smart cities

MDPI

Article

Mitigating Voltage Violations in Smart City Microgrids Under Coordinated False Data Injection Cyberattacks: Simulation and Experimental Insights

Ehsan Naderi [1] and Arash Asrari [2,*]

[1] Department of Electrical Engineering, College of Engineering and Computer Science, Arkansas State University, Jonesboro, AR 72401, USA; enaderi@astate.edu
[2] Department of Electrical and Computer Engineering, Purdue University Northwest, Hammond, IN 46323, USA
* Correspondence: aasrari@pnw.edu; Tel.: +1-(219)-989-2763

Highlights:

What are the main findings?

- Demonstrating the vulnerability of urban energy systems to coordinated cyberattacks targeting the voltage profile through simulation and experimental validations.
- Highlighting the negative impacts of systematic false data injection attacks while taking more than one objective function at a time.

What is the implication of the main finding?

- Enhancing the reliability of smart city energy systems.
- Providing a basis for designing resilient smart grid infrastructures against cyber threats.

Abstract: This article investigates the impacts of coordinated false data injection attacks (FDIAs) on voltage profiles in smart microgrids integrated with renewable-based distributed energy resources (DERs), a critical component of urban energy infrastructure in smart cities. By leveraging simulation and experimental methods, a coordinated framework is developed for understanding and mitigating these threats, ensuring the stability of renewable-based DERs integral to modern urban systems. In the examined framework, a team of attackers independently identify the optimal times of two different cyberattacks leading to undervoltage and overvoltage in a smart microgrid. The objective function of each model is to increase the voltage violation in the form of either overvoltage or undervoltage caused by the corresponding FDIA. In such a framework, the attackers design a multi-objective optimization problem (MOOP) simultaneously resulting in voltage violations in the most vulnerable regions of the targeted microgrid. Considering the conflict between objective functions in the developed MOOP, a Pareto-based solution methodology is utilized to obtain a set of optimal solutions, called non-dominated solutions, as well as the best compromise solution (BCS). The effectiveness of the unified FDIA is verified based on simulation and experimental validations. In this regard, the IEEE 13-node test feeder has been modified as a microgrid for the simulation analysis, whereas the experimental validation has been performed on a lab-scale hybrid PV/wind microgrid containing renewable energy resources.

Keywords: false data injection attack (FDIA); hardware-in-the-loop (HIL); overvoltage; simulation and experimental validations; smart cities; undervoltage; urban energy systems

Academic Editor: Pierluigi Siano

Received: 26 November 2024
Revised: 18 January 2025
Accepted: 26 January 2025
Published: 29 January 2025

Citation: Naderi, E.; Asrari, A. Mitigating Voltage Violations in Smart City Microgrids Under Coordinated False Data Injection Cyberattacks: Simulation and Experimental Insights. *Smart Cities* **2025**, *8*, 20. https://doi.org/10.3390/smartcities8010020

1. Introduction

1.1. Background, Definitions, and Motivation

The sustainable transition of conventional energy systems toward smarter power networks cannot come true without the concept of smart microgrids [1]. According to [2], a smart microgrid is defined as an ideal way to integrate renewable-based distributed energy resources (DERs) on the community level, allowing end-use customers to be able to contribute to the electricity enterprise. In addition, the sustainable transition strategies need to be in line with the Paris Agreement aiming at mitigating global warming by reducing greenhouse gas emissions [3]. This is where the significance of renewable-based DERs as the main assets of smarter power grids becomes clear from the viewpoint of system operators as well as policymakers. However, such smart energy systems need to be monitored and controlled via intertemporal communication platforms if an acceptable level of resilience and reliability is to be achieved [4]. In other words, although the intersection of energy and ICT (information and communication technology) infrastructures facilitates sustainable development in the field of power and energy, it introduces a noticeable attack surface in the cyber layer of smart power grids. In the context of smart cities, where power systems are increasingly integrated with digital technologies to optimize energy distribution, these vulnerabilities can compromise key objectives like energy efficiency, grid resilience, and urban innovation. As an illustration, adversaries in the form of man-in-the-middle (MiTM) can detour the security systems, penetrate the control center, and compromise the recorded information, resulting in different operational issues including but not limited to congestion in branches of systems [5], cascading failures [6], and blackouts [7]. One of the consequences of false data injection attacks (FDIAs) targeting modern power systems, especially smart urban microgrids, can be voltage violation in the form of overvoltage and undervoltage; hence, the motivation of this paper is to scrutinize such cyberattacks.

1.2. Literature Review

In [8], a distributed resilient control framework was introduced to restore the voltage profile of a cyber–physical microgrid, operated in standalone modality, that contained multiple energy storage systems. The proposed approach in [8] avoided the strictly increasing behavior of controller's gain to mitigate the impacts of faults and cyberattacks. In [9], the voltage regulation issues as the consequence of cyberattacks were studied in single-phase and three-phase microgrids in islanded modalities. The adaptive resilient secondary voltage and frequency control problem was investigated in [10], where an islanded microgrid was the target of data integrity attacks. The impacts of FDIAs over DC/DC voltage converters on a smart microgrid were investigated in [11], where time-varying FDIAs were launched to significantly affect the functionality of the system. In [12], two different models for FDIA were introduced to compromise voltage measurements in a DC microgrid, affecting the voltage regulation and current sharing. In [13], the stochastic stability of a standalone microgrid was analyzed in the presence of a denial of service (DoS) cyberattack. Further, a remedial action oriented toward control of secondary frequency regulation was proposed in [13] to mitigate the impacts of a DoS attack. In [14], the voltage profile of a smart grid integrated with photovoltaic (PV) units was the target of FDIAs resulting in voltage deviations in the forms of overvoltage and undervoltage. It is noted that the proposed framework in [14] contained different strategies to prevent and detect the cyberattacks targeting smart power grids. Moreover, in the earlier step of this research, a hardware-in-the-loop (HIL) setup was developed in order to (a) detect the presence of false data, stealthily injected into the sensors' readings of a lab-scale microgrid, and (b) distinguish transient phenomena from malicious FDIAs resulting in a shortage of power in the microgrid [15].

1.3. Research Gap and Contribution of This Work

Although relevant research works (e.g., [8–15]) are proposed in the field of analyzing the impacts of cyberattacks targeting voltage profile of smart grids, there is no work to develop and experimentally validate a multi-objective framework to scrutinize the impacts of FDIAs targeting smart microgrids to cause voltage violation (i.e., both overvoltage and undervoltage at the same time) when the microgrid is most vulnerable to deviation in voltage. To address the indicated research gap, we scrutinize a FDIA framework, which has the following contributions:

- Designing a multi-objective unified framework from attackers' standpoints to target smart microgrids at the most vulnerable time to undervoltage and overvoltage, resulting in a set of non-dominated solutions (i.e., Pareto-front) to obtain a range of overvoltage and undervoltage rates,
- Experimentally validating the developed framework on a lab-scale smart microgrid, containing wind turbines and PV modules, besides the simulation-based validation to identify the best compromise solution (BCS) between undervoltage and overvoltage.

In summary, the findings of this research address a critical gap in the ability to protect smart microgrids from cyberattacks targeting voltage regulation. By improving the security, efficiency, and resilience of urban energy systems, this work directly supports the development of secure, reliable, and adaptable infrastructures in smart cities. These advancements are essential for achieving the broader goals of energy efficiency, urban resilience, and the integration of innovative technologies in the urban ecosystem.

2. Materials and Methods

The developed framework in this section is validated through simulation and experimental tests. Specifically, the experimental validation of FDIA scenarios on a lab-scale microgrid provides a valuable prototype for real-world smart city scenarios by simulating critical components of urban microgrid configurations. In practice, smart cities integrate DERs (e.g., PV and wind units) with advanced control systems for energy management and distribution, much like the lab-scale microgrid used in this study. By replicating these elements within a controlled experimental setup, this research can model how cyberattacks could impact voltage stability, energy efficiency, and overall grid performance in a typical urban environment.

2.1. Developed Framework

The developed multi-objective framework is illustrated in Figure 1. According to Figure 1a, a typical smart microgrid can be targeted by N attackers to significantly enhance the negative impacts of the unified attack framework; however, for the sake of clarity as well as elaborating the idea, Figure 1b only includes two attackers. From Figure 1b, it can be inferred that Attacker 1 targets the microgrid, which can be operated in both grid-connected and standalone modalities, via a FDIA resulting in overvoltage (OV) at the most vulnerable time. In addition, Attacker 2 in another independent cyberattack targets the microgrid to cause undervoltage (UV) at the optimal time. It is noted that these two cyberattacks are designed as bi-objective optimization problems (BOOPs) to obtain a set of optimal solutions instead of one unique solution. The objective functions of these two BOOPs include (a) maximizing the rate of overvoltage/undervoltage in the microgrid and (b) minimizing the amount of false data (to be injected to the system) to ensure the intended rates of voltage violation. This is to ensure that the attackers can maximize the voltage violation while the injected false data vectors remain small enough. The results of these two attacks might not necessarily affect each other since (a) the objective functions are not in accord with each other and (b) the optimal time of the FDIAs may be different.

