

Article

Topology Robustness of State Estimation Against False Data Injection and Network Parameter Attacks on Power Monitoring and Control Systems

Yunhao Yu ¹, Yu Wang ², Fuhua Luo ¹, Meiling Dicha ¹, Song Li ³ and Zhenyong Zhang ^{4,*} 

¹ Electric Power Dispatching and Control Center, Guizhou Power Grid Co., Ltd., Guiyang 550002, China; gzwlaq@gz.csg.cn (Y.Y.); sd120378754@163.com (F.L.); dicml3660@163.com (M.D.)

² School of Electrical Engineering, Chongqing University, Chongqing 401331, China; yu_wang@cqu.edu.cn

³ China Association for Science and Technology, Beijing 100863, China; lisong@cnaiss.org.cn

⁴ State Key Laboratory of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang 550025, China

* Correspondence: zhangzy@gzu.edu.cn

Abstract

With the integration of information and communication systems, cyberattacks threaten the normal operation of the power grid. As a critical function, state estimation in the power monitoring and control system is an attractive target for attackers. There are two typical cyberattacks—false data injection attack (FDIA) and network parameter attack (NPA)—that produce incorrect state estimation results, threatening the control and operation of the power system. This paper introduces the first theoretical framework for analyzing the topology robustness of state estimation against FDIA, NPA, and coordinated FDIA+NPA, quantifying the inherent tolerance to injected errors under the DC model. Novel contributions include the following: (1) derivation of analytical bounds on relative state errors for FDIA and similar expressions for NPA and coordinated attacks; (2) proof that sensor measurements, network topology, and branch parameters are key factors influencing robustness, with larger robustness factor amplifying errors in dense or partially measured systems; and (3) validation through extensive MATPOWER simulations on IEEE 14-, 30-, 57-, 118-, and 300-bus systems, confirming bound tightness across scales. These insights enable preventive grid design to enhance resilience against cyber-physical threats.

Keywords: power system state estimation; topology robustness; false data injection attack; network parameter attack



Academic Editor: Andreas Mauthe

Received: 12 December 2025

Revised: 21 January 2026

Accepted: 26 January 2026

Published: 27 January 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and

conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

The modern power system has become more flexible and efficient through the integration of sensing and electronic devices. The large-scale system can be monitored, controlled, and operated with wide-area information sharing and coordination. However, the data transmission network and the remote control channel are vulnerable to cyberattacks [1]. For example, it has been demonstrated that smart meters can be tampered with [2] and that remote terminal units (RTUs) can be corrupted [3].

As a critical function, state estimation is vital for providing reliable data for subsequent applications, such as contingency analysis and optimal power flow. Since its computation requires sensor measurements from the supervisory control and data acquisition (SCADA) system and physical parameters from the transmission network, it is vulnerable to both internal and external attackers.

False data injection attack (FDIA) is a common attack that modifies sensor measurements to introduce bias into the estimation result [4]. Liu et al. [5] presented a framework for constructing stealthy FDIA if the attacker has full knowledge about the system network and branch parameters. Then, Kosut et al. [6] proposed two regimes of attack: if the attacker performs a stealthy attack, a graph-theoretic method is designed to find the minimum-size stealthy FDIA; if the attacker cannot launch a stealthy attack, a minimum-residue-energy attack is proposed as a trade-off between causing large estimation errors and a low detection probability. Yang et al. [7] first proved that the optimization problem of minimizing the number of compromised measurements required to modify a predetermined set of state variables is NP-hard. But with the insight that large-degree buses can be modeled as linear matrix transformations, they proposed a heuristic to solve this optimization problem efficiently. Based on the topology analysis, Deng et al. [8] provided that the attacker can arbitrarily modify the state variables of buses/superbuses that are connected by known branches. They leveraged a new countermeasure by actively perturbing branch admittances to prevent the attackers from obtaining the line parameters. More recently, Zhang et al. [9] proposed an FDIA that requires only the transmission topology, thereby reducing the need for branch parameters. The FDIA demonstrates the vulnerability of the sensor measurements used in state estimation. There are also studies that have explored FDIA in AC models, such as the unified framework for designing optimal AC FDIA proposed in [10], which demonstrates attack construction while highlighting vulnerabilities in nonlinear state estimation. There are many methods proposed to detect FDIA. Fusion deep learning methods for real-time FDIA countermeasures, emphasizing confidence-aware strategies for robustness against data drifts [11]. For FDIA detection in DC microgrids, the data-driven framework proposed in Wang et al., which uses adaptive residual generators for attack localization, demonstrates high accuracy in multi-generator systems [12]. Advances in ML-based countermeasures include stacking models for intrusion detection against cyber attacks in power systems, as in [13], which improves accuracy in identifying threats like FDIA. Another relevant work uses supervised ML for cyberattack detection in PV-powered systems, adaptable to state estimation scenarios [14]. However, most existing work has focused on FDIA design and detection, failing to reveal the state estimator's tolerance to the FDIA.

Another typical attack is the network parameter attack (NPA). The attacker can take control of Flexible Alternating Current Transmission System (FACTS) devices and inject unexpected capacitors into the transmission line [15,16]. FACTS is an equipment that is used to compensate for the reactive power with the resistor-inductor-capacitor circuit [17]. The compensation reference value is sent to the FACTS device, which is vulnerable to compromise and modification. Therefore, the network parameter is changed. Zhang et al. [18] introduced a stealthy physics-manipulated attack (SPMA) targeting FACTS devices, combining physical reactance manipulation with coordinated FDIA sensor data to evade detection. It analyzed the attack's stealthiness across varying levels of adversarial knowledge, quantified its economic and operational impacts, and proposed countermeasures, such as critical sensor protection and Thévenin-based impedance monitoring, to mitigate risks. Considering the dynamic environment of the power system, Zhang et al. [17] investigated the vulnerability of intelligent grid Load Frequency Control (LFC) to NPA, in which attackers manipulated the reactance values of transmission lines via compromised Thyristor-Controlled Series Compensators (TCSCs) to destabilize grid frequency. By analyzing eigenvalue sensitivity to identify critical transmission lines and formulating a resource-efficient attack strategy, the study demonstrated, through simulations on IEEE test systems, that NPAs could induce instability, underscoring the need for robust cybersecurity defenses in power systems. Although the papers above showed that NPA can affect system

operation, they did not provide a deep analysis of why the power system is vulnerable to these modifications.

As noted above, existing studies have primarily investigated how to design robust and stealthy attacks. The ability of state estimation to tolerate errors injected into sensor measurements and network parameters has not been sufficiently studied. To fill this gap, we analyze the topology robustness of power system state estimation against FDIA and NPA in this paper. In other words, we aim to quantify the tolerance of state estimation to injected errors. There is prior work studying this topic. Pajic et al. [19] proposed a robust method for attack-resilient state estimation in cyber-physical systems under noise and modeling errors, demonstrating that attackers cannot exploit model discrepancies to destabilize the system. Chakhchoukh and Ishii [20] proposed enhancing the security of the power system state estimation by deploying multiple robust least trimmed squares (LTS) estimators with varying breakdown points in parallel, reducing reliance on costly secure sensors. However, these studies primarily focused on improving the power system's topology robustness. The factors influencing topology robustness against cyberattacks remain unexplored. Therefore, by jointly modeling the attack and the system, we aim to identify which parameters are critical to the topology robustness of power system state estimation. The contributions are given in the following:

- First, we develop a unified model integrating FDIA (targeting sensor measurements) and NPA (targeting branch parameters via devices like FACTS) to analyze their combined impact on power system state estimation, providing a theoretical framework that quantifies topology robustness through norm-based sensitivity measures—unlike prior works that focus primarily on attack design without deriving tolerance bounds.
- Second, we derive closed-form analytical bounds for topology robustness, including the metric for FDIA in fully measured systems and the metric for partially measured cases, extended to NPA and coordinated attacks, enabling operators to evaluate vulnerability without exhaustive simulations.
- Finally, we conduct extensive simulations on IEEE test systems (14-, 30-, 57-, 118-, and 300-bus), validating that lower robustness values correlate with reduced error propagation (e.g., up to 30% robustness improvement with partial measurements), under scenarios including noise and topology variations.

