico Boxplot do EMA das tensões.



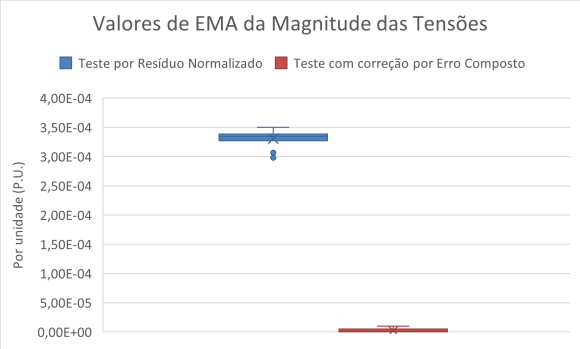
(b) Gráfico Boxplot do EMA dos ângulos.

Figura 6 – Resultados da estimação de estado utilizando a eliminação por resíduo normalizado e a correção das medidas com o erro composto para o Caso 3.a .

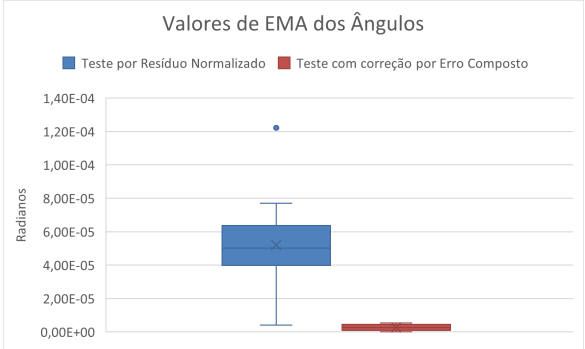
Fonte: Elaboração própria.

4.2.3.2 Caso 3.b

Observando os resultados desse caso, é possível perceber que com exceção da tensão e ângulo no barramento afetado pelo *FDI* os resultados foram bastante semelhantes ao caso 1. Ou seja, a correção por erro composto conseguiu corrigir as 2 medidas afetadas pelos erros grosseiros. Mas, os valores de EMA no barramento atacado pelo *FDI* foram respectivamente de 0,050545516 P.U. para tensão e 0,052279339 radianos para o ângulo ao utilizar o teste por resíduo normalizado. Além disso, utilizando a correção por erro composto os valores de EMA foram de 0,050188695 P.U. para tensão e 0,052181182 radianos, consequentemente ambos os métodos foram incapazes de detectar as medidas portadoras de *FDI*. Outrossim, nesse caso a medida V13 foi simultaneamente afetada por *FDIs* e EGs, mas foi detectada com sucesso por ambos critérios de detecção, o que pode implicar que a presença do erro grosseiro não prejudicou o suficiente a criação do *FDI*. Ademais, a medida P5, que possui maior valor de *UI*, ainda foi corretamente detectada pelo critério do erro composto. Nas Figuras 7.a e 7.b são apresentados os valores de EMA para cada um das técnicas de processamento de EGs consideradas. O barramento alvo do ataque foi o barramento 13.



(a) Gráfico Boxplot do EMA das tensões.



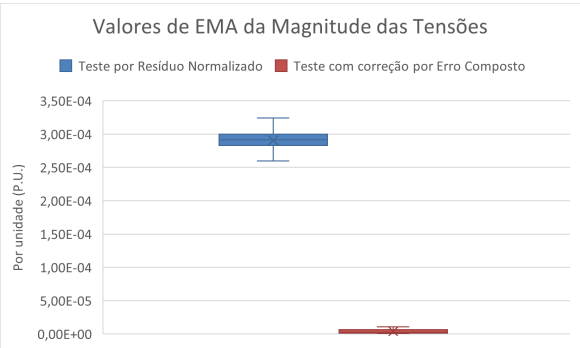
(b) Gráfico Boxplot do EMA dos ângulos.

Figura 7 – Resultados da estimação de estado utilizando a eliminação por resíduo normalizado e a correção das medidas com o erro composto para o Caso 3.b .

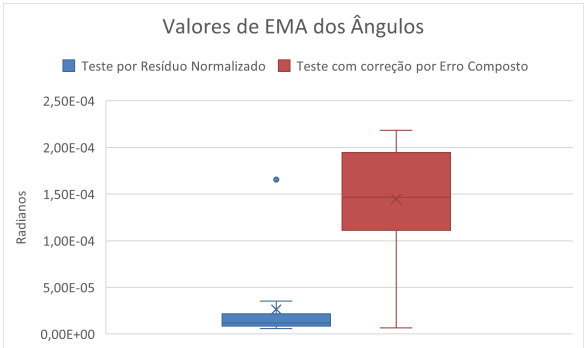
Fonte: Elaboração própria.

4.2.3.3 Caso 3.c

Esse cenário se distingue dos demais por apresentar uma acurácia inferior da correção por erro composto. Os valores de EMA no barramento atacado pelo *FDI* foram respectivamente de P.U. para tensão e 0,051675882 radianos para o ângulo ao utilizar o teste por resíduo normalizado. Além disso, utilizando a correção por erro composto os valores de EMA foram de 0,020103759 P.U. para tensão e 0,049556242 radianos. A correção por erro composto, ao utilizar o resíduo da medida para realizar a correção, é sensível à presença de *FDIs* no vetor das medidas. Assim, vemos que nesse caso houve uma piora na performance da correção do erro composto devido ao cálculo errôneo do erro composto para a medida V13 que foi detectada apenas pelo critério do erro composto. Mas, a medida P5 ainda foi corretamente detectada por ambos os métodos. Nas Figuras 8.a e 8.b são apresentados os valores de EMA para cada um das técnicas de processamento de EGs consideradas. O barramento alvo do ataque foi o barramento 4.



(a) Gráfico Boxplot do EMA das tensões.



(b) Gráfico Boxplot do EMA dos ângulos.

Figura 8 – Resultados da estimação de estado utilizando a eliminação por resíduo normalizado e a correção das medidas com o erro composto para o Caso 3.c .