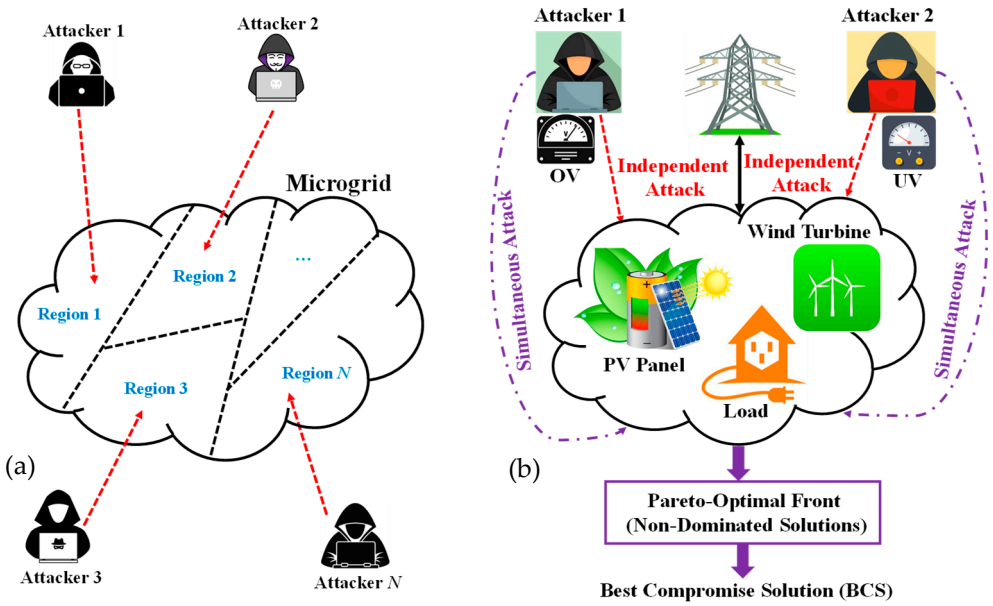

Figure 1. The developed FDIA framework leading to voltage violation in (**a**): general microgrid, and (**b**): critical building block of urban energy systems in smart cities.

It is noted that after each independent cyberattack, the microgrid operator may apply appropriate remedial action schemes to bring back the system to the normal operation. More importantly, the remedial actions might implement different techniques since the nature of the cyberattacks is different. However, in order to validate the worst-case scenario, this paper presents a unified FDIA, which is oriented to a multi-objective optimization problem (MOOP), including three different objective functions (i.e., simultaneously maximizing the rate of overvoltage, maximizing the rate of undervoltage, and minimizing the amount of false data to be injected to the cyber layer). In other words, the microgrid can be targeted by a unified stealthy cyberattack leading to overvoltage and undervoltage at the same time (i.e., the contribution of this paper). In addition, the vector of (to be injected) false data is minimized to reduce the chance of being caught by the microgrid's operator. Hence, the microgrid operator will need a powerful remedial action to be implemented against both cyberattacks. This will be the scope of our future work.

According to Figure 1b, in order to target the microgrid via two simultaneous FDIAs, the team of two attackers solves an MOOP to recognize the set of non-dominated solutions, called the Pareto-optimal front, and saves them in a repository. Although the MOOP has three objective functions, Figure 2 illustrates only overvoltage and undervoltage objective functions to obtain a better perspective about the Pareto-front. From Figure 2, it can be perceived that after solving the MOOP by the attackers, a set of optimal solutions (see the red circles presented in Figure 2) is obtained instead of one unique optimal solution. Hence, attackers can control the severity of undervoltage and overvoltage in the unified cyberattack and identify the best compromise solution (BCS) as a trade-off between objective functions.

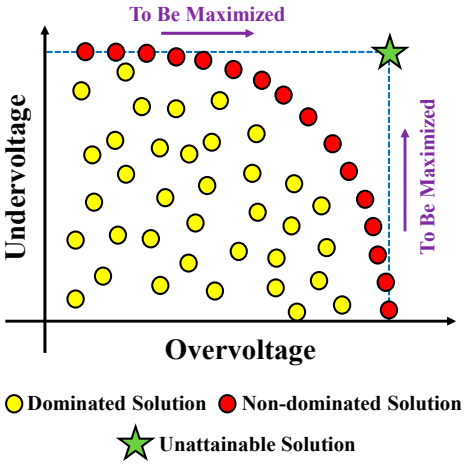

Figure 2. The typical two-dimensional Pareto-optimal front associated with the developed FDIA framework in this paper.

2.2. Problem Formulation

2.2.1. Pre-Attack Evaluation to Pinpoint the Most Vulnerable Node

This section presents an optimization problem that provides both attackers introduced in Figure 1b with better understandings about the most vulnerable node to deviation in voltage in the microgrid as well as the optimal time of the attack. To this end, both attackers solve Equation (1) considering Equations (2)–(8) as the technical constraints of the problem. It is noted that attackers have access to the original voltage profile of the microgrid. This is called realistic attack assumption, which has been adopted from [16–18]. As a real-world example, the attackers targeting the Ukraine power grid in 2015 managed to gain access to the computer networks and obtain sensitive information about the system's history, resulting in one to six hours of power shortage for 225,000 end-users [19]. Another example is the U.S. power grid, which, in 2018, was the target of attackers attempting to collect critical information about the power generation facilities [20]. After solving the optimization problem (i.e., Equations (1)–(8)) to maximize the voltage deviation in the microgrid, attackers will obtain a new voltage profile. Comparing these two voltage profiles (i.e., the original profile and the one obtained from solving Equations (1)–(8)), they can recognize the most vulnerable node to deviation in voltage and the optimal time of the (to be performed) cyberattacks.

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

$$P_t^{Generation} - P_t^{Demand} - P_t^{Loss} = 0 \tag{2}$$

$$Q_t^{Generation} - Q_t^{Demand} - Q_t^{Loss} = 0 \tag{3}$$

$$V_{\min} \leq V_{n,t} \leq V_{\max} \tag{4}$$

$$\delta_{\min} \leq \delta_{n,t} \leq \delta_{\max} \tag{5}$$

$$P_{\min} \leq P_{n,t} \leq P_{\max} \tag{6}$$

$$Q_{\min} \leq Q_{n,t} \leq Q_{\max} \tag{7}$$

$$I_{\min} \leq I_{b,t} \leq I_{\max} \tag{8}$$

where $V_{n,t}$ is the voltage magnitude of node n at tth time interval and 1.00 p.u. is the nominal voltage magnitude for buses throughout the distribution system; N_n is the total number of

nodes in the microgrid excluding the PCC; $P_t^{Generation}$, P_t^{Demand}, and P_t^{Loss} are, respectively, the total amount of active power generation, the total active demand, and the total active power loss of microgrid at tth time slot; $\delta_{n,t}$ is the voltage phase angle associated with node n at tth time slot; $P_{n,t}$ and $Q_{n,t}$ are, respectively, the net active and reactive power for node n at time t; and $I_{b,t}$ is the magnitude of current flowing into bth branch at tth time interval.

2.2.2. Intentional Voltage Alteration from Attackers' Standpoint

The equivalent circuit of a typical microgrid from the point of common coupling (PCC) is depicted in Figure 3, where Z_n^{Eq} is the equivalent impedance of the microgrid; V_n and VPCC are, respectively, the voltage magnitude at node n and PCC; I_{DER} is the magnitude of the current from the DERs (e.g., PV panel and wind turbine). If (a) the voltage at PCC is considered as the reference voltage and (b) power loss through Z_n^{Eq} is neglected, the magnitude of voltage at node n can be approximately written in (9).

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

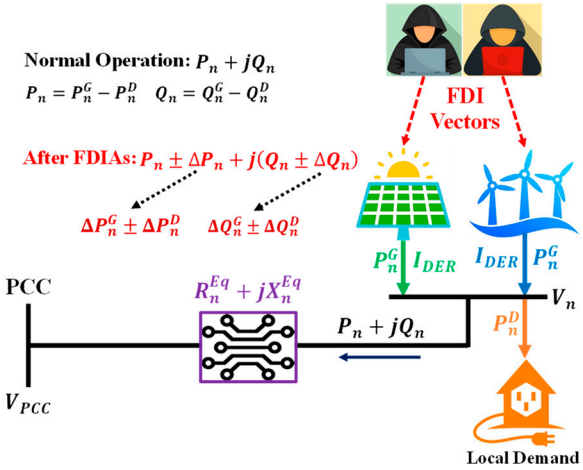

Figure 3. The equivalent circuit of a typical microgrid from the point of common coupling (PCC).

From Equation (9), it can be gathered that injecting false data (e.g., ΔP_n and ΔQ_n) to the net powers associated with node n (i.e., P_n and Q_n) results in different rates of violation in the voltage magnitude of node n. In other words, any positive or negative values of ΔP_n and ΔQ_n will result in different rates of deviation in both forms of overvoltage and undervoltage (see Figure 3). However, attackers need to ensure that the amount of false data injected into both load centers and generation units installed on each node will not trigger the security systems [16–18]. Toward this end, Equation (10) presents the developed optimization problem that needs to be solved by attackers to recognize the minimum false data vectors to be injected into the microgrid's control center. It is noted that the optimization problem presented in Equation (10) should be solved subject to satisfying Equations (2)–(8) to meet the technical constraints of the microgrid as well as Equations (11)–(14) to ensure that the cyberattacks do not violate the rated values.

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

$$-\partial \times P_{n,t}^G \le \Delta P_{n,t}^G \le \partial \times P_{n,t}^G \tag{11}$$

$$-\partial \times P_{n,t}^D \le \Delta P_{n,t}^D \le \partial \times P_{n,t}^D \tag{12}$$

$$-\partial \times Q^G_{n,t} \leq \Delta Q^G_{n,t} \leq \partial \times Q^G_{n,t} \tag{13}$$

$$-\partial \times Q^D_{n,t} \leq \Delta Q^D_{n,t} \leq \partial \times Q^D_{n,t} \tag{14}$$

where ∂ is the percentage of injected false data to the rated values of generation and demand, which will be up to 10% of the rated values; and Δ indicates the alteration associated with active and reactive powers, which is limited in order to decrease the chance of being caught by detection systems.

