

ORIGINAL RESEARCH

Open access

Enhancing Voltage Resilience in Smart City Microgrids against Coordinated False Data Injection Cyberattacks on DERs: A Unified Attack Model with Simulation and Real-Time Experimental Validation

Mina Takeda^{1*}, Haruto Suzuki¹

Abstract

This study explores the consequences of synchronized false data injection attacks (FDIAs) on voltage behavior in smart microgrids that rely on renewable-based distributed energy resources (DERs)—a cornerstone of modern smart city energy infrastructure. Employing both simulation-based and real-world experimental techniques, the work introduces a unified framework for analyzing and defending against coordinated threats, thereby safeguarding the reliable operation of renewable-integrated DERs, which are central to today's urban power ecosystems. In the proposed scenario, multiple attackers independently select the most effective moments to execute two complementary cyberattacks, one producing undervoltage and the other causing overvoltage within the same smart microgrid. Each attack model is driven by an objective function that maximizes the severity of voltage deviations—either excessive undervoltage or harmful overvoltage—induced by its corresponding FDIA. Under this coordinated scheme, the adversaries construct a multi-objective optimization problem (MOOP) that simultaneously provokes significant voltage violations across the microgrid's most exposed zones. Due to the competing objectives in this MOOP, a Pareto-front approach is applied to generate a set of non-dominated optimal solutions, along with a single best compromise solution (BCS). The potency of this combined FDIA strategy is substantiated through detailed simulation studies and laboratory-based experiments. Specifically, the well-known IEEE 13-node test feeder was reconfigured to represent a microgrid environment for the numerical simulations, while the physical validation utilized a small-scale hybrid photovoltaic/wind microgrid testbed featuring actual renewable generation sources.

Keywords False data injection attack (FDIA), Hardware-in-the-loop (HIL), Overvoltage, Simulation and experimental validations, Smart cities, Undervoltage

*Correspondence:

Mina Takeda

takeda.m@eng.kyoto-u.ac.jp

¹ Department of Power System Optimization, Faculty of Engineering, Osaka University, Osaka, Japan

Introduction

Background, definitions, and motivation

Achieving a sustainable evolution from legacy power systems to advanced, intelligent grids depends heavily on the widespread deployment of smart microgrids [1]. Kottayil [2] describes a smart microgrid as an especially effective mechanism for embedding renewable-based distributed energy resources (DERs) at the local/community level, thereby empowering consumers to take an active role in electricity generation and trading. Moreover, such transformations must

remain consistent with the objectives of the Paris Agreement, which prioritize reducing greenhouse gas emissions to combat climate change [3]. This underscores the strategic importance of renewable-based DERs as foundational elements in next-generation power networks, a view shared by grid operators and government decision-makers alike. That said, intelligent energy infrastructures demand real-time oversight and coordination through time-critical communication networks to ensure acceptable levels of dependability and robustness [4]. While merging energy systems with information and communication technology (ICT) undoubtedly accelerates progress toward sustainability, it simultaneously creates substantial cybersecurity vulnerabilities in the digital layer of modern power grids. Within smart-city environments—where digitalization is deeply embedded in energy management to improve distribution efficiency—these weaknesses can jeopardize critical aims such as optimal energy use, system durability, and continued urban technological advancement. As a concrete example, attackers utilizing man-in-the-middle (MiTM) tactics can circumvent protective measures, gain unauthorized access to control facilities, and alter stored measurement data, thereby triggering a range of serious operational problems such as line overloading [5], propagating outages [6], and complete power loss events [7]. A prominent outcome of false data injection attacks (FDIAs) against contemporary power infrastructures—especially those serving smart urban microgrids—is the emergence of unacceptable voltage excursions, namely overvoltage and undervoltage conditions. This reality forms the primary motivation for the present investigation.

Literature review

Deng et al. [8] proposed a distributed control architecture with resilience properties to correct voltage profiles in standalone cyber-physical microgrids equipped with multiple energy storage units. The technique described in Deng et al. [8] deliberately prevents the controller gain from increasing monotonically when counteracting disturbances or malicious cyber intrusions. In Zhou et al. [9], researchers analyzed the difficulties in voltage control arising from cyberattacks in both single-phase and three-phase islanded microgrids. An adaptive secondary control scheme designed to withstand data manipulation attacks was examined in Li et al. [10] for an islanded microgrid scenario. The influence of FDIAs on DC/DC converters in intelligent microgrids was studied by Habibi et al. [11], who found that attackers employed time-dependent injection strategies to degrade overall system performance severely. Two alternative FDIA formulations were developed in Habibi et al. [12] to falsify voltage sensor readings in DC microgrids, thereby impairing both voltage stability and equitable current distribution among sources. Liu et al. [13] assessed the probabilistic stability of an autonomous microgrid exposed to denial-of-service (DoS) attacks. It recommended a secondary frequency regulation strategy to lessen the disruption caused by such DoS events. In Aysheh et al. [14], FDIAs were applied to the voltage profile of a photovoltaic-integrated smart grid, resulting in noticeable deviations in both overvoltage and undervoltage regions. Importantly, the defense-oriented framework outlined by Aysheh et al. [14] includes multiple proactive and reactive measures to protect smart grids against similar cyber intrusions. Earlier in this line of inquiry, the authors constructed a hardware-in-the-loop (HIL) platform capable of (a) detecting covert false data secretly inserted into sensor outputs of a prototype-scale microgrid and (b) accurately separating legitimate transient disturbances from deliberate FDIA-induced power deficits [15].

Research gap and contribution of this work

While several studies (e.g., [8–15]) have examined the effects of cyberattacks on voltage profiles in smart grids, no prior work has proposed and experimentally verified a multi-objective approach specifically aimed at assessing the consequences of FDIAs in smart microgrids—namely, those designed to simultaneously provoke both overvoltage and undervoltage precisely when the system is most susceptible to voltage instability. To fill this identified research void, the present study investigates a coordinated FDIA framework with the following key contributions:

- Formulation of a multi-objective unified attack strategy from the attackers' perspective, timed to exploit periods of maximum vulnerability in smart microgrids to both overvoltage and undervoltage, thereby yielding a Pareto front of non-dominated solutions that span a spectrum of achievable overvoltage and undervoltage magnitudes,
- Real-world experimental validation of the proposed framework using a laboratory-scale smart microgrid that incorporates wind turbines and photovoltaic modules, complemented by simulation-based analysis, to determine the

optimal trade-off solution (best compromise solution, BCS) between the induced undervoltage and overvoltage effects.

In essence, the results of this study bridge a significant deficiency in understanding how to defend smart microgrids against voltage-targeted cyberattacks. By enhancing the cybersecurity, operational efficiency, and robustness of urban energy infrastructure, this research directly contributes to the development of secure, dependable, and flexible energy systems tailored for smart cities. Such progress is vital for advancing overarching objectives related to energy optimization, urban system durability, and the seamless incorporation of cutting-edge technologies into city-wide ecosystems.

Materials and Methods

The framework introduced in this work is validated through both numerical simulations and laboratory experiments. In particular, the experimental testing of FDIA scenarios on a prototype-scale microgrid serves as a realistic proxy for actual smart-city deployments by emulating essential features of urban microgrid architectures. In real-world smart cities, distributed energy resources (such as PV arrays and wind generators) are commonly combined with sophisticated control platforms to optimize energy generation, storage, and delivery—mirroring the configuration of the experimental microgrid employed here. By recreating these components in a controlled lab environment, the study effectively demonstrates the potential disruptions that cyberattacks could impose on voltage regulation, energy performance, and overall stability within representative urban grid settings.

Developed framework

The proposed multi-objective framework is depicted in **Figure 1**. As shown in **Figure 1a**, a standard smart microgrid can be subjected to attacks by N independent adversaries to amplify the overall detrimental effects of a coordinated attack strategy; however, for simplicity and to clearly convey the core concept, **Figure 1b** illustrates the scenario with only two attackers. From **Figure 1b**, it is evident that Attacker 1 launches an FDIA against the microgrid—which may operate in either grid-tied or islanded mode—aimed at inducing overvoltage (OV) during the period of greatest susceptibility. Concurrently, Attacker 2 executes a separate FDIA to generate undervoltage (UV) at its own optimally determined instant. Notably, each of these attacks is formulated as a bi-objective optimization problem (BOOP), yielding a set of Pareto-optimal solutions rather than a single point. The objectives for both BOOPs are twofold: (a) maximizing the extent of overvoltage or undervoltage throughout the microgrid, and (b) minimizing the magnitude of injected false data to achieve the desired voltage deviation levels while keeping the attack stealthy. This dual goal enables the attackers to inflict substantial voltage disruption with relatively small falsified data vectors. Because the objectives of the two attacks conflict and their optimal timing may differ, the outcomes of one attack do not necessarily interfere with those of the other.

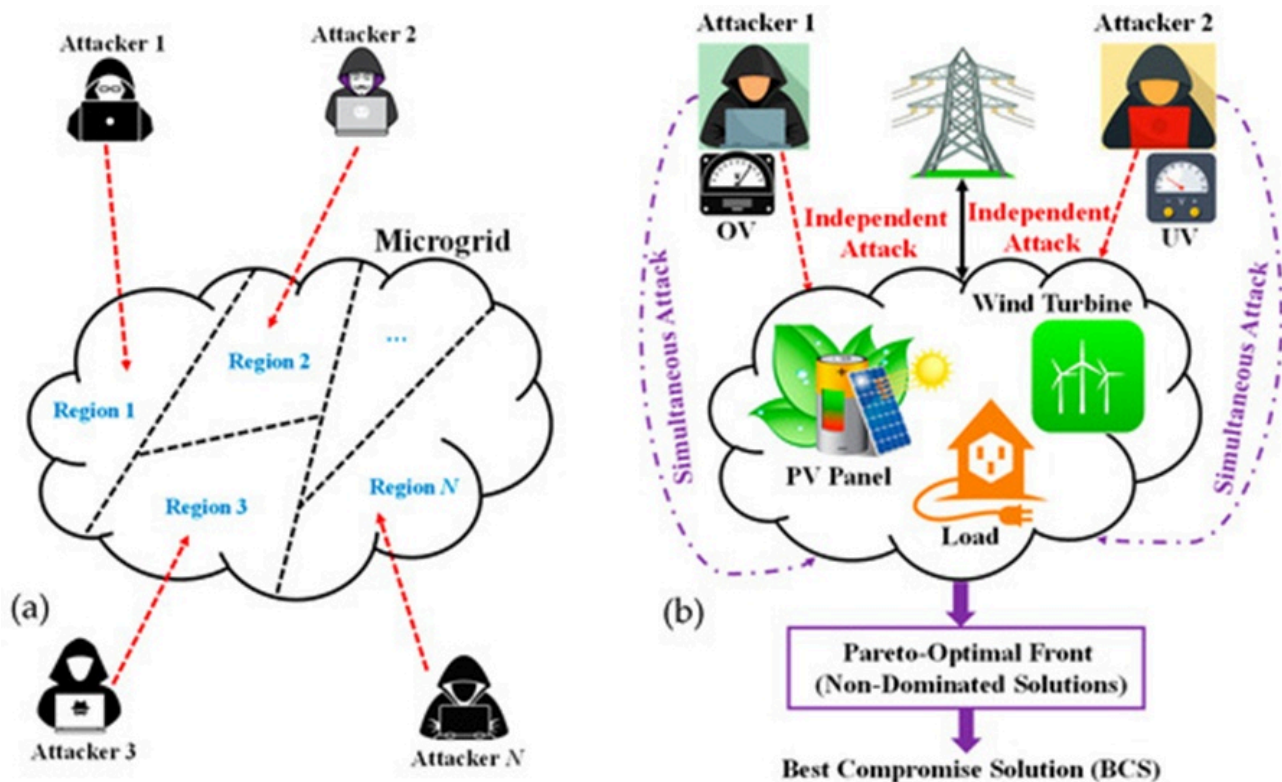


Figure 1. The proposed FDIA framework is designed to provoke voltage violations in (a): a general smart microgrid, and (b): a representative component of urban energy infrastructure in smart cities.

It should be emphasized that following each isolated cyberattack, the microgrid's control system may deploy suitable corrective measures to restore normal operating conditions. Moreover, the specific mitigation techniques could vary depending on the distinct characteristics of each attack. Nevertheless, to evaluate the most severe plausible scenario, this study introduces a unified FDIA formulated as a multi-objective optimization problem (MOOP) that simultaneously maximizes the degree of overvoltage, maximizes the degree of undervoltage, and minimizes the volume of false data injected into the communication layer. Stated differently, the microgrid becomes the target of a single, covert, coordinated cyberattack capable of triggering both overvoltage and undervoltage concurrently (representing the primary novelty of this work). Furthermore, by constraining the size of the injected false data vector, the attack reduces the likelihood of detection by the system operator. Consequently, defending against such a combined threat would require the implementation of a robust, comprehensive remedial strategy—an area designated for future investigation.

According to **Figure 1b**, to execute two concurrent FDIAs against the microgrid, the pair of attackers jointly addresses a multi-objective optimization problem (MOOP). This process yields a collection of non-dominated solutions, referred to as the Pareto-optimal front, which the attackers store in a dedicated repository. However, the MOOP incorporates three objective functions. **Figure 2** displays only the overvoltage and undervoltage objectives to provide a clearer visualization of the resulting Pareto front. As illustrated in **Figure 2**, solving the MOOP yields a diverse set of optimal solutions (represented by the red circles) rather than a single best point. Consequently, the attackers gain the flexibility to modulate the intensity of both undervoltage and overvoltage within the coordinated cyberattack and to select the most balanced trade-off, known as the best compromise solution (BCS), among the competing objectives.