In this paper, topology robustness refers to the inherent tolerance of the power system's state estimation process to errors injected by cyberattacks, specifically quantified as the bounded amplification of estimation errors relative to injected perturbations in sensor measurements (under FDIA) or network parameters (under NPA). This robustness is measured through analytical bounds, which capture the sensitivity of state estimates to topology, branch parameters, and sensor placement. Traditional security solutions, such as encryption and intrusion detection systems (IDS), are insufficient to fully mitigate these threats because FDIA and NPA can be designed to be stealthy—exploiting knowledge of the system topology to evade detection by maintaining consistency with bad data detection mechanisms—while NPA directly manipulates physical parameters via compromised field devices (e.g., FACTS), bypassing cyber-layer protections. Our analysis focuses on these intrinsic vulnerabilities to inform topology-aware defenses.

The organization of this paper is as follows: the system model and threat model are given in Section 2; the topology robustness of the power system state estimation against FDIA and NPA is analyzed in Section 3; the extensive simulations used to validate the theoretical results are in Section 4; Section 5 discusses some implications for Power Grid Planning and Operation and Section 6 concludes the paper.

2. System Model and Threat Model

Here, we introduce the power system state estimation and threat model for an easy understanding of the following derivations.

2.1. System Model

The DC model is usually used in power systems to analyze contingencies, faults, and market behavior [21]. Although it is linearized from the nonlinear AC model, the DC power flow model is designed for real-time operations, such as computing marginal price [22,23]. Therefore, although the DC model is simple, it captures the power system's physical characteristics. The state variables to be estimated are the voltage phase angles. The power flow is represented as

$$f_{ij} = -b_{ij}(\theta_i - \theta_j), p_i = \sum_{j \in Q_i} f_{ij}, \quad (1)$$

where f_{ij} denotes the power flow between bus i and j , b_{ij} represents the equivalent susceptance of branch $\{i, j\}$, θ_i and θ_j represent the voltage phase angles of bus i and j , respectively, p_i denotes the power injection of bus i , Q_i is a set containing neighboring buses connected to bus i . Considering a power transmission network having a set $\{1, 2, \dots, n+1\}$ of buses (bus 1 is the reference bus) and a set $\{k_1, k_2, \dots, k_l\}$ of branches. Apart from the reference bus, the rest n phase angles $\theta_1, \theta_2, \dots, \theta_n$ are state variables that should be estimated, denoted by $\mathbf{x} \in \mathbb{R}^n$. The branch/line $k_t = \{i, j\} \in \mathcal{L}$ incidents from bus i to bus j . If the power system is fully measured, meaning each bus is sensed by a meter and each branch is sensed by two meters (one in each direction), then there are $m = 2l + n + 1$ meters. The DC power flow model is formulated as

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \boldsymbol{\eta}. \quad (2)$$

in which, $\mathbf{H}$ denotes the measurement matrix, $\mathbf{z}$ represents the measurements of power injections and power flows.

2.2. Measurement Matrix

By using $\mathbf{V}$ to denote the branch–bus incidence matrix, we have

$$v_{ti} = \begin{cases} 1, & k_t \text{ starts from bus } i; \\ -1, & k_t \text{ ends at bus } i; \\ 0, & \text{otherwise,} \end{cases} \quad (3)$$

in which, v_{ti} denotes the element at position (t, i) of $\mathbf{V}$. Using $\mathbf{W}$ as the diagonal branch susceptance matrix, its element $\mathbf{w}_{tt}$ is $-b_{ij}$ with $k_t = \{i, j\}$. Hence, the symmetric admittance matrix is $\mathbf{B} = \mathbf{V}^T \mathbf{W} \mathbf{V}$ (invertible), and the branch-bus shift factor matrix is $\mathbf{S} = \mathbf{W} \mathbf{V}$. Besides, we have

$$\mathbf{f} = \mathbf{S}\boldsymbol{\theta}, \mathbf{p} = \mathbf{B}\boldsymbol{\theta}, \quad (4)$$

where $\mathbf{f}$ denotes a vector of power flows, $\mathbf{p}$ denotes a vector of power injections, and $\boldsymbol{\theta}$ denotes a vector of phase angles. In the fully measured case, the matrix $\mathbf{H} \in \mathbb{R}^{m \times n}$ is

$$\mathbf{H} = \begin{bmatrix} \mathbf{B} \\ \mathbf{S} \\ -\mathbf{S} \end{bmatrix}. \quad (5)$$

The matrix $\mathbf{H}$ is related to the transmission network and branch parameters (i.e., susceptance).

Suppose the system is partially measured, meaning some buses and branches are not equipped with meters. In that case, the measurement matrix is constructed by selecting several rows from the fully measured matrix. For any measurement matrix, it is of full column rank.

2.3. State Estimation

State estimation, a basic function for estimating the state variables with sensor measurements monitored by the SCADA system [24]. The state estimation is

$$\hat{\mathbf{x}} = (\mathbf{H}^T \mathbf{H})^{-1} \mathbf{H}^T \mathbf{z}. \quad (6)$$

The estimation $\hat{\mathbf{x}}$ is usually computed using the least squares method.

2.4. Threat Model

The power grid's security has attracted significant attention. For example, the US National Electric Sector Cybersecurity Organization Resource (NESCOR) reports incidents and impacts on the physical power systems [25–27]. The North American Electrical Reliability Council (NERC) issues lessons learned from physical failures and outages caused by cyber faults [28]. In this paper, we focus on two common cyberattacks: the false data injection attack (FDIA) and the network parameter attack (NPA). For these two attacks, we assume that the attacker has the following capabilities.

- FDIA: The attacker has the capability of tampering with the sensor measurements.
- NPA: The attacker has the capability of corrupting the control commands of the devices that adjust the branch parameter (i.e., the reactance).

For both FDIA and NPA, the attackers eavesdrop on the communication channels before the attack to collect the necessary topology information. The attacker is not assumed to have complete details about the power system. The attack feasibility is discussed as follows:

- FDIA Feasibility: FDIA typically requires cyber access rather than physical contact, achieved by injecting malware into SCADA systems, remote terminal units (RTUs), or smart meters via phishing, supply-chain compromises, or network vulnerabilities. Real-world examples underscore this: the 2015 Ukraine blackout, caused by Black-Energy malware, manipulated control systems to inject false commands, leading to widespread outages without physical intervention. Similarly, the Stuxnet worm (2010) targeted industrial controls, and more recent incidents, such as the 2019 Utah grid disruption and the 2021 ransomware attacks on U.S. and Australian power providers, demonstrate ongoing vulnerabilities. However, feasibility depends on attacker resources; stealthy FDIAs require topology knowledge, which can be obtained via reconnaissance or insider threats, but evading bad data detection (BDD) demands precise crafting to keep residuals below thresholds.
- NPA Feasibility: NPA often involves compromising devices like Flexible AC Transmission Systems (FACTS) or Thyristor-Controlled Series Compensators (TCSCs) to alter branch parameters (e.g., reactance). This can be cyber-based, requiring no physical access if control channels are hacked, as seen in simulations of physics-manipulated attacks. While fewer direct real-world examples exist than in FDIA, related incidents, such as the 2015 Ukraine attack, involved parameter manipulation in control logic. Detection is challenging, as NPAs can mimic legitimate variations (e.g., load changes) and bypass traditional BDD; advanced methods such as impedance monitoring or ML-based anomaly detection are needed, though not foolproof.

- **Coordinated Attacks and Overall Difficulty:** Coordinated FDIA+NPA increases impact but also complexity, requiring multi-domain access. Existing security measures (e.g., firewalls, encryption) raise the bar, but gaps in legacy systems persist, as evidenced by state-sponsored studies of grid vulnerabilities. Mitigation via robust estimators or moving target defenses can reduce feasibility.

As shown in Figure 1, we present the scenario diagram and attack entries. The key entities are divided into the following four functional layers: physical layer, cyber layer, control layer, and adversary capability.

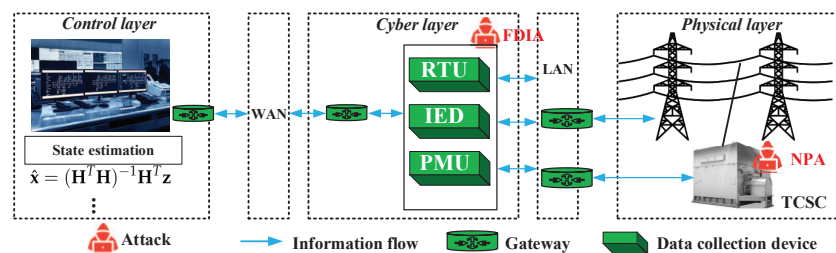


Figure 1. The scenario diagram and attack entries.

