

Unmanned Aerial Vehicle-Based Cyberattacks on Microgrids

Alexis P. Zhao , Shuangqi Li , Zhengmao Li* , Zixiao Ma* , Da Huo , Ignacio Hernando-Gil , Mohannad Alhazmi

Abstract—The increasing reliance on Networked Microgrids (NMGs) for decentralized energy management introduces unprecedented cybersecurity risks, particularly in the context of False Data Injection Attacks (FDIA). While traditional FDIA studies have primarily focused on network-based intrusions, this work explores a novel cyber-physical attack vector leveraging Unmanned Aerial Vehicles (UAVs) to execute sophisticated cyberattacks on microgrid operations. UAVs, equipped with communication jamming and data spoofing capabilities, can dynamically infiltrate microgrid communication networks, manipulate sensor data, and compromise power system stability. This paper presents a multi-objective optimization framework for UAV-assisted FDIA, incorporating Non-dominated Sorting Genetic Algorithm III (NSGA-III) to maximize attack duration, disruption impact, stealth, and energy efficiency. A comprehensive mathematical model is formulated to capture the intricate interplay between UAV operational constraints, cyberattack execution, and microgrid vulnerabilities. The model integrates flight path optimization, energy consumption constraints, signal interference effects, and adaptive attack strategies, ensuring that UAVs can sustain long-duration cyberattacks while minimizing detection risk. Results indicate that UAV-assisted cyberattacks can induce power imbalances of up to 15%, increase operational costs by 30%, and cause voltage deviations exceeding 0.10 p.u.. Furthermore, analysis of attack success rates vs. detection mechanisms highlights the limitations of conventional rule-based anomaly detection, reinforcing the need for adaptive AI-driven cybersecurity defenses. The findings underscore the urgent necessity for advanced intrusion detection systems, UAV tracking technologies, and resilient microgrid architectures to mitigate the risks posed by airborne cyber threats.

Index Terms—Cyberattack, False Data Injection Attack, Microgrids, Multi-objective Optimization, NSGA-III, Networked Microgrids, Unmanned Aerial Vehicles.

A. P. Zhao (alexzhao@stanford.edu) is with the Department of Energy Science and Engineering, Stanford Doerr School of Sustainability, Stanford University, Stanford, CA 94305, United States.

S. Li (shuangqi.li@polyu.edu.hk) is with the Department of Electrical and Electronic Engineering, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong.

Zhengmao Li (zhengmao.li@aalto.fi, corresponding author) is with the Department of Electrical Engineering and Automation, School of Electrical Engineering, Aalto University, Espoo, 02150, Finland.

Zixiao Ma (zma10@binghamton.edu, corresponding author) is with the Department of Electrical and Computer Engineering, Thomas J. Watson College of Engineering and Applied Science, State University of New York at Binghamton, Binghamton, NY 13902, United States.

Da Huo (Da.Huo@cranfield.ac.uk) is with the Centre for Energy Systems and Strategy, School of Water, Energy and Environment, Cranfield University, Cranfield, Bedford MK43 0AL, United Kingdom.

I. Hernando-Gil is with ESTIA Institute of Technology, University of Bordeaux, Bidart, France (i.hernandogil@estia.fr), and also with the Institute for Systems and Computer Engineering, Technology and Science (INESC TEC), Porto, Portugal (ignacio.gil@inesctec.pt).

M. Alhazmi (malhazmi@ksu.edu.sa) is with the Department of Applied Electrical Engineering, King Saud University, Riyadh 11451, Saudi Arabia.

I. INTRODUCTION

Networked microgrids (NMGs) have revolutionized modern power distribution by enabling decentralized, resilient, and efficient energy management [1, 2]. With the proliferation of distributed energy resources (DERs) such as renewable energy systems and energy storage, NMGs have become critical infrastructure for ensuring stable power supply in both urban and rural environments [3]. Their ability to operate independently or in coordination with the main grid provides flexibility in power system operation, but this interconnectivity comes at a cost: increased cybersecurity vulnerabilities. The reliance on information and communication technologies (ICTs) for real-time control, monitoring, and coordination introduces significant security risks, making microgrids an attractive target for cyberattacks [4, 5]. Among the most potent and stealthy forms of cyber threats are False Data Injection Attacks (FDIA), which involve the deliberate manipulation of measurement data to mislead microgrid state estimation [6, 7]. By altering sensor readings, FDIA can create false power flow conditions, trigger incorrect control responses, and ultimately disrupt system stability. While traditional FDIA studies have primarily focused on network-based intrusions, a new and more sophisticated attack vector has emerged—Unmanned Aerial Vehicles (UAVs). With their mobility, adaptability, and ability to access remote locations, UAVs introduce a paradigm shift in cyber-physical attacks, offering attackers an unprecedented advantage in launching FDIA against microgrids without the need for direct network penetration [8, 9]. Unlike static wireless intrusion points, UAVs provide spatial agility that enables attackers to dynamically reposition over vulnerable communication nodes, adapt to real-time system conditions, and optimize attack effectiveness while minimizing the risk of detection.

