

Residual-Evasive Attacks on ADMM in Distributed Optimization

Sabrina Bruckmeier , Huadong Mo , *Senior Member, IEEE*, and James Ciyu Qin *Member, IEEE*

Abstract—This paper presents two attack strategies designed to evade detection in ADMM-based systems by preventing significant changes to the residual during the attacked iteration. While many detection algorithms focus on identifying false data injection through residual changes, we show that our attacks remain undetected by keeping the residual largely unchanged. The first strategy uses a random starting point combined with Gram-Schmidt orthogonalization to ensure stealth, with potential for refinement by enhancing the orthogonal component to increase system disruption. The second strategy builds on the first, targeting financial gains by manipulating reactive power and pushing the system to its upper voltage limit, exploiting operational constraints. The effectiveness of the proposed attack-resilient mechanism is demonstrated through case studies on the IEEE 14-bus system. A comparison of the two strategies, along with commonly used naive attacks, reveals trade-offs between simplicity, detectability, and effectiveness, providing insights into ADMM system vulnerabilities. These findings underscore the need for more robust monitoring algorithms to protect against advanced attack strategies.

Index Terms—ADMM, Cybersecurity, Optimal Power Flow, Distributed Optimization, Data Manipulation.

I. INTRODUCTION

THE Alternating Direction Method of Multipliers (ADMM) has become a widely used optimization algorithm across various fields, including power systems, due to its scalability and effectiveness in solving large-scale, distributed optimization problems. As the adoption of ADMM continues to grow, its vulnerability to data manipulation attacks has become a significant concern. These attacks can undermine the integrity of the optimization process, potentially leading to compromised system performance and security. Consequently, there has been a growing focus on developing robust detection algorithms to identify and mitigate such threats. This section provides an overview of the most relevant detection techniques in the literature.

Alkhrajah et al. [1] introduced two detection mechanisms, Convergence Consistency (CC) and Solutions Consistency (SC), which identify data manipulation by monitoring convergence trajectories and consistency across iterations. In [2], this analysis was extended to the Auxiliary Problem Principle (APP) algorithm, proposing a neural network-based framework

trained on shared variable mismatches, highlighting the potential of data-driven approaches in distributed optimization.

Residual-based detection methods play a pivotal role for identifying False Data Injection Attacks (FDIAs). Obata et al. [3] used intermediate residuals from the ADMM process to detect attacks early by identifying sudden spikes, while Liao and Chakraborty [4] introduced the Round-Robin ADMM (RR-ADMM) algorithm, tracking spiked values to identify malicious agents. Both approaches rely on detecting abnormalities to flag malicious behavior. These mechanisms address basic attack strategies, such as naive false data injection, constant offset attacks, and random noise injection, forming a foundation for understanding ADMM’s vulnerabilities. Building on this, our work investigates how residual-based detection methods like CC and SC can be bypassed through a novel attack strategy.

Zhai et al. [5] proposed a robust optimization framework to address wind power uncertainty in integrated power and gas systems, utilizing Linear Decision Rules (LDRs) and Automatic Generation Control (AGC) to balance robustness and scalability. Similarly, Duan et al. [6] introduced a resilient DC Optimal Power Flow (DC-OPF) algorithm that combines Bayesian reputation functions with information estimation to detect and mitigate data integrity attacks. These methods highlight the need for dynamic, adaptable frameworks to handle sophisticated threats. Xu et al. [7] advanced the discussion on cyberattack resilience, demonstrating the effectiveness of Artificial Neural Network-based mechanisms to mitigate time-delay and data manipulation attacks, showcasing the potential of combining optimization techniques with machine learning to enhance security, particularly in scenarios requiring rapid response. Li et al. [8] employed federated deep learning with Transformer models to achieve high detection accuracy while maintaining data privacy.

In the broader context of machine learning applications, Xie et al. [9] reviewed advanced machine learning methods, including deep reinforcement learning (DRL), convolutional neural networks (CNNs), and ensemble learning, for tasks like stability assessment and outage prediction. They highlighted DRL’s ability to integrate perception and decision-making, while CNNs excelled in analyzing high-dimensional data for stability issues. Similarly, Tuyizere and Ihabwikuzo [10] showed that Random Forest models effectively detect and classify power system disturbances, distinguishing between natural events and cyberattacks with high accuracy. Chatterjee et al. [11] conducted a comprehensive review of cyberattacks on power systems, focusing on their mechanisms, impacts, and vulnerabilities across state estimation, AGC, energy markets,

Sabrina Bruckmeier is with the Graduate School of Mathematics, ETH Zurich, Zurich, Switzerland

Huadong Mo is with the School of Systems and Computing, University of New South Wales, New South Wales, Australia

James Qin is with the Reliability and Risk Engineering Laboratory, Institute of Energy and Process Engineering, Department of Mechanical and Process Engineering, ETH Zurich, Zurich, Switzerland

and particularly interesting for this paper voltage control. They highlighted attack strategies such as FDIA on state estimation and data integrity attacks on Load Tap Changing (LTC) transformers, Flexible AC Transmission System (FACTS) devices, and Locational Marginal Prices (LMPs). The review emphasized the challenges of detecting coordinated, well-crafted attacks and the urgent need for robust cybersecurity measures and real-time detection systems.

Unlike conventional attacks that cause detectable perturbations, our approach manipulates the system without altering the primary residual in the attacked iteration—a behavior we refer to as residual-evasive—thereby evading standard monitoring strategies. The main contributions of this paper as illustrated in Fig. 1 are three residual-evasive attacks, which underscore the vulnerability of distributed OPF algorithms.

- 1) We demonstrate that even random attack vectors can bypass residual-based detection.
- 2) We enhance the effect of random attacks by aligning them with directions orthogonal to the system’s projected trajectory, using Gram-Schmidt orthogonalization to maximize their deviation while preserving stealth.
- 3) We develop targeted residual-evasive attacks that steer the system toward specific undesirable states, with a focus on voltage control—a critical and financially incentivized function in power system operations—by exploiting vulnerabilities in the ADMM where natural fluctuations mask their effects.

The remainder of this paper is organized as follows. Section II provides background on ADMM and explains how it applies to OPF. Section III explores vulnerabilities in ADMM and introduces the notion of residual-evasive attacks, corresponding to our first contribution. Section IV presents the third and second contributions in order: we first develop targeted attacks that steer the system toward specific states, followed by optimized random attacks that maximize deviation while remaining undetected. Section V evaluates the effectiveness of the proposed strategies through a comprehensive case study on the IEEE 14-bus system. Finally, Section VI concludes the paper and discusses future research directions, including ways to strengthen ADMM against such vulnerabilities.