2.2.3. Independent FDIA Model Leading to Overvoltage

The main objective function from Attacker 1's point of view is presented in Equation (15), which is adopted from [21]. It is noted that the objective function of maximizing the intentional overvoltage (i.e., Equation (15)) and the objective function limiting the false data vectors (i.e., Equation (10)) should be optimized concurrently as a bi-objective optimization problem (BOOP).

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

where V_{ref} is the reference voltage associated with node n; and α is a parameter controlling the rate of overvoltage.

2.2.4. Independent FDIA Model Leading to Undervoltage

Adopted from [22], this section provides an optimization problem oriented to the undervoltage proximity index from the viewpoint of Attacker 2 (refer to Figure 1b). Therefore, the attacker maximizes the introduced index, as presented in Equation (16), along with minimizing Equation (10) as a BOOP in order to push the microgrid toward undervoltage in such a way that the vectors of injected false data remain below the threshold. Referring to [22,23], objective Function (16) indicates the conditions based on which the probability of undervoltage at node n is maximized.

$$\max \left\{ \left| 1 - \frac{\sum_{t=1}^{24} \sum_{m=1,m\neq n}^{N_n} V_{m,t} \times \frac{Y_{nm}}{\sum_{n=1,n\neq k}^{N_n} Y_{nk}}}{\sum_{t=1}^{24} V_{n,t}} \right| \right\} \tag{16}$$

where Y_{nm} is the admittance between nodes n and m.

2.2.5. Unified FDIA Leading to Voltage Violation

The developed coordinated FDIA resulting in both overvoltage and undervoltage at the same time needs to be solved as an MOOP with three objective functions. The first objective function is to maximize the overvoltage (i.e., Equation (15)), the second objective function maximizes the undervoltage (i.e., Equation (16)), and the third objective function ensures the false data vectors to be injected into load centers and generation units are small enough to prevent any violation in the rated values (i.e., Equation (10)). Therefore, the developed FDIA has three dimensions; however, as an illustration, Figure 2 demonstrates the Pareto-front associated with maximizing the main objective functions of this problem (i.e., Equations (15)–(16)) to facilitate capturing the idea. More information about the 2D and 3D Pareto-optimal fronts will be provided in Section 3.2.

2.2.6. Formulation of the Embedded Multi-Objective Methodology

Since the objective functions associated with the developed BOOPs (refer to Sections 2.2.3 and 2.2.4) and MOOP (see Section 2.2.5) lie in different numerical ranges, their values should be converted to the unified range of [0–1], as displayed in Figure 4 and written in Equation (17). According to this figure, called the trapezoidal membership function, one can infer that if the value of the function is equal to zero, the decision-maker is not satisfied with the objective function; however, when the numerical value of the membership function is equal to one, the decision-maker is fully satisfied [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 denotes the fuzzy set for kth objective function; f_k indicates kth objective function; f_k^{min} and f_k^{max} are, respectively, minimum and maximum boundaries for kth objective function and X is the vector of decision variables of the problem.

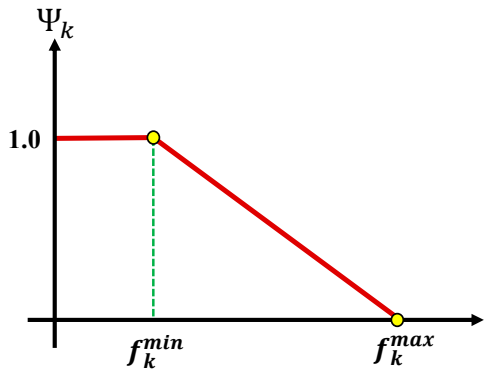

Figure 4. Trapezoidal membership function for all objective functions.

In order to recognize the set of non-dominated solutions (i.e., the Pareto-optimal front), first, an area will be defined for each solution stored in the repository. Then, by applying Equations (18) and (19), the dominated solutions will be recognized and removed from the repository. The rest is called the Pareto-optimal front. Based on Equations (18) and (19), considering a minimization problem (e.g., Equation (10)), x_1 dominates x_2 if the following statements are met: (a) x_1 is no worse than x_2 in all objective functions and (b) x_1 is better than x_2 in at least one of the objective functions [25].

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

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

After obtaining the Pareto-optimal front, Equation (20) will be applied on the repository to identify the BCS (i.e., the trade-off among objective functions). In Equation (20), Υ_Ψ indicates the BCS among objective functions; ξ_k denotes the weight factor for kth objective function; N_{obj} and N_{NDS} are, respectively, the number of objective functions and the number of non-dominated solutions in the repository [26].

$$\Upsilon_\Psi(k,i) = \frac{\sum_{k=1}^{N_{obj}} \xi_k \times \Psi_{k,i}}{\sum_{i=1}^{N_{NDS}} \sum_{k=1}^{N_{obj}} \xi_k \times \Psi_{k,i}} \quad (20)$$

The implementation steps of the framework are illustrated in Figure 5, covering the introduced FDIAs in Section 2.1 and Figure 1b. This chart illustrates the sequential flow of the study, mapping each step of the methodology to its corresponding section in the paper. The flow begins with the pre-attack evaluation to pinpoint the most vulnerable node in the microgrid by solving the optimization problem defined in Equations (1)–(8). This step identifies the nodes and time intervals most susceptible to voltage deviations, providing critical inputs for the subsequent attack strategies. Next, the framework models intentional voltage alteration from the attackers' standpoint by formulating independent optimization problems for overvoltage (Equation (15)) and undervoltage (Equation (16)) under constraints defined in Equations (10)–(14). These objective functions are normalized using the trapezoidal membership function described in Equation (17) to ensure compatibility across differing numerical ranges. Once normalized, the independent optimization problems are simultaneously solved as part of a multi-objective optimization problem (MOOP), capturing the attackers' ability to cause overvoltage and undervoltage simultaneously. Finally, the results are processed using Equations (18)–(20) to identify the set of non-dominated solutions, known as the Pareto-optimal front, and to determine the best compromise solution (BCS). This process highlights the attackers' capacity to optimize conflicting objectives while remaining undetected, which is crucial for analyzing vulnerabilities in the targeted microgrid.

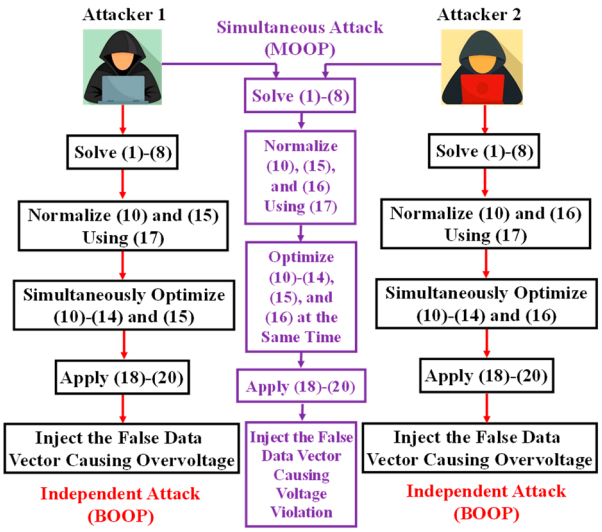

Figure 5. An overview of mathematical relationships in the developed coordinated FDIA framework in this paper.

2.2.7. Assumptions to Be Considered for This Type of Cyberattack

From an attacker's perspective, targeting power systems requires several key assumptions to be considered for effective exploitation [5,6]. First, it is assumed that attackers have access to critical infrastructure networks, which may be vulnerable due to weak or outdated cybersecurity measures or social engineering tactics like phishing. However, in real-world scenarios, obtaining such access would require attackers to breach multiple security layers, often involving significant risk and resource investment. For example, sophisticated attackers would need to navigate firewalls, intrusion detection systems, and encrypted communication protocols, which may delay or limit the effectiveness of their attack. Additionally, it is anticipated that power grids rely on complex, interconnected systems, where compromising one component (e.g., a substation or control center) could have cascading effects. However, it should be noted that the information attackers obtain may be incomplete or outdated, increasing the likelihood of errors or miscalculations during the attack. Communication delays and physical device limitations, such as hardware

performance constraints or bandwidth restrictions, are also practical challenges that may reduce the efficacy of an attack in real-world conditions.

Moreover, this study assumes that the grid's monitoring and incident response capabilities are insufficient or reactive rather than proactive, providing a window of opportunity to cause disruption before detection. While this assumption allows for the evaluation of worst-case scenarios, it is acknowledged that many power grid operators are continuously improving their cybersecurity measures, employing advanced detection techniques, and implementing redundancy to mitigate such threats. These assumptions align with the realistic attack models discussed in the existing literature [11,17,18], which recognize that while sophisticated attackers may exploit software vulnerabilities, manipulate control protocols, or sabotage hardware, they often face significant challenges in bypassing well-implemented security defenses. By explicitly including these considerations, this study aims to highlight both the potential vulnerabilities and the inherent difficulties in executing such coordinated cyberattacks. Future work will extend the framework to incorporate dynamic security measures and evaluate the robustness of the proposed attack scenarios under more stringent real-world constraints.

3. Simulation and Experimental Results

3.1. Initialization and Introducing the Case Studies

To evaluate the effectiveness of the developed multi-objective FDIA, two different case studies are implemented. In the simulation analysis, the modified version of the IEEE 13-node test feeder (see Figure 6) is utilized as a microgrid to highlight the impacts of the unified cyberattack on its voltage profile. To this end, a PV plant with a capacity of 200 kW is added to node #6. In addition, a wind turbine, manufactured by Wind World [27], with a rated power of 250 kW and blade diameter of 29.2 m is added to node #7. It is noted that the solar irradiance at standard test conditions and the operating irradiance point are, respectively, equal to 1000 W/m^2 and 120 W/m^2.