The integration of UAVs into cyberattack strategies presents unique challenges for power system security. UAVs can bypass traditional cybersecurity defenses by exploiting vulnerabilities in wireless communication networks, interfering with data transmission, and injecting malicious signals to manipulate microgrid operations [10]. Their ability to hover, maneuver, and dynamically adjust their attack strategies in real time makes them significantly more challenging to detect and mitigate. Unlike conventional cyber intrusions that rely on compromised devices or malware, UAV-assisted FDIA can be executed externally, reducing the reliance on insider threats and making the attack more difficult to trace [11]. Given the increasing availability and affordability of UAV technology, understanding their potential role in cyber-physical attacks on power infrastructure is crucial for developing robust countermeasures. Despite the growing cybersecurity concerns in power systems, research on UAV-assisted FDIA remains limited. Most cybersecurity studies focus on intrusion detection, network protection, and anomaly detection within static cyber environments. However, these approaches fail to address the dynamic nature of UAV-assisted cyberattacks, where attack vectors evolve based on environmental conditions, power system responses, and UAV operational constraints [12]. The lack of research on optimizing UAV-based cyberattacks highlights a significant gap in understanding the full scope of vulnerabilities facing microgrid infrastructure. This study seeks to bridge this gap by providing a detailed mathematical and optimization framework for UAV-assisted FDIA, demonstrating how UAVs can optimize their attack strategies to maximize impact while minimizing the risk of detection.

This research presents a novel approach to modeling and optimizing UAV-assisted cyberattacks on NMGs. Unlike traditional cyberattack models that assume static attack points, this work introduces a dynamic framework where UAVs actively adjust their positioning, attack intensity, and stealth measures in response to real-time microgrid conditions. The problem is formulated as a multi-objective optimization task, where the UAVs seek to maximize attack duration, maximize disruption impact, minimize detection probability, and minimize resource consumption. The optimization is performed using the Non-dominated Sorting Genetic Algorithm III (NSGA-III), a state-of-the-art evolutionary algorithm that enables efficient trade-off analysis among competing attack objectives. By leveraging NSGA-III, this study identifies optimal UAV attack strategies that balance effectiveness with stealth, demonstrating how UAVs can prolong cyberattacks without triggering immediate countermeasures. The primary contributions of this paper are fourfold:

First, it introduces UAV-assisted FDIA as a novel cyber threat to networked microgrids, highlighting the unique challenges posed by mobile attack platforms. By demonstrating how UAVs can dynamically execute cyberattacks while evading detection, this study expands the understanding of cyber-physical security risks in modern power systems.

Second, this research develops a multi-objective optimization framework that systematically evaluates trade-offs between attack duration, impact, stealth, and energy efficiency. Unlike previous works that rely on heuristic-based approaches, this study employs NSGA-III to generate optimal attack strategies under real-world constraints.

Third, the paper presents a comprehensive mathematical model that captures the interactions between UAV operations, cyberattack execution, and microgrid vulnerabilities. This includes UAV energy management, flight path constraints, jamming effectiveness, and attack impact metrics, providing a rigorous analytical foundation for studying UAV-assisted cyberattacks.

Finally, the research serves as a critical reference for cybersecurity defense strategies by exposing previously unidentified vulnerabilities in microgrid security. By analyzing optimal attack strategies, this study informs future research on UAV detection techniques, adaptive anomaly detection systems, and cyber-physical security measures for protecting critical energy infrastructure.

II. LITERATURE REVIEW

The cybersecurity of NMGs has gained increasing attention due to the rapid digitalization of power systems and the rise of sophisticated cyber threats. While extensive research has explored FDIA in power grids, the potential for UAV-assisted FDIA remains largely unexamined. This literature review provides an overview of existing research on FDIA, UAVs in cybersecurity, optimization-based attack strategies, and defense mechanisms for microgrid resilience.

FDIA has been widely studied as a critical cyber threat to power systems, particularly in state estimation and control algorithms. Initial research focused on the theoretical foundations of FDIA, demonstrating that attackers can bypass bad data detection mechanisms by injecting well-crafted measurement errors into supervisory control and data acquisition (SCADA) systems [13, 14]. Such attacks manipulate sensor data, leading to incorrect operational decisions that can disrupt power dispatch, cause economic losses, or even trigger cascading failures. Several studies have examined the mathematical modeling of FDIA, particularly in relation to optimal attack vector construction. Researchers have proposed graph-theoretical models and convex optimization techniques to identify the most critical measurement points for effective FDIA execution. These works emphasize that intelligent attack strategies can be designed to minimize detection probability while maximizing operational disruption [15]. However, most studies assume that the attacker already has access to the network, either through compromised nodes or insider threats. Recent studies have expanded FDIA research by integrating machine learning techniques to improve attack strategies. Reinforcement learning, deep neural networks, and adversarial AI have been employed to develop

adaptive cyberattacks that evolve in response to grid defenses [16]. However, a key limitation of these studies is their assumption of static attack points—they do not consider the possibility of mobile attack platforms, such as UAVs, dynamically adjusting their attack strategies based on system response. This highlights a critical research gap in understanding how UAVs can execute and optimize FDIA in real time, exploiting their mobility to evade detection and sustain long-term attacks.