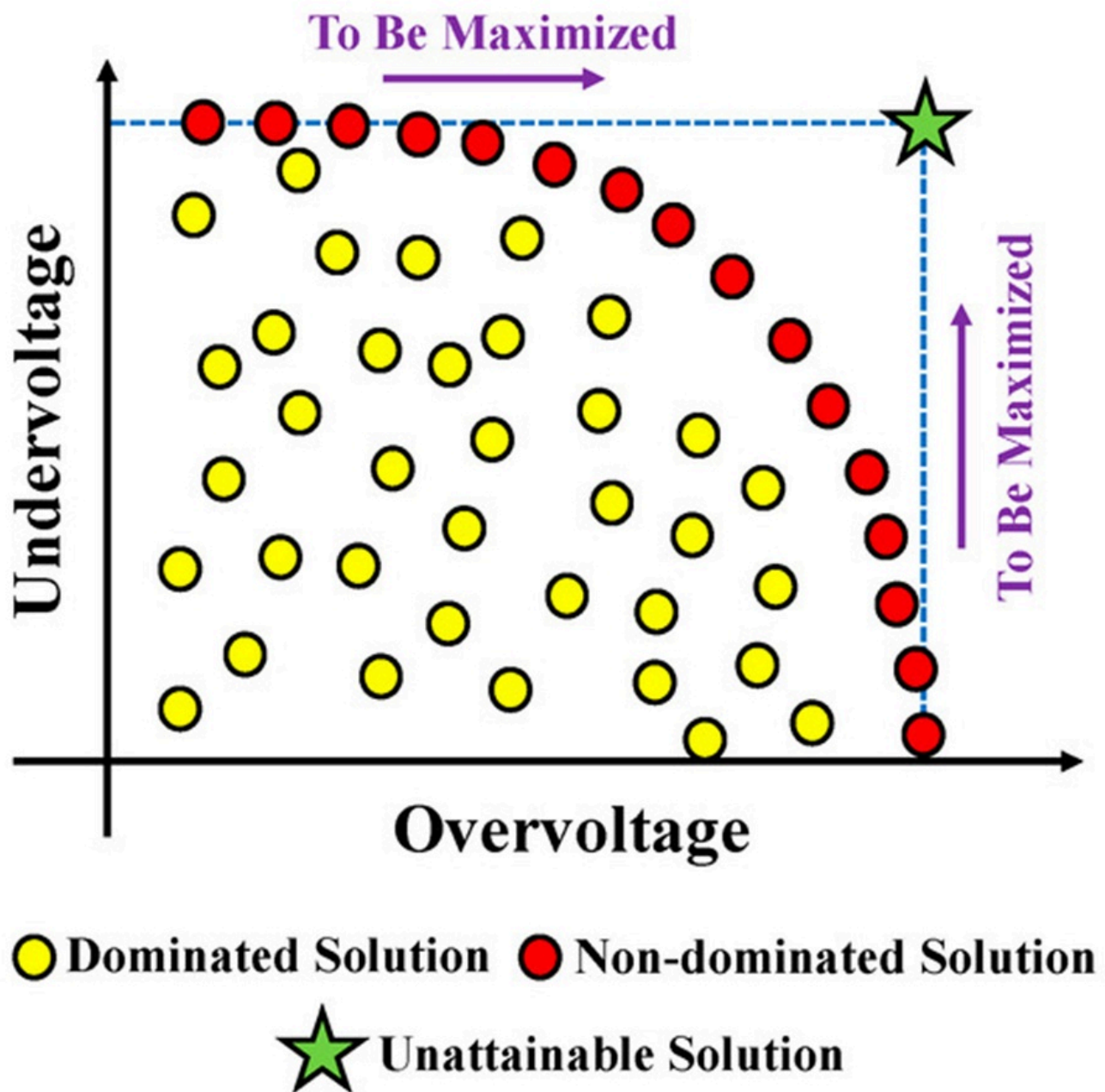


Figure 2. Representative two-dimensional Pareto-optimal front corresponding to the FDIA framework proposed in this study.

Problem formulation

Pre-attack assessment to identify the most vulnerable node

This subsection introduces an optimization model that equips both attackers ([Figure 1b](#)) with critical insights into the node most prone to voltage instability within the microgrid and the optimal timing for launching the attack. To achieve this, both attackers solve [Eq. 1](#) subject to the technical constraints given in [Eqs. 2–8](#). It is assumed that the attackers possess knowledge of the microgrid's baseline voltage profile—a realistic attack premise adopted from [Zhuang et al. \[16\]](#), [Abhinav et al. \[17\]](#), and [Liang et al. \[18\]](#). In practice, for instance, the perpetrators of the 2015 Ukraine power grid incident successfully infiltrated the utility's computer systems. They extracted detailed historical data on the network, ultimately

causing power outages lasting 1 to 6 hours for approximately 225,000 customers [19]. Similarly, in 2018, intruders targeted the U.S. electric grid to gather sensitive operational details about power generation infrastructure [20].

Upon solving the optimization model (Eqs. 1–8) to maximize voltage deviation across the microgrid, the attackers obtain an altered voltage profile. By comparing this manipulated profile with the original (pre-attack) voltage profile, they can accurately determine both the node most sensitive to voltage changes and the optimal time to initiate the planned FDIAs.

$$\max \left\{ \sum_{t=1}^{24} \sum_{n=1}^{N_n} |1.00 - V_{n,t}| \right\} \quad (1)$$

$$P_t^{\text{Generation}} - P_t^{\text{Demand}} - P_t^{\text{Loss}} = 0 \quad (2)$$

$$Q_t^{\text{Generation}} - Q_t^{\text{Demand}} - Q_t^{\text{Loss}} = 0 \quad (3)$$

$$V_{\min} \leq V_{n,t} \leq V_{\max} \quad (4)$$

$$\delta_{\min} \leq \delta_{n,t} \leq \delta_{\max} \quad (5)$$

$$P_{\min} \leq P_{n,t} \leq P_{\max} \quad (6)$$

$$Q_{\min} \leq Q_{n,t} \leq Q_{\max} \quad (7)$$

$$I_{\min} \leq I_{b,t} \leq I_{\max} \quad (8)$$

Where $V_{n,t}$ denotes the voltage magnitude at node n during the t th time interval, with 1.00 p.u. representing the nominal voltage level for all buses in the distribution network; N_n indicates the total number of nodes in the microgrid, excluding the point of common coupling (PCC); $P_t^{\text{Generation}}$, P_t^{Demand} , and P_t^{Loss} represent, respectively, the aggregate active power generation, total active power demand, and total active power losses in the microgrid at time slot t ; $\delta_{n,t}$ is the voltage phase angle at node n at time t ; $P_{n,t}$ and $Q_{n,t}$ are the net active and reactive power injections at node n at time t ; and $I_{b,t}$ is the current magnitude flowing through the b th branch at time t .

Deliberate voltage manipulation from the attackers' perspective

Figure 3 illustrates the equivalent circuit of a typical microgrid as viewed from the point of common coupling (PCC), where Z_n^{Eq} represents the equivalent impedance of the microgrid; V_n and V_{PCC} denote the voltage magnitudes at node n and at the PCC, respectively; and I_{DER} is the current magnitude supplied by the distributed energy resources (e.g.,

photovoltaic panels and wind turbines). Assuming (a) the PCC voltage serves as the reference and (b) power losses across Z_n^{Eq} are negligible, the approximate voltage magnitude at node n can be expressed as shown in Eq. 9.

$$V_n = \frac{(P_n^G - P_n^D) \times R_n^{Eq} + (Q_n^G - Q_n^D) \times X_n^{Eq}}{V_{PCC}} + V_{PCC} \quad (9)$$

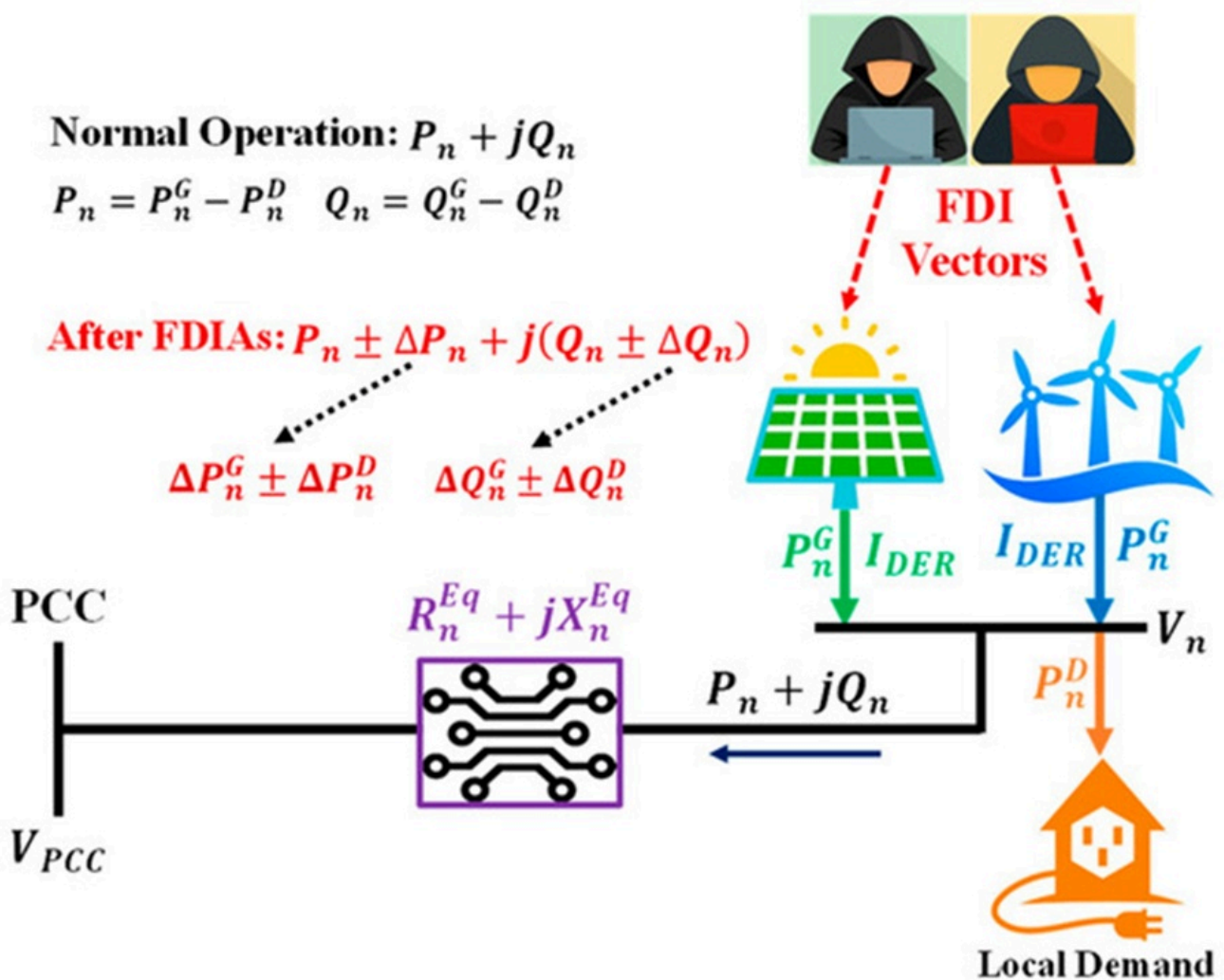


Figure 3. Equivalent circuit representation of a standard microgrid as observed from the point of common coupling (PCC).

From Eq. 9, it follows that by injecting falsified data—such as ΔP_n and ΔQ_n —into the net active and reactive powers (P_n and Q_n) at node n, varying degrees of voltage magnitude deviation can be induced at that node. Put differently, both positive and negative perturbations in ΔP_n and ΔQ_n result in varying degrees of voltage excursions, manifesting as overvoltage or undervoltage conditions (Figure 3). Nevertheless, attackers must ensure that the falsified data introduced at load points and generation units across all nodes remains below the thresholds that would activate existing security mechanisms [16–18]. To accomplish this, Eq. 10 defines the optimization model that attackers must solve to determine the smallest possible false data vectors to inject into the microgrid's control system. Importantly, the optimization problem

defined in Eq. 10 is subject to the technical constraints outlined in Eqs. 2–8, as well as the additional bounds specified in Eqs. 11–14 to guarantee that the cyberattacks do not exceed the permissible rated limits.

$$\min \left\{ \sum_{t=1}^{24} \sum_{n=1}^{N_n} |\Delta P_{n,t}^G + \Delta P_{n,t}^D + \Delta Q_{n,t}^G + \Delta Q_{n,t}^D| \right\} \quad (10)$$

$$-\partial \times P_{n,t}^G \leq \Delta P_{n,t}^G \leq \partial \times P_{n,t}^G \quad (11)$$

$$-\partial \times P_{n,t}^D \leq \Delta P_{n,t}^D \leq \partial \times P_{n,t}^D \quad (12)$$

$$-\partial \times Q_{n,t}^G \leq \Delta Q_{n,t}^G \leq \partial \times Q_{n,t}^G \quad (13)$$

$$-\partial \times Q_{n,t}^D \leq \Delta Q_{n,t}^D \leq \partial \times Q_{n,t}^D \quad (14)$$

Where ∂ represents the percentage of falsified data relative to the nominal rated values of generation and demand, capped at a maximum of 10% of those rated values; and Δ signifies the intended modification applied to active and reactive power quantities, deliberately constrained to minimize the risk of detection by monitoring systems.

Independent FDIA model designed to induce overvoltage

The primary objective function from the perspective of Attacker 1 is given in Eq. 15, which is adapted from Purlu and Turkey [21]. Note that this objective—aimed at maximizing intentional overvoltage (Eq. 15)—must be optimized simultaneously with the constraint on false data magnitude (Eq. 10) within a bi-objective optimization problem (BOOP).

$$\max \left\{ \frac{\sum_{t=1}^{24} \sum_{n=1}^{N_n} V_{n,t} - 24 \times \alpha \times V_{ref}}{\sum_{n=1}^{N_n} V_{n,t}} \right\} \quad (15)$$

Where V_{ref} denotes the reference voltage level at node n , and α serves as a tuning parameter that governs the desired intensity of the overvoltage condition.

Independent FDIA model designed to induce undervoltage

Drawing from Balamourougan et al. [22], this subsection presents an optimization formulation centered on the undervoltage proximity index, viewed from the standpoint of Attacker 2 (Figure 1b). Accordingly, the attacker seeks to maximize this index, as expressed in Eq. 16, while concurrently minimizing the false data injection volume, as defined in Eq. 10, thereby forming a BOOP that drives the microgrid toward undervoltage while keeping the injected data vectors

beneath detectable thresholds. As explained in Balamourougan et al. [22] and Micky et al. [23], the objective function in Eq. 16 quantifies the conditions under which the likelihood of undervoltage occurrence at node n is maximized.

$$\max \left\{ 1 - \frac{\sum_{l=1}^{24} \sum_{m=1, m \neq n}^{N_n} V_{m,l} \times \frac{Y_{nm}}{\sum_{n=1, n \neq k}^{N_n} Y_{nk}}}{\sum_{l=1}^{24} V_{n,l}} \right\} \quad (16)$$

Where Y_{nm} represents the admittance of the line connecting nodes n and m .

Unified FDIA designed to provoke simultaneous voltage violations

The proposed coordinated FDIA strategy, which induces both overvoltage and undervoltage concurrently, is formulated as a multi-objective optimization problem (MOOP) comprising three distinct objective functions. The first objective maximizes overvoltage (Eq. 15), the second maximizes undervoltage (Eq. 16), and the third minimizes the magnitude of false data injected into load centers and generation units to avoid breaching rated limits (Eq. 10). Consequently, the overall FDIA problem is three-dimensional; however, for illustrative purposes, Figure 2 depicts only the two-dimensional Pareto front corresponding to the primary voltage-related objectives (Eqs. 15 and 16) to aid conceptual understanding.