II. BACKGROUND

ADMM, introduced in the 1970s by Glowinski and Marocco [12] and Gabay and Mercier [13], is an optimization algorithm designed to solve large-scale convex problems. It combines the decomposability of dual ascent methods with the convergence robustness of the method of multipliers, making it suitable for distributed optimization in fields such as machine learning, signal processing, and power systems. The optimization problem it solves is formally written as

$$\min f(x) + g(z) \text{ s.t. } Ax + Bz = c \quad (1)$$

where $f(x)$ and $g(z)$ are convex functions, and x and z are optimization variables subject to linear constraints defined by A , B and c . ADMM solves this using an augmented La-

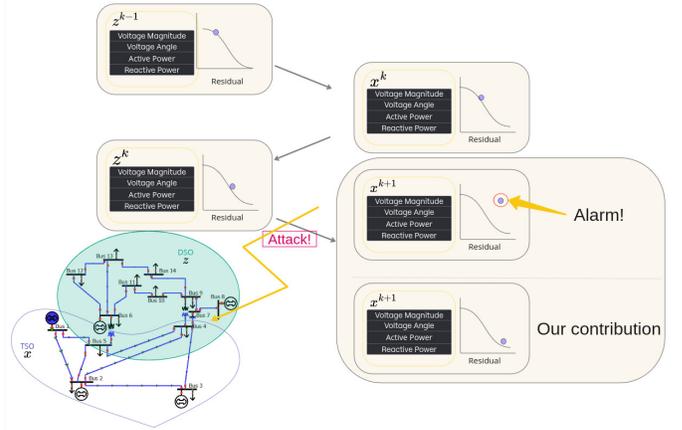


Fig. 1. Our contribution: Evasion through minimal residual changes.

grangian, introducing a penalty alongside the usual Lagrangian for constraint violations:

$$L_\rho(x, z, \lambda) = f(x) + g(z) + \lambda^T(Ax + Bz - c) + \frac{\rho}{2} \|Ax + Bz - c\|_2^2 \quad (2)$$

where λ is the dual variable (Lagrange multiplier) and $\rho > 0$ is a penalty parameter. The algorithm proceeds iteratively with updates for x , z , and λ :

Update x :

$$x^{k+1} = \arg \min_x \left(f(x) + \frac{\rho}{2} \|Ax + Bz^k - c + \lambda^k\|_2^2 \right),$$

Update z :

$$z^{k+1} = \arg \min_z \left(g(z) + \frac{\rho}{2} \|Ax^{k+1} + Bz - c + \lambda^k\|_2^2 \right),$$

Update λ :

$$\lambda^{k+1} = \lambda^k + Ax^{k+1} + Bz^{k+1} - c.$$

ADMM converges under standard conditions, ensuring that both residuals—the primary residual $r = \|Ax^k + Bz^k - c\|$ and the dual residual $s = \rho \|B^T(z^k - z^{k-1})\|$ —decrease to zero, signaling feasibility and stability. These residuals serve as indicators of the algorithm’s convergence, and when both fall below predefined tolerances, ADMM is considered to have converged. This iterative process decomposes the problem into smaller subproblems, making ADMM well-suited for distributed computing environments [14].

OPF is a key problem in power system operations, aiming to determine optimal settings for control variables like generator outputs, voltage magnitudes, and reactive power injections to minimize an objective function while meeting physical and operational constraints. Common objectives include minimizing generation costs, power losses, or emissions. OPF is crucial for ensuring efficient and reliable power system operation, particularly as the grid evolves to accommodate renewable energy sources, dynamic loads, and decentralized energy resources. The problem is inherently non-convex due to the nonlinear power flow equations, making it computationally challenging to solve, particularly for large systems. Various

formulations and solution techniques have been developed, including traditional AC-OPF and simplified DC-OPF models. Additionally, convex relaxations like semidefinite programming (SDP) and second-order cone programming (SOCP) offer computationally tractable approximations that provide near-optimal solutions. A detailed survey of these techniques is available in [15].

We apply ADMM to solve the OPF problem by decomposing it into subproblems. Leveraging the existing network structure, we divide the problem into its Transmission System Operator (TSO) and Distribution System Operator (DSO) components. The boundary buses between regions are duplicated, ensuring each TSO and DSO has its own copy of the relevant variables. Power flows through transformers are modeled differently in each region: in the TSO, power flows are treated as loads at boundary buses, while in the DSO, they are treated as generators. To ensure consistency across regions, we enforce the following equality constraints:

$$p_i = -p_{i,\text{copy}}, q_i = -q_{i,\text{copy}}, V_i = V_{i,\text{copy}}, \Theta_i = \Theta_{i,\text{copy}}$$

where p_i , q_i , V_i and Θ_i represent active power, reactive power, voltage magnitude, and voltage angle at boundary bus i in the TSO, and their counterparts $p_{i,\text{copy}}$, $q_{i,\text{copy}}$, $V_{i,\text{copy}}$ and $\Theta_{i,\text{copy}}$ represent the corresponding values in the DSO. Let x denote the vector of variables in the TSO regions:

$$x^i := \begin{pmatrix} V_i \\ \Theta_i \\ p_i \\ q_i \end{pmatrix}, \text{ for each boundary bus } i \text{ in the TSO}$$

and let z represent the corresponding variables in the DSO:

$$z^i := \begin{pmatrix} V_{i,\text{copy}} \\ \Theta_{i,\text{copy}} \\ -p_{i,\text{copy}} \\ -q_{i,\text{copy}} \end{pmatrix}, \text{ for each boundary bus } i \text{ in the DSO.}$$

This setup allows independent optimization within each region while ensuring coordination at the boundaries. For ADMM applied to OPF, we use $A = I, B = -I, c = 0$, simplifying the primary residual to $r^k = \|x^k - z^k\|$.

III. VULNERABILITIES OF THE ADMM ALGORITHM

One method to detect tampering during ADMM iterations is to monitor the residual, which decreases as the algorithm converges, with significant deviations potentially indicating interference. However, if an attacker modifies the vector z^k to $z_a^k = z^k + a$ by introducing an attack vector a , while ensuring that the residual remains unchanged, i.e.

$$\|x^k - z^k\|^2 = \|x^k - z_a^k\|^2,$$

the attack can bypass detection. The following theorem formalizes this condition. For simplicity, we may omit the superscript k when the iteration is not relevant.

Theorem 1 (Residual Evasion Criterion). *If an attack vector a satisfies the Residual Evasion Criterion*

$$a^T(a - 2(x - z)) = 0 \quad (3)$$

the residual r retains its exact numerical value when z is modified by the attack, i.e., when $z_a = z + a$.

Proof: The claim follows directly from a straightforward computation:

$$\begin{aligned} r_a^2 &= \|x - z_a\|^2 \\ &= \|x - (z + a)\|^2 \\ &= \|x - z\|^2 + \|a\|^2 - 2a^T(x - z) \\ &= \|x - z\|^2 + a^T(a - 2(x - z)) \\ &= \|x - z\|^2 = r^2. \end{aligned}$$

With the condition for undetectable attacks established, the natural question is how to construct an attack vector a that satisfies this condition. In the next section, we explore methods for identifying such vectors, addressing both feasibility and practical challenges.

A. Constructing Random Undetectable Attack Vectors

We demonstrate how to construct attack vectors a that satisfy the Residual Evasion Criterion. Starting with a initial random vector, we use orthogonal decomposition to compute the attack vectors. Orthogonal decomposition expresses a vector as the sum of two components: one within a subspace and one orthogonal to it. Formally, for a vector v and a subspace W , the decomposition is:

$$v = v_{\parallel} + v_{\perp},$$

where $v_{\parallel} \in W$ and $v_{\perp} \perp W$. This decomposition is uniquely defined and has widespread applications in optimization and numerical linear algebra [16]. This method simplifies constructing the attack vector a by splitting it into parallel and orthogonal components relative to $y = x - z$. We express $a = \lambda y + b$, where λ is a scalar, y is the parallel component, and b is orthogonal to y . To find b , we use the Gram-Schmidt orthogonalization process (for a detailed introduction refer to [16]), which ensures b is orthogonal to y by subtracting the projection of a vector c onto y :

$$c - \frac{c^T y}{y^T y} y.$$

After constructing a candidate for b , we scale it and choose λ such that the Residual Evasion Criterion is satisfied:

$$\begin{aligned} a^T(a - 2y) &= (\lambda y + b)^T(\lambda y + b - 2y) = 0 \\ \iff \|b\|^2 &= -\lambda(\lambda - 2)\|y\|^2. \end{aligned}$$

With the relationship between λ , b , and y firmly in place, we proceed with a specific example to illustrate their selection:

Proposition 1. *Setting*

$$\lambda = 1$$

and

$$b = \frac{\|y\|}{\|c - \frac{c^T y}{\|y\|^2} y\|} \left(c - \frac{c^T y}{\|y\|^2} y \right)$$

yields a vector a satisfying Theorem 1 for $y = x - z$.