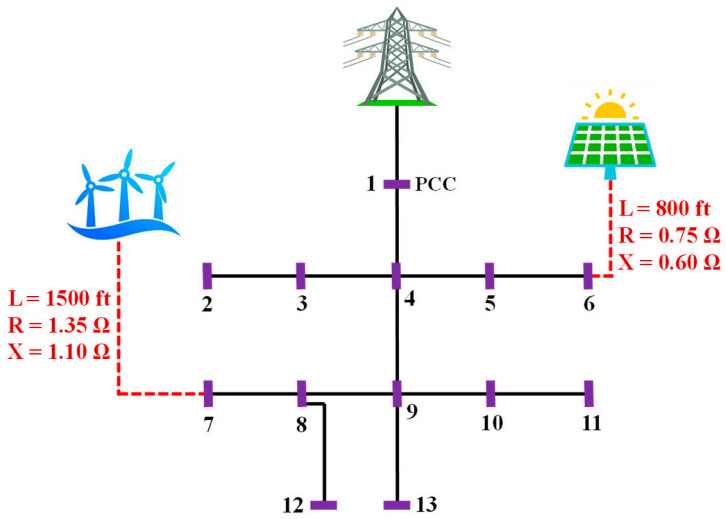

Figure 6. The modified IEEE 13-node test system as a microgrid as a building block of real-world smart cities.

It is also noted that the hourly active and reactive power profiles in a 24 h horizon are adopted from [28,29], which are depicted in Figure 7. The rest of the system's data can be found in [30,31].

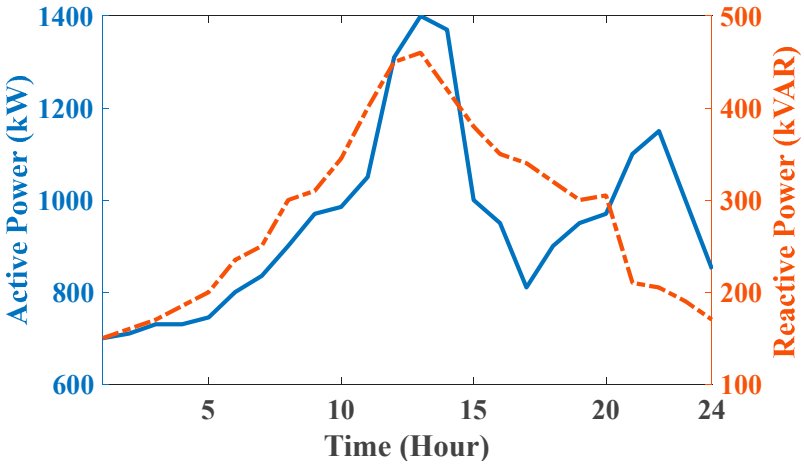

Figure 7. Total hourly active and reactive power profiles for the modified IEEE 13-node test case.

The lab-scale microgrid developed in the first step of this research (see Figure 8) is chosen for the experimental analysis [32,33]. According to Figure 8, one can perceive that the lab-scale microgrid encompasses two horizontal axis and vertical axis wind turbines, respectively, rated at 500 W and 400 W, two 160 W solar panels, a fan with 19,500 cubic feet per minute (CFM) airflow to produce wind in the lab, four 2200 W LED lights to produce solar radiation in the lab, two grid-connected power inverters rated at 500 W, one standalone inverter and its controller rated at 2000 W, a hybrid energy storage system (i.e., a combination of batteries and supercapacitors), and the corresponding buses, switches, and charge controllers. Interested readers are directed to the earlier steps of this research to obtain detailed information about the lab-scale microgrid and its assets [32,33].

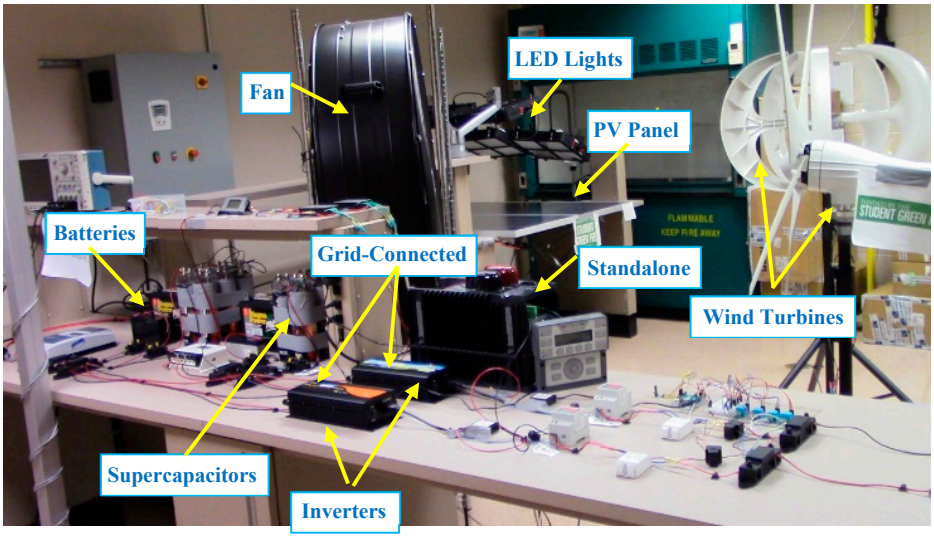

Figure 8. The lab-scale smart microgrid developed at Power System Design Laboratory, containing wind turbines and PV modules.

Figure 9 presents the HIL setup for the lab-scale microgrid [33–37]. The reliability of the analysis results is validated through a combination of simulation using the IEEE 13-node test system and experimental testing on a lab-scale microgrid. The lab-scale microgrid utilizes HIL testing, integrating physical components such as PV panels, wind turbines, and hybrid storage systems with real-time simulation. This setup closely mimics real-world operational conditions, providing a reliable benchmark for evaluating the proposed framework. These results demonstrate the framework's effectiveness in reflecting realistic behaviors within smart microgrid systems under coordinated cyberattacks.

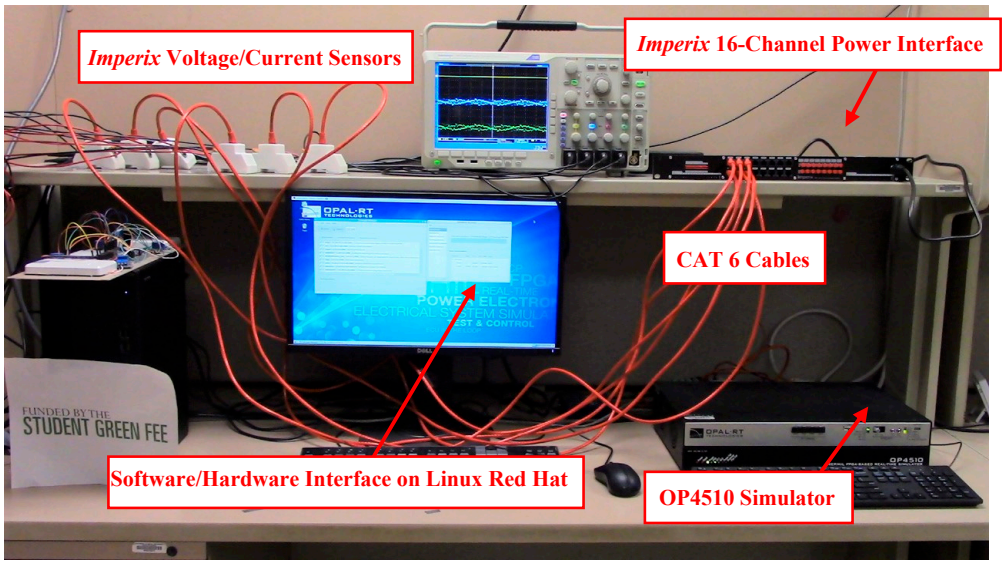

Figure 9. The HIL setup for the developed lab-scale microgrid illustrated in Figure 8 [33–37].

The optimization problems were modeled in MATLAB R2018b on an Intel (R) Core (TM) CPU i5-7500 @ 3.4 GHz. Additionally, the MATPOWER package, a powerful tool for simulating and optimizing electric power systems, was used to perform the Newton–Raphson power flow calculations. Moreover, the problems were solved using the modified whale optimization algorithm-wavelet mutation (MWOA-WM), introduced in [25].

In this regard, the size of whales' population and the maximum number of iterations are, respectively, set to 200 and 100. Interested readers are directed to [25] for more information about the rationale behind the MWOA-WM and its performance over a variety of complicated optimization problems including but not limited to power- and energy-related problems.

3.2. Simulation Results on the Modified IEEE 13-Node System

The main goal of the pre-attack evaluation is to recognize the most vulnerable node to deviation in voltage as well as the optimal time of the FDIAs. In this regard, attackers solve Equations (1)–(8), aiming at increasing the voltage deviation in the microgrid. The difference between the original voltage profile and the one obtained by the attackers is provided in Figure 10. According to this figure, one can infer that only nodes #10, #11, and #13 from 11 AM to 1 PM are susceptible to voltage deviation. However, the pre-attack evaluation confirms that node #11 is the most vulnerable node in IEEE 13-node test systems and the optimal time of the cyberattacks is 11 AM (see Figure 10).

Simultaneously optimizing objective Functions (10) and (15), Attacker 1 identifies the non-dominated solutions as shown in Figure 11, causing different rates of overvoltage in the microgrid. From Figure 11, it can be perceived that the Pareto-optimal front is well distributed; hence, Attacker 1 can select one of these optimal solutions (e.g., the cyan circles) and inject the corresponding false data vector to the load centers and generation units to push the microgrid toward overvoltage. As an illustration, if Attacker 1 selects the yellow triangle, the summation of false data injected into the system will be minimal; however, the rate of overvoltage will be minimal, as well. If the attacker opts for the purple diamond, although the rate of overvoltage will be maximal, the summation of false data to be injected to the system will also be maximal. This is where the significance of approaching this problem as a BOOP comes under the spotlight. Thus, if the importance of both objective functions is equal, Attacker 1 sets ξ_k to 0.5 (see (20)) to find the best compromise solution (BCS), as demonstrated by the red pentagram in Figure 11. It is worth stating that the

percentage of conflict between the objective functions (i.e., yellow triangle and purple diamond) is almost 95%, which is obtained by applying the Pythagorean Theorem (see Figure 11).