Formulation of the embedded multi-objective solution approach

Because the objective functions involved in the developed BOOPs and the MOOP operate across disparate numerical scales, they must first be normalized to a common interval of [0, 1], as illustrated in Figure 4 and mathematically defined in Eq. 17. This figure introduces a trapezoidal membership function, from which it can be observed that a membership value of zero indicates complete dissatisfaction with the objective by the decision-maker. In contrast, a value of one signifies satisfaction [24].

$$\psi_k(X) = \begin{cases} 0 & f_k \geq f_k^{\max} \\ \frac{f_k^{\max} - f_k}{f_k^{\max} - f_k^{\min}} & f_k^{\min} \leq f_k \leq f_k^{\max} \\ 1 & f_k \leq f_k^{\min} \end{cases} \quad (17)$$

Where ψ_k represents the fuzzy membership set associated with the k th objective function, f_k denotes the k th objective function, $f_k^{\min}$ and $f_k^{\max}$ are the lower and upper bounds, respectively, of the k th objective function, and X is the vector containing the decision variables of the optimization problem.

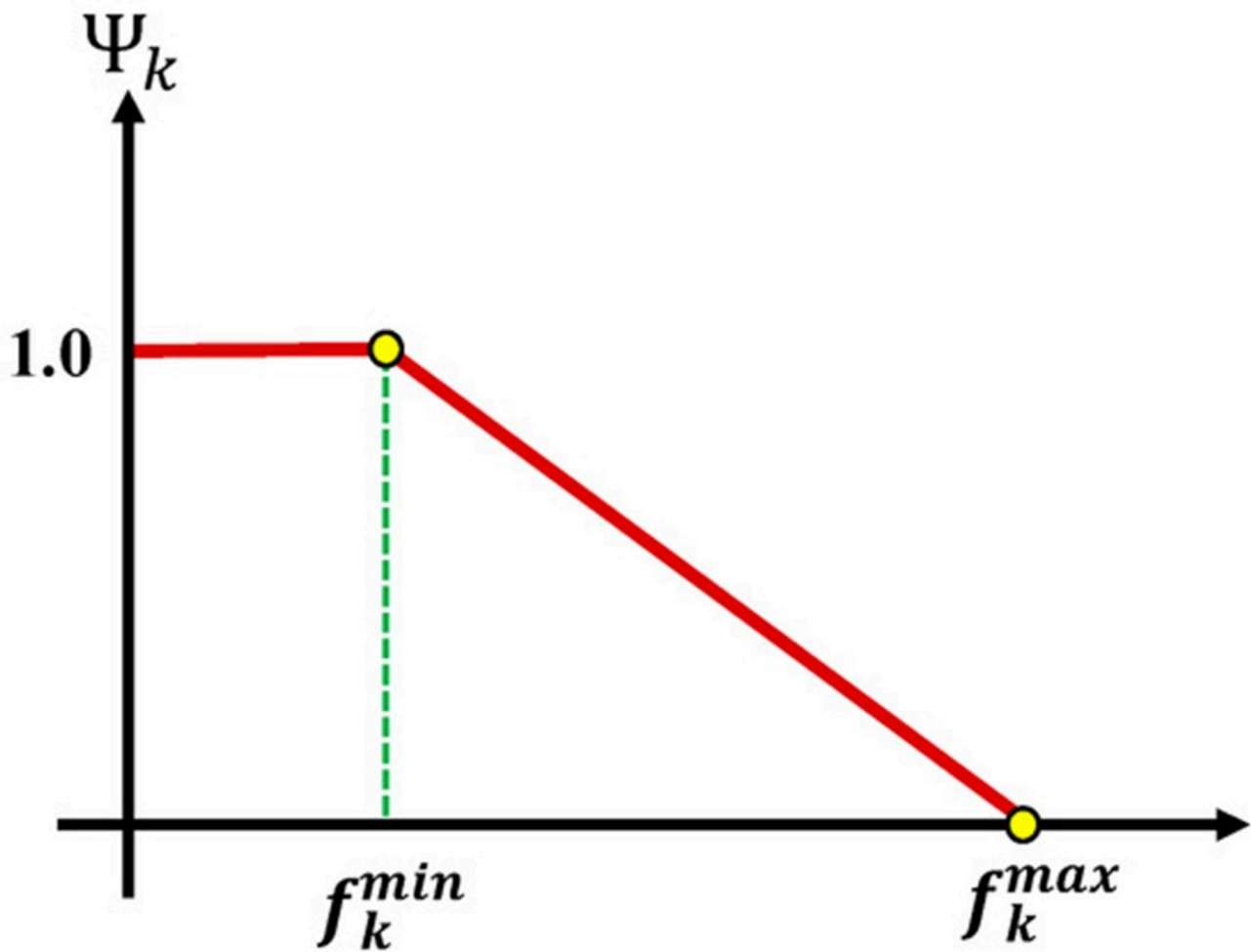


Figure 4. A trapezoidal membership function is applied to normalize all objective functions.

To determine the set of non-dominated solutions (i.e., the Pareto-optimal front), an initial step defines a dominance region for each candidate solution held in the repository. Subsequently, [Eqs. 18 and 19](#) are used to identify and eliminate dominated solutions, leaving only the non-dominated set, which constitutes the Pareto-optimal front. For a minimization problem ([Eq. 10](#)), solution x_1 is said to dominate x_2 when: (a) x_1 performs at least as well as x_2 across every objective function, and (b) x_1 strictly outperforms x_2 in at least one objective function [\[25\]](#).

$$f_k(x_1) \leq f_k(x_2), \forall f \quad (18)$$

$$f_k(x_1) < f_k(x_2), \exists f \quad (19)$$

Once the Pareto-optimal front has been established, [Eq. 20](#) is applied to the repository to select the best compromise solution (BCS), representing the optimal trade-off among the conflicting objectives. In [Eq. 20](#), Y_ψ denotes the BCS; ξ_k represents the weighting coefficient assigned to the k th objective function; N_{obj} and N_{NDS} stand for the total number of objective functions and the total number of non-dominated solutions stored in the repository, respectively [\[26\]](#).

$$Y_{\psi}(k, i) = \frac{\sum_{k=1}^{N_{obj}} \bar{\zeta}_k \times \psi_{k,i}}{\sum_{i=1}^{N_{NDS}} \sum_{k=1}^{N_{obj}} \bar{\zeta}_k \times \psi_{k,i}} \quad (20)$$

The complete sequence of operations within the proposed framework is outlined in **Figure 5** and encompasses the coordinated FDIAs illustrated in **Figure 1b**. This flowchart outlines the methodology's step-by-step progression and links each phase to its corresponding discussion in the paper. The process commences with a pre-attack vulnerability assessment that solves the optimization model in **Eqs. 1–8** to locate the node(s) and time slot(s) most prone to voltage instability, thereby supplying essential parameters for the ensuing attack design. Following this, the framework formulates deliberate voltage manipulations from the attackers' viewpoint by constructing separate optimization models for inducing overvoltage (**Eq. 15**) and undervoltage (**Eq. 16**), both constrained by **Eqs. 10–14**. These disparate objective functions are then normalized via the trapezoidal membership function given in **Eq. 17** to enable consistent comparison across scales. After normalization, the independent BOOPs are integrated and solved concurrently within a unified multi-objective optimization problem (MOOP), enabling simultaneous provocation of overvoltage and undervoltage. Finally, **Eqs. 18–20** are applied to extract the Pareto-optimal front of non-dominated solutions and to pinpoint the BCS. This sequence underscores the attackers' capability to balance opposing goals while evading detection, offering valuable insight into exploitable weaknesses in the targeted microgrid.

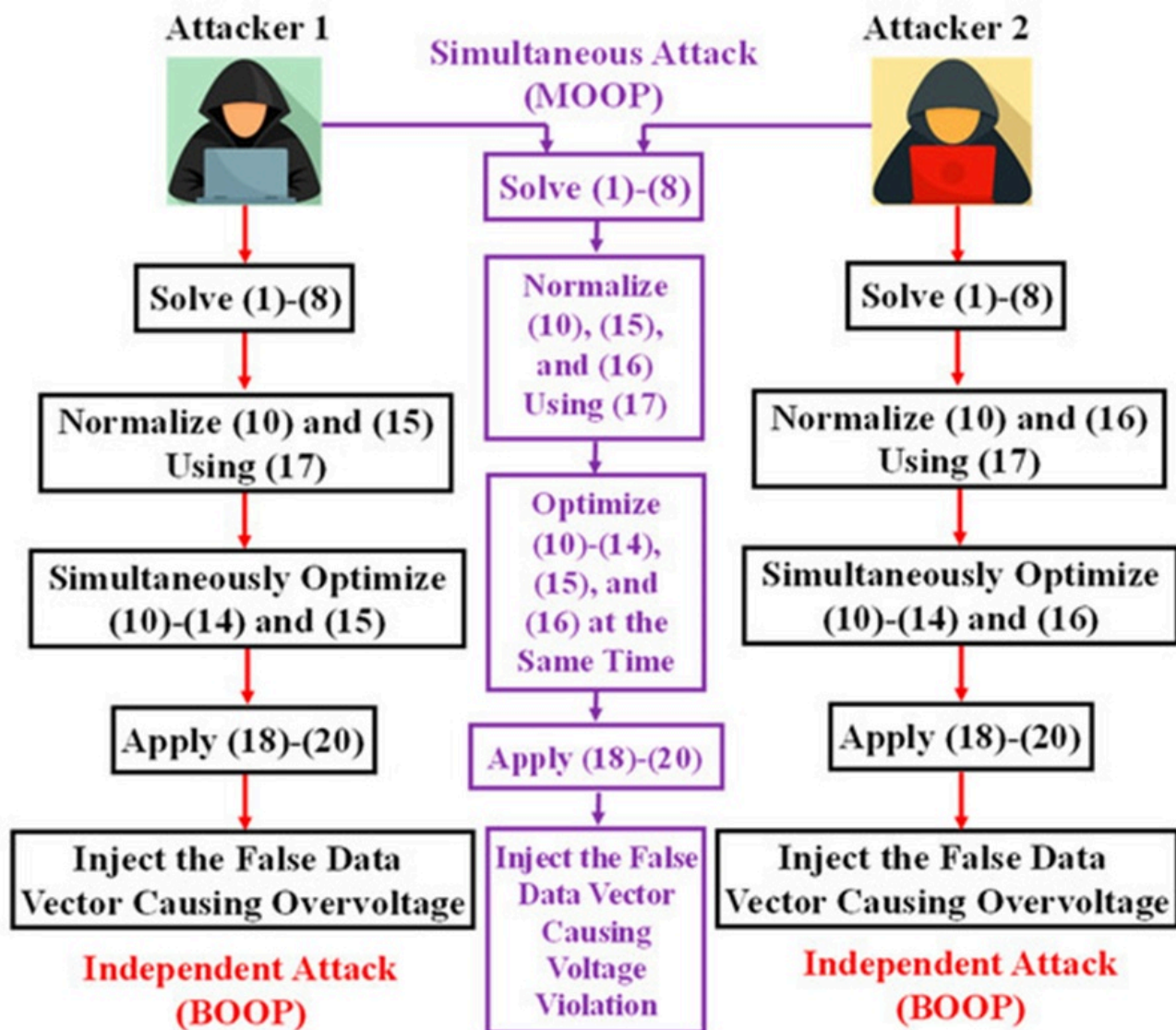


Figure 5. Schematic overview of the mathematical interdependencies within the coordinated FDIA framework developed in this study.

Key assumptions for this category of cyberattack

From the attackers' standpoint, mounting an effective assault on power systems necessitates several foundational assumptions [5, 6]. It is presumed that adversaries can gain access to critical network infrastructure, potentially through the exploitation of inadequate or legacy cybersecurity controls or via social engineering methods such as phishing campaigns. In practice, however, securing such access typically requires overcoming multiple defensive layers—including firewalls, intrusion detection systems, and encrypted channels—which entails considerable effort, time, and risk exposure. Furthermore, modern power grids are highly interconnected, meaning that breaching a single element (e.g., a substation or a central control facility) can propagate widespread effects. Yet, attackers frequently contend with partial, stale, or inaccurate system information, increasing the risk of flawed execution or unanticipated outcomes. Additional real-world impediments include communication channel latency and physical constraints on devices, such as processing power or network bandwidth, which can diminish attack performance under operational conditions.

The study also posits that the grid's monitoring systems and incident response mechanisms are primarily reactive rather than anticipatory, thereby creating a temporal window for damage to occur before detection and mitigation. While this

premise facilitates analysis of worst-case outcomes, it is recognized that contemporary grid operators are actively strengthening defenses through advanced anomaly detection, continuous monitoring, and built-in redundancies. These assumptions are consistent with realistic attack scenarios documented in prior research [11, 17, 18], which acknowledge that even advanced adversaries—capable of exploiting software flaws, tampering with control signals, or compromising physical assets—encounter substantial obstacles when confronting robust, well-maintained security architectures. By clearly articulating these assumptions, the present work seeks to illuminate exploitable weaknesses in smart microgrids and the practical barriers to coordinated cyberattacks. Future extensions of this framework will incorporate adaptive defensive strategies and assess the resilience of the proposed attack models against more realistic and stringent cybersecurity countermeasures.

Simulation and Experimental Results

Initialization and case study descriptions

To assess the performance of the proposed multi-objective FDIA, two distinct case studies are conducted. For the simulation-based evaluation, the IEEE 13-node test feeder—modified as shown in Figure 6—is employed as a representative microgrid to demonstrate the effects of the coordinated cyberattack on its voltage behavior. Specifically, a photovoltaic (PV) installation with a rated capacity of 200 kW is integrated at node #6. Additionally, a Wind World [27] wind turbine, with a rated power of 250 kW and a rotor diameter of 29.2 m, is connected at node #7. Note that the standard test condition irradiance is 1000 W/m², while the actual operating irradiance level is set to 120 W/m².