Proof: We have shown that the Residual Evasion Criterion is equivalent to:

$$-(\lambda^2 - 2\lambda)\|y\|^2 = \|b\|^2.$$

For simplicity, we express b as $b = \frac{\|y\|}{\|d\|}d$, where $d = c - \frac{c^T y}{\|y\|^2}y$. Using this representation, we calculate:

$$\|b\|^2 = \left\| \frac{\|y\|}{\|d\|}d \right\|^2 = \frac{\|y\|^2}{\|d\|^2}\|d\|^2 = \|y\|^2.$$

Substituting $\|b\|^2 = \|y\|^2$ back into the Residual Evasion Criterion and setting $\lambda = 1$ confirms the condition is satisfied. Since the vector b is constructed using Gram-Schmidt, it is inherently orthogonal to $x - z$ by design. This can be easily verified with a straightforward calculation. ■

IV. GOAL-ORIENTED ATTACKS IN ADMM

In this section, we move from adding random noise to a more targeted approach: designing attacks with specific goals, such as targeting particular variables or system components, while minimizing detection risk. Building on the previous example, we adapt our methodology to achieve these objectives and demonstrate the effectiveness of these strategies in comparison with existing ones on the IEEE 14-bus system in Section V.

A. Voltage Control as A Target

Voltage control is crucial for power system stability, making it a strategic target for adversarial attacks. Network participants manage reactive power to support voltage stability and receive financial incentives for compliance. Disrupting these mechanisms can have significant economic and operational consequences. Swissgrid, Switzerland's national TSO, oversees the high-voltage transmission grid and integrates it with the European network. It developed a voltage control framework to regulate reactive power exchange among power plants, distribution networks, and end-users, aiming to reduce system losses and improve efficiency. Updated in 2020, the system incentivizes compliance through financial rewards and penalties [17]. Similar voltage control mechanisms are adopted by TSOs globally, including in Europe (e.g., TenneT, RTE, National Grid ESO), the United States (e.g., PJM, CAISO), and Asia (e.g., State Grid Corporation of China, Power Grid Corporation of India). These efforts highlight the universal necessity of voltage control for preventing equipment damage, optimizing power delivery, and maintaining stability. Swissgrid's framework incentivizes behavior within defined tolerance bands. Participants exchanging reactive power within these ranges are financially rewarded, while those outside are penalized. Active participants, like power plants, receive higher rewards, while semi-active participants, such as distribution networks and end-users, receive lower rewards. Compliance is ensured through real-time monitoring and monthly thresholds. For active participants, compensation and penalties are calculated based on the volume of reactive power exchanged and the deviation from the target voltage range, adjusted by predefined tolerance limits. Semi-active participants have a similar structure but include a free exchange zone around zero, where no

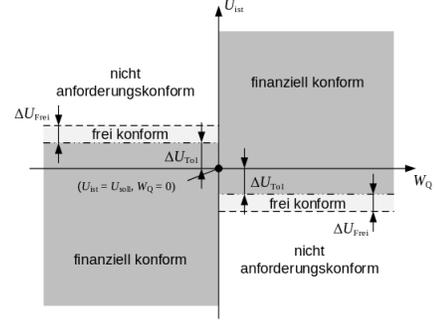


Fig. 2. Voltage control for active role. U_{ist} is the actual voltage and U_{soll} is the target voltage at the feed-in node. ΔU_{Tol} is the billing tolerance, and ΔU_{Frei} is the free conformity band. W_Q is the net reactive power exchange for the quarter-hour. The left side represents capacitance-like behavior (delivering reactive power), while the right side represents inductance-like behavior (consuming reactive power). Source: Swissgrid [17]

charges apply. The tariff model is recalibrated annually based on historical data and projected costs, ensuring transparency and alignment with operational requirements [18]. Fig. 2 illustrates compliance zones:

- Financially Compliant Zone (finanziell konform): Within this tolerance (ΔU_{Tol}), reactive power exchanges are rewarded. The tolerance values are set at 1 kV for the 220-kV level and 2 kV for the 380-kV level.
- Free Compliant Zone: Beyond the compliant zone, within an additional tolerance (ΔU_{Frei} , set at 1 kV for both voltage levels), exchange is neither compensated nor penalized. This zone allows technical flexibility but is not incentivized as it does not actively support the system.
- Non-Compliant Zone: Exchanges outside the free zone incur penalties for failing to meet stability requirements.

In this section, we manipulate the set of variables $\{z_4^i : i \in \mathfrak{A}\}$, where \mathfrak{A} represents the targeted boundary buses to influence financial rewards. The attacker uses a dual-pronged strategy targeting both voltage and reactive power at a boundary bus. The goal is to minimize payment by reducing $|z_4^i|$ while subtly pushing the network towards the voltage boundary for a brief period. This calculated maneuver leverages the natural fluctuations in the ADMM algorithm, which reduces the likelihood of detection. Simultaneously, the attack magnitude is kept small and the Residual Evasion Criterion is satisfied, both to avoid triggering alarms and to maintain the system's perceived stability. This can be formalized as:

$$\min \|a\|^2 + \sum_{i \in \mathfrak{A}} |z_4^i + a_4^i| \quad (4)$$

$$\text{s.t. } z_1^i + a_1^i - V_u \geq 0 \quad \forall i \in \mathfrak{A}, \quad (5)$$

$$a^T(a - 2y) = 0. \quad (6)$$

where $z_1^i = V_i$, $z_4^i = -q_i$ and V_u is the upper voltage limit. The objective (4) minimizes the attack magnitude and payment, while (5) pushes the system to the upper voltage boundary, and (6) is the Residual Evasion Criterion. While the voltage peak may seem suspicious, we show that the final

voltage values remain well within the acceptable range. Furthermore, such transient peaks during the iterative computation process are entirely normal and can occur even in the absence of attacks. While our focus has been on the primal residual, the secondary residual can also indicate an attack. However, significant deviations in the secondary residual are rare when the primary residual remains unaffected. Nonetheless, if the attacker wishes to exercise additional caution, it is straightforward to incorporate safety measures into the optimization problem, for instance adding a constraint to ensure that the secondary residual does not exceed the average of the previous three iterations. Notably, the problem defined by (4)–(6) can be efficiently addressed using standard off-the-shelf solvers.

B. Random Attacks with Maximum Deviation

Building on the previous section, we now examine the rationale behind setting λ and b as defined in Proposition 1, and explore how to construct attack vectors that maximize their disruptive impact. Rather than injecting arbitrary perturbations, a carefully designed attack can exploit the system's vulnerabilities while remaining undetected. By leveraging the orthogonal component b , we ensure that the attack influences the system in directions that significantly deviate from its expected trajectory, amplifying its disruptive effect. The equation $\|b\|^2 = -(\lambda - 1)^2\|y\|^2 + \|y\|^2$ is a direct consequence of the Residual Evasion Criterion and highlights the trade-off between λ and b , where maximizing one requires minimizing the other. Setting $\lambda = 1$ maximizes the norm of the orthogonal component b , which can be computed using Gram-Schmidt and a random vector c :

$$b = \frac{\|y\|}{\|c - \frac{c^T y}{\|y\|^2} y\|} \left(c - \frac{c^T y}{\|y\|^2} y \right).$$