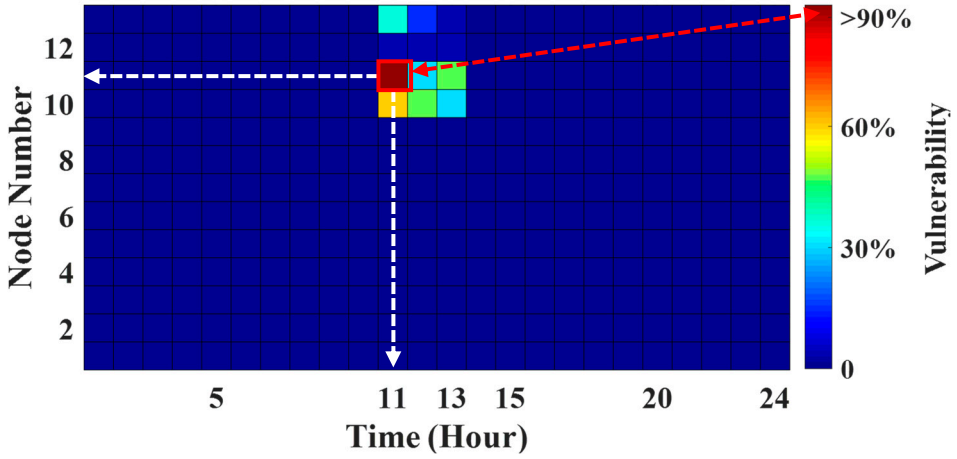

Figure 10. Vulnerability of the nodes in IEEE 13-node systems to voltage deviation.

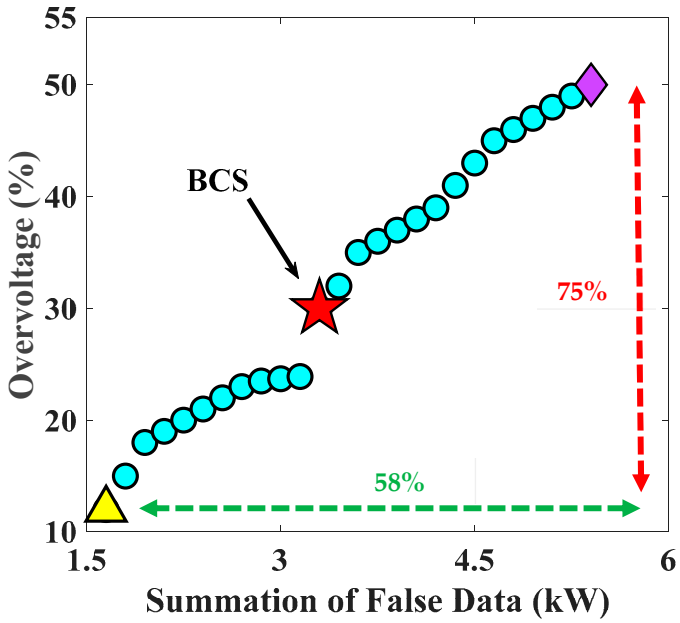

Figure 11. Two-dimensional Pareto-optimal front resulting in overvoltage in node #11.

Likewise, Attacker 2 targets the microgrid by (a) optimizing objective Functions (10) and (16), (b) identifying the non-dominated solutions and storing them in a repository (see Figure 12), (c) injecting the false data vector for the magenta pentagram, and (d) pushing the microgrid toward undervoltage.

It is noted that the percentage of conflict between minimizing objective Function (10) and maximizing objective Function (16) is more than 95%, obtained by applying the Pythagorean Theorem, confirming the significance of solving such a problem as a BOOP. To obtain a better perspective about the impacts of injecting the vectors of false data, associated with pentagrams displayed in Figures 11 and 12, into the control center, Figure 13 demonstrates the voltage profile of the microgrid after the FDIAs resulting in overvoltage and undervoltage.

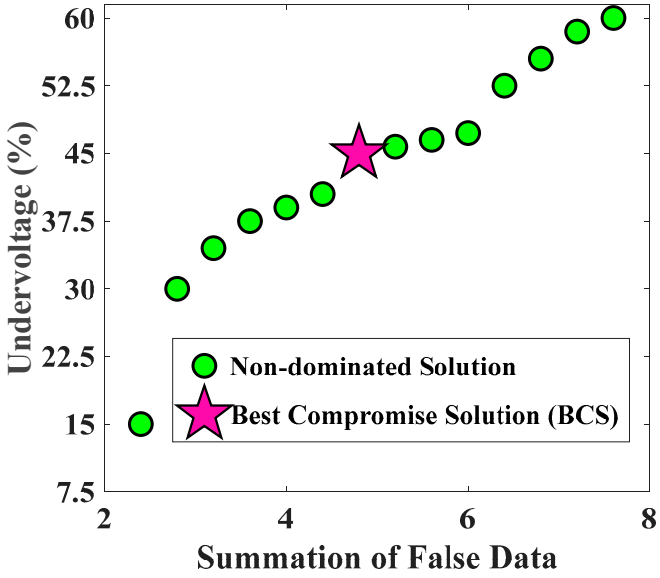

Figure 12. Two-dimensional Pareto-optimal front resulting in undervoltage in node #11.

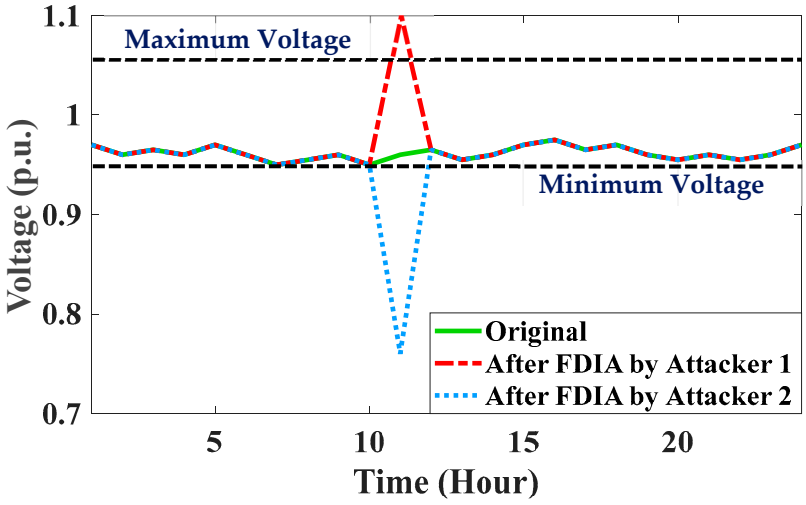

Figure 13. The daily voltage profiles of node #11 after the cyberattacks at 11 AM.

To cause voltage violation (i.e., both overvoltage and undervoltage at the same time), attackers optimize objective functions (10), (15), and (16) concurrently. Although the related 3D Pareto-optimal front is demonstrated in Figure 14, where the BCS among the three indicated objectives is obtained by applying (20) and setting ξ_k to 1/3 for all three functions (see the green hexagram), attackers have access to the set of 34 optimal solutions (see the yellow circles displayed in Figure 14). Thus, they can control the rate of voltage violation in the microgrid by opting for different solutions among the non-dominated solutions (i.e., yellow circles). As an illustration, if the intention is to increase the rate of overvoltage compared to undervoltage, the attackers can set ξ_1 (i.e., the weight factor associated with overvoltage objective function) to 0.6, ξ_2 (i.e., the weight factor corresponding to undervoltage objective function) to 0.1, and ξ_3 (i.e., the weight factor related to false data vector) to 0.3 to ensure that the microgrid experiences a higher rate of overvoltage compared to undervoltage by keeping the attack stealthy. It is noted that any other combinations are valid since the repository includes 34 optimal solutions (i.e., yellow circles displayed in Figure 14).

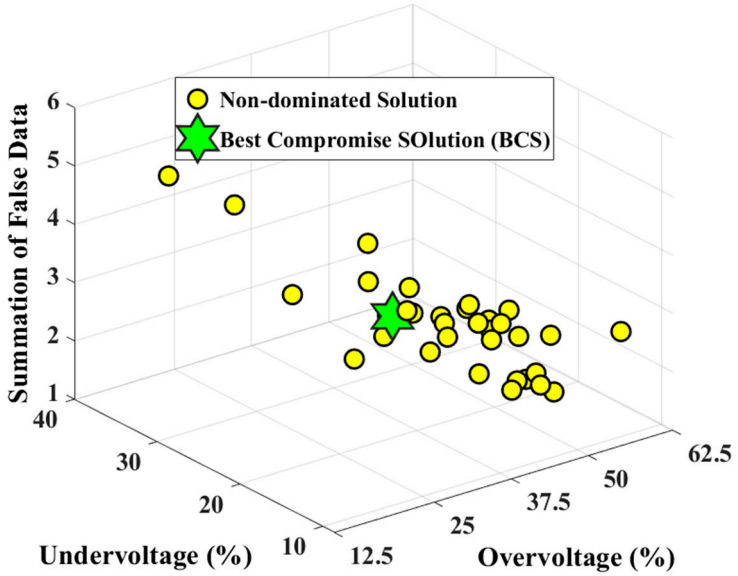

Figure 14. Three-dimensional Pareto-optimal front resulting in overvoltage and undervoltage in the microgrid at the same time (i.e., voltage violation).