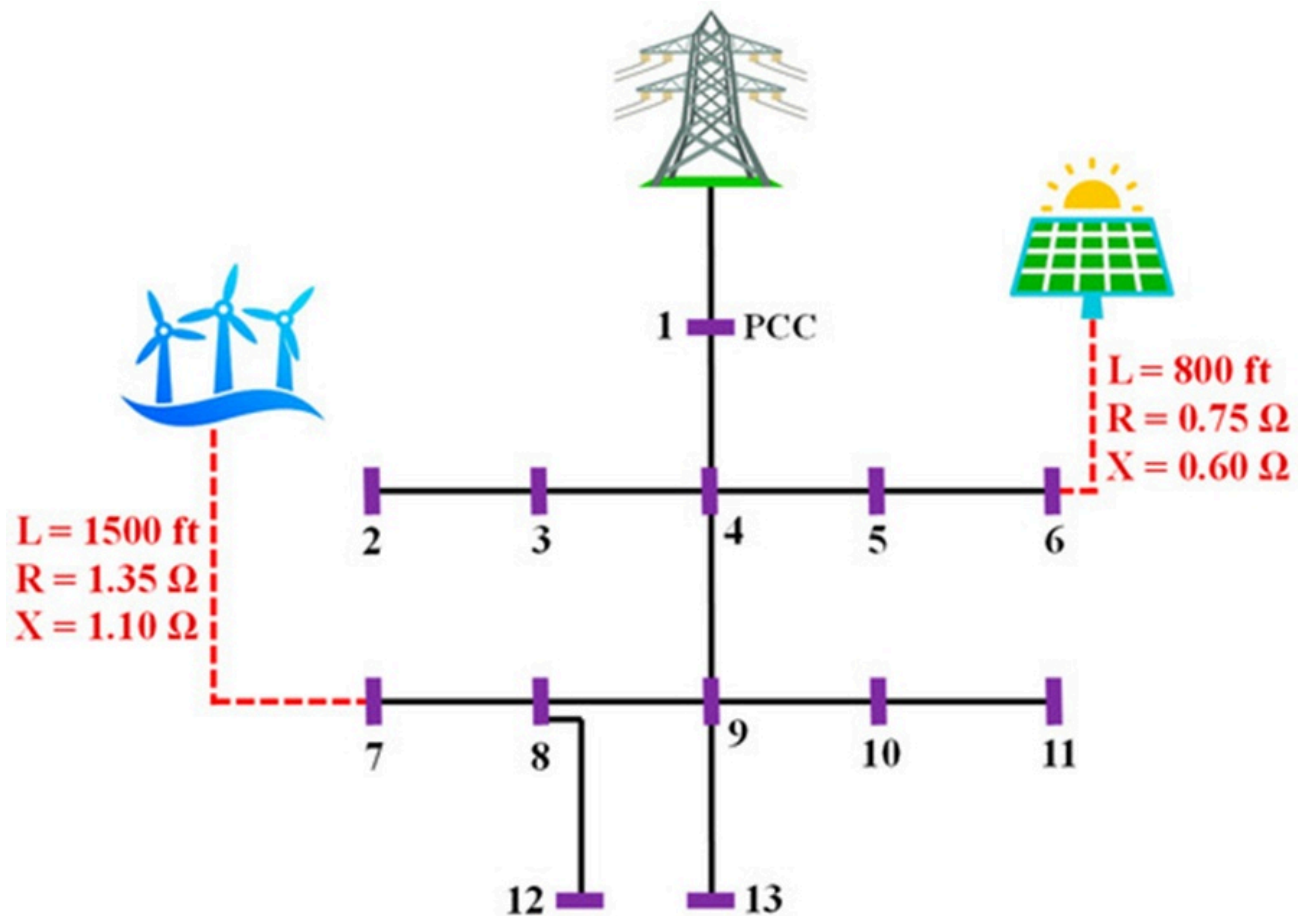


Figure 6. Modified IEEE 13-node test feeder configured as a microgrid, serving as a representative element of real-world smart city energy infrastructure.

Furthermore, the hourly active and reactive power demand and generation profiles over 24 hours are sourced from the Commercial and Residential Hourly Load Profile dataset [28] and Kumar et al. [29], and are illustrated in Figure 7. Additional system parameters are available in Kersting [30] and Yousaf et al. [31].

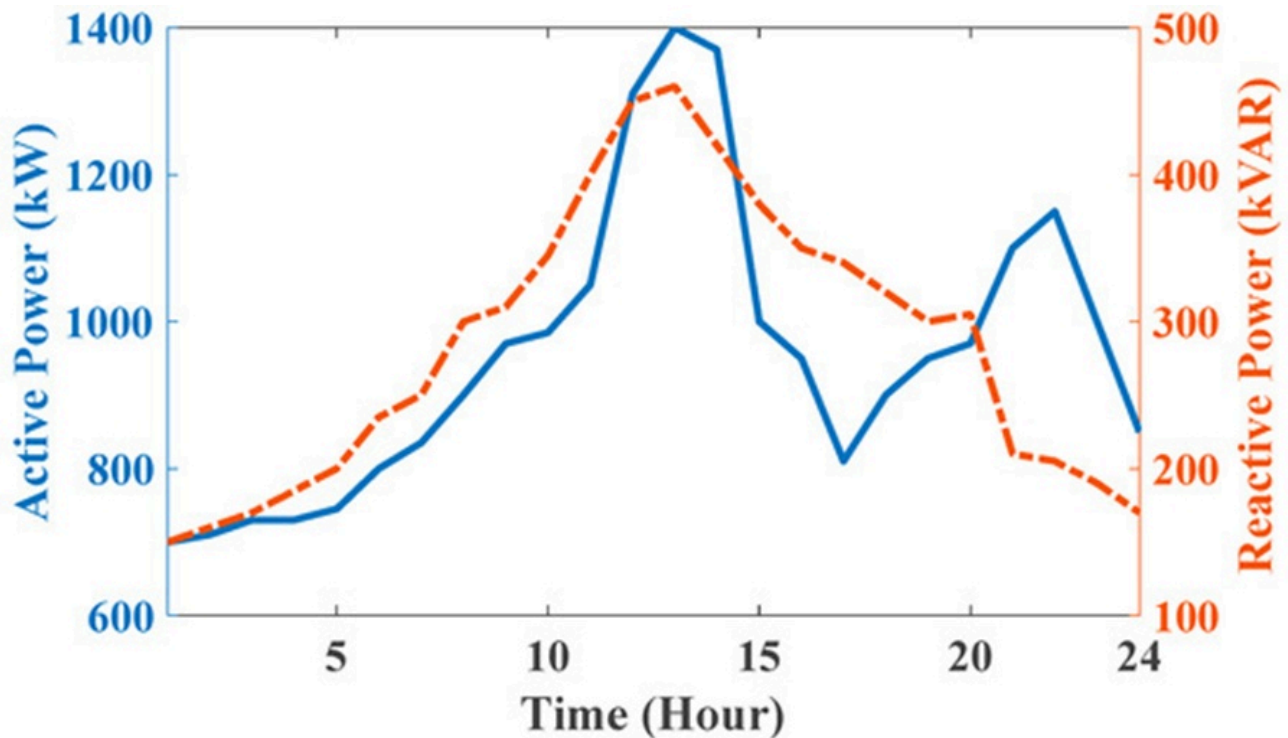


Figure 7. Hourly aggregate active and reactive power profiles for the modified IEEE 13-node test system.

For the experimental validation, the laboratory-scale microgrid developed in the initial phase of this research (Figure 8) is utilized [32, 33]. As shown in Figure 8, this prototype microgrid includes two wind turbines—one horizontal-axis rated at 500 W and one vertical-axis rated at 400 W—along with two 160 W photovoltaic panels. To simulate environmental conditions in the laboratory, a fan delivering 19,500 cubic feet per minute (CFM) of airflow generates wind, while four 2200 W LED lamps emulate solar irradiance. The system also incorporates two 500 W grid-tied inverters, one 2000 W standalone inverter with its controller, a hybrid energy storage unit (combining batteries and supercapacitors), and the associated buses, switches, and charge controllers. For comprehensive details on the lab-scale microgrid configuration and components, refer to the earlier publications of this research [32, 33].

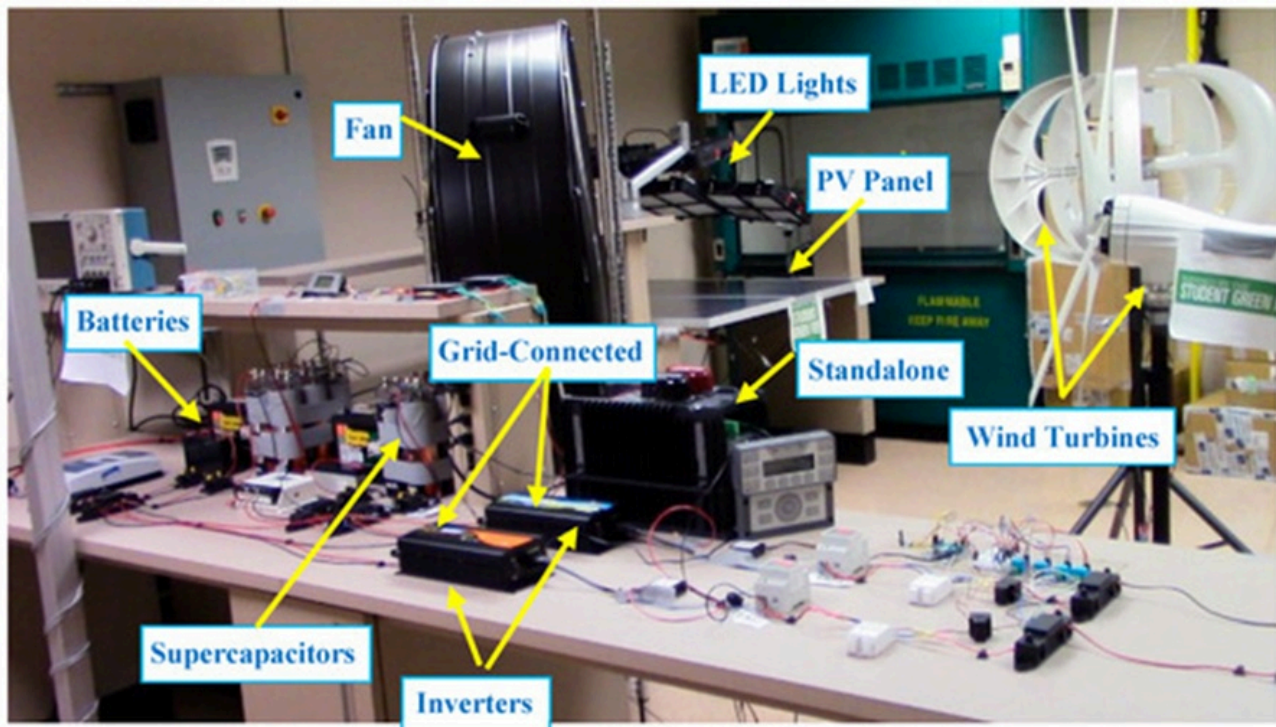


Figure 8. Laboratory-scale smart microgrid constructed at the Power System Design Laboratory, featuring wind turbines and PV modules.

The hardware-in-the-loop (HIL) experimental platform for this lab-scale microgrid is presented in [Figure 9](#) [33–37]. The validity and reliability of the results are confirmed through a dual approach: numerical simulations of the modified IEEE 13-node system, combined with physical experimentation on the laboratory microgrid. By integrating real hardware components—such as PV arrays, wind turbines, and hybrid storage—with real-time simulation, the HIL setup closely replicates actual operating environments, offering a credible platform for testing the proposed attack framework. These combined results effectively illustrate the framework’s ability to capture realistic responses of smart microgrids subjected to coordinated false-data-injection attacks.

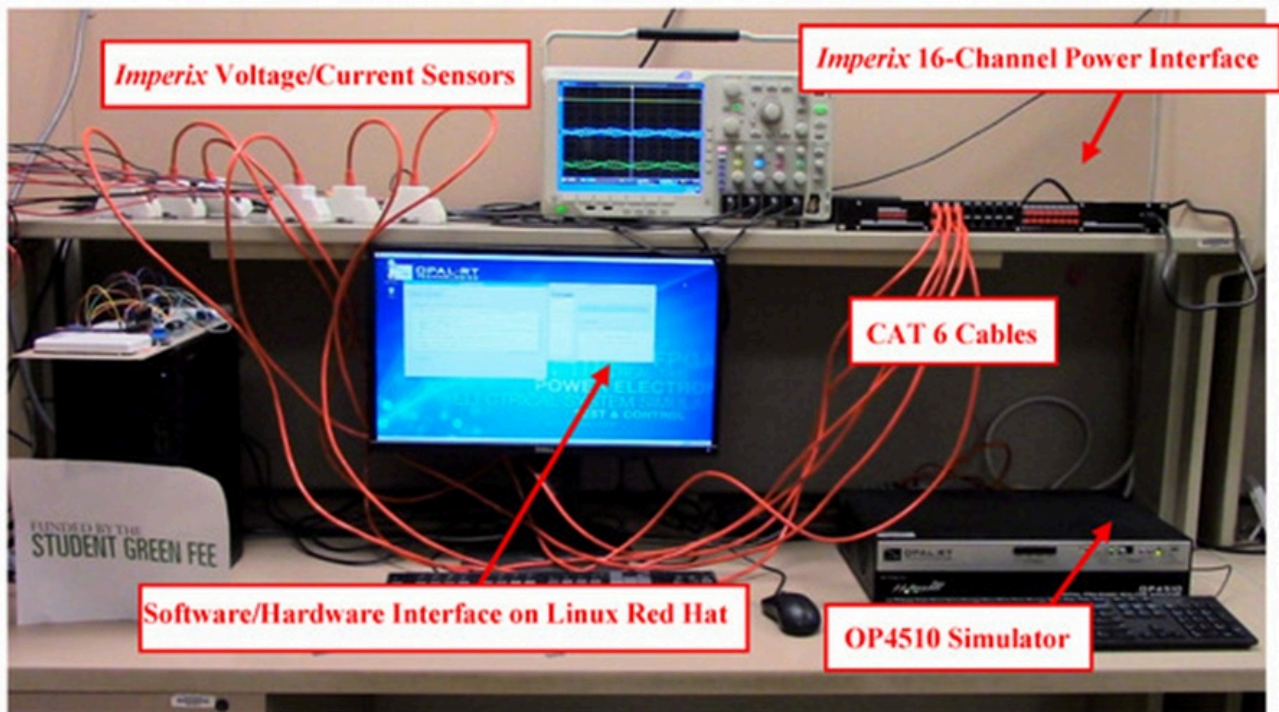


Figure 9. Hardware-in-the-loop (HIL) configuration for the lab-scale microgrid shown in [Figure 8](#) [33–37].

All optimization models were implemented in MATLAB R2018b running on an Intel® Core™ i5-7500 CPU operating at 3.4 GHz. Power flow computations were performed using the Newton–Raphson method via the MATPOWER toolbox, a widely recognized tool for power system simulation and analysis. The problems were solved employing the modified whale optimization algorithm with wavelet mutation (MWOA-WM), as proposed in Mukherjee *et al.* [25].

In this implementation, the whale population size was set to 200, and the maximum number of iterations was limited to 100. For further explanation of the design principles underlying MWOA-WM and its superior performance across a range of challenging optimization tasks—including those in power and energy systems—readers are referred to Mukherjee *et al.* [25].

Simulation results on the modified IEEE 13-node system

The primary purpose of the pre-attack assessment is to determine the node most sensitive to voltage fluctuations and to identify the most effective timing for launching the FDIAs. Toward this end, the attackers solve [Eqs. 1–8](#) to maximize voltage deviation throughout the microgrid. The discrepancy between the baseline voltage profile and the altered profile generated by the attackers is illustrated in [Figure 10](#). From this figure, it is evident that only nodes #10, #11, and #13 exhibit significant susceptibility to voltage deviation, with this occurring specifically between 11 AM and 1 PM. The pre-attack analysis further reveals that node #11 is the most vulnerable bus in the modified IEEE 13-node system, with the optimal attack window centered at 11 AM ([Figure 10](#)).