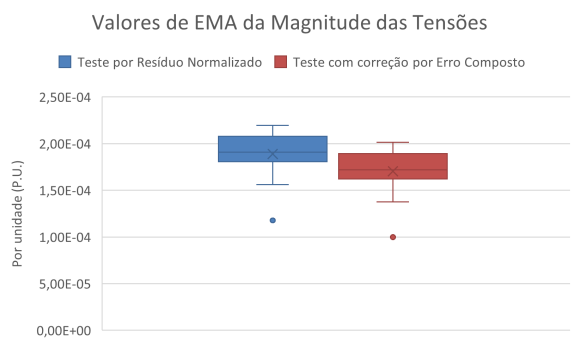
Fonte: Elaboração própria.

4.3 Casos com ruído

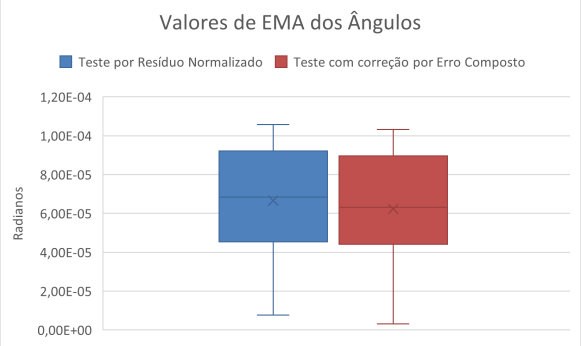
Para avaliar a influência do ruído nas medidas utilizadas na construção dos ataques *FDI*, os casos anteriores foram repetidos considerando ruído gaussiano nas medidas.

4.3.1 Caso 4 - Erros Grosseiros com ruído

Ao adicionar ruído no plano de medidas, nota-se uma redução notável da acurácia do método de correção por erro composto. Nesse exemplo, a medida P5 não conseguiu mais ser detectada pelo critério do erro composto, levando à redução na acurácia. Entretanto, a correção da medida V13 explica a acurácia superior do erro composto que ainda pode ser notada. Nas Figuras 9 são apresentados os valores de EMA para cada um das técnicas de processamento de EGs consideradas



(a) Gráfico Boxplot do EMA das tensões.



(b) Gráfico Boxplot do EMA dos ângulos.

Figura 9 – Resultados da estimação de estado utilizando eliminação por resíduo normalizado e a correção das medidas com o erro composto para o Caso 4 .

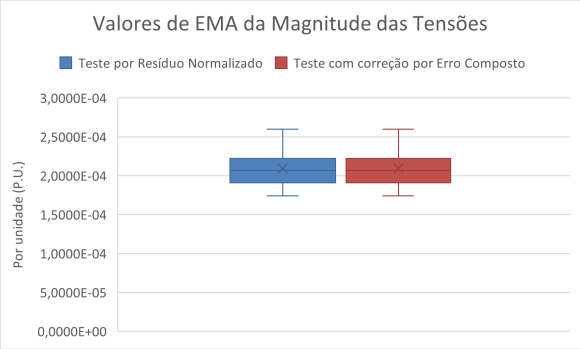
Fonte: Elaboração própria.

4.3.2 Caso 5 - Ataques FDI com ruído

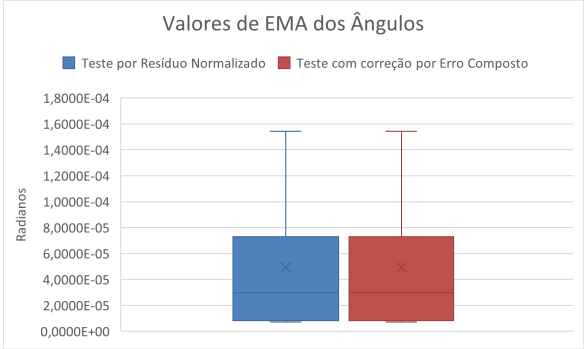
A inclusão de ruído nas medidas a serem contaminadas pelo *FDI* não foi capaz de facilitar a detecção das medidas influenciadas pelo *FDI*. Nos 3 casos expostos aqui ainda não foi possível a detecção do *FDI* e, consequentemente, a acurácia foi a mesma utilizando os 2 critérios de detecção de erros grosseiros. A inclusão do ruído, conforme o esperado, também propiciou uma redução da acurácia no processo de ESSEP.

4.3.2.1 Caso 5.a

Nesse caso, o teste por resíduo normalizado obteve um EMA de 0,021897181 P.U. na tensão no barramento atacado e 0,051711711 radianos. Como não foram detectadas as medidas contaminadas pelo *FDI* não houve diferença na acurácia da estimação. Nas Figuras 10.a e 10.b são apresentados os valores de EMA para cada um das técnicas de processamento de EGs consideradas. O barramento alvo do ataque foi o barramento 11.



(a) Gráfico Boxplot do EMA das tensões.



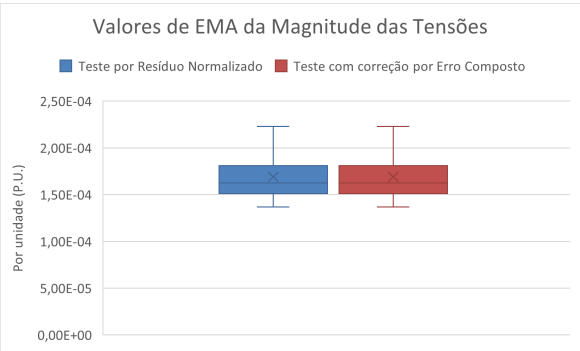
(b) Gráfico Boxplot do EMA dos ângulos.

Figura 10 – Resultados da estimação de estado utilizando eliminação por resíduo normalizado e a correção das medidas com o erro composto para o Caso 5.a .

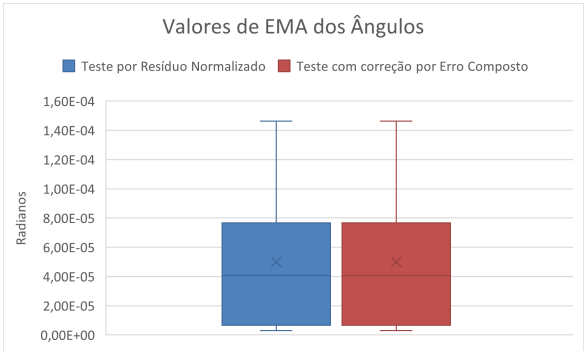
Fonte: Elaboração própria.