Rather than using a random c , a more sophisticated attack explicitly defines a and finds a suitable c to construct b . By choosing c already orthogonal to $x - z$, we simplify:

$$a = \lambda(x - z) + b = (x - z) + \frac{\|x - z\|}{\|c\|} c.$$

Rewriting this component-wise and squaring both sides yields:

$$\frac{c_j^2}{\|c\|^2} = \frac{(a_j - x_j + z_j)^2}{\|x - z\|^2}.$$

If $a_j = x_j - z_j$, then $c_j = 0$, but $c \neq 0$ must hold by definition of a . For simplicity, we assume $a_j \neq x_j - z_j$ for $j = 1, \dots, 4n$ where n is the number of boundary buses. If this condition does not hold, the same reasoning applies to a subsystem containing only the subvector of c where $c_j \neq 0$. Rearranging the terms results in:

$$\left(1 - \frac{\|x - z\|^2}{(a_j - x_j + z_j)^2} \right) c_j^2 + \sum_{\substack{i=1 \\ i \neq j}}^{4n} c_i^2 = 0.$$

With a slight abuse of notation, define $A \in \mathbb{R}^{4n \times 4n}$ such that $A_{ij} = d_i$ if $i = j$ and 1 if $i \neq j$, $y := x - z$, $d_i := 1 - \frac{\|y\|^2}{(a_i - y_i)^2}$ and $c^2 := (c_1^2, \dots, c_{4n}^2)^T$, we arrive at the following theorem:

Theorem 2. *If there exists a vector c such that:*

$$c^T y = 0, \quad A c^2 = 0, \quad c \neq 0$$

then it is possible to define an attack $a := y + \frac{\|y\|}{\|c\|} c$ that satisfies the Residual Evasion Criterion (Theorem 1).

Next, we determine when this system is solvable.

Theorem 3. *It is possible to define an attack $a := y + \frac{\|y\|}{\|c\|} c$ satisfying the Residual Evasion Criterion if for $j = 1, \dots, 4n$ the signs of $c_j := \pm \frac{a_j - y_j}{\|y\|}$ can be chosen such that $c^T y = 0$.*

Before proving this, we introduce two helpful lemmas. Let e denote the all-one vector of appropriate size.

Lemma 1. *For a matrix $A \in \mathbb{R}^{n \times m}$ there exists an x satisfying*

$$A x = 0, \quad x \geq 0, \quad x \neq 0 \quad (7)$$

if and only if there exists a y such that

$$A y = 0, \quad y \geq 0, \quad e^T y = 1. \quad (8)$$

Proof: Assume x^* solves (7) and set $y^* := \frac{x^*}{e^T x^*}$. Then

$$A y^* = A \frac{x^*}{e^T x^*} = \frac{1}{e^T x^*} A x^* = \frac{1}{e^T x^*} 0 = 0.$$

Since $x^* \geq 0$ it follows that $y^* \geq 0$. Additionally, $e^T y^* = 1$. Thus y^* satisfies (8). Conversely, if y^* solves (8), then $y^* \neq 0$ because $e^T y^* = 1$ and y^* is also a solution to (7). ■

We now proceed to the second lemma.

Lemma 2. *Let $A \in \mathbb{R}^{n \times n}$ be a matrix defined by*

$$A_{ij} = \begin{cases} d_i, & \text{if } i = j, \\ 1, & \text{if } i \neq j. \end{cases}$$

There exists a vector x satisfying (7) if and only if $d_j < 1$ for $j = 1, \dots, n$ and

$$\sum_{i=1}^n \frac{1}{1 - d_i} = 1.$$

Additionally, the solution is $x_j = \frac{1}{1 - d_j}$ for $j = 1, \dots, n$.

Proof: By Lemma 1 such an x exists if and only if there is a y satisfying (8). We show that these conditions hold for $y_j^* := \frac{1}{1 - d_j}$ for $j = 1, \dots, n$. It is straightforward to verify that y^* is also a solution to (7). Since $d_j < 1$, we have $y^* \geq 0$. Moreover, $e^T y^* = \sum_{i=1}^n \frac{1}{1 - d_i} = 1$. Now for $A y^*$

$$(A y^*)_j = d_j y_j^* + \sum_{\substack{i=1 \\ i \neq j}}^n y_i^* = d_j y_j^* + \sum_{i=1}^n y_i^* - y_j^* = 0.$$

Conversely, assume feasibility and let y^* satisfy (8). From $A y^* = 0$ and $e^T y^* = 1$ we immediately get $y_j = \frac{1}{1 - d_j}$. Since $y \geq 0$ this implies $d_j < 1$. Finally, $1 = e^T y^*$ gives $\sum_{i=1}^n \frac{1}{1 - d_i} = 1$ completing the proof. ■

We are now prepared for the proof of Theorem 3.

Proof: First, we note that the subsystem

$$A c^2 = 0 \\ c \neq 0$$

is, due to the square, equivalent to system (7). According to Lemma 2 this system is feasible if and only if $d_j < 1$ for $j = 1, \dots, n$ and $\sum_{i=1}^n \frac{1}{1-d_i} = 1$. Since $d_j = 1 - \frac{\|y\|^2}{(a_j - y_j)^2}$ and $a = y + \frac{\|y\|}{\|c\|}c$, we immediately conclude that $d_j < 1$ because $y \neq 0$. Rearranging the terms in the definition of the attack vector a gives the second condition:

$$\|a - y\|^2 = \left\| \frac{\|y\|}{\|c\|}c \right\|^2 = \frac{\|y\|^2}{\|c\|^2} \|c\|^2 = \|y\|^2$$

and hence,

$$\sum_{i=1}^n \frac{1}{1-d_i} = \sum_{i=1}^n \frac{(a_i - y_i)^2}{\|y\|^2} = \frac{1}{\|y\|^2} \|a - y\|^2 = \frac{\|y\|^2}{\|y\|^2} = 1.$$

Therefore, following Lemma 2, we obtain the unique solution

$$c_j^2 = \frac{1}{1-d_j} = \frac{(a_j - y_j)^2}{\|y\|^2}$$

and consequently,

$$c_j = \pm \frac{a_j - y_j}{\|y\|}.$$

This means that if we can adjust the signs of c_j such that $c^T y = 0$, we have identified a vector c that satisfies the system in Theorem 2. As a result, this constructs an attack vector a that avoids detection by monitoring ADMM residuals. ■

V. SIMULATION RESULTS

We conclude by demonstrating the effectiveness of our proposed attack strategies on the IEEE 14-bus system. First, we describe the experimental setup, followed by a detailed analysis of the results, examining how various parameters influence both the stealth and impact of the attacks.

A. Experimental Setup

The IEEE 14-bus test case, a simplified representation of the American Electric Power system as of February 1962, consists of 14 buses, 5 generators, and 11 loads, offering a practical model for analyzing power systems. Further details about the test case, including system configuration and parameters, can be found in [19]. We partition the IEEE 14-bus network into a TSO part and a DSO part with the boundary defined at Bus 4 and Bus 5. Hence, duplicate Bus 4 and Bus 5, such that TSO and DSO both have their own copies to facilitate independent modeling. Then remove the transformers that originally connected the regions (i.e., transformers connecting Buses 5-6, 4-9, and 4-7). In the TSO network the power flows through these transformers are added to the loads at Buses 4 and 5, respectively. In the DSO network, generators are introduced at Buses 4 and 5 to represent the power flows coming from the TSO. A visual representation is provided in Fig. 3. Lastly, we assume an upper voltage limit of 1.1 p.u. and a lower voltage limit of 0.9 p.u.