3. Topology Robustness of the Power System State Estimation Against FDIA and NPA

In this section, we analyze the power grid's topology robustness against FDIA and NPA. FDIA is an attack on the power grid that targets the sensor measurements. The measurement $\mathbf{m}$ is perturbed by adding noise to the original sensor measurements. NPA is a command-modification attack that corrupts the capacitance injection of the series capacitor compensator, thereby causing unexpected changes in network parameters [17]. These two cyberattacks can push the system states beyond their physical limits, inducing dangerous operating conditions. In the following, we discuss the power grid's topology robustness against FDIA and NPA.

3.1. Topology Robustness Under FDIA

Considering the threat of FDIA, the topology robustness of power system state estimation is its tolerance to injected measurement errors. Taking state estimation as the critical function, we examine the change in the estimated state when the sensor measurements are modified. Based on the deployed sensors, two cases should be analyzed: the fully measured case and the partially measured case.

3.1.1. Fully-Measured Case for FDIA

If the power network is fully measured, then we have

$$\mathbf{z} = \mathbf{H}\mathbf{x} = \begin{bmatrix} \mathbf{B} \\ \mathbf{S} \\ -\mathbf{S} \end{bmatrix} \mathbf{x}. \quad (7)$$

$$\text{Since } \mathbf{z} = \begin{bmatrix} \tilde{\mathbf{p}} \\ \tilde{\mathbf{f}} \\ -\tilde{\mathbf{f}} \end{bmatrix}, \text{ we have}$$

$$\tilde{\mathbf{p}} = \mathbf{B}\mathbf{x}, \tilde{\mathbf{f}} = \mathbf{S}\mathbf{x}, \quad (8)$$

where $\tilde{\mathbf{p}}$ and $\tilde{\mathbf{f}}$ are measurements of the injection powers and power flows. Usually, since the first state of $\mathbf{x}$ is set as a reference, the first column of the branch-bus incident matrix $\mathbf{A}$ is removed, which is denoted by $\bar{\mathbf{A}}$. Thus, we have

$$\tilde{\mathbf{p}} = \bar{\mathbf{B}}\bar{\mathbf{x}}, \quad (9)$$

where $\bar{\mathbf{B}} = \bar{\mathbf{A}}^T \mathbf{D} \bar{\mathbf{A}}$ is an invertible square matrix and $\bar{\mathbf{x}}$ represents the state vector by deleting the first state variable. Furthermore, we can use Equation (9) to assess the topology robustness of the state estimation against FDIA and NPA.

Under FDIA, the sensor measurements are corrupted by the attacker. The impact of FDIA on the state estimation is analyzed as follows.

Proposition 1. *The topology robustness of the power system state estimation against FDIA depends on $\gamma = \|\bar{\mathbf{B}}^{-1}\| \cdot \|\bar{\mathbf{B}}\|$.*

Proof. With (9), we have

$$\tilde{\mathbf{p}} + \epsilon\tilde{\mathbf{p}} = \bar{\mathbf{B}}(\bar{\mathbf{x}} + \epsilon\bar{\mathbf{x}}), \quad (10)$$

where $\epsilon\tilde{\mathbf{p}}$ and $\epsilon\bar{\mathbf{x}}$ are the error injected into the measurement and the state error caused by FDIA, respectively. We can derive that

$$\epsilon\bar{\mathbf{x}} = \bar{\mathbf{B}}^{-1}\epsilon\tilde{\mathbf{p}} \quad (11)$$

According to the compatibility condition of the norm, we have

$$\|\epsilon\bar{\mathbf{x}}\| \leq \|\bar{\mathbf{B}}^{-1}\| \cdot \|\epsilon\tilde{\mathbf{p}}\|, \|\tilde{\mathbf{p}}\| \leq \|\bar{\mathbf{B}}\| \cdot \|\bar{\mathbf{x}}\|, \quad (12)$$

where $\|\cdot\|$ denotes any norm. Therefore, we can derive that

$$\frac{\|\epsilon\bar{\mathbf{x}}\|}{\|\bar{\mathbf{x}}\|} \leq \|\bar{\mathbf{B}}^{-1}\| \cdot \|\bar{\mathbf{B}}\| \cdot \frac{\|\epsilon\tilde{\mathbf{p}}\|}{\|\tilde{\mathbf{p}}\|} = \gamma \frac{\|\epsilon\tilde{\mathbf{p}}\|}{\|\tilde{\mathbf{p}}\|}. \quad (13)$$

From above, the state change induced by FDIA is related to $\gamma = \|\bar{\mathbf{B}}^{-1}\| \cdot \|\bar{\mathbf{B}}\|$, which dominates the impact of FDIA on the state estimation. $\square$

Since $\bar{\mathbf{B}}$ is constructed according to the transmission topology and branch parameters, the topology robustness of the power system state estimation against FDIA is related to the physical parameters. The smaller the γ is, the less sensitive the state is to the injected measurement error. Once $\gamma \gg 1$, the state estimation is vulnerable to the measurement error injected by FDIA. Therefore, in a transmission system, if the transmission topology and branch parameters make γ much smaller than 1, the system is more robust to measurement errors injected by FDIA.

For computing γ , we provide a special example: the norm in Equation (12) is the 2-norm. Based on the singular value decomposition, the largest and smallest singular values (i.e., $\alpha_{\min}$ and $\alpha_{\max}$) of matrix $\bar{\mathbf{B}}$ have the following relationship:

$$\alpha_{\min} = \frac{1}{\|\bar{\mathbf{B}}^{-1}\|_2}, \alpha_{\max} = \|\bar{\mathbf{B}}\|_2 \quad (14)$$

Therefore, we have $\gamma = \frac{\alpha_{\max}}{\alpha_{\min}}$. Since $\bar{\mathbf{B}}$ is a symmetry positive matrix, we can derive that $\gamma = \frac{\zeta_{\max}}{\zeta_{\min}}$, where $\zeta_{\min}$ and $\zeta_{\max}$ are the maximum and minimum eigenvalues of matrix $\bar{\mathbf{B}}$.

3.1.2. Partially-Measured Case for FDIA

Next, we consider a more general case where the transmission system is not fully measured. In this case, we have $\mathbf{z} = \mathbf{H}\mathbf{x}$, and the matrix $\mathbf{H}$ is full column rank.

To assess the topology robustness of the state estimation against FDIA, we conclude as follows.

Proposition 2. *The topology robustness of the state estimation against FDIA depends on $\gamma' = \frac{\alpha'_{\max}}{\alpha'_{\min}}$, where $\alpha'_{\max}$ is the maximum singular value of matrix $\mathbf{H}$ and $\alpha'_{\min}$ is the minimum singular value but not the zero singular value of matrix $\mathbf{H}$.*

Proof. Since the sensor measurements are injected with errors by FDIA, we have

$$\mathbf{z} + \epsilon\mathbf{z} = \mathbf{H}(\mathbf{x} + \epsilon\mathbf{x}), \quad (15)$$

where $\epsilon\mathbf{z}$ and $\epsilon\mathbf{x}$ are the error injected into the sensor measurement and the state error caused by FDIA, respectively. Therefore, we obtain that

$$\epsilon\mathbf{x} = \mathbf{H}^* \epsilon\mathbf{z}, \quad (16)$$

where $\mathbf{H}^*$ is the Moore-Penrose pseudoinverse of $\mathbf{H}$. Similar to the proof of Proposition 1, we can derive that

$$\frac{\|\epsilon\mathbf{x}\|}{\|\mathbf{x}\|} \leq \|\mathbf{H}^*\| \cdot \|\mathbf{H}\| \cdot \frac{\|\epsilon\mathbf{z}\|}{\|\mathbf{z}\|}. \quad (17)$$

Considering that the norm is 2-norm, we have

$$\|\mathbf{H}\| = \alpha'_{\max}, \|\mathbf{H}^*\| = \frac{1}{\alpha'_{\min}}, \quad (18)$$

where $\alpha'_{\max}$ denotes the maximum singular value of the measurement matrix $\mathbf{H}$ and $\alpha'_{\min}$ denotes the minimum singular value of $\mathbf{H}$ but not the zero singular value. Since $\gamma' = \frac{\alpha'_{\max}}{\alpha'_{\min}}$, we have

$$\frac{\|\epsilon\mathbf{x}\|}{\|\mathbf{x}\|} \leq \gamma' \cdot \frac{\|\epsilon\mathbf{z}\|}{\|\mathbf{z}\|}. \quad (19)$$

Therefore, the topology robustness of the state estimation depends on γ' . $\square$

Since $\mathbf{H}$ is constructed from the positions of deployed sensors, the transmission topology, and the branch parameters, the topology robustness of the state estimation against FDIA depends on these parameters. A smaller γ' indicates the better topology robustness of the state estimation. If $\gamma' \ll 1$, the state estimation is not sensitive to the measurement error injected by FDIA.