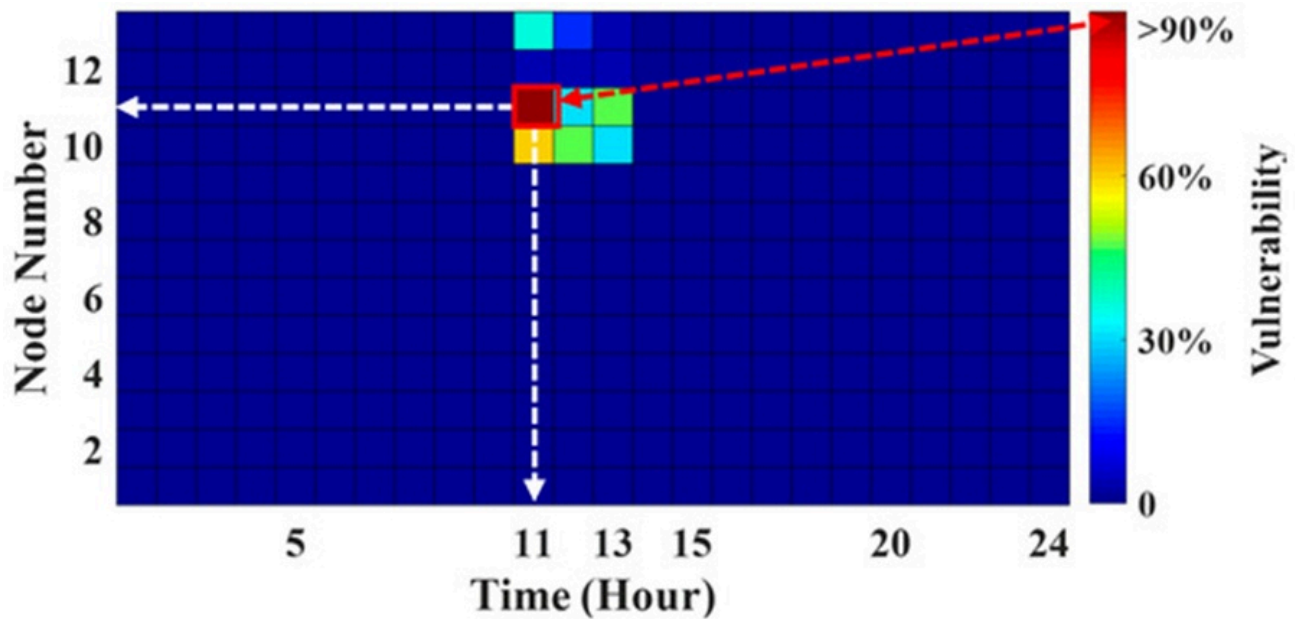


Figure 10. Vulnerability assessment of nodes in the IEEE 13-node system with respect to voltage deviation.

By simultaneously optimizing objective functions (10) and (15), Attacker 1 obtains the set of non-dominated solutions depicted in **Figure 11**, which correspond to varying degrees of induced overvoltage across the microgrid. As shown in **Figure 11**, the resulting Pareto-optimal front exhibits good diversity and spread. This distribution allows Attacker 1 to choose any point along the front (for example, one of the cyan circles) and apply the associated false data vector to load points and generation units, thereby driving the microgrid into an overvoltage state. For instance, selecting the yellow triangle minimizes the total volume of injected false data while yielding the smallest overvoltage magnitude. Conversely, choosing the purple diamond maximizes the severity of overvoltage while requiring the largest volume of falsified data. This trade-off clearly demonstrates the value of framing the problem as a bi-objective optimization problem (BOOP). When both objectives are considered equally important, Attacker 1 assigns equal weights by setting $\xi_k = 0.5$ in **Eq. 20**, thereby identifying the best compromise solution (BCS), which is marked by the red pentagram in **Figure 11**. Notably, the degree of conflict between the two extreme solutions (yellow triangle and purple diamond) reaches approximately 95%, as calculated using the Pythagorean Theorem (**Figure 11**).

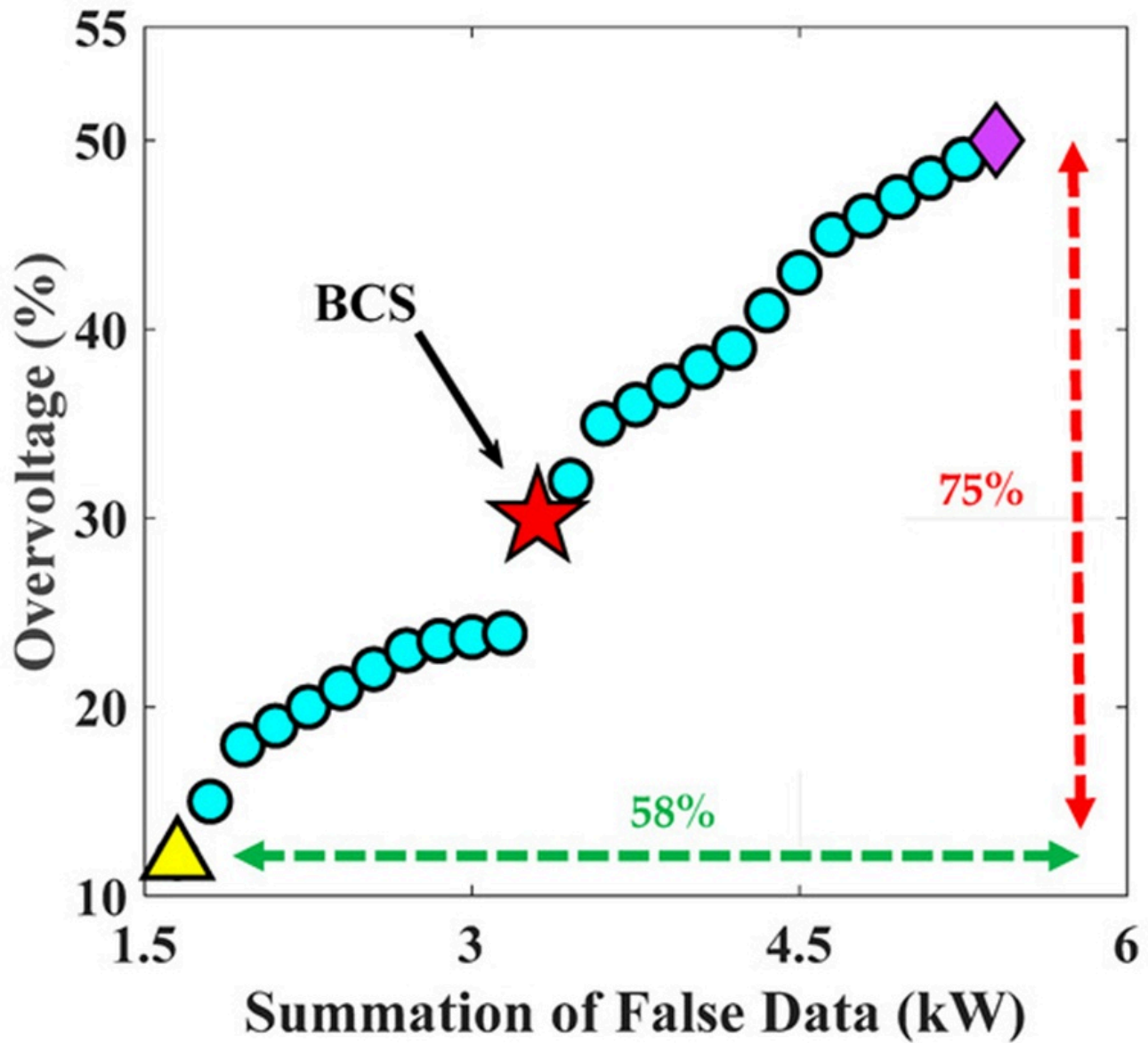


Figure 11. Two-dimensional Pareto-optimal front corresponding to overvoltage induction at node #11.

In a parallel manner, Attacker 2 attacks the microgrid by (a) jointly optimizing objective functions Eqs. 10, 16, (b) generating and archiving the non-dominated solutions in a repository (Figure 12), (c) selecting and injecting the false data vector associated with the magenta pentagram, and (d) forcing the microgrid into an undervoltage condition.

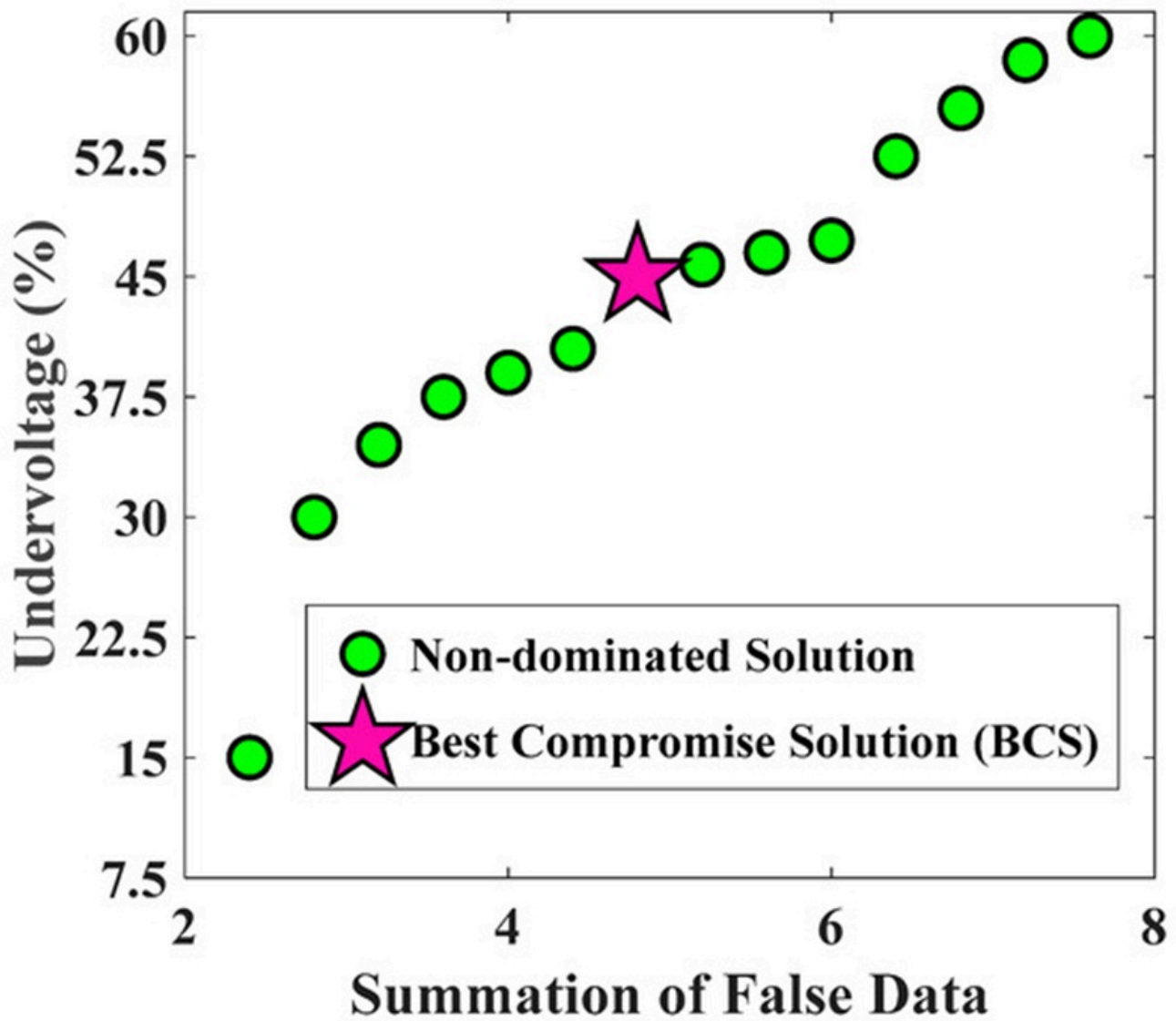


Figure 12. Two-dimensional Pareto-optimal front corresponding to undervoltage induction at node #11.

It should be highlighted that the conflict between minimizing objective function Eq. 10 and maximizing objective function (16) exceeds 95%, again determined via the Pythagorean Theorem, reinforcing the necessity of treating this scenario as a BOOP. To provide clearer insight into the consequences of applying the false data vectors linked to the pentagram points in Figures 11-13 presents the resulting voltage profiles of the microgrid following execution of the FDIAs, which produce both overvoltage and undervoltage conditions.

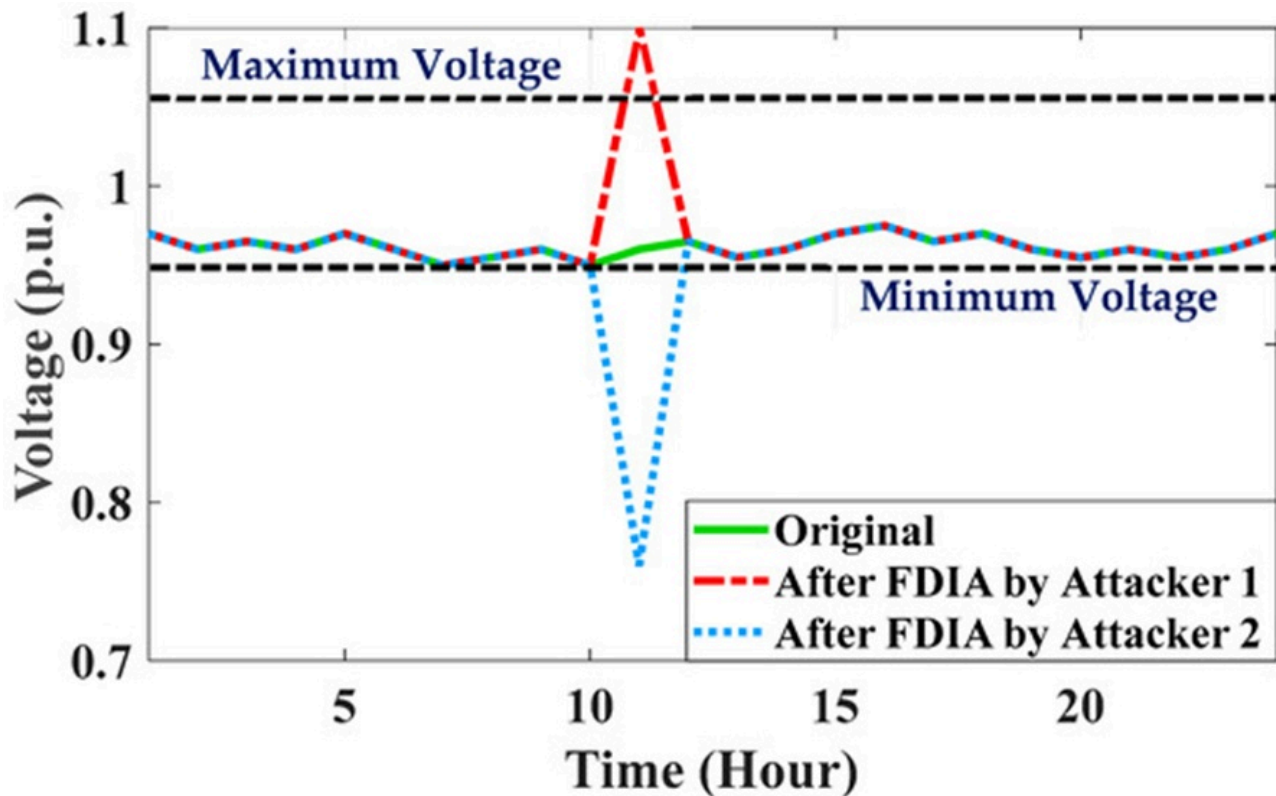


Figure 13. Daily voltage profiles at node #11 following the cyberattacks executed at 11 AM.