We systematically evaluate several scenarios to investigate the impact and secrecy of different attack strategies. We start with naive attacks where a fixed percentage is added during a single iteration. We compare these simplistic attacks against the strategy described in Section III-A explicitly focusing on

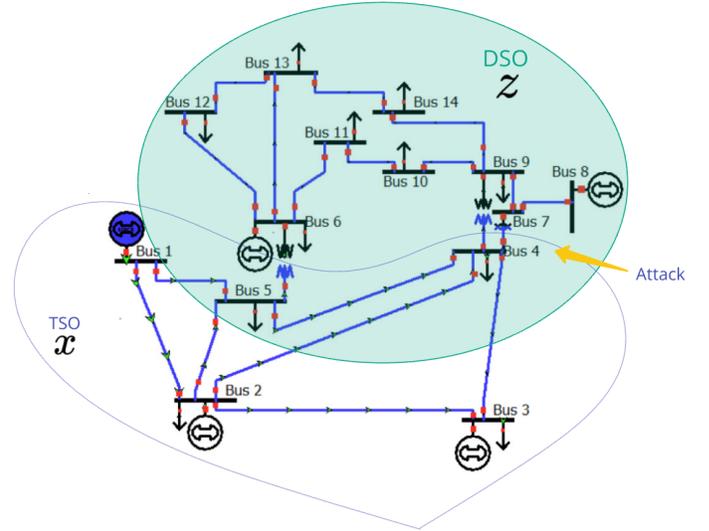


Fig. 3. IEEE 14-bus test case and the split in TSO and DSO.

Random Attacks with Maximum Deviation, i.e. Proposition 1. Finally, we turn our attention to the optimized attack vectors derived from problem (4) - (6), assessing their ability to balance stealth and effectiveness. The attacks are restricted to boundary buses by design, with Bus 4 consistently chosen as the target for controlled comparison across strategies. Each experiment involves a single attack during the ADMM calculation process to isolate its impact on system stability and performance. It is important to note that more powerful attacks could be devised by repeated targeting, increasing instability and manipulation. However, for the purposes of this study, we focus on single-step attacks to better understand their individual characteristics and detectability.

In the clean scenario, i.e., without cyber-attacks, the ADMM algorithm converges after 214 iterations. To evaluate the impact of attacks, we examine injections at different iterations. A complete list of attack scenarios can be found in Table I. To enhance reproducibility, we have also documented the specific attack vectors used in Table II in the Appendix. The attack vector refers to the perturbation introduced in an attacked iteration k , modifying the variable z^k as $z_a^k = z^k + a$. The random vectors are generated using Python `numpy.random.rand()`, which produces random numbers sampled from a uniform distribution over the interval $[0, 1)$.

B. Results

The financial reward depends on the total absolute reactive power at the boundary buses. Fig. 4 shows this value across scenarios, with a column plot for mean values and a boxplot for distribution. In most cases, the mean equals the attack value, except for attacks from Proposition 1, where the starting point is randomized. To account for variability, we averaged 10 trials. In the clean scenario, about 0.4 VAR per unit is generated, covered by the TSO. Naive attacks struggle to balance impact and stealth; even a 50% reduction in Scenario 13 has a smaller effect than Proposition 1. The sharp drop in reactive

TABLE I. Attack scenarios at select iterations on boundary bus 4 of TSO (x) or DSO (z).

Scenario	Type	Iteration	Atk. variable
1	Clean	-	-
2	+10% in q	3	x
3	+3.5% in q	3	x
4	-10% in q	3	x
5	-3% in q	3	x
6	+5% in q	210	x
7	+3.5% in q	210	x
8	+50% in q	3	z
9	+100% in q	3	z
10	+150% in q	3	z
11	+250% in q	3	z
12	+3% in q	3	z
13	-50% in q	3	z
14	+10% in V , -25% in q	3	z
15	+10% in V , +50% in Θ , +20% in p , -25% in q	3	z
16	+5% in q	210	z
17	+3% in q	210	z
18 - 27	Proposition 1	3	z
28 - 37	Proposition 1	20	z
38 - 47	Proposition 1	50	z
48 - 57	Proposition 1	100	z
58 - 67	Proposition 1	150	z
68 - 77	Proposition 1	210	z
78	Problem (4) - (6)	3	z
79	Problem (4) - (6)	20	z
80	Problem (4) - (6)	50	z
81	Problem (4) - (6)	100	z
82	Problem (4) - (6)	150	z
83	Problem (4) - (6)	210	z

power at boundary bus 4 further underscores the limitations of such simple strategies (Fig. 5). Fig. 4 illustrates the influence of attack timing. The effectiveness of both the random undetectable attack (Proposition 1) and the optimization problem (4)–(6) varies depending on the iteration at which the attack is applied. A clear trend emerges: later-stage attacks tend to have a weaker impact. This is due to Theorem 1, which depends on the distance between x and z , decreasing as the algorithm converges. This effect is especially pronounced in Proposition 1, where its influence diminishes beyond a certain iteration. In contrast, the optimization approach exhibits greater resilience, sustaining a more distributed impact across iterations, albeit still influenced by attack timing. Depending on the random starting point, Proposition 1 can be more or less effective than the optimization problem (4)–(6) or the naive attacks in the first 17 scenarios. Its key advantage is higher stealth while still achieving meaningful impact in many cases. Some random starting points may outperform the optimization approach, as the latter only approximates shifting the optimal power flow solution in a favorable direction. Scenario 22, a lower outlier in the boxplot, demonstrates that we have not identified the true optimal solution for the manipulated optimal power flow problem, as finding this solution would be excessively complex and computationally infeasible within a reasonable timeframe.

Fig. 6 illustrates the primary residual for selected attack scenarios within the first 10 iterations. For randomized attacks, the mean residual (dark blue) is shown with individual scenarios (light blue) and a ± 1 standard deviation shaded region. Colors indicate attack types as per the legend. This

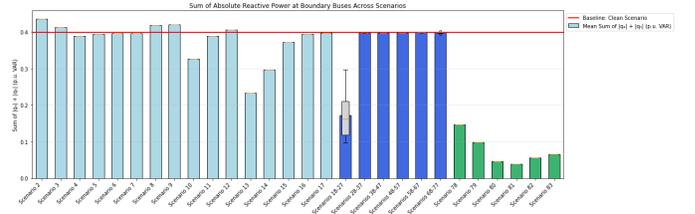


Fig. 4. Financial impact of the attacks.

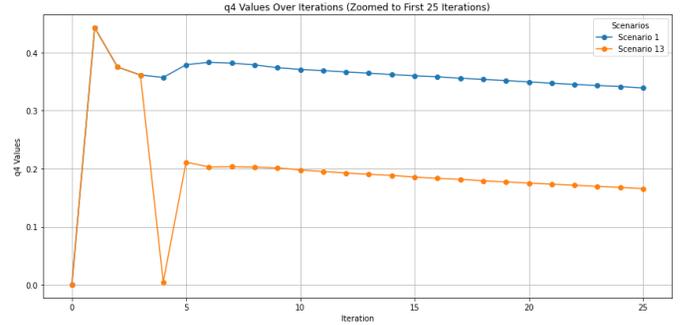


Fig. 5. Reactive power at boundary bus 4 during ADMM, depicting a notable drop under attack.

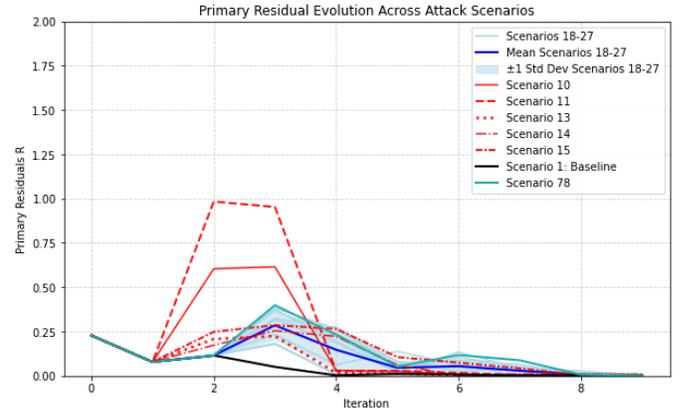


Fig. 6. Zoomed-in view of the primary residual, highlighting noticeable peaks in naive attacks.

figure highlights a key flaw of the simple attacks: they fail to control the residual, causing detectable peaks. In contrast, our approach generates significantly smaller peaks that blend with normal fluctuations, making detection more difficult. Similarly, Fig. 7 illustrates the trade-off between stealth and effectiveness. While random undetectable attacks (Scenarios 58–68) had little impact in Fig. 4, their residual effects are nearly imperceptible. Note the plot's small scale necessary to even visualize these changes, which closely resemble the clean scenario (Scenario 1). Such attacks are valuable when stealth is paramount, enabling prolonged evasion of detection or subtle manipulation of system dynamics without raising alarms.