4.3.2.2 Caso 5.b

Nesse caso, o teste por resíduo normalizado obteve um EMA de 0,050058887 P.U. na tensão no barramento atacado e 0,052186259 radianos. Como não foram detectadas as medidas contaminadas pelo *FDI* não houve diferença na acurácia da estimação. Nas Figuras 11.a e 11.b são apresentados os valores de EMA para cada um das técnicas de processamento de EGs consideradas. O barramento alvo do ataque foi o barramento 13.



(a) Gráfico Boxplot do EMA das tensões.



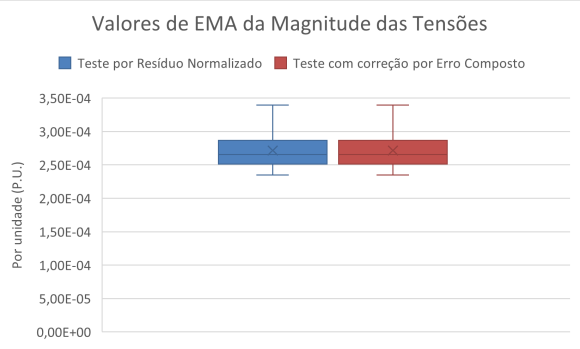
(b) Gráfico Boxplot do EMA dos ângulos.

Figura 11 – Resultados da estimação de estado utilizando eliminação por resíduo normalizado e a correção das medidas com o erro composto para o Caso 5.b .

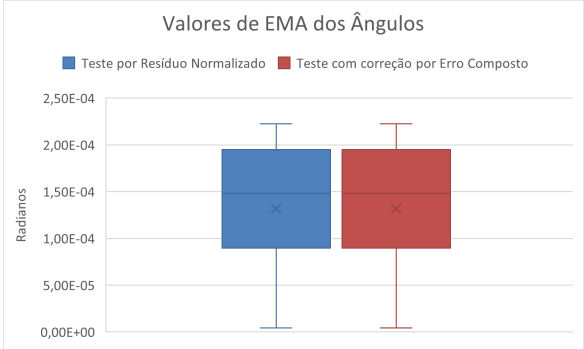
Fonte: Elaboração própria.

4.3.2.3 Caso 5.c

Nesse caso, o teste por resíduo normalizado obteve um EMA de 0,019875883 P.U. na tensão no barramento atacado e 0,049648773 radianos. Como não foram detectadas as medidas contaminadas pelo *FDI* não houve diferença na acurácia da estimação. Nas Figuras 12.a e 12.b são apresentados os valores de EMA para cada um das técnicas de processamento de EGs consideradas. O barramento alvo do ataque foi o barramento 4.



(a) Gráfico Boxplot do EMA das tensões.



(b) Gráfico Boxplot do EMA dos ângulos.

Figura 12 – Resultados da estimação de estado utilizando eliminação por resíduo normalizado e a correção das medidas com o erro composto para o Caso 5.c .

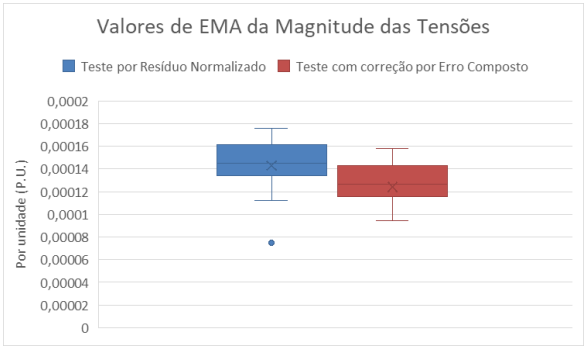
Fonte: Elaboração própria.

4.3.3 Caso 6 - Ataques FDI com Erros Grosseiros e ruído

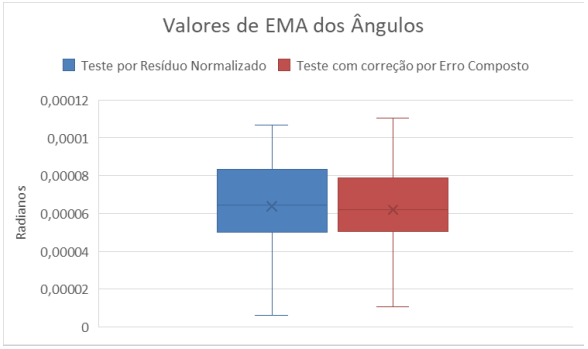
A seguir, foram realizados 3 testes com ocorrência de EGs, ruído e presença de ataques de *FDI*. Os 3 casos a seguir diferem em quais medidas foram afetadas pelo *FDI* similarmente ao que foi feito nos testes anteriores. Entretanto, em todos os casos apenas as medida V13 foi corretamente detectada.

4.3.3.1 Caso 6.a

Para o caso 6.a, como nos demais casos, não houve diferença significativa no valor dos EMAs da tensão e ângulo do barramento afetado, com o resultado de 0,022258687 P.U. e 0,000106862 radianos utilizando o teste do resíduo normalizado, e 0,022239481 P.U. e 0,051673683 radianos utilizando a correção por erro composto. Como pode ser visto na figura 13, o resultado do erro composto é ainda consideravelmente melhor. Tal fato, é coerente com o esperado pois a correção com erro composto ainda detectou a medida V13. Esse resultado, mostra novamente que a correção por erro composto possui boa acurácia na ausência de *FDIs* na medida. Novamente, em ambos os casos apenas a medida V13 foi detectada. Nas Figuras 13.a e 13.b são apresentados os valores de EMA para cada um das técnicas de processamento de EGs consideradas. O barramento alvo do ataque foi o barramento 11.



(a) Gráfico Boxplot do EMA das tensões.



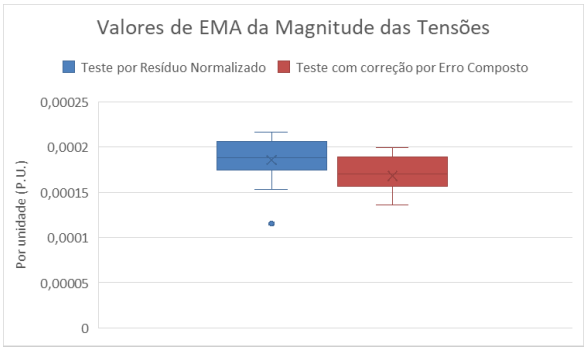
(b) Gráfico Boxplot do EMA dos ângulos.