To simultaneously induce both overvoltage and undervoltage (i.e., provoke voltage violation), the attackers concurrently optimize objective functions (10), (15), and (16). While the corresponding three-dimensional Pareto-optimal front is presented in **Figure 14**—where the best compromise solution (BCS) among the three objectives is determined by applying **Eq. 20** and assigning equal weights $\xi_k = 1/3$ to each function (marked by the green hexagram)—the attackers have access to a set of 34 non-dominated optimal solutions (represented by the yellow circles in **Figure 14**). This collection enables them to precisely modulate the severity of voltage violations in the microgrid by selecting different points from the Pareto front. For example, if the goal is to emphasize overvoltage more than undervoltage while preserving attack stealthiness, the attackers can assign $\xi_1 = 0.6$ (weight for the overvoltage objective), $\xi_2 = 0.1$ (weight for the undervoltage objective), and $\xi_3 = 0.3$ (weight for the false data minimization objective). Numerous other weight combinations remain feasible given the availability of 34 optimal solutions (yellow circles in **Figure 14**).

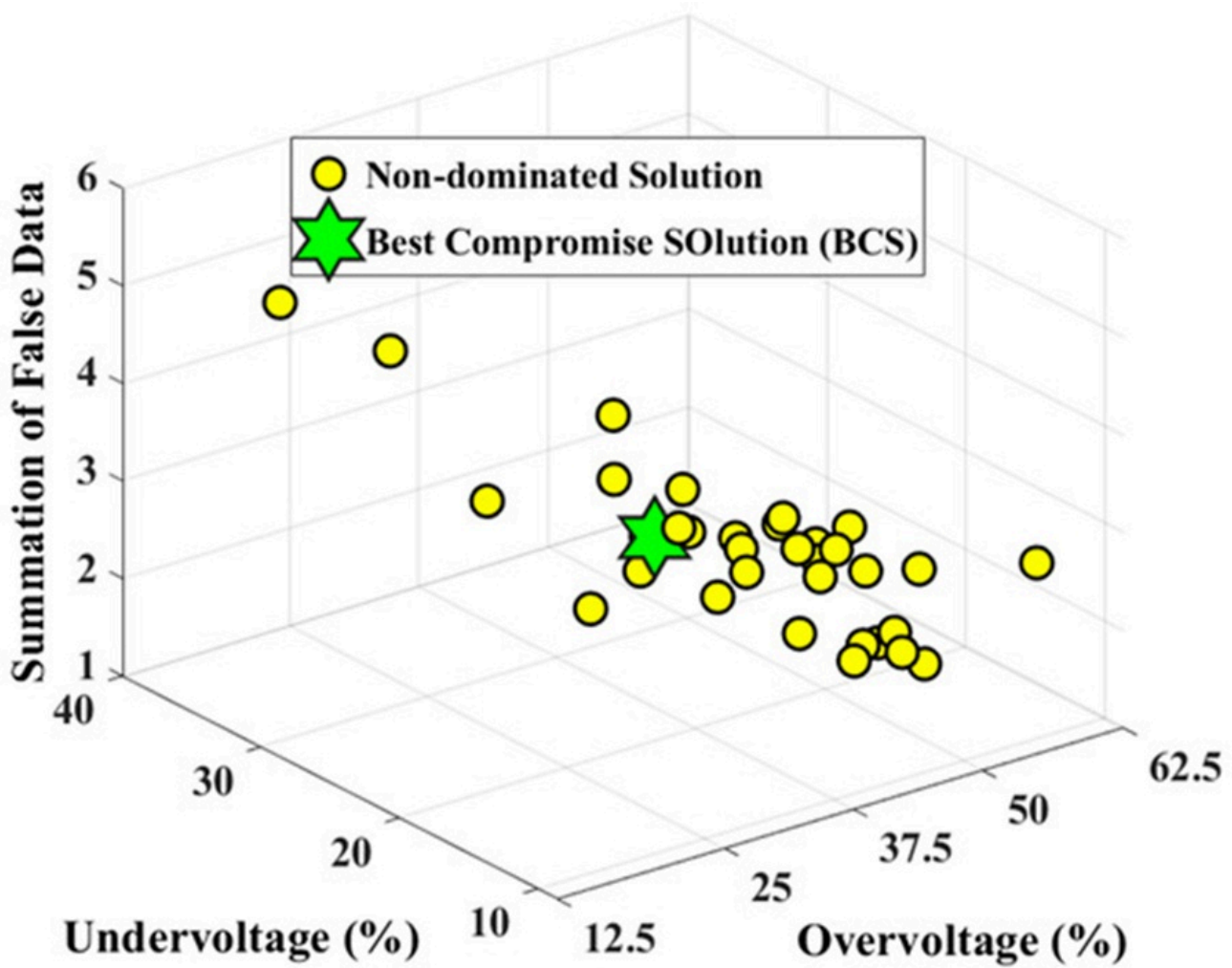


Figure 14. Three-dimensional Pareto-optimal front corresponding to simultaneous overvoltage and undervoltage induction in the microgrid (i.e., voltage violation).

To rigorously evaluate the proposed attack framework, **Table 1** compares its performance against two widely recognized smart grid cybersecurity countermeasures: moving target defense (MTD) [38] and a deep learning-based false data detection approach [39]. This side-by-side analysis reveals the framework’s ability to circumvent these defenses and exposes key shortcomings in current protection technologies when confronted with coordinated false data injection attacks (FDIAs).

Table 1. Performance of the proposed FDIA framework against two prominent defense strategies on the modified IEEE 13-node test system.

Attack/Defense scenario	Developed FDIA targeting node #11	Moving target defense [38]	Deep learning-based detector [39]
Overvoltage (maximized via Eq. 15)	27.6%	16.6%	27.6%
Undervoltage (maximized via Eq. 16)	39.1%	21.4%	39.1%

As described in Naderi and Asrari [38], the MTD strategy bolsters grid security by dynamically and repeatedly altering the system's attack surface, thereby increasing uncertainty for potential adversaries. Nevertheless, MTD is primarily effective against fixed or slowly evolving attack patterns and struggles to fully neutralize the stealthy, synchronized data manipulation achieved by the proposed FDIA framework. According to Table 1, the developed framework produces voltage deviations of up to 27.6% (overvoltage) and 39.1% (undervoltage) at the most vulnerable node (#11). In contrast, MTD mitigates them to 16.6% and 21.4%, respectively, owing to its reconfiguration capability.

Likewise, the deep learning-based anomaly detector described by Naderi and Asrari [39] aims to safeguard data integrity and system stability by identifying anomalies in measurement streams. Although successful against conventional cyber threats, it proves inadequate against the subtle, multi-pronged data alterations introduced by the proposed FDIA approach. The detector's prolonged training requirements and limited flexibility to novel patterns enable the attack framework to evade detection completely, resulting in voltage deviations identical to those observed in the undefended case.

These results indicate that, while established defenses perform adequately against conventional single-vector cyberattacks, they fall short when facing coordinated, multi-objective FDIA strategies. Moreover, Table 1 illustrates how synchronizing attack schedules and simultaneously targeting multiple distributed energy resources (DERs) enables the proposed framework to generate significantly larger voltage excursions than isolated single-attacker attempts, highlighting its elevated disruptive capability.

This evaluation emphasizes the urgent requirement for more sophisticated, adaptive defense strategies—such as real-time anomaly detection supported by digital twin technology—to effectively counter coordinated cyberattacks in next-generation smart grids. Readers seeking in-depth information on the capabilities and constraints of the referenced defense approaches are referred to Naderi and Asrari [38, 39].

Although moving target defense (MTD) and deep learning-based false data detectors offer meaningful layers of protection, both exhibit important weaknesses when challenged by advanced coordinated FDIAs. MTD creates unpredictability through frequent reconfiguration of the attack surface, yet its efficacy diminishes against attackers who adaptively exploit timing windows or employ dynamic strategies. Similarly, deep learning detectors depend critically on comprehensive and representative training datasets, rendering them vulnerable to attacks that closely resemble legitimate behavior or exploit blind spots in the training process.

To strengthen the cybersecurity and robustness of smart grids, integrating complementary defense layers represents a promising path forward. For instance, combining MTD with AI-driven real-time anomaly detection could address both predictable/static and evolving/dynamic threats: MTD complicates the discovery of exploitable entry points, while AI-based systems detect and respond to coordinated, subtle manipulations as they occur. Incorporating strong encrypted communication channels alongside these measures would further protect data confidentiality and integrity.

The suitability of specific defenses also varies depending on the attack context. For example:

- Single-attacker scenarios: MTD alone may provide sufficient disruption by raising the difficulty of locating and exploiting vulnerabilities.
- Coordinated multi-attacker scenarios: A multi-layered strategy—merging MTD, advanced anomaly detection, and robust encryption—is essential to counter synchronized assaults across multiple DERs.
- Stealthy FDIAs: Detectors equipped with continuous, adaptive learning can improve identification rates by regularly refining models using live system telemetry.

Implementing these defenses in operational environments necessitates balancing security gains against deployment costs and operational complexity. MTD offers computational efficiency and can often be integrated with minimal hardware

upgrades, whereas AI-based detectors may demand greater processing power and reliable high-bandwidth links. A prioritized, hybrid deployment—guided by asset-criticality assessments and ongoing vulnerability analyses—can maximize protection while effectively managing resource allocation.

By strategically layering defenses, tailoring responses to specific threat profiles, and optimizing deployment based on risk, the resilience of smart grid infrastructures can be substantially improved. Future research will aim to develop an integrated defense framework that unifies these techniques and quantitatively assesses their collective performance in mitigating coordinated FDIAs under realistic smart grid conditions.

Experimental results on the lab-scale microgrid

The laboratory-scale microgrid shown in **Figures 8 and 9** is modeled as a single-bus system connected to the point of common coupling (PCC). Consequently, the pre-attack evaluation—solving **Eqs. 1–8**—yields only the optimal timing for the FDIAs rather than identifying a specific vulnerable node. Upon solving **Eqs. 1–8**, Attacker 1 determines 9:30 A.M. as the most effective time to induce overvoltage, while Attacker 2 identifies 12:30 P.M. as the ideal moment to provoke undervoltage in the microgrid.

To emphasize the role of distributed energy resources (DERs) in the voltage violations triggered by Attackers 1 and 2, two distinct attack scenarios are examined experimentally as follows:

- Attacker 1 focuses on the photovoltaic (PV) panels to generate overvoltage within the microgrid. Additionally, the attacker falsifies the load sensor measurements by injecting only ΔPD , derived after minimizing the objective function (10),
- Attacker 2 targets the wind turbines to produce varying levels of undervoltage across the laboratory-scale microgrid.

These scenarios are implemented and validated using the hardware-in-the-loop (HIL) platform developed earlier.

The resulting voltage profiles of the microgrid following the FDIAs executed by Attackers 1 and 2 (as outlined in the flowchart of **Figure 5**) are presented in **Figure 15**. These profiles clearly demonstrate successful induction of both overvoltage and undervoltage relative to the system's baseline (original) voltage profile (represented by the green solid curve). The best compromise solutions (BCSs), together with their associated Pareto-optimal fronts that produce the overvoltage and undervoltage conditions shown in **Figure 15**, are illustrated in **Figure 16**.

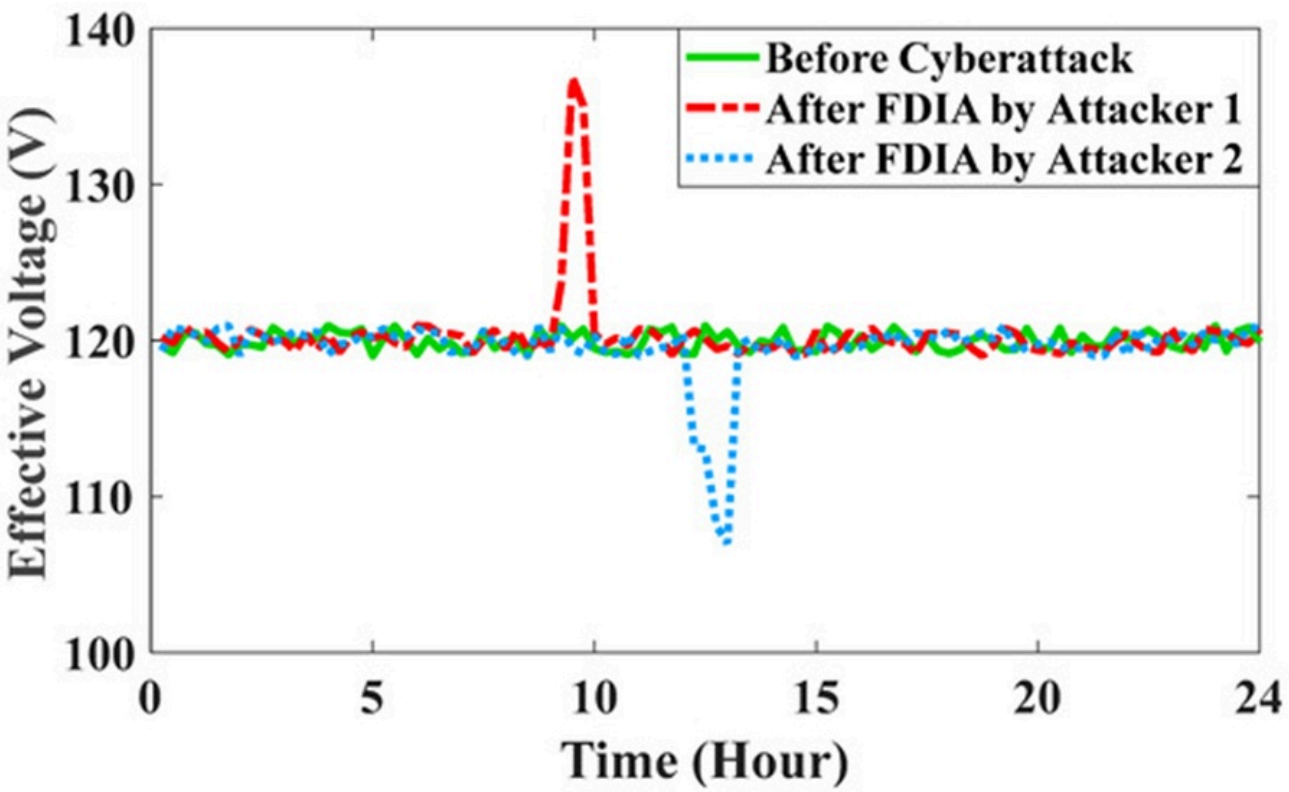


Figure 15. Voltage profile of the targeted microgrid following the FDIAs executed at their respective optimal times.