Beyond residual monitoring, one might consider other ADMM parameters for attack detection, such as computation time or iteration count. However, as Fig. 8 and Fig. 9 show, these metrics remain remarkably stable across all attacks,

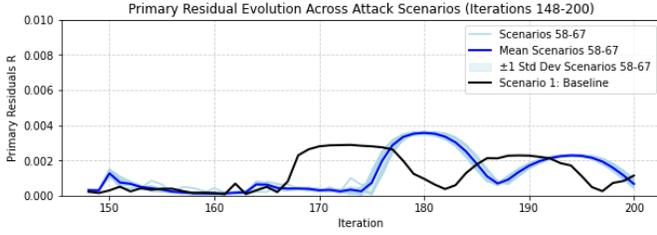


Fig. 7. Zoomed-in view of the primary residual, demonstrating the stealth of the proposed attack.

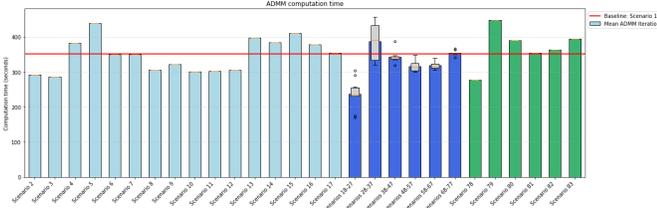


Fig. 8. Stable ADMM computation time provides cover.

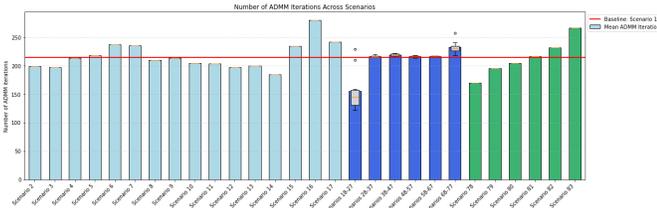


Fig. 9. Consistency in ADMM iterations obscure detection.

providing a convenient cover. Attacks can effectively hide behind this stability, as their impact on these parameters is either negligible or, in some cases, even reduces iterations and computation time—though not enough to raise suspicion. While certain attacks are designed to explicitly disrupt these parameters, the ones studied here exploit their consistency to remain undetected.

While ADMM convergence is typically assessed using both the primal and dual residuals, our approach emphasizes the primal residual. This focus is justified, as the dual residual—although not directly controlled—in most cases remains within typical ranges and does not exhibit significant deviations that would undermine the reliability of the method, particularly in comparison to naive attack strategies. This observation is supported by Fig. 10, which also reveals that the dual residual often exceeds the primal residual. We focus on the first 10 iterations, where residual fluctuations are most pronounced before stabilizing. In a similar fashion as before, for Scenarios 18–27, the mean and ± 1 standard deviation highlight the variability of randomized attacks.

Detecting attacks within the network itself, rather than through ADMM monitoring, is another potential approach. Voltage safety bounds are set at 1.1 and 0.9 p.u., yet Fig. 11 shows that even under random attacks, the system remains stable with no significant disturbances. This robustness provides a strategic advantage for an attacker, as it allows manipulations to remain concealed within normal operating

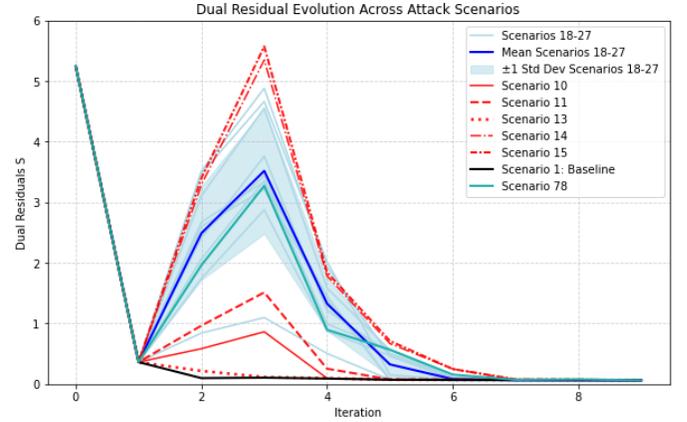


Fig. 10. Zoomed-in dual residual, illustrating the advantage over naive strategies.

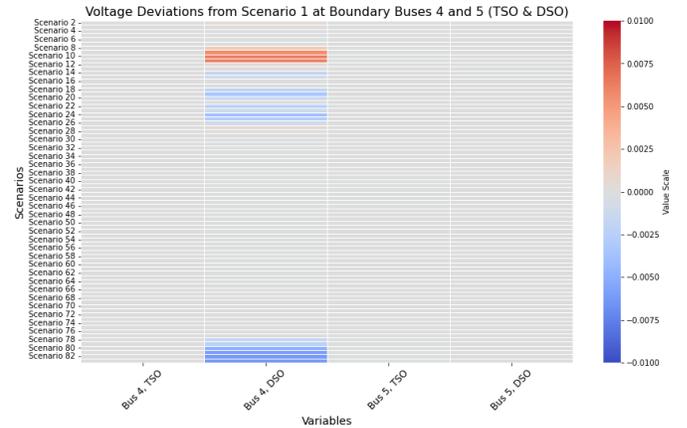


Fig. 11. Heatmap of voltage deviations from the baseline, showing system stability and the potential to conceal attacks.

conditions. Interestingly, our optimization-based attack (4)–(6) not only evades detection but even contributes to system stability, all while generating substantial financial gains for one party. Voltage deviations remain minor across all attack scenarios, ensuring the system stays within the financially favorable range, even with substantial Q adjustments. Also on the network level, measuring balancing errors is a potential strategy for attack detection. In the context of optimal power flow, balancing errors are defined as the discrepancies between the computed power injections and the network’s actual power demands. These errors emerge when the sum of generated power, minus the loads and network losses, fails to achieve the ideal condition of zero balance. However, our results in Fig. 12 show that the deviation of the balancing errors from the baseline remain minimal across all attack scenarios. This reinforces how the network’s inherent stability can be leveraged by attackers to conceal their actions.

VI. CONCLUSION

In this paper, we designed two attack strategies that effectively evade detection by avoiding changes to the primary residual in the attacked iteration. Since many monitoring

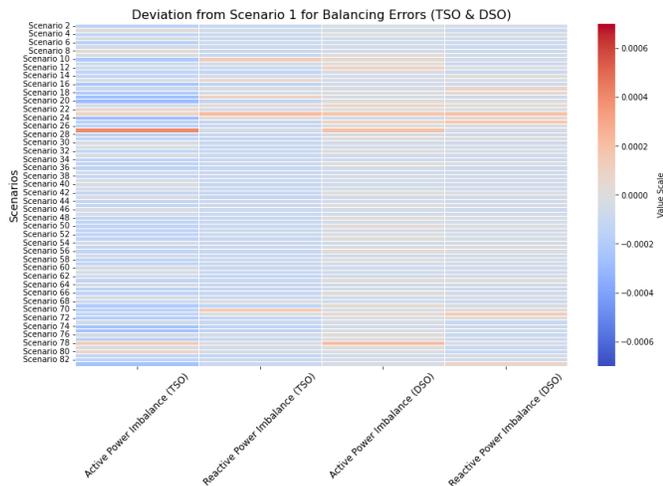


Fig. 12. Heatmap of differences from baseline balancing errors, showcasing how attackers can exploit system stability.

algorithms rely on residual analysis, this approach enables the attacks to bypass standard detection mechanisms.