Figura 13 – Resultados da estimação de estado utilizando eliminação por resíduo normalizado e a correção das medidas com o erro composto para o Caso 6.a .

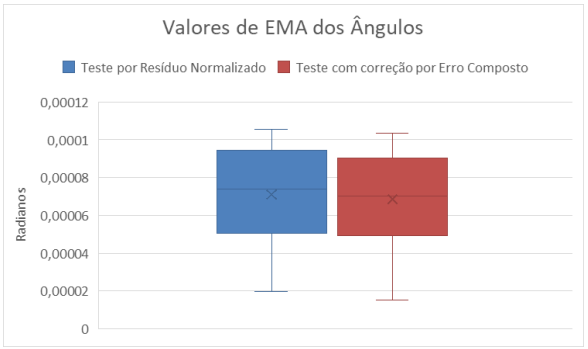
Fonte: Elaboração própria.

4.3.3.2 Caso 6.b

Os valores de EMA no barramento atacado pelo *FDI* foram respectivamente de 0,050545516 P.U. para tensão e 0,052279339 radianos para o ângulo ao utilizar o teste por resíduo normalizado. Além disso, utilizando a correção por erro composto os valores de EMA foram de 0,050188695 P.U. para tensão e 0,052181182 radianos. O resultado obtido pelo critério do erro composto ainda apresentou uma acurácia superior devido a correção da medida. Nas Figuras 14.a e 14.b são apresentados os valores de EMA para cada um das técnicas de processamento de EGs consideradas. O barramento alvo do ataque foi o barramento 13.



(a) Gráfico Boxplot do EMA das tensões.



(b) Gráfico Boxplot do EMA dos ângulos.

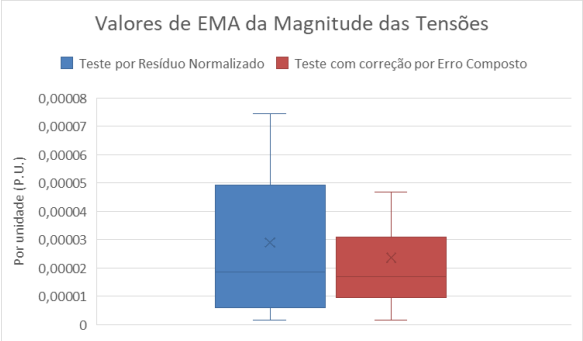
Figura 14 – Resultados da estimação de estado utilizando eliminação por resíduo normalizado e a correção das medidas com o erro composto para o Caso 6.b .

Fonte: Elaboração própria.

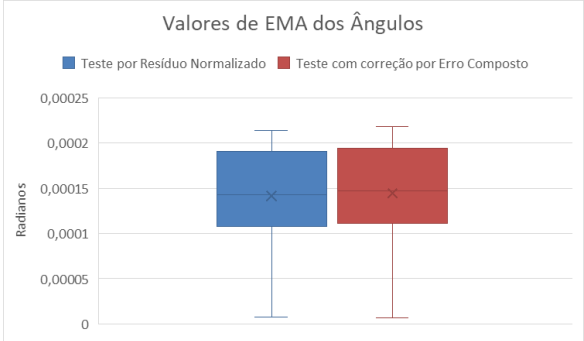
4.3.3.3 Caso 6.c

Os valores de EMA no barramento atacado pelo *FDI* foram respectivamente de 0,020169956 P.U. para tensão e 0,049610858 radianos para o ângulo ao utilizar o teste por resíduo normalizado. Além disso, utilizando a correção por erro composto os valores de

EMA foram de 0,020149491 P.U. para tensão e 0,049610858 radianos. Nesse resultado, observa-se uma redução na acurácia utilizando o critério do erro composto, o que é coerente com a hipótese anteriormente apresentada que o calculo do erro composto é prejudicado na presença de *FDIs* nas medidas. Nas Figuras 15.a e 15.b são apresentados os valores de EMA para cada um das técnicas de processamento de EGs consideradas. O barramento alvo do ataque foi o barramento 4.



(a) Gráfico Boxplot do EMA das tensões.



(b) Gráfico Boxplot do EMA dos ângulos.

Figura 15 – Resultados da estimação de estado utilizando eliminação por resíduo normalizado e a correção das medidas com o erro composto para o Caso 6.c .

Fonte: Elaboração própria.

4.4 Casos com aumento no número de EGs

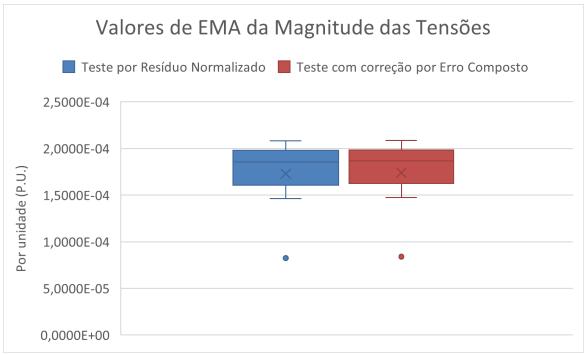
Os casos deste grupo foram construídos para avaliar o impacto de um número crescente de EGs simultaneamente à presença de medidas sob ataque *FDI*. O vetor de medidas de referência é o mesmo do Caso 6.a, sendo apenas aumentada a quantidade de medidas contaminadas por EGs.

Os resultados indicam que, mesmo com a remoção de um número significativo de medidas, os ataques *FDI* mantêm alta capacidade de permanecer ocultos. Uma explicação plausível é a baixa esparsidade do vetor de ataque a, que em diversos cenários afeta cerca de 21 medidas, tornando difícil expor o ataque sem remover um conjunto muito grande de medições.