To provide a technical assessment of the developed attack framework, Table 1 compares its impact with two mainstream smart grid security defense mechanisms: moving target defense (MTD) [38] and a deep learning-based false data detector [39]. This comparison highlights the strengths of the proposed framework in bypassing these defenses and underscores the limitations of existing technologies against coordinated false data injection attacks (FDIAs).

Table 1. Effectiveness of the developed FDIA framework against two mainstream defense mechanisms on the modified IEEE 13-node test system.

	Attack Phase	**Defense Phase**	
	Developed FDIA Targeting Node #11 (i.e., The Most Vulnerable Node to Voltage Deviation)	**Moving Target [38]**	**Deep Learning [39]**
Overvoltage Based on (15)	27.6%	16.6%	27.6%
Undervoltage Based on (16)	39.1%	21.4%	39.1%

The MTD mechanism, as detailed in [38], enhances grid security by frequently reconfiguring system attack surfaces, introducing unpredictability that makes it harder for adversaries to exploit vulnerabilities. However, MTD primarily addresses static attack vectors and cannot fully mitigate the stealthy and coordinated manipulation of data introduced by the developed FDIA framework. For example, as shown in Table 1, the developed framework achieves voltage deviations of up to 27.6% (overvoltage) and 39.1% (undervoltage) at the most vulnerable node (#11), whereas MTD reduces these deviations to 16.6% and 21.4%, respectively, due to its dynamic nature.

Similarly, the deep learning-based false data detector, described in [39], focuses on maintaining data integrity and system reliability by detecting anomalies in data streams. While effective against traditional cyber threats, it fails to counteract the subtle, coordinated manipulation of data by the proposed FDIA framework. The excessive training duration and limited adaptability of the detector allowed the developed framework to bypass it entirely, leading to the same voltage deviations as observed without the detector in place.

These findings demonstrate that while existing defenses are effective against traditional cyberattacks, they are less capable of addressing the challenges posed by coordinated,

bi-objective FDIA strategies. Furthermore, the results in Table 1 show that by synchronizing attack timings and targeting multiple distributed energy resources (DERs), the proposed framework amplifies voltage deviations beyond those observed in single-attacker scenarios, emphasizing its disruptive potential.

This comparative analysis underscores the need for more advanced and adaptive defense mechanisms, such as real-time anomaly detection powered by digital twin, to effectively counteract coordinated cyberattacks in modern smart grid systems. Interested readers are directed to [38,39] for further details on the strengths and limitations of the referenced defense mechanisms.

While the existing defense mechanisms, such as moving target defense (MTD) and deep learning-based false data detectors, provide valuable protection, they have notable limitations when countering sophisticated coordinated FDIAs. MTD, for instance, introduces unpredictability by frequently changing the attack surface, but its effectiveness is reduced when attackers employ adaptive strategies or exploit timing vulnerabilities. Similarly, deep learning-based detectors rely heavily on the quality and diversity of training data, making them susceptible to attacks that mimic normal system behavior or exploit gaps in training datasets. To enhance the overall security and resilience of smart grids, combining multiple defense mechanisms can be an effective strategy. For example, integrating MTD with real-time anomaly detection powered by artificial intelligence (AI) could address both static and dynamic attack vectors. MTD would limit the attacker's ability to exploit known vulnerabilities, while AI-based detectors would identify and respond to subtle, coordinated attacks in real time. Additionally, encrypted communication protocols can be combined with these mechanisms to further secure data integrity and confidentiality. The effectiveness of defense mechanisms also depends on the specific attack scenario. For example,

- *Single-Attacker Scenarios*: MTD alone may suffice by increasing the complexity of identifying vulnerabilities.
- *Coordinated Multi-Attacker Scenarios*: a layered defense strategy, combining MTD, anomaly detection, and advanced encryption, would be required to counteract synchronized attacks targeting multiple DERs.
- *Stealthy FDIAs*: AI-based detectors with adaptive learning capabilities can enhance detection accuracy by continuously updating models with real-time system data.

Deployment in real systems requires careful consideration of trade-offs between implementation costs and system security. For instance, MTD is computationally efficient and can be deployed without significant infrastructure changes, while AI-based detectors may require additional computational resources and robust communication networks. A hybrid approach, where defenses are prioritized based on the criticality of assets and vulnerability assessments, could optimize both costs and security. By combining multiple mechanisms, considering scenario-specific effectiveness, and strategically deploying defenses, the overall security of smart grids can be significantly enhanced. Future work will focus on developing a unified framework that integrates these approaches and evaluates their combined impact on mitigating coordinated FDIAs in real-world smart grid environments.

3.3. Experimental Results on the Lab-Scale Microgrid

The lab-scale microgrid illustrated in Figures 8 and 9 is considered as a single node connected to the PCC; hence, only the optimal time of the FDIAs will be the outcome of the pre-attack evaluation (i.e., (1)–(8)) on the lab-scale microgrid. To this end, solving (1)–(8), Attackers 1 and 2, respectively, obtain 9:30 A.M. and 12:30 P.M. as the optimal times for their FDIAs to cause overvoltage and undervoltage on the microgrid.

To highlight the impacts of DERs in the voltage violations caused by Attackers 1 and 2, two different scenarios of attack are taken into account as follows:

- Attacker 1 targets the PV panels to cause overvoltage in the microgrid. Further, the attacker manipulates the sensor's reading associated with the system's load by injecting only ΔP^D, obtained after minimizing objective function (10),
- Attacker 2 targets the wind turbines to cause different rates of undervoltage in the lab-scale microgrid.

It is noted that the indicated scenarios are *experimentally* accomplished via taking advantage of the developed HIL setup (refer to Section 3.1)

The voltage profiles of the microgrid after the FDIAs launched by Attackers 1 and 2 (refer to Figure 5) are demonstrated in Figure 15, confirming successful overvoltage and undervoltage with respect to the original voltage profile of the system (i.e., the green solid curve). The BCSs along with the corresponding Pareto-optimal fronts, resulting in the indicated overvoltage and undervoltage in Figure 15, are displayed in Figure 16.

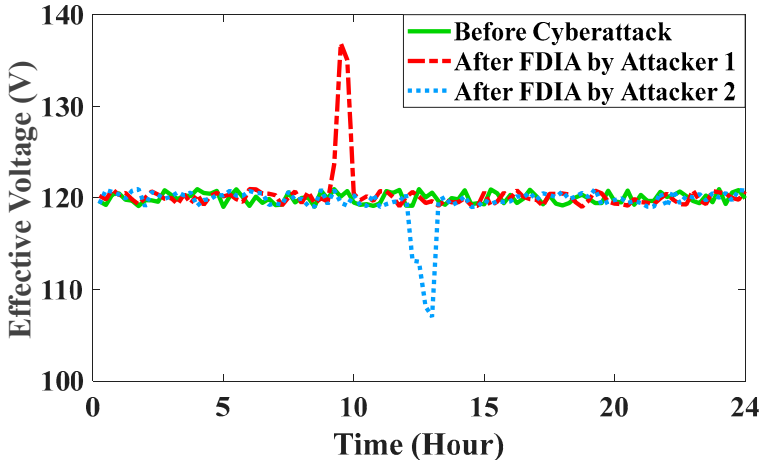

Figure 15. Voltage profile of the targeted microgrid after the FDIAs at the optimal times.

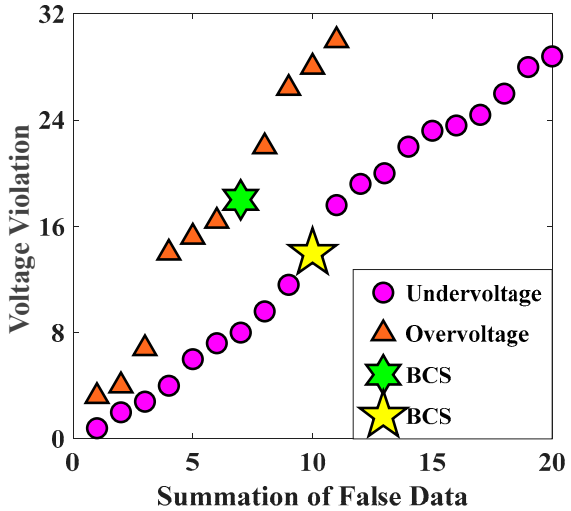

Figure 16. Two-dimensional Pareto-optimal fronts associated with FDIAs resulting in overvoltage and undervoltage.

According to Figure 16, it can be gathered that the Pareto-fronts, which are well distributed, provide a range of overvoltage and undervoltage from 1% to more than 31%. In addition, the BCSs (i.e., green hexagram and yellow pentagram) are obtained while ξ_k for both objective functions (i.e., summation of false data plus either overvoltage or undervoltage) is equal to 0.5. Hence, the attackers can change the severity of voltage violations by setting the weight factors to other values.

To highlight the impacts of the unified FDIA targeting both renewable-based DERs (i.e., PV panel and wind turbine), Figure 17 illustrates the voltage profile of the targeted microgrid (black solid curve) compared to the original voltage profile (i.e., green dashed curve) as well as those obtained after the independent cyberattacks (i.e., Figure 15). From Figure 17, one can perceive that when the microgrid is targeted by a unified cyberattack causing voltage violation (i.e., overvoltage and undervoltage), the system experiences a malicious voltage profile for a longer period (i.e., more than six hours) compared to the time periods at which the microgrid is targeted by two independent FDIAs (see Figure 15).