3.2. Topology Robustness Under NPA

Considering the threat of NPA, the topology robustness of the state estimation is its tolerance to injected errors in the physical parameters. Here, we assume that the attacker targets the branch parameter. This attack is usually carried out by modifying the control commands of field electronic devices. A typical target is the Flexible Alternating Current Transmission System (FACTS). By compromising the channel carrying the control signal, the attacker can change the branch reactance by injecting an unexpected capacitor. In the following, we analyze the topology robustness of the state estimation against NPA in two cases.

3.2.1. Fully-Measured Case for NPA

Similar to the analysis given in Section 3.1.1, the Equation (9) is used to derive the result. Under NPA, the branch parameter (i.e., reactance) is modified. The impact of this modification is analyzed as follows.

Proposition 3. *The topology robustness of the state estimation against NPA is closely related to $\gamma = \|\bar{\mathbf{B}}^{-1}\| \cdot \|\bar{\mathbf{B}}\|$.*

Proof. Under NPA, the matrix $\bar{\mathbf{B}}$ is changed. With (9), we can derive that

$$\tilde{\mathbf{p}} = (\bar{\mathbf{B}} + \epsilon\bar{\mathbf{B}})(\bar{\mathbf{x}} + \epsilon\bar{\mathbf{x}}), \quad (20)$$

where $\epsilon\bar{\mathbf{B}}$ is the change caused by NPA and $\epsilon\bar{\mathbf{x}}$ is the resulted state error. Since the attacker cannot change the transmission parameters on a large scale, $\epsilon\bar{\mathbf{B}}$ is a small perturbation with respect to the matrix $\bar{\mathbf{B}}$. Assume that $\|\bar{\mathbf{B}}^{-1}\epsilon\bar{\mathbf{B}}\| < 1$; then the term $(\mathbf{E} + \bar{\mathbf{B}}^{-1} \cdot \epsilon\bar{\mathbf{B}})^{-1}$ exists, where $\mathbf{E}$ is the identity matrix. According to (9), we can derive that

$$\epsilon\bar{\mathbf{x}} = -(\mathbf{E} + \bar{\mathbf{B}}^{-1} \cdot \epsilon\bar{\mathbf{B}})^{-1}\bar{\mathbf{B}}^{-1}(\epsilon\bar{\mathbf{B}})\mathbf{x}. \quad (21)$$

Since $\|\bar{\mathbf{B}}^{-1}\epsilon\bar{\mathbf{B}}\| < 1$, then the matrix $\bar{\mathbf{B}} + \epsilon\bar{\mathbf{B}}$ is nonsingular (i.e., invertible). The inverse matrix of it is as follows:

$$(\bar{\mathbf{B}} + \epsilon\bar{\mathbf{B}})^{-1} = (\mathbf{E} + \bar{\mathbf{B}}^{-1} \cdot \epsilon\bar{\mathbf{B}})^{-1}\bar{\mathbf{B}}^{-1}. \quad (22)$$

According to the Neumann series, we have

$$(\mathbf{E} + \bar{\mathbf{B}}^{-1} \cdot \epsilon\bar{\mathbf{B}})^{-1} = \mathbf{E} - \bar{\mathbf{B}}^{-1} \cdot \epsilon\bar{\mathbf{B}} + (\bar{\mathbf{B}}^{-1} \cdot \epsilon\bar{\mathbf{B}})^2 - (\bar{\mathbf{B}}^{-1} \cdot \epsilon\bar{\mathbf{B}})^3 + \dots \quad (23)$$

Then, the norm satisfies the following relationship:

$$\|(\bar{\mathbf{B}} + \epsilon\bar{\mathbf{B}})^{-1}\| \leq \frac{\|\bar{\mathbf{B}}^{-1}\|}{1 - \|\bar{\mathbf{B}}^{-1}\epsilon\bar{\mathbf{B}}\|}. \quad (24)$$

Further, we can derive that

$$\|\epsilon\bar{\mathbf{x}}\| \leq \frac{\|\bar{\mathbf{B}}^{-1}\| \cdot \|\epsilon\bar{\mathbf{B}}\| \cdot \|\mathbf{x}\|}{1 - \|\bar{\mathbf{B}}^{-1}\epsilon\bar{\mathbf{B}}\|}. \quad (25)$$

Since $\|\bar{\mathbf{B}}^{-1}\| \cdot \|\epsilon\bar{\mathbf{B}}\| < 1$, we have

$$\frac{\|\epsilon\bar{\mathbf{x}}\|}{\|\bar{\mathbf{x}}\|} \leq \frac{\|\bar{\mathbf{B}}^{-1}\| \cdot \|\bar{\mathbf{B}}\| \cdot \frac{\|\epsilon\bar{\mathbf{B}}\|}{\|\bar{\mathbf{B}}\|}}{1 - \|\bar{\mathbf{B}}^{-1}\| \cdot \|\bar{\mathbf{B}}\| \cdot \frac{\|\epsilon\bar{\mathbf{B}}\|}{\|\bar{\mathbf{B}}\|}} = \frac{\gamma \cdot \frac{\|\epsilon\bar{\mathbf{B}}\|}{\|\bar{\mathbf{B}}\|}}{1 - \gamma \cdot \frac{\|\epsilon\bar{\mathbf{B}}\|}{\|\bar{\mathbf{B}}\|}}. \quad (26)$$

Further, we can derive that

$$\frac{\|\epsilon\bar{\mathbf{x}}\|}{\|\bar{\mathbf{x}}\|} \leq \frac{1}{\frac{1}{\gamma} \cdot \frac{\|\bar{\mathbf{B}}\|}{\|\epsilon\bar{\mathbf{B}}\|} - 1}. \quad (27)$$

To enhance clarity, we will introduce a relative perturbation parameter $\vartheta = \frac{\|\epsilon\bar{\mathbf{B}}\|}{\|\bar{\mathbf{B}}\|}$, which simplifies the expression while preserving its meaning. The revised equation will be reformatted as follows:

$$\frac{\|\epsilon\bar{\mathbf{x}}\|}{\|\bar{\mathbf{x}}\|} \leq \frac{\gamma\vartheta}{1 - \gamma\vartheta},$$

under the assumption that $\gamma\vartheta < 1$.

Therefore, the topology robustness of the state estimation against NPA is closely related to $\gamma = \|\bar{\mathbf{B}}^{-1}\| \cdot \|\bar{\mathbf{B}}\|$. $\square$

Since γ is related to the transmission topology and branch parameters, the topology robustness of the power system state estimation against NPA is affected by these parameters. The smaller the γ is, the less sensitive the state estimation is to the modification of the branch parameter. If $\gamma \ll 1$, then the power system state estimation is robust against NPA.

3.2.2. Partially Measured Case for NPA

Next, we consider the general case in which the power network is partially measured. Thus, the sensor deployment determines the construction of $\mathbf{H}$. Since NPA modifies the branch parameter, $\mathbf{H}$ is changed accordingly. Here is the conclusion about the topology robustness of the state estimation against NPA.