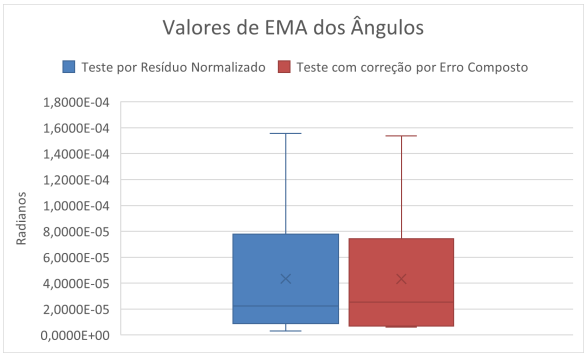
4.4.0.1 Caso com 3 EGs

Para a criação do vetor de medidas desse caso, foi adicionado um erro grosseiro na injeção de potência reativa no barramento 5 (Q5). Os valores de EMA para a tensão e ângulo com a eliminação por resíduo normalizado são, respectivamente, de 0,0234762113 P.U. e 0,0517307376 radianos. Já utilizando o erro composto, o EMA da tensão e do ângulo são, respectivamente, de 0,0234779339 P.U. e 0,0517346500 radianos. Ademais, apenas as medidas V13 e Q5 foram detectadas em ambos os casos como portadoras de

erros grosseiros. Nas Figuras 16.a e 16.b são apresentados os valores de EMA para cada um das técnicas de processamento de EGs consideradas.



(a) Gráfico Boxplot do EMA das tensões com 3 erros grosseiros.



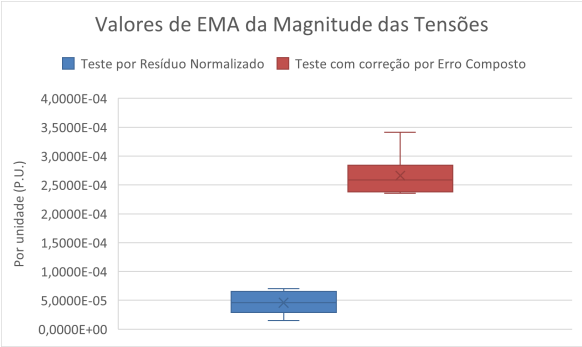
(b) Gráfico Boxplot do EMA dos ângulos com 3 erros grosseiros.

Figura 16 – Resultados da estimação de estado para o exemplo com 3 erros grosseiros.

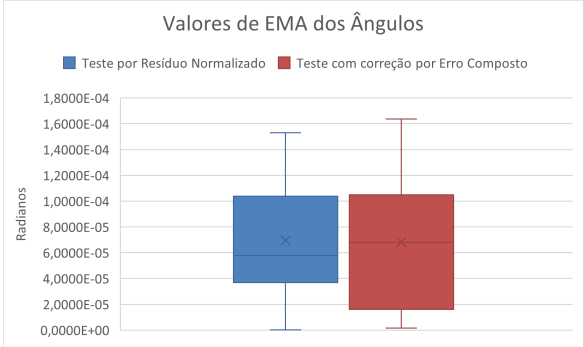
Fonte: Elaboração própria.

4.4.0.2 Caso com 4 EGs

Para criar o vetor de medidas desse caso, foi adicionado ao vetor de medidas do caso anterior um erro grosseiro no valor da medida de tensão no barramento 3 (V3). Os valores de EMA para a tensão e ângulo com a eliminação por resíduo normalizado são, respectivamente, de 0,0233269509 P.U. e 0,0516513792 radianos. Já utilizando o erro composto, o EMA da tensão e do ângulo são, respectivamente, de 0,0230136662 P.U. e 0,0515881060 radianos. Ademais, as medidas V13, Q5 e V3 foram detectadas em ambos os casos como portadoras de erros grosseiros mas o método de correção por erro composto voltou a detectar a medida P5, escolhida por possuir um *UI* alto. A correção dessa medida parece estar associada à redução de performance da correção por erro composto em casos com a presença de *FDI*. Nas Figuras 17.a e 17.b são apresentados os valores de EMA para cada um das técnicas de processamento de EGs consideradas.



(a) Gráfico Boxplot do EMA das tensões com 4 erros grosseiros.



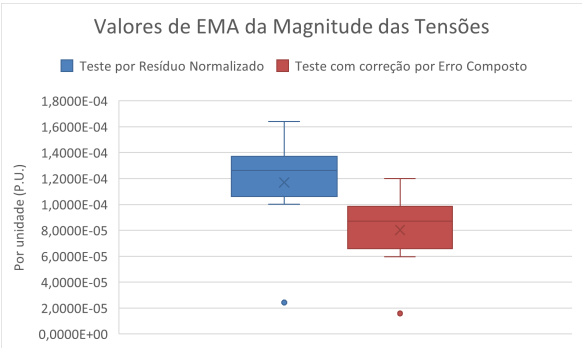
(b) Gráfico Boxplot do EMA dos ângulos com 4 erros grosseiros.

Figura 17 – Resultados da estimação de estado para o exemplo com 4 erros grosseiros.

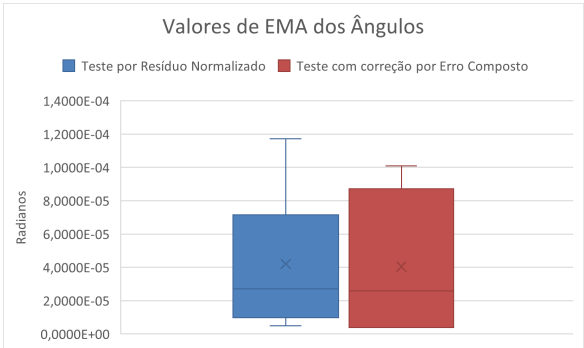
Fonte: Elaboração própria.

4.4.0.3 Caso com 5 EGs

Para a criação do vetor de medidas desse caso, foi adicionado um erro grosseiro na injeção de potência ativa no barramento 2 (P2). Os valores de EMA para a tensão e ângulo com a eliminação por resíduo normalizado são, respectivamente, de 0,0234101713 P.U. e 0,0517374863 radianos. Já utilizando o erro composto, o EMA da tensão e do ângulo são, respectivamente, de 0,0233676274 P.U. e 0,0517060739 radianos. Ademais, apenas as medidas V13, Q5, V3 e P2 foram detectadas em ambos os casos como portadoras de erros grosseiros. Consequentemente, nesse caso, pode-se perceber uma melhora na performance da correção por erro composto, o que condiz com a hipótese de que a correção da medida P5 reduz a acurácia da estimação. Nas Figuras 18.a e 18.b são apresentados os valores de EMA para cada um das técnicas de processamento de EGs consideradas.



(a) Gráfico Boxplot do EMA das tensões com 5 erros grosseiros.



(b) Gráfico Boxplot do EMA dos ângulos com 5 erros grosseiros..

Figura 18 – Resultados da estimação de estado para o exemplo com 5 erros grosseiros.

Fonte: Elaboração própria.