UAVs have traditionally been used for surveillance, reconnaissance, and military operations, but their application in cybersecurity threats has only recently gained attention [17]. The increasing accessibility of low-cost UAVs equipped with wireless hacking tools has introduced new attack possibilities, particularly in network intrusion, communication jamming, and cyber-physical disruption. Several studies have explored UAV-assisted jamming as a means of disrupting wireless networks. Research has shown that UAVs can deploy directional antennas and frequency hopping techniques to interfere with power system communications [18]. Some works have proposed game-theoretic models to optimize UAV positioning for maximum jamming effectiveness, demonstrating that an intelligent attacker can selectively jam high-priority control signals to cause microgrid instability [11]. Another growing area of UAV cybersecurity research is aerial cyber espionage, where UAVs intercept wireless signals to collect sensitive data from industrial control systems. Several experiments have demonstrated how UAVs can exploit unsecured Wi-Fi, ZigBee, and RF-based communication protocols to eavesdrop on energy management systems. These studies highlight the vulnerabilities in current microgrid communication architectures, suggesting that UAVs could be leveraged to execute more advanced cyberattacks, such as FDIA, without requiring direct physical access to power system infrastructure [19, 20]. Although both jamming and FDIA can disrupt microgrid operations, they operate through fundamentally different mechanisms. Jamming targets the communication channel to prevent data delivery, while FDIA focuses on injecting deceptive but syntactically valid data into the system to mislead state estimation. This study emphasizes the latter, where UAVs are not simply interrupting signals, but are used to deliver false data crafted to exploit control logic vulnerabilities within the microgrid. Despite these advances, existing UAV cybersecurity studies do not consider UAVs as autonomous, multi-objective attack agents. Most research focuses on single-action attacks, such as signal jamming or interception, without considering how UAVs can optimize cyberattacks dynamically based on real-time system responses. This study fills this gap by integrating UAV movement, power consumption, attack strategies, and detection avoidance into a unified optimization model, providing a more comprehensive perspective on UAV-assisted cyberattacks.

While extensive research has focused on defending microgrids against cyber threats, most countermeasures remain reactive rather than proactive. Traditional defense mechanisms, such as intrusion detection systems (IDS), focus on anomaly detection using machine learning and statistical methods [21, 22]. However, these methods often struggle to detect stealthy attacks, such as UAV-assisted FDIA, which can be executed in a manner that mimics legitimate system behavior [23]. Some studies have proposed blockchain-based security frameworks for securing microgrid data integrity, ensuring that manipulated measurement data cannot be injected without detection [24]. While blockchain offers strong data immutability, it comes at the cost of increased computational overhead and latency, making it unsuitable for real-time attack mitigation [25]. More recent work has focused on game-theoretic cyber defense strategies, where defenders optimize their response strategies against potential attackers [24]. These approaches employ Stackelberg games, Markov decision processes, and adversarial machine learning to anticipate and neutralize cyber threats. However, existing defense models do not account for dynamic, UAV-assisted cyberattacks, where the attacker's mobility introduces additional layers of complexity. Given these challenges, there is an urgent need to develop adaptive, UAV-aware defense mechanisms that can track, detect, and neutralize airborne cyber

threats before they inflict widespread damage on power systems. This research aims to inspire future work in developing countermeasures that specifically target UAV-assisted cyberattacks, such as real-time UAV tracking, adversarial anomaly detection, and adaptive microgrid control mechanisms that can mitigate the impact of stealthy cyber intrusions.