Proposition 4. *The topology robustness of the state estimation against NPA is related to $\gamma' = \frac{\alpha'_{max}}{\alpha'_{min}}$, where α'_{max} denotes the maximum singular value of matrix $\mathbf{H}$ and α'_{min} denotes the minimum singular value but not the zero singular value of $\mathbf{H}$.*

Proof. Suppose $\mathbf{H}^*$ is the Moore–Penrose pseudoinverse of $\mathbf{H}$, we have

$$\mathbf{x} + \epsilon\mathbf{x} = (\mathbf{H} + \epsilon\mathbf{H})^* \mathbf{z}. \quad (28)$$

The error $\epsilon\mathbf{H}$ injected by NPA is usually small. According to the Neumann series, we have

$$(\mathbf{H} + \epsilon\mathbf{H})^* \approx \mathbf{H}^* - \mathbf{H}^* \epsilon \mathbf{H} \mathbf{H}^* + \mathbf{H}^* (\mathbf{H}^*)^T (\epsilon\mathbf{H})^T (\mathbf{E} - \mathbf{H} \mathbf{H}^*). \quad (29)$$

Therefore, the state error can be approximated with

$$\epsilon\mathbf{x} \approx -\mathbf{H}^* (\epsilon\mathbf{H}) \mathbf{x} + \mathbf{H}^* (\mathbf{H}^*)^T (\epsilon\mathbf{H})^T (\mathbf{E} - \mathbf{H} \mathbf{H}^*) \mathbf{z}. \quad (30)$$

Since $(\mathbf{E} - \mathbf{H} \mathbf{H}^*) \mathbf{z} = 0$, we have

$$\epsilon\mathbf{x} \approx -\mathbf{H}^* (\epsilon\mathbf{H}) \mathbf{x}. \quad (31)$$

Since $\mathbf{H}$ usually has full column rank, we have

$$\|\epsilon\mathbf{x}\| \leq \|\mathbf{H}^*\| \cdot \|\epsilon\mathbf{H}\| \cdot \|\mathbf{x}\|. \quad (32)$$

Further, we can derive that

$$\frac{\|\epsilon\mathbf{x}\|}{\|\mathbf{x}\|} \leq \|\mathbf{H}^*\| \cdot \|\epsilon\mathbf{H}\| = \|\mathbf{H}^*\| \|\mathbf{H}\| \cdot \frac{\|\epsilon\mathbf{H}\|}{\|\mathbf{H}\|}. \quad (33)$$

According to the proof of Proposition 2, we have

$$\frac{\|\epsilon\mathbf{x}\|}{\|\mathbf{x}\|} \leq \gamma' \frac{\|\epsilon\mathbf{H}\|}{\|\mathbf{H}\|}. \quad (34)$$

$\square$

Since γ' depends on sensor deployment, the transmission topology, and branch parameters, the topology robustness of the state estimation against NPA is also tied to these parameters. In other words, if the system operator wants to enhance the topology robustness of the state estimation, they can select appropriate sensors for the analysis. From a

construction perspective, topology planning and the materials used for power transmission can be considered to defend against NPA. Anyway, the goal is to obtain a sufficiently small γ' .

3.3. Topology Robustness Under the Coordinated FDIA and NPA

Furthermore, we consider the coordinated attack (CA) by simultaneously executing FDIA and NAP. This is a more powerful yet practical attack in a real-world case (e.g., BlackEnergy on the Ukrainian power grid [29]). The topology robustness of the state estimation against CA is analyzed in the following. Here, we only consider the fully measured case. The reason will be explained after the detailed analysis. Under CA, we have

$$\tilde{\mathbf{p}} + \epsilon\tilde{\mathbf{p}} = (\tilde{\mathbf{B}} + \epsilon\tilde{\mathbf{B}})(\tilde{\mathbf{x}} + \epsilon\tilde{\mathbf{x}}). \quad (35)$$

Proposition 5. Let $\eta = \phi\gamma$, $\frac{\|\tilde{\mathbf{B}}\|}{\|\epsilon\tilde{\mathbf{B}}\|} \leq \phi$, and $\frac{\|\epsilon\tilde{\mathbf{p}}\|}{\|\tilde{\mathbf{p}}\|} \leq \phi$. If $\phi < \frac{1}{\gamma}$, then we have $\frac{\|\epsilon\tilde{\mathbf{x}}\|}{\|\tilde{\mathbf{x}}\|} \leq \frac{2\phi}{1-\eta}\gamma$, where $\gamma = \|\tilde{\mathbf{B}}^{-1}\| \cdot \|\tilde{\mathbf{B}}\|$.

Proof. First, since $\tilde{\mathbf{B}}$ is invertible, we have

$$\|\tilde{\mathbf{B}}^{-1}(\epsilon\tilde{\mathbf{B}})\| \leq \|\tilde{\mathbf{B}}^{-1}\| \cdot \|\epsilon\tilde{\mathbf{B}}\| \leq \phi\|\tilde{\mathbf{B}}^{-1}\| \cdot \|\tilde{\mathbf{B}}\| = \eta < 1 \quad (36)$$

According to the Neumann series, from (23), we analyze the term $\tilde{\mathbf{B}}^{-1}(\epsilon\tilde{\mathbf{B}})$. We have

$$\|\tilde{\mathbf{B}}^{-1}(\epsilon\tilde{\mathbf{B}})\| \leq \|\tilde{\mathbf{B}}^{-1}\| \|\epsilon\tilde{\mathbf{B}}\| = \|\tilde{\mathbf{B}}^{-1}\| \|\tilde{\mathbf{B}}\| \frac{\|\epsilon\tilde{\mathbf{B}}\|}{\|\tilde{\mathbf{B}}\|} \leq \gamma\phi = \eta. \quad (37)$$

Therefore, we can derive that

$$\|(\mathbf{E} + \tilde{\mathbf{B}}^{-1}(\epsilon\tilde{\mathbf{B}}))^{-1}\| \leq \frac{1}{1-\eta}. \quad (38)$$

Therefore, the matrix $\mathbf{E} + \tilde{\mathbf{B}}^{-1}(\epsilon\tilde{\mathbf{B}})$ is invertible. Furthermore, we have $\tilde{\mathbf{B}}(\mathbf{E} + \tilde{\mathbf{B}}^{-1}(\epsilon\tilde{\mathbf{B}})) = \tilde{\mathbf{B}} + \epsilon\tilde{\mathbf{B}}$ is also invertible.

Next, by multiplying $\tilde{\mathbf{B}}^{-1}$ with both sides of Equation (35), we have

$$(\mathbf{E} + \tilde{\mathbf{B}}^{-1}(\epsilon\tilde{\mathbf{B}}))(\tilde{\mathbf{x}} + \epsilon\tilde{\mathbf{x}}) = \tilde{\mathbf{x}} + \tilde{\mathbf{B}}^{-1}(\epsilon\tilde{\mathbf{p}}). \quad (39)$$

Thus, we have

$$\tilde{\mathbf{x}} + \epsilon\tilde{\mathbf{x}} = (\mathbf{E} + \tilde{\mathbf{B}}^{-1}(\epsilon\tilde{\mathbf{B}}))^{-1}(\tilde{\mathbf{x}} + \tilde{\mathbf{B}}^{-1}(\epsilon\tilde{\mathbf{p}})). \quad (40)$$

Further, we obtain

$$\begin{aligned} \|\tilde{\mathbf{x}} + \epsilon\tilde{\mathbf{x}}\| &\leq \|(\mathbf{E} + \tilde{\mathbf{B}}^{-1}(\epsilon\tilde{\mathbf{B}}))^{-1}\| (\|\tilde{\mathbf{x}}\| + \phi\|\tilde{\mathbf{B}}^{-1}\| \|\tilde{\mathbf{p}}\|) \\ &\leq \frac{1}{1-\eta} (\|\tilde{\mathbf{x}}\| + \eta \frac{\|\tilde{\mathbf{p}}\|}{\|\tilde{\mathbf{B}}\|}). \end{aligned} \quad (41)$$

Since $\|\tilde{\mathbf{p}}\| \leq \|\tilde{\mathbf{B}}\| \cdot \|\tilde{\mathbf{x}}\|$, we have

$$\|\tilde{\mathbf{x}} + \epsilon\tilde{\mathbf{x}}\| \leq \frac{1}{1-\eta} (\|\tilde{\mathbf{x}}\| + \eta\|\tilde{\mathbf{x}}\|). \quad (42)$$