The first strategy uses a random starting point combined with Gram-Schmidt orthogonalization to ensure stealth. This approach can be refined by emphasizing the orthogonal component to maximize the disruption in the system. The second strategy extends the first one by allowing to target financial gains by simultaneously attacking reactive power and pushing the system to its upper voltage limit, exploiting the boundaries of operational constraints. An in-depth analysis and comparison of the two strategies highlighted the trade-offs between simplicity, detectability and effectiveness, providing valuable insights into the vulnerabilities of ADMM-based systems and the mechanisms by which they can be exploited. These findings emphasize the importance of designing more robust monitoring algorithms to protect against sophisticated attack strategies.

Future research could build on the foundation established in this paper by exploring attacks that target multiple buses or span multiple iterations. Coordinated strategies could leverage gradual, iterative adjustments to steer the system toward a desired state while remaining undetected. Additionally, while this paper employs a strict Residual Evasion Criterion to ensure stealth, future work could investigate the potential for relaxing this condition under practical assumptions, enabling the design of more adaptable and impactful attack strategies. These extensions would complement the findings of this study and contribute to a deeper understanding of system vulnerabilities. We conclude by noting that in Scenario 81, the total absolute reactive power remains nearly constant, yet boundary buses 4 and 5 show significant shifts, including sign changes. This suggests potential directions for future attack strategies to expand the scope of this study.

In detection, many strategies focus on singular aspects, like monitoring residuals. However, a more robust algorithm could integrate multiple detection mechanisms. For example, in addition to residuals, analyzing changes in voltage, active power, and reactive power during ADMM iterations could help

identify spikes indicative of an attack. This approach was exemplified in Fig. 5, where a naive attack left the residual unchanged but caused clear peaks in other parameters. Implementing multifaceted detection, however, presents challenges. Balancing false positives and false negatives is crucial, as setting the right threshold for detecting peaks is key to avoiding missed attacks without overloading the system. As detection strategies become more complex, careful calibration is needed to balance sensitivity and accuracy. Machine learning-based methods also offer promising potential for attack detection. Research, such as [20] and [21], shows how these techniques can detect patterns missed by traditional methods, providing an extra layer of security. Combining these methods with the insights from this paper could lead to a more resilient ADMM framework.

ACKNOWLEDGMENTS

The authors express their gratitude to Swissgrid for their support in this research. They extend special thanks to Ambra Toletti and Raphael Wu for their insightful discussions and valuable feedback, which greatly contributed to this work.

APPENDIX

TABLE II. Attack Vector Values

Scenario	Attack Vector
18	[0.02121068 0.0130993 0.12314844 0.0864099]
19	[0.07341862 0.06317238 0.11244587 0.03505106]
20	[0.05369313 0.00871949 0.12110739 0.07501809]
21	[0.01541827 0.07886334 0.11617012 0.05745474]
22	[0.06255644 0.01532933 0.11979587 0.06895177]
23	[0.05273261 0.09606387 0.10602196 0.00201061]
24	[0.06933667 0.02945763 0.11788314 0.06067893]
25	[0.04830191 0.05887625 0.11715014 0.06107415]
26	[0.01850385 0.08056118 0.11569358 0.05510166]
27	[0.03478083 0.10240982 0.10712628 0.00895416]
28	[6.52923e-05 1.11296e-04 9.81143e-05 -1.25645e-04]
29	[8.28166e-05 1.71912e-05 1.57168e-04 -1.01030e-04]
30	[2.33227e-05 9.23689e-05 1.45938e-04 -1.08116e-04]
31	[6.57201e-05 9.67342e-05 1.21174e-04 -1.17061e-04]
32	[1.17634e-04 7.47446e-05 6.61172e-05 -1.35156e-04]
33	[8.55322e-05 8.13466e-05 1.20480e-04 -1.16682e-04]
34	[8.27203e-05 8.71954e-05 1.16819e-04 -1.18198e-04]
35	[3.01434e-06 7.89714e-05 1.58809e-04 -1.02943e-04]
36	[5.52432e-05 1.04791e-04 1.18457e-04 -1.18312e-04]
37	[1.28545e-04 4.18002e-05 8.94557e-05 -1.25657e-04]
38	[0.00033554 0.00060707 0.00127095 0.00013236]
39	[6.06571e-04 4.56323e-04 1.23767e-03 7.72225e-05]
40	[0.0001615 0.00090441 0.00112068 -0.00011829]
41	[0.0004926 0.00083299 0.00106443 -0.00021075]
42	[0.00025234 0.00065363 0.00126768 0.00012666]
43	[8.81615e-04 3.67449e-05 1.15372e-03 -6.53645e-05]
44	[5.56211e-04 5.30295e-04 1.23234e-03 6.85818e-05]
45	[0.00024766 0.00066986 0.00126115 0.00011582]
46	[6.42585e-04 6.34219e-04 1.13597e-03 -9.14259e-05]
47	[0.00028043 0.00027531 0.00136882 0.00029301]
48	[1.10091e-04 7.24838e-05 -4.05319e-05 -1.30556e-04]
49	[7.70328e-05 1.04375e-04 -1.01420e-04 -9.45919e-05]
50	[3.68833e-05 1.29133e-04 -8.66583e-05 -1.02549e-04]
51	[4.36177e-05 1.26842e-04 -4.52692e-05 -1.26574e-04]
52	[8.86995e-05 1.02790e-04 -6.93971e-05 -1.13192e-04]
53	[7.31012e-05 9.23426e-05 -8.29755e-06 -1.48735e-04]
54	[1.51510e-05 8.37389e-05 2.48265e-05 -1.67940e-04]
55	[5.45215e-05 1.22520e-04 -8.69528e-05 -1.02553e-04]
56	[9.88206e-05 8.50837e-05 -3.48270e-05 -1.33582e-04]
57	[1.14445e-04 6.52528e-05 -4.08441e-05 -1.30529e-04]

Continued on next page...

Scenario	Attack Vector
58	[1.52442e-04 6.38828e-05 2.64114e-04 -1.48861e-04]
59	[0.00013494 0.00018196 0.00018477 -0.00018379]
60	[2.31975e-04 5.33502e-05 1.48807e-04 -2.01080e-04]
61	[0.00010482 0.00014033 0.00025586 -0.00015195]
62	[1.73608e-04 3.61746e-05 2.53083e-04 -1.54066e-04]
63	[1.47308e-05 1.81783e-04 2.49261e-04 -1.54410e-04]
64	[1.91624e-04 9.71710e-05 2.06146e-04 -1.74863e-04]
65	[1.72501e-04 7.49430e-05 2.42232e-04 -1.58701e-04]
66	[0.00010181 0.00021101 0.00016562 -0.00019213]
67	[1.41356e-04 5.52496e-05 2.74632e-04 -1.44149557e-04]
68	[8.19125e-05 4.59841e-04 1.08182e-03 5.64933e-04]
69	[0.00060425 0.00040423 0.0010303 0.00034295]
70	[0.00050432 0.00034494 0.00105841 0.0004627]
71	[0.00075692 0.0002196 0.00101032 0.00025642]
72	[5.461385e-05 3.43557e-04 1.09533e-03 6.21999e-04]
73	[0.00035637 0.00059902 0.00103831 0.00037914]
74	[4.72707e-04 9.57743e-05 1.08032e-03 5.54913e-04]
75	[5.74563e-04 7.05504e-04 9.36370e-04 -5.47820e-05]
76	[0.00025254 0.00075649 0.00100612 0.00024358]
77	[0.00073719 0.00054561 0.00092492 -0.00010501]
78	[0.06150997 0.0029498 0.08841819 -0.10452701]
79	[6.02433e-02 -6.51130e-06 4.28351e-05 -4.23917e-02]
80	[5.78314e-02 4.18136e-06 8.05939e-04 -4.40490e-02]
81	[5.66638e-02 2.08856e-06 -6.12412e-05 -4.42714e-02]
82	[5.64804e-02 1.22251e-06 9.13973e-05 -4.44684e-02]
83	[5.64435e-02 -2.77430e-09 9.01191e-04 -4.44423e-02]

End of table.