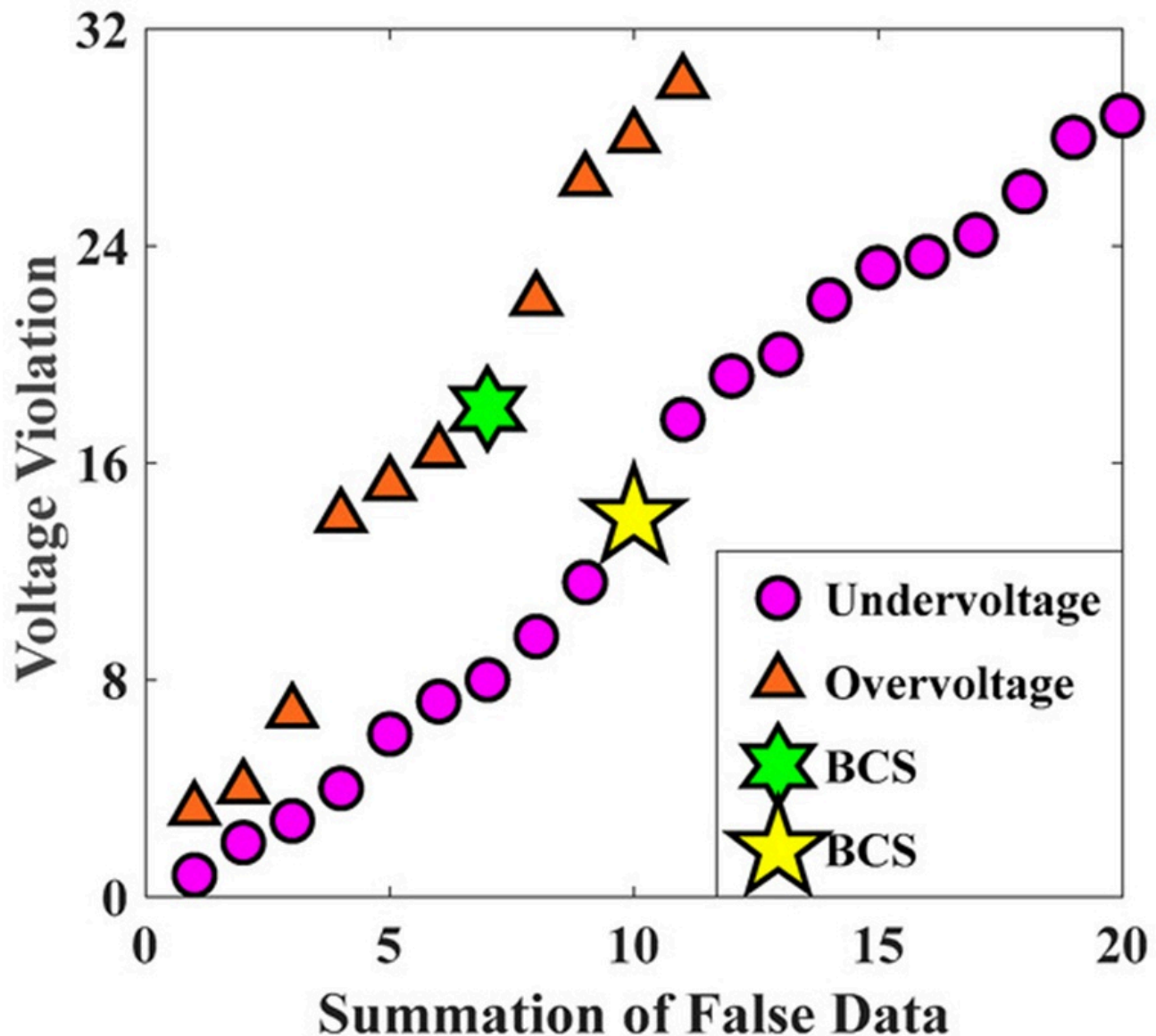


Figure 16. Two-dimensional Pareto-optimal fronts corresponding to the FDIAs that induce overvoltage and undervoltage.

From **Figure 16**, it is evident that the Pareto fronts are well distributed, offering a broad spectrum of achievable voltage deviations, ranging from approximately 1% to over 31% for both overvoltage and undervoltage. Moreover, the BCSs—marked by the green hexagram (for overvoltage) and yellow pentagram (for undervoltage)—are obtained by assigning equal weights ($\xi_k = 0.5$) to the two objective functions in each case (i.e., minimization of total injected false data combined with either maximization of overvoltage or maximization of undervoltage). Consequently, attackers retain the flexibility to adjust the intensity of the voltage violations by modifying the weight factors to alternative values.

To demonstrate the amplified effects of the unified FDIA that simultaneously targets both renewable-based DERs (PV panels and wind turbines), **Figure 17** compares the voltage profile of the microgrid under the coordinated attack (black solid curve) against the original baseline profile (green dashed curve) and the profiles resulting from the independent cyberattacks (**Figure 15**). As depicted in **Figure 17**, when subjected to the unified cyberattack that provokes simultaneous overvoltage and undervoltage (i.e., voltage violation), the microgrid exhibits a maliciously distorted voltage profile persisting for an extended duration—exceeding six hours—far longer than the time windows affected by the two separate FDIAs (**Figure 15**).

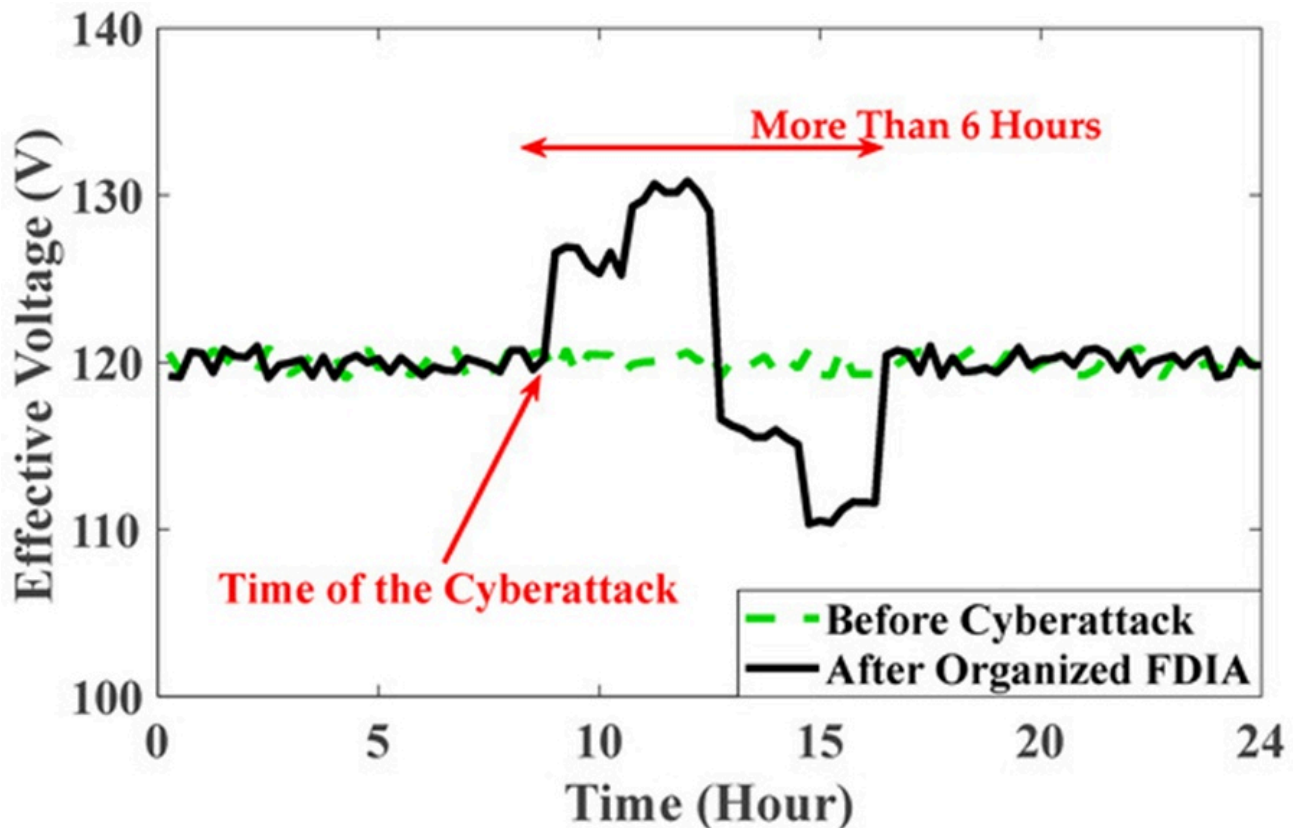


Figure 17. Comparative voltage profiles: independent FDIAs versus the proposed coordinated FDIA.

According to **Figures 15-17**, with particular emphasis on **Figure 16**, the interplay among DER output variability, load fluctuations, false data injection, and resulting voltage deviations can be examined through their combined effects on the system's power flow equilibrium. Variations in load demand and renewable generation directly alter the balance of active and reactive power, thereby influencing the overall voltage distribution across the network. For example, elevated DER production tends to cause overvoltage, while sudden load increases often lead to undervoltage. In contrast, injecting spurious data misleads the control infrastructure by providing inaccurate measurements that either inflate or deflate the perceived system state, thereby exacerbating these voltage excursions. The magnitude of such deviations is further modulated by critical network characteristics, including line impedance values, the degree of DER integration, the voltage sensitivity coefficients with respect to active and reactive power adjustments, and the latency or agility of existing control loops. Notably, networks with high levels of inverter-interfaced resources are more vulnerable to manipulated data inputs because these devices are inherently sensitive to erroneous control signals. Throughout the experimental campaign, these system parameters were held constant to clearly isolate the contributions of false data injection and power flow perturbations. This examination underscores the need for integrated defense approaches that account for both the underlying physical dynamics of the grid and the resilience of control algorithms against cyber threats. A deeper grasp of these interdependencies enables utility operators to strategically allocate resources toward enhanced real-time observability and adaptive control technologies, thereby reducing exposure to both cyberattacks and routine operational variability.

It should be noted that, for the purpose of maintaining focus and clarity, the primary emphasis of this study has been placed on detailing the proposed coordinated multi-objective attack framework involving two attackers with complementary yet distinct goals; nevertheless, the developed methodology is inherently scalable and can be readily extended to accommodate N attackers targeting microgrids of greater size and complexity through FDIAs with diverse objective functions. In such generalized scenarios, the framework can be adapted to support coordination among multiple adversaries (e.g., N attackers), each pursuing independent yet synergistic objectives—such as inducing overvoltage,

undervoltage, line congestion, or even widespread outages—while targeting distinct operational facets of the system. To capture the added intricacy of these multi-agent coordinated false data injection attacks, the optimization formulation presented herein (Eqs. 1–20) can be augmented with an explicit coordination constraint. This constraint would promote complementarity among the attackers’ actions, discouraging mutually canceling behaviors and thereby intensifying the aggregate disruption inflicted on the microgrid. Such coordination may be realized through a multi-agent optimization paradigm, in which individual attackers address localized subproblems while contributing to a collective global objective. The coordination mechanism would impose penalties on conflicting decisions and align incentives to maximize the overall detrimental outcome. Moreover, temporal synchronization can be achieved by defining a time-varying vulnerability index, enabling attackers to pinpoint and align their interventions during periods of peak system susceptibility. These extensions ensure that the generalized framework accurately models realistic large-scale coordinated attack vectors and quantifies their compounded effects on voltage stability and system performance.

Simulation results on the large-scale 136-node distribution system

This section evaluates the effectiveness of the proposed attack strategy using a well-established 136-bus distribution network [40], which has been adapted to an unbalanced three-phase configuration to reflect better the structural characteristics, scale, and operational complexity of actual urban microgrids. Additional details regarding this test case are available in Nirbhavane et al. [41]. Table 2 summarizes the outcomes of the simulated FDIA targeting the most vulnerable bus in this system.

Table 2. Results of the FDIA targeting the most vulnerable bus in the 136-node distribution system.

Description	Susceptible buses/Most vulnerable bus	Optimal result execution time (s)	False load data injected into smart meters (kW)	Voltage deviation (%)
Buses are susceptible to voltage violations	#21, #30, #36, #78, #91, #115	17.22	—	—
The most vulnerable bus	#91	2.6	—	—
Overvoltage (OV)	—	—	23.91	21.35
Undervoltage (UV)	—	—	21.01	21.84

From the data presented in Table 2, it is apparent that although the developed attack framework induces significant voltage violations across the 136-bus network, the system is more susceptible to undervoltage conditions. This is illustrated by the fact that a relatively modest volume of injected false data (e.g., 21.01 kW) at smart meters produces a disproportionately large voltage deviation (e.g., 21.84%). Furthermore, the findings in Table 2 confirm the proposed framework’s ability to generate substantial voltage disturbances across distribution systems spanning a wide range of sizes and complexities.

To assess the robustness of the multi-objective attack framework under highly constrained conditions—specifically, when attackers possess only limited and incomplete knowledge of the 136-node distribution system—a series of Monte Carlo-style simulations was performed using randomized false data injections. These tests demonstrate that meaningful voltage violations can still be achieved despite severe information limitations. Table 3 presents a comparison of attack performance under partial knowledge versus the baseline assumption of full system observability. For instance, with incomplete information, the peak overvoltage deviation was reduced by up to 17.2%. In comparison, the loss of precise timing control extended the required attack duration by approximately 7.3% to attain comparable disruption levels. To generate these results efficiently, the optimization solver was modified to incorporate probabilistic uncertainty constraints reflecting imperfect attacker knowledge of key system parameters. By adopting these more realistic assumptions, the updated framework delivers a thorough assessment of attack viability in practical settings, revealing that coordinated

FDIAs retain considerable disruptive potential even when adversaries operate with significantly reduced situational awareness.

Table 3. Results of FDI attacks under limited knowledge of the actual distribution system, producing varying degrees of overvoltage.