As $\epsilon\tilde{\mathbf{x}} = \tilde{\mathbf{B}}^{-1}(\epsilon\tilde{\mathbf{p}}) - \tilde{\mathbf{B}}^{-1}(\epsilon\tilde{\mathbf{B}})(\tilde{\mathbf{x}} + \epsilon\tilde{\mathbf{x}})$, we can derive that

$$\|\epsilon\tilde{\mathbf{x}}\| \leq \|\tilde{\mathbf{B}}^{-1}\| \cdot \|\epsilon\tilde{\mathbf{p}} - \epsilon\tilde{\mathbf{B}}(\tilde{\mathbf{x}} + \epsilon\tilde{\mathbf{x}})\|. \quad (43)$$

According to the triangle inequality, we obtain that

$$\|\epsilon\bar{\mathbf{x}}\| \leq \phi\|\tilde{\mathbf{B}}^{-1}\| \cdot \|(\epsilon\tilde{\mathbf{p}})\| + \phi\|\tilde{\mathbf{B}}^{-1}\| \cdot \|\tilde{\mathbf{B}}\| \cdot \|\bar{\mathbf{x}} + \epsilon\bar{\mathbf{x}}\|. \quad (44)$$

Hence, we can derive that

$$\frac{\|\epsilon\bar{\mathbf{x}}\|}{\|\bar{\mathbf{x}}\|} \leq \phi\gamma \frac{\|(\epsilon\tilde{\mathbf{p}})\|}{\|\tilde{\mathbf{B}}\| \cdot \|\bar{\mathbf{x}}\|} + \phi\gamma \frac{\|\bar{\mathbf{x}} + \epsilon\bar{\mathbf{x}}\|}{\|\bar{\mathbf{x}}\|} \leq \frac{2\phi}{1-\eta}\gamma \quad (45)$$

Therefore, the proof is completed. $\square$

From the above results, the topology robustness of power system state estimation against CA is also related to γ , which depends on the transmission topology and branch parameters. A sufficiently small γ can enhance the topology robustness of the state estimation against CA. In the partially measured case, the inverse operation is replaced by the Moore-Penrose pseudoinverse. The derivation process is similar to Proposition 5.

4. Simulation Results

Here, we carry out extensive simulations to validate the derived theoretical results. The IEEE 14-bus, 30-bus, 39-bus, 118-bus, and 300-bus power systems are used to evaluate the topology robustness of the state estimation against FDIA and NPA. The MATPOWER data and settings are used by default in most scenarios. The key settings are as follows:

- Simulations are conducted on IEEE 14-, 30-, 57-, 118-, and 300-bus benchmark systems, sourced from MATPOWER's case files (e.g., case14.m). These represent varying scales: small (14-bus, 20 branches, average degree 2.86) for detailed analysis, up to large (300-bus, 411 branches, average degree 2.74) to assess scalability. Topology matrices $\tilde{\mathbf{B}}$ are derived from nominal branch parameters, with susceptances b_{ij} in per-unit (p.u.) ranging from 0.1 (long lines) to 10 (short/high-capacity lines), reflecting realistic transmission reactance values.
- Measurement Configurations: For fully measured cases, $m = 2l + n + 1$ meters include all bus injections and bidirectional branch flows. Partial measurements reduce redundancy to 1.5–2.5 (e.g., all injections plus forward flows only), ensuring observability via rank checks on $\mathbf{H}$. Sensor placements prioritize critical buses (e.g., high-degree or generator-connected) to minimize γ , with noise $\eta \sim \mathcal{N}(0, 0.01^2)$ p.u.
- Software and Computational Settings: MATPOWER 7.1 on MATLAB R2019a, with default tolerances (1×10^{-8} for convergence) and DC model flags. Runtime per system: 0.1s (14-bus) to 5s (300-bus) on a standard CPU.

4.1. Topology Robustness with Different Power Systems

Regardless of FDIA, NPA, or CA, the topology robustness of the state estimation is closely related to the parameter γ ; we compute its values with different power systems and present them in Table 1. We can see that the value of γ increases with the size of the power system. This indicates that state estimation in a larger power system is less robust to FDIA, NPA, and CA. The primary reason is that the extensive power system requires more resilient operation to withstand disturbances. The increase in γ with system size (e.g., from IEEE 14-bus to 118-bus) is indeed influenced by fundamental network properties: in larger systems, the admittance matrix $\tilde{\mathbf{B}}$ (or measurement matrix $\mathbf{H}$) tends to exhibit higher robustness due to increased connectivity (higher average node degree, leading to denser matrices with more off-diagonal elements) and greater variability in branch parameter distributions (e.g., susceptances spanning a wider range from short urban lines to long transmission lines, resulting in eigenvalues that are more spread out). This makes

the state estimation more sensitive to perturbations, as the ratio of maximum to minimum eigenvalues/singular values grows.

Table 1. The topology robustness of the power system state estimation with different power systems from MATPOWER test cases.

Power System	14-Bus	30-Bus	39-Bus	118-Bus	300-Bus
γ	121.2855	492.5221	1.3525×10^3	1.0566×10^4	7.5631×10^4

4.2. Topology Robustness with Different System Parameters

Next, we analyze the topology robustness of the state estimation against FDIA and NPA with different system parameters. Here, we take the IEEE 14-bus power system as an example. Figure 2 shows the topology of the power system. The transmission topology remains unchanged. We consider varying the branch parameters to assess the impact of FDIA and NPA on the estimation error. There are two configuration cases for the branch parameters, as shown in Table 2. The values of γ (calculated according to Proposition 3, i.e., $\gamma = \|\mathbf{B}^{-1}\| \cdot \|\mathbf{B}\|$) for these two cases are 121.2855 and 133.8930, respectively. According to the analysis in Section 3, state estimation with the system parameters in case 2 is more sensitive to changes caused by FDIA and NPA.

Table 2. Branch susceptances for two configuration cases.

Branch Number	Susceptance (Case 1)	Susceptance (Case 2)
k_1	16.90	16.90
k_2	4.48	1.35
k_3	5.05	5.05
k_4	5.67	5.16
k_5	5.75	5.75
k_6	5.85	1.75
k_7	23.74	21.37
k_8	4.78	2.87
k_9	1.80	1.80
k_{10}	3.97	3.97
k_{11}	5.03	4.68
k_{12}	3.91	3.64
k_{13}	7.68	7.68
k_{14}	5.68	1.70
k_{15}	9.09	5.45
k_{16}	11.83	11.12
k_{17}	3.70	3.70
k_{18}	5.21	1.56
k_{19}	5.00	5.00
k_{20}	2.87	2.87

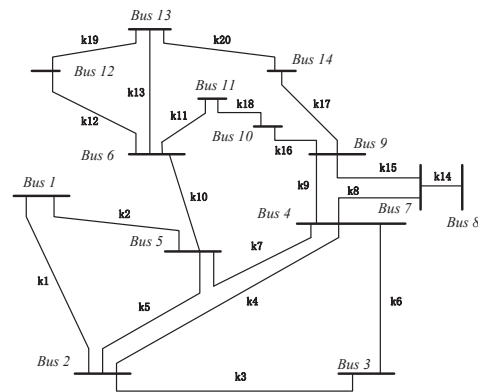


Figure 2. The IEEE 14-bus power system.

To validate further, the sensor measurements and branch parameters are randomly changed with 10 different values. The “Test” of the x-axis means these 10 trials. The bound parameters $\gamma_{\frac{\|\epsilon \tilde{\mathbf{p}}\|}{\|\tilde{\mathbf{p}}\|}}$ and $\gamma_{\frac{\|\epsilon \tilde{\mathbf{B}}\|}{\|\tilde{\mathbf{B}}\|}}$ of FDIA and NPA are shown in Figures 3 and 4. In both cases, the bound parameters for case 2 are larger than those for case 1. This indicates that the state estimation with the system parameters in case 1 is more robust than in case 2. The results are consistent with the analytical results obtained in Section 3.

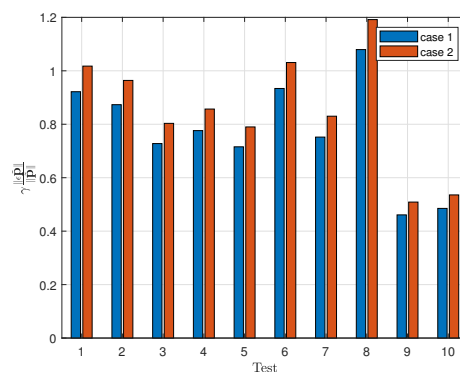


Figure 3. Upper bound parameter of the topology robustness of the power system state estimation against FDIA.