4.5 Considerações sobre os resultados obtidos

De forma geral, os ataques *FDI* simulados neste capítulo permaneceram não detectados pelos procedimentos tradicionais de detecção de EGs, em especial na presença simultânea de ruído e de múltiplos EGs. O critério baseado no erro composto mostrou-se promissor em cenários mais simples, sobretudo na identificação de medidas com alto valor de *UI*, mas sua acurácia foi comprometida em alguns casos pela própria presença dos ataques *FDI* nas medidas que servem de base para o cálculo do resíduo.

Os casos com aumento do número de EGs indicam que, mesmo removendo um conjunto significativo de medidas, ainda é possível manter ataques ocultos, especialmente quando o vetor de ataque a apresenta baixa esparsidade e afeta muitas medidas simultaneamente. Esses resultados reforçam a necessidade de desenvolver métodos adicionais de análise de vulnerabilidade e mecanismos de proteção específicos para o processo de EESEP frente a ataques *FDI*.

Tabela 1 – Comparação dos métodos de tratamento de erros grosseiros.

Método	**Restaura o valor correto das medidas?**	**Detecta EGs?**	**Detecta *FDIs*?**
Eliminação de medidas pelo teste de maior rN	Não	Sim, mas pode falhar na presença de medidas com UI alto	Não
Correção de medidas utilizando EC	Sim, mas a correção pode falhar na presença de *FDIs*	Sim	Não

Fonte: elaboração própria.

5 CONCLUSÕES

Os recentes desenvolvimentos nos SEPs indicam uma tendência à maior eficiência, flexibilidade e segurança operacional, impulsionada pela adoção de tecnologias associadas às redes inteligentes. Entretanto, a crescente digitalização e a dependência de processos automatizados também tornam esses sistemas mais suscetíveis a ataques cibernéticos, especialmente aqueles que exploram vulnerabilidades do processo de EESEP. Dado o papel central da estimação de estado na operação e no planejamento seguro dos SEPs, torna-se essencial que tal processo apresente elevados níveis de robustez e confiabilidade.

A partir do estudo do processo tradicional de EESEP e da análise de metodologias recentes baseadas no índice *UI* e no erro composto, foram realizadas simulações computacionais para avaliar o comportamento de ataques do tipo *FDI* em cenários mais próximos da prática. Esses cenários diferem de grande parte da literatura ao considerar um estimador não linear, incluir ruídos e EGs nas medições e investigar o potencial da métrica do erro composto como ferramenta adicional de detecção.

Os resultados obtidos mostram que ataques *FDI* podem permanecer imperceptíveis aos métodos convencionais de detecção, em especial na presença de ruído ou EGs. Embora o critério do erro composto apresente desempenho promissor para identificar medidas portadoras de EGs, sua eficácia na presença de *FDIs* não foi consistente, em parte devido à influência direta do ataque sobre o cálculo dos resíduos utilizados na correção.

Observou-se também que a simples remoção de um número elevado de medidas durante o processamento de EG pelo método do maior resíduo normalizado, situação que pode ocorrer na presença de múltiplos EGs, não foi suficiente para expor os ataques simulados. Uma possível explicação é a baixa esparsidade dos vetores de ataque construídos, que afetaram simultaneamente um número expressivo de medidas, tornando o processo de detecção mais complexo.

Como perspectivas para trabalhos futuros, recomenda-se: (i) investigar a aplicação da remoção de medidas guiada pelo erro composto, em vez da correção direta, possivelmente ampliando a capacidade de revelação dos ataques; (ii) estudar cenários com ataques menos densos (maior esparsidade), mais compatíveis com modelos realistas de agentes maliciosos; (iii) analisar metodologias híbridas que combinem métricas robustas, como o índice *UI*, com técnicas de aprendizado de máquina ou mecanismos de redundância temporal; (iv) ampliar o estudo para sistemas de maior porte, onde efeitos de topologia e redundância podem alterar significativamente a detectabilidade dos ataques.

Dessa forma, conclui-se que, embora o processo tradicional de EESEP seja eficiente para lidar com ruídos e EGs isolados, sua vulnerabilidade a ataques *FDI* permanece um

desafio relevante, reforçando a necessidade de novas abordagens de detecção e mitigação voltadas à segurança cibernética de SEPs modernos.

REFERÊNCIAS

ABUR, A.; EXPOSITO, A. G. **Power system state estimation: theory and implementation**. [*S.l.: s.n.*]: CRC press, 2004.

ALMASABI, S. *et al.* A novel technique to detect false data injection attacks on phasor measurement units. **Sensors**, v. 21, n. 17, 2021. ISSN 1424-8220. Disponível em: https://www.mdpi.com/1424-8220/21/17/5791.

ALMASABI, S. *et al.* Improving fdi detection for pmu state estimation using adversarial interventions and deep auto-encoder. **IEEE Access**, v. 12, p. 116398–116414, 2024.

ALMEIDA, M. C. de; ASADA, E. N.; GARCIA, A. V. Effects of load imbalance and system asymmetry on three-phase state estimation. *In*: IEEE. **2006 IEEE Power Engineering Society General Meeting**. [*S.l.: s.n.*], 2006. p. 6–pp.

ASHOK, A.; GOVINDARASU, M.; AJJARAPU, V. Online detection of stealthy false data injection attacks in power system state estimation. **IEEE Transactions on Smart Grid**, v. 9, n. 3, p. 1636–1646, 2018.

BENEDITO, R. A. *et al.* Power system state estimation: Undetectable bad data. **International Transactions on Electrical Energy Systems**, Wiley Online Library, v. 24, n. 1, p. 91–107, 2014.

BENEDITO, R. A. d. S. **Índice de não-detecção de erros grosseiros no processo de estimação de estado em sistemas elétricos de potência**. 2011. Tese (Doutorado) — Universidade de São Paulo, 2011.

BI, S.; ZHANG, Y. J. Graphical methods for defense against false-data injection attacks on power system state estimation. **IEEE Transactions on Smart Grid**, IEEE, v. 5, n. 3, p. 1216–1227, 2014.

BRETAS, A. *et al.* **Cyber-physical power systems state estimation**. [*S.l.: s.n.*]: Elsevier, 2021.

CUTSEM, T. V.; RIBBENS-PAVELLA, M.; MILI, L. Hypothesis testing identification: A new method for bad data analysis in power system state estimation. **IEEE Transactions on Power Apparatus and Systems**, IEEE, n. 11, p. 3239–3252, 1984.