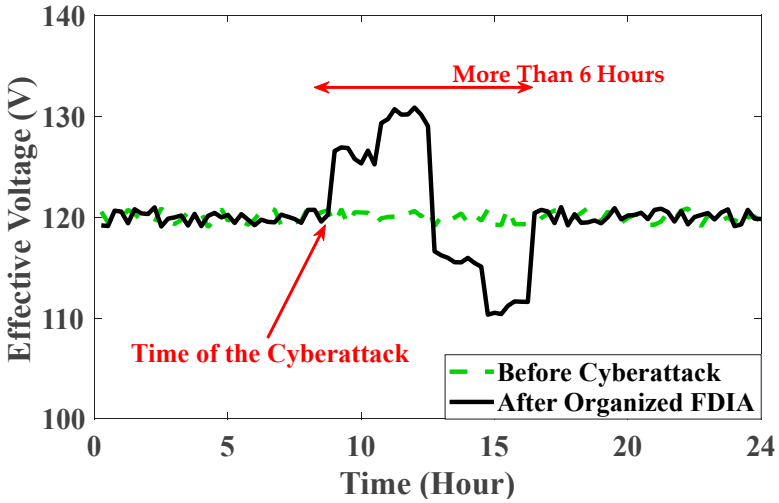

Figure 17. Comparison of voltage profiles after independent FDIAs and the developed coordinated FDIA.

According to Figures 15–17, particularly Figure 16, the relationship between output fluctuations, load changes, spurious data injection, and voltage deviation can be analyzed through the interaction of these factors with the power flow dynamics in the system. Load variations and DER output fluctuations directly influence the active and reactive power balance, which, in turn, impacts the voltage profile. For instance, an increase in DER output leads to overvoltage conditions, whereas load surges can cause undervoltage. Spurious data injection, on the other hand, disrupts the control system by introducing false signals that either overestimate or underestimate the actual system state, amplifying these voltage deviations. The extent of voltage deviation is also affected by key system parameters such as line impedance, the level of DER penetration, the sensitivity of voltage to active and reactive power changes, and the delay or responsiveness of control mechanisms. For example, systems with higher DER penetration exhibit greater sensitivity to spurious data due to the reliance on inverter-based resources, which are more susceptible to control errors. During the experiments, these parameters were kept constant to isolate the effects of spurious data injection and power flow changes. This analysis highlights the need for coordinated defense strategies that address not only the physical system dynamics but also the robustness of control algorithms against cyber intrusions. By understanding these relationships, grid operators can prioritize investments in real-time monitoring and adaptive control solutions to mitigate the risks posed by cyberattacks and operational disturbances.

It is noted that, for the sake of clarity, the focus of this paper was to elaborate the developed coordinated multi-objective attack framework with two attackers with different objectives; however, the developed framework can be generalized to N attackers to target larger scale microgrids via FDIAs with various objective functions. Toward that end, the proposed framework in this paper can be extended to accommodate scenarios involving multiple attackers (e.g., N attackers) coordinating their actions to maximize the negative impact on the microgrid. In such scenarios, each attacker can independently select distinct

objectives (e.g., overvoltage, undervoltage, system congestion, power outages, etc.), targeting different aspects of the system. To model the complexity of such coordinated false data injection (FDI) cyberattacks, the optimization problem presented in this paper (i.e., Equations (1)–(20)) can be reformulated to include an additional coordination constraint. This constraint ensures that the actions of different attackers are complementary rather than conflicting, thereby amplifying the overall attack impact. This coordination can be implemented using a multi-agent optimization approach, where attackers solve a shared global optimization problem that includes individual subproblems specific to each attacker. The coordination constraint would penalize conflicting actions and align objectives to maximize the attack's cumulative consequences. Furthermore, timing strategies can be incorporated through the introduction of a time-dependent vulnerability function, which enables attackers to identify and synchronize their actions at the most effective time intervals. These enhancements ensure that the extended framework realistically simulates coordinated attack scenarios and captures the compounded impact of multiple attackers on voltage stability.

3.4. Simulation Results on the Large-Scale 136-Node Distribution System

This section validates the proposed RAS using a widely recognized 136-bus distribution system [40], which has been modified into an unbalanced three-phase system to better represent the nature, scale, and complexity of real-world and actual urban microgrids. For further details on this case study, readers are referred to [41]. Table 2 outlines the results obtained from the modeled FDI cyberattack.

Table 2. Results obtained from targeting the most vulnerable bus in 136-node distribution system.

		Optimal Result	**Execution Time (s) to Obtain the Result from the Attackers' Perspective**
Buses Susceptible to Voltage Violation		#21, #30, #36, #78, #91, #115	17.22
The Most Vulnerable Bus		#91	2.6
Overvoltage (OV)	False Load Data Injected into Smart Meters (kW)	23.91	34.1
	% of OV	21.35	
Undervoltage (UV)	False Load Data Injected into Smart Meters (kW)	21.01	33.3
	% of UV	21.84	

Based on the information in this table, it can be concluded that while the developed attack framework causes significant voltage violations in the 136-bus distribution system, the system is particularly more vulnerable to undervoltage. This is evident as injecting a relatively small amount of false data into the smart meters of the nodes (e.g., 21.01 kW) results in a higher percentage of voltage deviation (e.g., 21.84%). Additionally, the results in Table 2 confirm that the proposed attack framework can induce substantial voltage violations in power systems of various sizes.

To show the effectiveness of the multi-objective attack framework while attackers have access to a very limited information about the 136-node distribution system, a series of simulated attacks were conducted using random false data injections, demonstrating that significant voltage violations can still be induced under such constraints. Table 3 displays the differences in attack effectiveness under these conditions compared to the original assumption of full attacker access. For instance, with incomplete information, the maximum voltage deviation observed during overvoltage scenarios decreased by a

maximum of 17.2%, while the timing precision constraint resulted in a 7.3% increase in the duration required to achieve the same level of disruption. To efficiently simulate these results, we adjusted the optimization algorithm to include probabilistic constraints on attacker knowledge, representing uncertainty in system parameters. By integrating these more realistic assumptions, the revised framework provides a comprehensive evaluation of attack strategies under practical constraints, highlighting the reduced but still significant impact of coordinated attacks when attackers operate with incomplete information.

Table 3. Results obtained from FDI attack with limited information about the actual distribution system to result in different levels of overvoltage.

	Undervoltage (%)	**Execution Time (s)**
Original Attack Scenario	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	19.17	36.04

4. Conclusions and Future Work

In this article, a unified multi-objective framework was presented to scrutinize the impacts of coordinated false data injection attacks (FDIAs) on smart city microgrids to result in voltage violation. The effectiveness of the developed framework was verified based on (1) simulation on the IEEE 13-node test system, modified as a building block of urban energy systems, and (2) experimental validation on a physical lab-scale smart microgrid containing wind turbines and PV modules. The obtained simulation and experimental results demonstrate that modeling the investigated FDIAs as multi-objective optimization problems can be a more effective approach with respect to the available single-objective alternatives in the literature. This is due to the fact that the objective functions are not necessarily in the same line, meaning that they need to be optimized concurrently. To be more specific, the following simulation/experimental-based observations are extracted from the results:

- In the simulation-based validation, the percentage of conflict between minimizing the false data vectors and maximizing the rate of voltage violation (e.g., overvoltage, undervoltage, or both) was more than 94% in all simulated scenarios. Hence, such objective functions cannot be aggregated with penalty weights to ensure simultaneous optimization. This is where the significance of solving the problem as a multi-objective optimization problem, providing a set of optimal solutions, comes under the spotlight.
- In the *experimental*-based validation, although the microgrid experienced rates of overvoltage and undervoltage of, respectively, 17% and 15% after the independent FDIAs, the period of voltage violation was on the minute basis. On the other hand, in the unified cyberattack, the microgrid experienced a lower rate of voltage violation (i.e., almost 11%); however, the microgrid was affected for more than 6 h, which significantly reduced the reliability of the microgrid. This is where the importance of the introduced attack framework comes under the spotlight, since the investigated issue can be more noticeable in larger scale microgrids with thousands of end-users.

The research explicitly considered factors such as the severity and timing of FDIA scenarios, employing an optimization framework to maximize voltage violations (overvoltage and undervoltage) while minimizing false data injection. It also accounted for microgrid

operational modes, accommodating both grid-connected and standalone configurations, and included experimental validation through an HIL setup, using a lab-scale microgrid with PV panels, wind turbines, and hybrid storage systems to replicate critical urban energy components. A Pareto-based solution methodology was used to manage conflicts between multiple objectives, ensuring a robust framework. However, certain factors were excluded to maintain tractability, including dynamic topology changes, weather-induced variability, real-world communication network delays, and economic or market considerations. These exclusions were necessary to focus on the study's core objectives, but future research could expand this work by integrating dynamic topology, communication delays, and economic impacts to further enhance the framework's applicability.

In future research, we will extend the proposed framework to include a detailed model and analysis of coordinated attacks involving multiple attackers. This extension will focus on specific implementation details, including the design of a multi-agent optimization framework where attackers share information and coordinate their actions to achieve maximum impact. Each attacker will be modeled as an independent agent with specific objectives, such as inducing overvoltage, undervoltage, or targeting system reliability. A shared global optimization problem will be formulated, incorporating coordination constraints and information-sharing protocols to align the objectives of multiple attackers. The model will also explore trade-offs between different attack targets by introducing a weighting mechanism that balances the relative importance of each objective (e.g., maximizing voltage deviations vs. inducing power outages). For instance, attackers may prioritize voltage deviations in one scenario while focusing on system congestion in another, depending on the attack's overall goals and resource constraints. This trade-off analysis will allow for a more comprehensive understanding of how attackers allocate their resources to maximize disruption. To evaluate the impact of these coordinated attacks, future studies will include simulation and experimental validations under different scenarios. Dynamic test cases, such as varying load profiles and real-time renewable energy fluctuations, will be used to assess the effectiveness of coordinated strategies. Experimental validations will involve adapting the lab-scale microgrid to simulate inter-attacker communication and coordination mechanisms, providing practical insights into the compounded effects of multi-attacker scenarios. These studies will not only deepen the understanding of multi-attacker coordinated attacks but also serve as a foundation for developing more robust defense strategies.