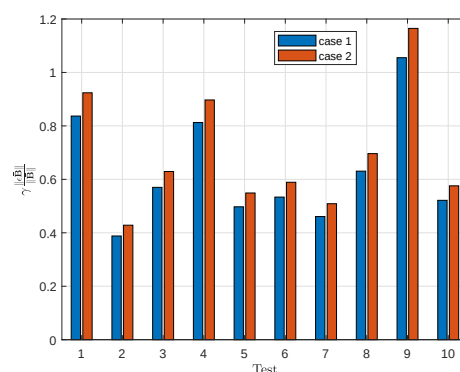


Figure 4. Upper bound parameter of the topology robustness of the power system state estimation against NPA.

Figure 5 shows the change of the estimation results with respect to the change of the sensor measurements. We can see that the relative error $\frac{\|\epsilon \mathbf{x}\|}{\|\mathbf{x}\|}$ with the system parameters in case 1 is always smaller than that with the system parameters in case 2, although the size of the injection error changes. Therefore, the value of γ determines the topology robustness of the power system state estimation against FDIA. While γ is related to the

branch parameters. Changes in branch parameters affect the topology robustness of the state estimation against FDIA.

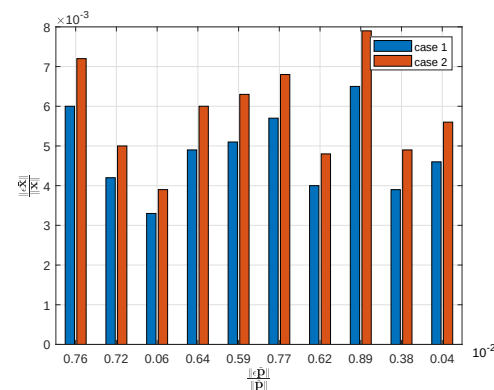


Figure 5. Topology robustness of the power system state estimation against FDIA.

Figure 6 shows the change of the estimation results with respect to the change of the branch parameter. We can see that the relative error $\frac{\|ex\|}{\|x\|}$ with the system parameters in case 1 is always smaller than that with the system parameters in case 2, although the size of the injection error of NPA changes. Therefore, the value of γ determines the topology robustness of the state estimation against NPA. While γ is related to the branch parameters. Changes in branch parameters affect the topology robustness of the state estimation against NPA.

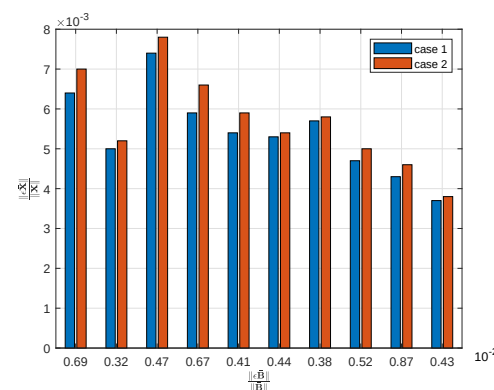


Figure 6. Topology robustness of the power system state estimation against NPA.

4.3. Topology Robustness against FDIA with the Partially Measured Cases

Next, we evaluate the topology robustness of the state estimation under partial measurement. Here, we assume that the power injections are not measured. Only the power flowing in one direction along the transmission lines is measured. Therefore, we have $\mathbf{H} = \mathbf{S}$ in this partially measured case. Considering the branch parameters given in Table 2, we can obtain that the topology robustness parameters are 21.0950 and 24.5300 for case 1 and case 2, respectively. We take the topology robustness against FDIA as a typical example. Therefore, the state estimation against FDIA is more sensitive to case 2 than to case 1. The upper bound parameter is shown in Figure 7. We observe that the bound parameter for case 2 is always larger than that for case 1. The results are consistent with the conclusions obtained in Section 3. Besides, the relative estimation error with respect to the injected measurement error is shown in Figure 8. We observe that the estimation error for case 2 is always larger than that for case 1. Therefore, the simulation results demonstrate the correctness of the analytical results provided in Section 3.

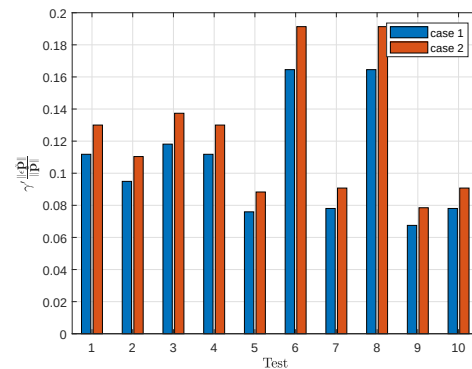


Figure 7. Upper bound parameter of the topology robustness of the state estimation against FDIA (partially measured case).

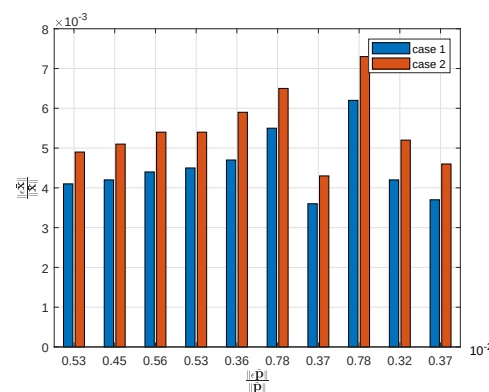


Figure 8. Topology robustness of the power system state estimation against FDIA (partially measured case).

5. Implications for Power Grid Planning and Operation

Topology Design to Reduce γ : To mitigate error amplification, grids should be designed with balanced connectivity, avoiding over-reliance on high-degree buses that increase eigenvalue spread in $\tilde{\mathbf{B}}$. For instance, modular or decentralized topologies (e.g., microgrid integrations) can lower γ by reducing matrix ill-conditioning, as shown in larger IEEE systems where denser networks elevate γ . Additionally, active perturbation of branch admittances via FACTS devices can dynamically adjust parameters to prevent attackers from exploiting fixed topologies, enhancing resilience as demonstrated in moving target defense (MTD) approaches.

Sensor Deployment to Optimize γ : Optimal placement of phasor measurement units (PMUs) should prioritize increasing redundancy in vulnerable areas (e.g., high- γ branches identified via eigenvalue analysis), ensuring observability while minimizing the condition number of $\mathbf{H}$. Strategies include graph-based algorithms for PMU allocation that protect against coordinated FDIA, such as placing PMUs at critical buses to transform unprotected measurements into secure ones. Simulations on IEEE 118-bus systems show that targeted deployments can reduce γ by up to 20–30% in partially measured scenarios.

Integrated Planning Considerations: Combine topology modifications with cybersecurity measures, such as consensus-based estimators for distributed systems under attacks, to achieve holistic robustness. For future grids with renewables, adaptive designs accounting for dynamic topologies (e.g., via temporal graph convolutional networks) are recommended to maintain low γ amid uncertainties.

6. Conclusions

This study advances the field of power system cybersecurity by providing the first comprehensive theoretical framework for quantifying topology robustness in state estimation against FDIA, NPA, and coordinated attacks. Unlike prior works that primarily focus on designing stealthy attacks or enhancing robustness through estimators, our approach derives analytical bounds (e.g., $\frac{\|\epsilon\tilde{x}\|}{\|\tilde{x}\|} \leq \gamma \cdot \frac{\|\epsilon\tilde{p}\|}{\|\tilde{p}\|}$ for FDIA) that reveal key influencing factors—sensor measurements, network topology, and branch parameters—without assuming complete attacker knowledge. This originality lies in shifting from reactive defenses to preventive insights, enabling grid planners to optimize γ (e.g., via balanced connectivity or PMU placements) for inherent resilience. Simulations on IEEE benchmarks validate these bounds, demonstrating their tightness and scalability, thus paving the way for topology-informed cyber-physical security in modern grids.

There are several limitations in this paper. First, the analysis in this paper is based on the linearized DC power flow model. While the DC model is a standard industry tool for contingency analysis and state estimation, it ignores reactive power, voltage magnitude fluctuations, and line losses. In a real-world AC environment, the nonlinear relationship between measurements and state variables could introduce complexities that the current γ factor may not fully capture. Second, the research provides a method to quantify and identify vulnerabilities (the “diagnostic” phase) but does not propose an automated, real-time mitigation algorithm to actively reconfigure the topology or sensor placement once a high-risk γ value is detected.