Sabrina Bruckmeier is a Ph.D. student in discrete optimization at ETH Zurich. She holds a Bachelor's degree in Industrial Mathematics, which combines Electrical Engineering, Computer Science, and Mathematics, as well as a Master's degree in Mathematics with honors from Friedrich Alexander University Erlangen-Nürnberg. Her research focuses on robust optimization in power systems, sparse approximation in signal processing and machine learning, and flows over time in hypergraphs. Sabrina's interests include mathematical optimization, algorithm design, and cybersecurity in critical infrastructure.

Dr. Huadong Mo is a Senior Lecturer at the University of New South Wales in Australia and Coordinator of the Systems Engineering Discipline within the School of Systems and Computing. Previously, he was a Postdoctoral Fellow at the Swiss Federal Institute of Technology, Zurich. He earned his Ph.D. from the City University of Hong Kong. His research focuses on enhancing the reliability, resilience, and security of complex systems using learning-based algorithms, with applications in power systems, cyber-physical systems, and manufacturing. He has published over 80 SCI-indexed papers and secured approximately 5 million AUD in research funding. A recipient of the 2024 IEEE SMC Early Career Award—the fourth since its inception—Dr. Mo was also awarded the 2023 Visiting Research Fellowship (Pre-award of the Jean d'Alembert Pour Fellowship) in France. He is a Senior Member of IEEE, Chair of the IEEE SMC ACT Chapter, and serves on the editorial boards of multiple SCI-indexed journals.

James Ciyu Qin received a BE (Hons) degree in Mechanical and Manufacturing Engineering and a PhD in Systems Engineering from the University of New South Wales, Australia, in 2019 and 2024, respectively. He is currently a Postdoctoral Researcher at the Reliability and Risk Engineering Laboratory, Institute of Energy Technology, ETH Zürich, Switzerland. His primary research focuses on enhancing the resilience, performance, and security of complex systems through various robust optimisation techniques. His research interests include developing preventive and corrective procedures that account for the risk of system failures and providing risk-aware prevention measures for resilience enhancement.

REFERENCES

- [1] M. Alkhrajah, R. Harris, S. Litchfield, D. Huggins, and D. K. Molzahn, "Detecting shared data manipulation in distributed optimization algorithms," *arXiv preprint arXiv:2310.13252*, 2023. [Online]. Available: <https://arxiv.org/pdf/2310.13252>
- [2] —, "Analyzing malicious data injection attacks on distributed optimal power flow algorithms," *2022 North American Power Symposium (NAPS)*, pp. 1–6, 2022. [Online]. Available: <https://api.semanticscholar.org/CorpusID:244135751>
- [3] S. Obata, K. Kobayashi, and Y. Yamashita, "Detection of false data injection attacks in distributed state estimation of power networks," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E106-A, no. 5, pp. 729–735, 2023. [Online]. Available: <http://hdl.handle.net/2115/90179>
- [4] M. Liao and A. Chakraborty, "A round-robin admn algorithm for identifying data-manipulators in power system estimation," in *2016 American Control Conference (ACC)*, 2016, pp. 3539–3544.
- [5] J. Zhai, Y. Jiang, J. Li, C. N. Jones, and X.-P. Zhang, "Distributed adjustable robust optimal power-gas flow considering wind power uncertainty," *International Journal of Electrical Power and Energy Systems*, vol. 139, p. 107963, 2022.
- [6] J. Duan, W. Zeng, and M.-Y. Chow, "Resilient distributed dc optimal power flow against data integrity attack," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3543–3552, 2018.
- [7] J. Xu, K. Li, M. Abusara, and Y. Zhang, "Admm-based opf problem against cyber attacks in smart grid," in *2021 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2021, pp. 1418–1423.
- [8] Y. Li, X. Wei, Y. Li, Z. Dong, and M. Shahidehpour, "Detection of false data injection attacks in smart grid: A secure federated deep learning approach," *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4862–4872, 2022.
- [9] J. Xie, I. Alvarez-Fernandez, and W. Sun, "A review of machine learning applications in power system resilience," in *2020 IEEE Power and Energy Society General Meeting (PESGM)*, 2020, pp. 1–5.
- [10] D. Tuyizere and R. Ihabwikuzo, "Machine learning to detect cyber-attacks and discriminating the types of power system disturbances," *J Electrical Electron Eng*, vol. 2, no. 3, pp. 328–331, 2023.
- [11] K. Chatterjee, V. Padmini, and S. Khaparde, "Review of cyber attacks on power system operations," *07 2017*, pp. 1–6.
- [12] R. Glowinski and A. Marroco, "Sur l'approximation, par éléments finis d'ordre un, et la résolution, par pénalisation-dualité d'une classe de problèmes de Dirichlet non linéaires," *Revue française d'automatique, informatique, recherche opérationnelle. Analyse numérique*, vol. 9, no. R2, pp. 41–76, 1975. [Online]. Available: http://www.numdam.org/item/M2AN_1975__9_2_41_0/
- [13] D. Gabay and B. Mercier, "A dual algorithm for the solution of nonlinear variational problems via finite element approximation," *Computers and Mathematics with Applications*, vol. 2, no. 1, pp. 17–40, 1976. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/0898122176900031>
- [14] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, *Distributed Optimization and Statistical Learning via the Alternating Direction Method of Multipliers*. Now Publishers, 2011, vol. 3, no. 1.
- [15] D. K. Molzahn, F. Dörfler, I. A. Hiskens, C. L. DeMarco, and S. Backhaus, "A survey of relaxations and approximations of the power flow equations," *Proceedings of the IEEE*, vol. 107, no. 4, pp. 1–37, 2019.
- [16] G. Strang, *Introduction to Linear Algebra*. Wellesley-Cambridge Press, 2009.
- [17] S. AG, *Spannungshaltungskonzept: Konzept für die Spannungshaltung im Übertragungsnetz der Schweiz ab 2020*, Swissgrid AG, Aarau, Switzerland, 2019, version 1.0, January 7, 2019. [Online]. Available: <https://www.swissgrid.ch/de/home/customers/topics/ancillary-services/voltage-support.html>
- [18] —, *Abrechnung von Blindenergie ab dem 01.01.2020*, Swissgrid AG, Aarau, Switzerland, 2019, version 1.0, January 7, 2019. [Online]. Available: <https://www.swissgrid.ch>
- [19] Illinois Center for a Smarter Electric Grid (ICSEG), "Ieee 14-bus system," <https://icseg.iti.illinois.edu/ieee-14-bus-system/>, University of Illinois at Urbana-Champaign, accessed: 2025-01-10.
- [20] J. Xie, I. Alvarez-Fernandez, and W. Sun, "A review of machine learning applications in power system resilience," in *2020 IEEE Power and Energy Society General Meeting (PESGM)*, 2020, pp. 1–5.
- [21] D. Tuyizere and R. Ihabwikuzo, "Machine learning to detect cyber-attacks and discriminating the types of power system disturbances," *SSRN Electronic Journal*, June 29 2023.