Scenario description	Undervoltage deviation (%)	Execution time (s)
Original Attack Scenario (full knowledge, most vulnerable bus)	21.84	33.32
Targeting a Random Bus within a Set of 10 Buses	18.08	35.76
Targeting a Random Bus within a Set of 50 Buses	18.21	36.11
Targeting a Random Bus within a Set of 100 Buses	19.63	36.20
Targeting a Random Bus within a Set of 136 Buses (entire system)	19.17	36.04

Conclusion

This paper introduced a coordinated multi-objective framework designed to investigate the consequences of synchronized false data injection attacks (FDIAs) on smart microgrids deployed in urban environments, with a specific focus on inducing voltage violations (overvoltage and undervoltage). The validity and effectiveness of the proposed framework were confirmed through (1) numerical simulations conducted on the IEEE 13-node test feeder, reconfigured to represent a fundamental component of city-scale energy infrastructure, and (2) laboratory-based experimental testing performed on a physical prototype smart microgrid equipped with wind turbines and photovoltaic (PV) modules. Both the simulation and experimental results indicate that formulating FDIAs as multi-objective optimization problems offers a superior modeling approach compared to single-objective methods commonly used in the existing literature. This superiority arises because the objective functions are frequently conflicting and cannot be optimized independently or through simple aggregation; they must instead be addressed simultaneously. More specifically, the following key insights were derived from the simulation and experimental findings:

- In the simulation study, the degree of conflict between minimizing the volume of injected false data and maximizing the extent of voltage violation (whether overvoltage, undervoltage, or both simultaneously) exceeded 94% across all tested cases. Consequently, combining these opposing objectives via weighted penalty terms fails to achieve genuine simultaneous optimization. This observation underscores the critical advantage of adopting a multi-objective optimization paradigm, which yields a diverse set of non-dominated solutions rather than forcing a single compromised point.
- In the experimental validation, independent FDIAs produced peak overvoltage and undervoltage deviations of approximately 17% and 15%, respectively, but these disturbances remained confined to short durations measured in minutes. By contrast, the unified coordinated FDIA produced a more moderate voltage violation magnitude (around 11%) but sustained abnormal voltage conditions for over 6 hours, markedly degrading the microgrid's overall reliability. This prolonged impact highlights the particular potency of the proposed attack framework, an effect that would likely become far more severe in large-scale urban microgrids serving thousands of customers.

The study deliberately incorporated key aspects, including the timing and intensity of FDIA execution. It used an optimization-based approach to maximize voltage deviations (both overvoltage and undervoltage) while constraining the volume of falsified data. It further accounted for different microgrid operating states (grid-connected and islanded modes). It included rigorous experimental verification via a hardware-in-the-loop (HIL) platform featuring PV arrays, wind turbines, and hybrid energy storage to emulate key components of real urban energy networks. A Pareto-front solution strategy

was employed to effectively handle trade-offs among conflicting objectives, delivering a comprehensive and robust attack model.

Nevertheless, to preserve computational tractability and maintain focus on the central research questions, certain real-world complexities were intentionally omitted, including dynamic network reconfiguration, weather-dependent renewable variability, actual communication latency, and economic/market-related factors. These simplifications were necessary for the present scope. Still, they open clear avenues for future refinement by incorporating topology dynamics, network delays, and socio-economic dimensions to increase the framework's practical relevance.

Looking ahead, future work will extend the current framework to encompass detailed modeling and analysis of coordinated attacks executed by multiple adversaries. This expansion will emphasize concrete implementation aspects, such as the development of a multi-agent optimization architecture in which attackers exchange limited information and synchronize their efforts to maximize overall disruption. Each attacker will be represented as an autonomous agent pursuing its own specialized goal—such as provoking overvoltage, undervoltage, line congestion, or reliability degradation—while contributing to a unified global objective. The formulation will introduce explicit coordination constraints and information-sharing rules to ensure alignment and complementarity among the agents' strategies. Trade-off mechanisms will be integrated through adjustable weighting parameters that allow attackers to prioritize different disruption targets depending on strategic priorities and resource availability (e.g., emphasizing voltage instability in one context versus inducing widespread congestion in another). This analysis will offer deeper insight into how attackers allocate limited resources to achieve maximal system impact. To assess these multi-attacker strategies, future investigations will conduct both simulation-based studies and experimental validations across diverse operating conditions, incorporating time-varying load patterns and stochastic renewable generation profiles. The laboratory microgrid will be adapted to emulate inter-agent communication channels and coordination protocols, enabling a realistic evaluation of the compounded effects of synchronized multi-party attacks. These advancements will enhance understanding of large-scale coordinated threats and lay the groundwork for more effective, proactive defense countermeasures.

In the subsequent phase of this research, which will concentrate on developing remedial action schemes to counteract such cyberattacks, a comprehensive evaluation of the associated economic costs and societal consequences will be undertaken. Additional constraints and performance indicators will be incorporated to quantify these dimensions explicitly. Attack-side economic modeling will include costs associated with required computational infrastructure, specialized hardware, and the risks/effort required to evade existing protections. Defense-side costs will encompass expenditures on advanced cybersecurity tools, continuous monitoring platforms, and workforce training programs. A dedicated societal impact metric will be defined to capture the broader repercussions of voltage instability across different user groups: industrial consumers may experience production interruptions, equipment damage, and efficiency losses, while residential users may experience appliance failures, prolonged outages, and diminished quality of life. These economic and social dimensions will be embedded into the optimization models as either additional objectives or penalty terms, facilitating a balanced evaluation of investment trade-offs between attack feasibility and defense requirements. By integrating these considerations, the expanded framework will provide a more holistic assessment of the true costs—financial and human—of maintaining secure and stable smart city microgrids. Such analysis will highlight the profound risks posed by coordinated FDIAs to urban energy systems and deliver evidence-based guidance for policymakers and utilities seeking to prioritize cost-effective, high-impact resilience investments.

Finally, forthcoming extensions will incorporate dynamic environmental and operational variables—such as fluctuating weather conditions, unpredictable load patterns, and intermittent renewable output—directly into the attack modeling process. These time-varying factors exert substantial influence on voltage behavior and the overall efficacy of FDIAs. By embedding real-time meteorological inputs and probabilistic load/generation forecasts, the refined framework will better replicate realistic operating environments and more accurately predict attack outcomes under uncertainty. These improvements will strengthen the realism of vulnerability assessments and generate critical insights for engineering adaptive, environment-aware defense solutions tailored to the evolving challenges of modern smart grid ecosystems.

Acknowledgements

None

Conflict of interest

None

Financial support

This work was supported in part by the National Science Foundation (NSF) under Grant #2348420.

Ethics statement

None

Received: 14 Apr 2022

Revised: 26 May 2022

Accepted: 02 Jul 2022

Published online: 20 September 2022

Rights and permissions

Open Access The author(s) retain copyright. This article is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. It may be shared and adapted for non-commercial purposes with appropriate attribution, an indication of changes, and distribution of adaptations under the same license. Third-party material may be subject to separate terms identified in its credit line. View the license at <https://creativecommons.org/licenses/by-nc-sa/4.0/>.

References

- Yan J, Menghwar M, Asghar E, Panjwani MK, Liu Y. Real-time energy management for a smart-community microgrid with battery swapping and renewables. *Appl Energy*. 2019;238:180-94.
- Kottayil SK. *Smart Microgrids*, 1st ed; CRC Press: Boca Raton, FL, USA; Taylor and Francis Group: Boca Raton, FL, USA, 2020.
- Kabeyi MJB, Olanrewaju OA. Sustainable energy transition for renewable and low carbon grid electricity generation and supply. *Front Energy Res*. 2022;9:743114.
- Villanueva-Rosario JA, Santos-García F, Aybar-Mejía ME, Mendoza-Araya P, Molina-García A. Coordinated ancillary services, market participation and communication of multi-microgrids: A review. *Appl Energy*. 2022;308:118332.
- Khazaei J. Stealthy cyberattacks on loads and distributed generation aimed at multi-transmission line congestions in smart grids. *IEEE Trans Smart Grid*. 2021;12:2518-28.
- Wang Y, Liu Y, Li J. Deducing cascading failures caused by cyberattacks based on attack gains and cost principle in cyber-physical power systems. *J Mod Power Syst Clean Energy*. 2019;7:1450-60.
- Liang G, Weller SR, Zhao J, Luo F, Dong ZY. The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE Trans Power Syst*. 2017;32:3317-8.

Deng C, Wang Y, Wen C, Xu Y, Lin P. Distributed resilient control for energy storage systems in cyber–physical microgrids. *IEEE Trans Ind Inform*. 2021;17:1331-41.

Zhou J, Xu Y, Yang L, Sun H. Attack-resilient distributed control for islanded single-/three-phase microgrids based on distributed adaptive observers. *J Mod Power Syst Clean Energy*. 2022;10:109-19.

Li X, Xu Q, Blaabjerg F. Adaptive resilient secondary control for islanded AC microgrids with sensor faults. *IEEE J Emerg Sel Top Power Electron*. 2021;9:5239-48.

Habibi MR, Baghaee HR, Dragicevic T, Blaabjerg F. False data injection cyber-attacks mitigation in parallel DC/DC converters based on artificial neural networks. *IEEE Trans Circuits Syst II Express Briefs*. 2021;68:717-21.

Habibi MR, Baghaee HR, Dragičević T, Blaabjerg F. Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks. *IEEE J Emerg Sel Top Power Electron*. 2021;9:5294-310.

Liu S, Hu Z, Wang X, Wu L. Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks. *IEEE Trans Ind Inform*. 2019;15:4066-75.

Aysheh NGA, Khattab T, Massoud A. Cyber-attacks against voltage profile in smart distribution grids with highly-dispersed PV generators: Detection and protection. In: *Proceedings of the IEEE Electric Power and Energy Conference (EPEC)*; Edmonton, AB, Canada;2020. p. 1-6.

Xu Y. A review of cyber security risks of power systems: From static to dynamic false data attacks. *Prot Control Mod Power Syst*. 2020;5:1-12.

Zhuang P, Deng R, Liang H. False data injection attacks against state estimation in multiphase and unbalanced smart distribution systems. *IEEE Trans Smart Grid*. 2019;10:6000-13.

Abhinav S, Modares H, Lewis FL, Ferrese F, Davoudi A. Synchrony in networked microgrids under attacks. *IEEE Trans Smart Grid*. 2018;9:6731-41.

Liang G, Zhao J, Luo F, Weller SR, Dong ZY. A review of false data injection attacks against modern power systems. *IEEE Trans Smart Grid*. 2017;8:1630-38.

Analysis of the Cyber Attack on the Ukrainian Power Grid. 2016. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf (accessed on 1 October 2024).

Vox Website. 2021. <https://www.vox.com/world/> (accessed on 1 October 2024).

Purlu M, Turkay BE. Optimal allocation of renewable distributed generations using heuristic methods to minimize annual energy losses and voltage deviation index. *IEEE Access*. 2022;10:21455-21474.

Balamourougan V, Sidhu TS, Sachdev MS. Technique for online prediction of voltage collapse. *IEE Proc Gener Transm Distrib*. 2004;151:453-60.

Micky RR, Lakshmi R, Sunitha R, Ashok S. Assessment of voltage stability in microgrid. In: *Proceedings of the International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*; Chennai, India;2016. p. 1268-73.

Chang CT, Wu WJ, Lin SW. Fuzzy multi-choice goal programming and artificial bee colony algorithm for triangular and trapezoidal membership functions. *IEEE Access*. 2021;9:95267-81.

Mukherjee V, Mukherjee A, Prasad D. Whale Optimization Algorithm With Wavelet Mutation for the Solution of Optimal Power Flow Problem. In: Kim D, Roy SS, Lämsivaara T, Deo R, Samui P, editors. *Hand-book of Research on Predictive Modeling and Optimization Methods in Science and Engineering*. Hershey (PA): IGI Global Scientific Publishing; 2018. p. 500-53.

Niknam T, Narimani MR, Jabbari M, Malekpour AR. A modified shuffle frog leaping algorithm for multi-objective optimal power flow. *Energy*. 2011;36:6420-32.

Wind-Turbine-Models Website. <https://en.wind-turbine-models.com/> (accessed on 10 June 2022).

Commercial and Residential Hourly Load Profile. <https://openei.org/doe-opendata/dataset/commercial-and-residential-hourly-load-profiles-for-all-tmy3-locations-in-the-united-states> (accessed on 1 October 2024).

Kumar B, Bihari A, Khan S. Analysis of 13 Nodes Test Feeder Integrated With Renewable Energy Sources and Electrical Vehicle. In: *Proceedings of the 2021 IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON)*; Kuala Lumpur, Malaysia. 2021.p. 1-5.

Kersting WH. Radial distribution test feeders. In *Proceedings of the IEEE Power Engineering Society Winter Meeting. Conference Proceedings* (Cat. No.01CH37194), Columbus, OH, USA, 2001. p. 908-12.

Yousaf M, Muttaqi KM, Sutanto D. Overcurrent Protection Scheme for the IEEE 13-Node Benchmark Test Feeder with Improved Selectivity. In: *Proceedings of the 2020 IEEE Power and Energy Society General Meeting (PESGM)*; Montreal, QC, Canada;2020. p. 1-5.

Naderi E, Bibek KC, Ansari M, Asrari A. Experimental validation of a hybrid storage framework to cope with fluctuating power of hybrid renewable energy-based systems. *IEEE Trans Energy Convers*. 2021;36:1991-2001.

Naderi E, Asrari A. Hardware-in-the-loop experimental validation for a lab-scale microgrid targeted by cyberattacks. In *Proceedings of the 9th International Conference on Smart Grid (icSmartGrid)*, Setubal, Portu-gal; 2021.p. 57–62.

OP4510. System Descriptions. https://blob.opal-rt.com/medias/L00161_0124.pdf (accessed on 1 October 2024).

Imperix Power Electronics. 800 V Voltage Sensor Descriptions. https://blob.opal-rt.com/medias/L00161_0549.pdf (accessed on 1 October 2024).

Imperix Power Electronics. 50 A Current Sensor Descriptions. <https://imperix.com/wp-content/uploads/document/DIN-50A.pdf> (accessed on 1 October 2024).

Imperix Power Electronics. Power Interface for OPAL-RT Hardware. https://imperix.com/wp-content/uploads/document/Power-Interface_OPAL-RT.pdf (accessed on 1 October 2024).

Naderi E, Asrari A, Ramos B. Moving Target Defense Strategy to Protect a PV/Wind Lab-Scale Microgrid Against False Data Injection Cyberattacks: Experimental Validation. In: *Proceedings of the IEEE Power and Energy Society General Meeting (PESGM)*; Orlando, FL, USA; 2023. p. 1-5.

Naderi E, Asrari A. Toward detecting cyberattacks targeting modern power grids: a deep learning framework. In: *Proceedings of the 2022 IEEE World AI IoT Congress (Allot)*; Seattle, WA, USA;2022. p. 357-63.

Mantovani JRS, Casari F, Romero RA. Reconfiguração de sistemas de distribuição radiais utilizando o critério de queda de tensão. *SBA Controle Automação*. 2000;11:150-9.

Nirbhavane PS, Corson L, Rizvi SMH, Srivastava AK. TPCPF: Three-Phase Continuation Power Flow Tool for Voltage Stability Assessment of Distribution Networks With Distributed Energy Resources. *IEEE Trans Ind Appl*. 2021;57:5425-36.