Author Contributions: Conceptualization, Y.Y., Y.W., F.L., M.D., S.L. and Z.Z.; methodology, Y.Y. and Z.Z.; validation, Y.Y. and Z.Z.; formal analysis, Y.Y. and Z.Z.; investigation, Y.Y. and Z.Z. resources, Y.Y. and Z.Z.; data curation, Y.Y. and Z.Z.; writing—original draft preparation, Y.Y. and Z.Z.; writing—review and editing, Y.Y. and Z.Z.; visualization, Y.Y. and Z.Z.; supervision, Z.Z.; project administration, Z.Z.; funding acquisition, Z.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Natural Science Foundation of China no. 62303126.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: Authors Yunhao Yu, Fuhua Luo, and Meiling Dicha were employed by the company Electric Power Dispatching and Control Center, Guizhou Power Grid Co., Ltd. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Kea, K.; Han, Y.; Kim, T.-K. Enhancing anomaly detection in distributed power systems using autoencoder-based federated learning. *PLoS ONE* **2023**, *18*, e0290337. [CrossRef]
2. Illera, A.G.; Vidal, J.V. Lights Off! The Darkness of the Smart Meters. 2014. Available online: http://youtube.be/Z_y_vjYtAWM (accessed on 30 December 2025).
3. Konstantinou, C.; Maniatakis, M. A case study on implementing false data injection attacks against nonlinear state estimation. In Proceedings of the 2nd ACM Workshop Cyber-Physical Systems Security Privacy (CPS-SPC), Vienna, Austria, 28 October 2016; pp. 81–91.
4. Deng, R.; Xiao, G.; Lu, R.; Liang, H.; Vasilakos, A.V. False Data Injection on State Estimation in Power Systems Attacks, Impacts, and Defense: A Survey. *IEEE Trans. Ind. Inform.* **2017**, *13*, 411–423. [CrossRef]
5. Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grid. *ACM Trans. Inform. Syst. Secur.* **2011**, *14*, 13. [CrossRef]
6. Kosut, O.; Jia, L.; Thomas, R.J.; Tong, L. Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures. In Proceedings of the IEEE 1st International Conference Smart Grid Communications (SmartGridComm), Gaithersburg, MD, USA, 4–6 October 2010; pp. 1–6.

7. Yang, Q.; Yang, J.; Yu, W.; An, D.; Zhang, N.; Zhao, W. On false data-injection attacks against power system state estimation: Modeling and countermeasures. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 717–729. [CrossRef]
8. Deng, R.; Liang, H. False data injection attacks with limited susceptance information and new countermeasures in smart grid. *IEEE Trans. Ind. Informat.* **2019**, *15*, 1619–1628. [CrossRef]
9. Zhang, Z.; Deng, R.; Yau, D.K.; Chen, P. Zero-parameter-information data integrity attacks and countermeasures in IoT-based smart grid. *IEEE Internet Things J.* **2021**, *8*, 6608–6623. [CrossRef]
10. Iranpour, M.; Narimani, M.R. AC False Data Injection Attacks in Power Systems: Design and Optimization. In Proceedings of the North American Power Symposium (NAPS), El Paso, TX, USA, 13–15 October 2024; pp. 1–7.
11. Moayyed, H.; Moradzadeh, A.; Abdeltawab, H.; Mohammadi-Ivatloo, B.; Faria, P.; Muyeen, S.M.; Vale, Z. Innovative defense strategies: Fusion deep learning approach to counter false data injection attacks in power systems. *Reliab. Eng. Syst. Saf.* **2026**, *268*, 112003. [CrossRef]
12. Wang, X.; Zhu, H.; Luo, X.; Guan, X. Data-Driven-Based Detection and Localization Framework Against False Data Injection Attacks in DC Microgrids. *IEEE Internet Things J.* **2025**, *12*, 36079–36093. [CrossRef]
13. Pramanick, N.; Mathew, J.; Selvarajan, S.; Agarwal, M. Leveraging stacking machine learning models and optimization for improved cyberattack detection. *Sci. Rep.* **2025**, *15*, 16757. [CrossRef] [PubMed]
14. Akpolat, A.N.; Kalay, M.S. Defense Mechanism of PV-Powered Energy Islands Against Cyber-Attacks Utilizing Supervised Machine Learning. *Appl. Sci.* **2023**, *15*, 5021. [CrossRef]
15. Divan, D.; Johal, H. Distributed FACTS: A new concept for realizing grid power flow control. *IEEE Trans. Power Electron.* **2007**, *22*, 2253–2260. [CrossRef]
16. Li, B.; Lu, R.; Deng, R.; Bao, H. On Feasibility and Limitations of Detecting False Data Injection Attacks on Power Grid State Estimation Using D-FACTS Devices. *IEEE Trans. Ind. Inform.* **2020**, *16*, 854–864. [CrossRef]
17. Zhang, Z.; Deng, R.; Yau, D.K. Vulnerability of the load frequency control against the network parameter attack. *IEEE Trans. Autom. Control* **2023**, *15*, 921–933. [CrossRef]
18. Zhang, Z.; Deng, R.; Tian, Y.; Cheng, P.; Ma, J. SPMA: Stealthy physics-manipulated attack and countermeasures in cyber-physical smart grid. *IEEE Trans. Inf. Forensics Secur.* **2022**, *18*, 581–596. [CrossRef]
19. Pajic, M.; Weimer, J.; Bezzo, N.; Tabuada, P.; Sokolsky, O.; Lee, I. Robustness of attack-resilient state estimators. In Proceedings of the 2014 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), Berlin, Germany, 14–17 April 2014.
20. Chakhchoukh, Y.; Ishii, H. Enhancing Robustness to Cyber-Attacks in Power Systems Through Multiple Least Trimmed Squares State Estimations. *IEEE Trans. Power Syst.* **2016**, *31*, 4395–4405. [CrossRef]
21. PLEXOS Software. Plexos Overview & Tutorial. 2019. Available online: www.plexos.info (accessed on 30 December 2025).
22. Li, F.; Wei, Y.; Adhikari, S. Improving an unjustified common practice in EX Post LMP calculation: An expanded version. In Proceedings of the IEEE Power & Energy Society General Meeting (PESGM), Minneapolis, MN, USA, 25–29 July 2010; pp. 1–4.
23. Zhang, Q.; Li, F.; Shi, Q.; Tomsovic, K.; Sun, J.; Ren, L. Profit-Oriented False Data Injection on Electricity Market: Reviews, Analyses, and Insights. *IEEE Trans. Ind. Inform.* **2021**, *17*, 5876–5886. [CrossRef]
24. Wood, A.; Wollenberg, B.; Sheblé, G.B. *Power Generation, Operation, and Control*, 3rd ed.; John Wiley and Sons: Hoboken, NJ, USA, 2013.
25. NESCOR. Electric Sector Failure Scenarios and Impact Analyses Version 3.0. 2019. Available online: <http://smartgrid.epri.com/doc/NESCOR%20Failure%20Scenarios%20v3%2012-11-15.pdf> (accessed on 30 December 2025).
26. Naderi, E.; Asrari, A. A Remedial Action Scheme To Mitigate Market Power Caused by Cyberattacks Targeting a Smart Distribution System. *IEEE Trans. Ind. Inform.* **2024**, *20*, 3197–3208. [CrossRef]
27. Sun, X.; Tang, Q.; Lu, Q. Security load frequency control model of interconnected power system based on deception attack. *PLoS ONE* **2024**, *19*, e0298889. [CrossRef] [PubMed]
28. NERC. Learned Lessons. 2019. Available online: <https://www.nerc.com/pa/rrm/ea/Pages/Lessons-Learned.aspx> (accessed on 30 December 2025).
29. Case, D.U. *Analysis of the Cyber Attack on the Ukrain Power Grid*; Electricity Information Sharing and Analysis Center: Washington, DC, USA, 2016. Available online: [http://ics.sans.org/media/E-ISAC\\$_\\$SANS\\$_\\$Ukraine\\$_\\$DUC\\$_\\$5.pdf](http://ics.sans.org/media/E-ISAC$_$SANS$_$Ukraine$_$DUC$_$5.pdf) (accessed on 30 December 2025).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.