DENG, R. *et al.* False data injection on state estimation in power systems—attacks, impacts, and defense: A survey. **IEEE Transactions on Industrial Informatics**, v. 13, n. 2, p. 411–423, 2017.

FALCAO, D.; ARIAS, M. State estimation and observability analysis based on echelon forms of the linearized measurement models. **IEEE Transactions on Power Systems**, v. 9, n. 2, p. 979–987, 1994.

FALCẠO, D. M.; ASSIS, S. M. de. Linear programming state estimation: Error analysis and gross error identification. **IEEE Transactions on Power Systems**, v. 3, p. 809 – 815, 1988. Disponível em: https://www.osti.gov/biblio/6672450.

HABIB, A. A. *et al.* False data injection attack in smart grid cyber physical system: Issues, challenges, and future direction. **Computers and Electrical Engineering**, v. 107, p. 108638, 2023. ISSN 0045-7906. Disponível em: https://www.sciencedirect.com/science/article/pii/S0045790623000630.

HANSEN, C.; DEBS, A. Power system state estimation using three-phase models. **IEEE transactions on power systems**, IEEE, v. 10, n. 2, p. 818–824, 2002.

HUG, G.; GIAMPAPA, J. A. Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks. **IEEE Transactions on Smart Grid**, v. 3, n. 3, p. 1362–1370, 2012.

HUSNOO, M. A. *et al.* False data injection threats in active distribution systems: A comprehensive survey. **Future Generation Computer Systems**, v. 140, p. 344–364, 2023. ISSN 0167-739X. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167739X22003363.

IRVING, M.; OWEN, R.; STERLING, M. Power-system state estimation using linear programming. *In*: IET. **Proceedings of the Institution of Electrical Engineers**. [*S.l.: s.n.*], 1978. v. 125, n. 9, p. 879–885.

JONES, K. D.; THORP, J. S.; GARDNER, R. M. Three-phase linear state estimation using phasor measurements. *In*: IEEE. **2013 IEEE Power & Energy Society General Meeting**. [*S.l.: s.n.*], 2013. p. 1–5.

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

KOSUT, O. *et al.* Limiting false data attacks on power system state estimation. *In*: **2010 44th Annual Conference on Information Sciences and Systems (CISS)**. [*S.l.: s.n.*], 2010. p. 1–6.

KOTIUGA, W. W.; VIDYASAGAR, M. Bad data rejection properties of weughted least absolute value techniques applied to static state estimation. **IEEE Transactions on Power apparatus and systems**, IEEE, n. 4, p. 844–853, 2007.

LIU, C. *et al.* Reactance perturbation for detecting and identifying fdi attacks in power system state estimation. **IEEE Journal of Selected Topics in Signal Processing**, v. 12, n. 4, p. 763–776, 2018.

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)**, ACM New York, NY, USA, v. 14, n. 1, p. 1–33, 2011.

MILI, L.; PHANIRAJ, V.; ROUSSEEUW, P. J. Least median of squares estimation in power systems. **IEEE Transactions on Power Systems**, IEEE, v. 6, n. 2, p. 511–523, 2002.

MONTICELLI, A. **State estimation in electric power systems: a generalized approach**. [*S.l.: s.n.*]: Springer Science & Business Media, 2012.

MONTICELLI, A.; GARCIA, A. Reliable bad data processing for real-time state estimation. **IEEE transactions on power apparatus and systems**, IEEE, n. 5, p. 1126–1139, 2007.

MOUDOUD, H. *et al.* Detection and prediction of fdi attacks in iot systems via hidden markov model. **IEEE Transactions on Network Science and Engineering**, v. 9, n. 5, p. 2978–2990, 2022.

RAHMAN, M. A.; MOHSENIAN-RAD, H. False data injection attacks with incomplete information against smart power grids. *In*: **2012 IEEE Global Communications Conference (GLOBECOM)**. [*S.l.: s.n.*], 2012. p. 3153–3158.

SANDBERG, H.; TEIXEIRA, A.; JOHANSSON, K. H. On security indices for state estimators in power networks. *In*: **First workshop on secure control systems (SCS), Stockholm**. [*S.l.: s.n.*], 2010. v. 2010, p. 1–6.

Schweppe, F. C.; Handschin, E. J. Static state estimation in electric power systems. **IEEE Proceedings**, v. 62, n. 7, p. 972–982, jul. 1974.

SCHWEPPE, F. C.; ROM, D. B. Power system static-state estimation, part ii: Approximate model. **IEEE Transactions on Power Apparatus and Systems**, PAS-89, n. 1, p. 125–130, 1970.

SCHWEPPE, F. C.; WILDES, J. Power system static state estimation, part: exact model. **IEEE Trans on Power Apparatus and Systems**, v. 89, n. 1, p. 120–125, 1970.

SONG, Y. *et al.* Isolation forest based detection for false data attacks in power systems. *In*: **2019 IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia)**. [*S.l.: s.n.*], 2019. p. 4170–4174.

STEFOPOULOS, G. K. *et al.* On three-phase state estimation in the presence of gps-synchronized phasor measurements. *In*: IEEE. **2007 39th North American Power Symposium**. [*S.l.: s.n.*], 2007. p. 406–412.

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**, Elsevier, v. 99, p. 45–56, 2018.

ZELLAGUI, M.; BOUDOUR, M. Impact of renewable energy source penetration on total harmonic distortion using harmonic power flow. *In*: . [*S.l.: s.n.*], 2014.

ZHANG, J. *et al.* False data injection attacks on power system state estimation with limited information. *In*: **2016 IEEE Power and Energy Society General Meeting (PESGM)**. [*S.l.: s.n.*], 2016. p. 1–5.

ZHANG, Z. *et al.* Strategic protection against fdi attacks with moving target defense in power grids. **IEEE Transactions on Control of Network Systems**, v. 9, n. 1, p. 245–256, 2022.

ZHONG, S.; ABUR, A. Effects of nontransposed lines and unbalanced loads on state estimation. *In*: IEEE. **2002 IEEE Power Engineering Society Winter Meeting. Conference Proceedings (Cat. No. 02CH37309)**. [*S.l.: s.n.*], 2002. v. 2, p. 975–979.