Moreover, in the next phase of this research, where a remedial action will be proposed for this type of cyberattack, the economic costs and social impacts associated with attack and defense strategies will be thoroughly investigated. Additional constraints and evaluation metrics will be included to quantify these factors. The economic costs of attack implementation will be modeled by incorporating parameters such as hardware expenses, computational resources required to design and execute the attack, and the risks and efforts involved in circumventing existing security measures. Similarly, the economic costs of defense measures will include investments in cybersecurity infrastructure, real-time monitoring systems, and personnel training. These considerations will allow for a balanced assessment of the resource investments needed for both attack and defense. Additionally, a societal impact function will be introduced to evaluate the broader consequences of voltage violations caused by FDIAs. For industrial users, this will include production downtimes, damage to sensitive equipment, and reduced operational efficiency. For residential users, disruptions such as appliance malfunctions, energy outages, and reduced quality of life will be quantified. These social and economic costs will be integrated into the optimization problem as objective functions or penalty terms to simulate the trade-offs between security investments and potential losses. By incorporating these factors, the

extended framework will enable a more comprehensive analysis of the overall economic and social benefits of maintaining stable and secure smart city microgrids. This integration will not only emphasize the severity of coordinated FDIAs on urban energy infrastructure but also provide actionable insights for policymakers and grid operators to prioritize investments in advanced defense strategies that balance cost-effectiveness with societal benefits. Future extensions of this research will also incorporate dynamic environmental factors, such as weather changes, load fluctuations, and varying renewable energy outputs, into the proposed attack framework. These dynamic conditions significantly influence voltage distribution and the overall impact of coordinated FDIAs. By integrating real-time weather data and stochastic load profiles, the extended framework will simulate the interactions between environmental variability and attack strategies. This will enable a more comprehensive evaluation of the framework's effectiveness and stability under realistic operating conditions. These enhancements will not only improve the accuracy of the attack impact analysis but also provide valuable insights for designing more resilient and adaptive defense mechanisms for smart grid environments.

Author Contributions: Conceptualization, E.N. and A.A.; methodology, E.N.; validation, E.N. and A.A.; formal analysis, E.N.; investigation, E.N. and A.A.; resources, E.N. and A.A.; data curation, E.N. and A.A.; writing—original draft preparation, E.N.; writing—review and editing, A.A.; visualization, E.N. and A.A.; supervision, A.A.; project administration, A.A.; funding acquisition, A.A. All authors have read and agreed to the published version of the manuscript.

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

Data Availability Statement: All the relevant and utilized data in this research have been properly referenced throughout the paper.

Conflicts of Interest: The authors declare no conflicts of interest. In addition, the funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Yan, J.; Menghwar, M.; Asghar, E.; Panjwani, M.K.; Liu, Y. Real-time energy management for a smart-community microgrid with battery swapping and renewables. *Appl. Energy* **2019**, *238*, 180–194. [CrossRef]
2. Kottayil, S.K. *Smart Microgrids*, 1st ed.; CRC Press: Boca Raton, FL, USA; Taylor & Francis Group: Boca Raton, FL, USA, 2020.
3. Kabeyi, M.J.B.; Olanrewaju, O.A. Sustainable energy transition for renewable and low carbon grid electricity generation and supply. *Front. Energy Res.* **2022**, *9*, 743114. [CrossRef]
4. Villanueva-Rosario, J.A.; Santos-García, F.; Aybar-Mejía, M.E.; Mendoza-Araya, P.; Molina-García, A. Coordinated ancillary services, market participation and communication of multi-microgrids: A review. *Appl. Energy* **2022**, *308*, 118332. [CrossRef]
5. Khazaei, J. Stealthy cyberattacks on loads and distributed generation aimed at multi-transmission line congestions in smart grids. *IEEE Trans. Smart Grid* **2021**, *12*, 2518–2528. [CrossRef]
6. 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*, 1450–1460. [CrossRef]
7. Liang, G.; Weller, S.R.; Zhao, J.; Luo, F.; Dong, Z.Y. The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE Trans. Power Syst.* **2017**, *32*, 3317–3318. [CrossRef]
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*, 1331–1341. [CrossRef]
9. 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*, 109–119. [CrossRef]
10. 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*, 5239–5248. [CrossRef]
11. Habibi, M.R.; Baghaee, H.R.; 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*, 717–721. [CrossRef]

12. Habibi, M.R.; Baghaee, H.R.; 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*, 5294–5310. [CrossRef]
13. 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*, 4066–4075. [CrossRef]
14. Aysheh, N.G.A.; 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, 9–10 November 2020; pp. 1–6.
15. 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. [CrossRef]
16. 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*, 6000–6013. [CrossRef]
17. Abhinav, S.; Modares, H.; Lewis, F.L.; Ferrese, F.; Davoudi, A. Synchrony in networked microgrids under attacks. *IEEE Trans. Smart Grid* **2018**, *9*, 6731–6741. [CrossRef]
18. Liang, G.; Zhao, J.; Luo, F.; Weller, S.R.; Dong, Z.Y. A Review of False Data Injection Attacks Against Modern Power Systems. *IEEE Trans. Smart Grid* **2017**, *8*, 1630–1638. [CrossRef]
19. Analysis of the Cyber Attack on the Ukrainian Power Grid. 2016. Available online: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf (accessed on 1 October 2024).
20. Vox Website. 2021. Available online: https://www.vox.com/world/ (accessed on 1 October 2024).
21. Purlu, M.; Turkay, B.E. Optimal allocation of renewable distributed generations using heuristic methods to minimize annual energy losses and voltage deviation index. *IEEE Access* **2022**, *10*, 21455–21474.
22. Balamourougan, V.; Sidhu, T.S.; Sachdev, M.S. Technique for online prediction of voltage collapse. *IEE Proc. Gener. Transm. Distrib.* **2004**, *151*, 453–460. [CrossRef]
23. Micky, R.R.; 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, 3–5 March 2016; pp. 1268–1273.
24. Chang, C.-T.; Wu, W.-J.; Lin, S.-W. Fuzzy multi-choice goal programming and artificial bee colony algorithm for triangular and trapezoidal membership functions. *IEEE Access* **2021**, *9*, 95267–95281. [CrossRef]
25. Mukherjee, V.; Mukherjee, A.; Prasad, D. Whale Optimization Algorithm With Wavelet Mutation for the Solution of Optimal Power Flow Problem. In *Handbook of Research on Predictive Modeling and Optimization Methods in Science and Engineering*; Kim, D., Roy, S.S., Länsivaara, T., Deo, R., Samui, P., Eds.; IGI Global Scientific Publishing: Hershey, PA, USA, 2018; pp. 500–553.
26. Niknam, T.; Narimani, M.R.; Jabbari, M.; Malekpour, A.R. A modified shuffle frog leaping algorithm for multi-objective optimal power flow. *Energy* **2011**, *36*, 6420–6432. [CrossRef]
27. Wind-Turbine-Models Website. Available online: https://en.wind-turbine-models.com/ (accessed on 10 June 2022).
28. Commercial and Residential Hourly Load Profile. Available online: 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).
29. 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, 24-26 September 2021; pp. 1–5.
30. Kersting, W.H. Radial distribution test feeders. In Proceedings of the IEEE Power Engineering Society Winter Meeting. Conference Proceedings (Cat. No.01CH37194), Columbus, OH, USA, 28 January–1 February 2001; pp. 908–912.
31. Yousaf, M.; Muttaqi, K.M.; Sutanto, D. Overcurrent Protection Scheme for the IEEE 13-Node Benchmark Test Feeder with Improved Selectivity. In Proceedings of the 2020 IEEE Power & Energy Society General Meeting (PESGM), Montreal, QC, Canada, 2–6 August 2020; pp. 1–5.3.
32. Naderi, E.; Bibek, K.C.; 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. [CrossRef]
33. 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, Portugal, 29 June–1 July 2021; pp. 57–62.
34. OP4510. System Descriptions. Available online: https://blob.opal-rt.com/medias/L00161_0124.pdf (accessed on 1 October 2024).
35. Imperix Power Electronics. 800 V Voltage Sensor Descriptions. Available online: https://blob.opal-rt.com/medias/L00161_0549.pdf (accessed on 1 October 2024).
36. Imperix Power Electronics. 50 A Current Sensor Descriptions. Available online: https://imperix.com/wp-content/uploads/document/DIN-50A.pdf (accessed on 1 October 2024).
37. Imperix Power Electronics. Power Interface for OPAL-RT Hardware. Available online: https://imperix.com/wp-content/uploads/document/Power-Interface_OPAL-RT.pdf (accessed on 1 October 2024).

38. 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 & Energy Society General Meeting (PESGM), Orlando, FL, USA, 16–20 July 2023; pp. 1–5.
39. 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 (AIIoT), Seattle, WA, USA, 6–9 June 2022; pp. 357–363.
40. Mantovani, J.R.S.; Casari, F.; Romero, R.A. Reconfiguração de sistemas de distribuição radiais utilizando o critério de queda de tensão. *SBA Controle Automação* **2000**, *11*, 150–159.
41. Nirbhavane, P.S.; Corson, L.; Rizvi, S.M.H.; Srivastava, A.K. TPCPF: Three-Phase Continuation Power Flow Tool for Voltage Stability Assessment of Distribution Networks With Distributed Energy Resources. *IEEE Trans. Ind.* **2021**, *57*, 5425–5436. [CrossRef]