APÊNDICES

APÊNDICE A – RESULTADOS DO FLUXO DE POTÊNCIA DO IEEE 14 BARRAS.

Tabela 2 – Valores de fluxos de potência ativos.

De	Para	Valor	Precisão
2	1	-1.52585290193055	0.02
5	1	-0.727475092317839	0.02
1	2	1.5688289052907	0.02
3	2	-0.709143099033194	0.02
4	2	-0.544548381065819	0.02
5	2	-0.406124616641475	0.02
2	3	0.732375792375032	0.02
4	3	0.23659135052517	0.02
2	4	0.561314959386018	0.02
3	4	-0.232856900959124	0.02
5	4	0.616726500377423	0.02
7	4	-0.280741759157107	0.02
9	4	-0.160797575828688	0.02
1	5	0.755103818242975	0.02
2	5	0.415162150172569	0.02
4	5	-0.611582304445026	0.02
6	5	-0.440873208591682	0.02
5	6	0.440873208591682	0.02
11	6	-0.0729790365884335	0.02
12	6	-0.0771425777102339	0.02
13	6	-0.175358914668027	0.02
4	7	0.280741759157107	0.02
8	7	0	0.02
9	7	-0.280741759161205	0.02
7	8	0	0.02
4	9	0.160797575828688	0.02
7	9	0.280741759161205	0.02
10	9	-0.0521467761859585	0.02
14	9	-0.0931022693863167	0.02
9	10	0.0522755246946892	0.02
11	10	0.0379790365900031	0.02
6	11	0.0735327698237673	0.02
10	11	-0.0378532238120033	0.02
6	12	0.0778606701517501	0.02
13	12	-0.0160795951279655	0.02
6	13	0.177479768619105	0.02
12	13	0.0161425777111503	0.02
14	13	-0.0558977306114584	0.02
9	14	0.0942638102997431	0.02
13	14	0.0564385097972978	0.02

Fonte: elaboração própria.

Tabela 3 – Valores de fluxo de potência reativa.

De	Para	Valor	Precisão
2	1	0.276762497267168	0.02
5	1	0.0222935870995798	0.02
1	2	-0.204042916832819	0.02
3	2	0.0160223287346465	0.02
4	2	0.0302068746582519	0.02
5	2	-0.0209903396678539	0.02
2	3	0.0356020295065425	0.02
4	3	-0.0483565249833349	0.02
2	4	-0.0155035040023363	0.02
3	4	0.0447311562354791	0.02
5	4	-0.142010045531075	0.02
7	4	0.113842799424769	0.02
9	4	0.017323220066676	0.02
1	5	0.038549911417576	0.02
2	5	0.0117099785755685	0.02
4	5	0.158236419367272	0.02
6	5	-0.0804951819051061	0.02
5	6	0.124706798102785	0.02
11	6	-0.034445143046987	0.02
12	6	-0.0235395916612973	0.02
13	6	-0.0679891303859263	0.02
4	7	-0.0968106571670679	0.02
8	7	0.176234513668186	0.02
9	7	-0.0497662186825494	0.02
7	8	-0.171629705099278	0.02
4	9	-0.00427611182285537	0.02
7	9	0.0577869056879141	0.02
10	9	-0.0418493707853425	0.02
14	9	-0.0336293092411079	0.02
9	10	0.0421913779839467	0.02
11	10	0.0164451430478714	0.02
6	11	0.0356047297021554	0.02
10	11	-0.0161506292115484	0.02
6	12	0.0250341423688409	0.02
13	12	-0.00748260741957995	0.02
6	13	0.0721657538811188	0.02
12	13	0.00753959166150952	0.02
14	13	-0.0163706907557335	0.02
9	14	0.0361000623854097	0.02
13	14	0.0174717378057301	0.02

Fonte: elaboração própria.

Tabela 4 – Valores de injeção de potência ativa.

De	Para	Valor	Precisão
1	-1	2.32393272353367	0.02
2	-1	0.183000000003071	0.02
3	-1	-0.941999999992318	0.02
4	-1	-0.477999999999877	0.02
5	-1	-0.0759999999902057	0.02
6	-1	-0.111999999997058	0.02
7	-1	0	0.02
8	-1	0	0.02
9	-1	-0.294999999995461	0.02
10	-1	-0.0899999999979642	0.02
11	-1	-0.0349999999984298	0.02
12	-1	-0.0609999999990833	0.02
13	-1	-0.134999999998694	0.02
14	-1	-0.148999999997775	0.02

Fonte: elaboração própria.

Tabela 5 – Valores de injeção de potência reativa.

De	Para	Valor	Precisão
1	-1	-0.165493005415243	0.02
2	-1	0.308571001346948	0.02
3	-1	0.0607534849701281	0.02
4	-1	0.0390000000522761	0.02
5	-1	-0.0159999999965663	0.02
6	-1	0.0523094440470118	0.02
7	-1	0	0.02
8	-1	0.176234513668186	0.02
9	-1	-0.165999999991794	0.02
10	-1	-0.0579999999968912	0.02
11	-1	-0.0179999999991161	0.02
12	-1	-0.0159999999997886	0.02
13	-1	-0.0579999999997778	0.02
14	-1	-0.0499999999968415	0.02

Fonte: elaboração própria.

Tabela 6 – Valores de tensão em cada barramento.

De	Para	Valor	Precisão
1	-1	1.06000000000117	0.01
2	-1	1.04500000000107	0.01
3	-1	1.01000000000142	0.01
4	-1	1.01767085369644	0.01
5	-1	1.01951385982278	0.01
6	-1	1.07000000000188	0.01
7	-1	1.06151953249639	0.01
8	-1	1.09000000000332	0.01
9	-1	1.05593172064265	0.01
10	-1	1.05098462500521	0.01
11	-1	1.05690651854418	0.01
12	-1	1.05518856319952	0.01
13	-1	1.05038171363134	0.01
14	-1	1.03552994585868	0.01

Fonte: elaboração própria.

APÊNDICE B – VALORES DE UI DAS MEDIDAS AFETADAS POR ERROS GROSSEIROS.

Tabela 7 – Valores de UI das medidas com Erro Grosseiro.

Medida	Valor de *UI*
P5	5.55745
Q5	3.61128
P2	3.30957
Q3	0.47749
V13	0.14933

Fonte: elaboração própria.