III. PROBLEM FORMULATION

The UAV-assisted FDIA framework is formulated as a multi-objective optimization problem, integrating UAV trajectory planning, energy constraints, attack execution strategies, and microgrid disruption impact. This section presents the detailed mathematical formulation, including the objective functions and operational constraints that govern the UAV-based attack execution. The mathematical model accounts for multiple interdependent factors, such as UAV flight endurance, signal interference effectiveness, microgrid vulnerability, and attack detectability, ensuring a comprehensive representation of real-world attack scenarios. To ensure tractability in solving the high-dimensional multi-objective optimization problem, certain subsystem processes—such as detection responses, signal propagation effects, and energy discharge dynamics—are represented using simplified or normalized functional forms. These abstractions preserve computational solvability while enabling the model to capture the strategic behavior of UAV attackers under realistic physical and operational constraints. The mathematical formulation is structured into two main components: (i) objective functions, which define the attacker's strategic goals, including maximizing attack duration, increasing microgrid disruption, minimizing detection probability, and optimizing resource utilization, and (ii) constraints, which impose realistic operational limits on UAV behavior, microgrid state variations, and cybersecurity defenses. While certain functional simplifications are adopted, the model maintains the essential structural features required to represent realistic UAV behavior, including trade-offs between stealth, energy, and disruption effectiveness. In particular, UAV mobility plays a critical role in this framework by enabling the attacker to dynamically position over high-value or vulnerable nodes. Unlike static attackers, UAVs can adapt their spatial deployment based on real-time system conditions, which directly influences the optimization of attack duration, stealth, and disruption metrics.

To ensure clarity in the mathematical formulation, all variables and parameters used in this study are defined in the following nomenclature table.

Symbol	Description	Unit
Ψ_{sig}	Signal interference cost factor	-
Γ_{bat}	Battery energy consumption coefficient	W
T	Total attack duration	s
E	Total energy consumed by the UAV	Wh
P_{jam}	Jamming power emitted by the UAV	W
P_{thresh}	Detection power threshold of the IDS	W
x_t	UAV horizontal coordinate at time t	m
y_t	UAV vertical coordinate at time t	m
z_t	UAV altitude at time t	m
v_t	UAV velocity at time t	m/s
Δt	Time interval between UAV control steps	s
θ_t	UAV orientation angle at time t	rad
I_t	Interference effectiveness at time t	-
C	Total system disruption cost	-
η	Stealthiness penalty coefficient	-
δ	Energy-to-distance efficiency ratio	Wh/m
λ	Weighting factor in the optimization objective	-
Ω	Total optimization objective value	-
f_1	Objective: maximize disruption	-
f_2	Objective: minimize detection	-
f_3	Objective: minimize energy consumption	-
Note: '-' represents no unit.		

A UAV Energy Constraints and Flight Modeling

To model the physical and energy limitations of UAVs during the attack process, we formulate the flight energy consumption, jamming power behavior, and trajectory boundaries as the following constraints. These equations ensure that all optimization outputs remain feasible in terms of the UAV's operational capacity.

$$\max_{\Lambda, \Psi, \Omega} \sum_{t=1}^T \sum_{u \in \mathcal{U}} \left[\phi_u \left(\frac{\zeta_{u,t}^{\text{fly}}}{\theta_u^{\text{max}}} \right) + \rho_u \left(\frac{\zeta_{u,t}^{\text{hover}}}{\xi_u^{\text{max}}} \right) + \sum_{j \in \mathcal{J}} \kappa_j \cdot \left(\frac{\psi_{u,j,t}^{\text{sig}}}{\Psi_j^{\text{max}}} \right) \right] - \sum_{t=1}^T \sum_{u \in \mathcal{U}} \sum_{i \in \mathcal{I}} \left[\vartheta_i \cdot \left(\frac{\Omega_{u,i,t}^{\text{data}}}{\Omega_i^{\text{cap}}} \right) + \sigma_u \cdot \left(\frac{\Gamma_{u,t}^{\text{bat}}}{\Gamma_u^{\text{max}}} \right) \right] \quad (1)$$

This equation models the maximization of UAV attack duration, balancing energy consumption across flight, hovering, and signal interference while ensuring resource constraints are respected. The first term accounts for energy utilization during flight $\zeta_{u,t}^{\text{fly}}$ and hovering $\zeta_{u,t}^{\text{hover}}$, normalized by their respective limits θ_u^{max} and ξ_u^{max} , weighted by coefficients ϕ_u and ρ_u . In our implementation, θ_u^{max} is set to 0.52 rad, consistent with UAV pitch angle constraints under stable flight conditions, while ξ_u^{max} is defined as 30%, representing the maximum tolerable signal interference intensity without triggering immediate detection in microgrid communication protocols. The second term penalizes excessive power drain on UAV batteries $\Gamma_{u,t}^{\text{bat}}$ and signal transmission.

$$\max_{\Xi, \Lambda} \sum_{t=1}^T \sum_{u \in \mathcal{U}} \left[\varphi_u \cdot \left(\frac{\Pi_{u,t}^{\text{hover}}}{\Theta_u^{\text{max}}} \right) + \beta_u \cdot \left(\frac{\Xi_{u,t}^{\text{flight}}}{\Gamma_u^{\text{max}}} \right) \right] - \sum_{t=1}^T \sum_{u \in \mathcal{U}} \sum_{j \in \mathcal{J}} \left[\gamma_j \cdot \left(\frac{\Lambda_{u,j,t}^{\text{attack}}}{\Lambda_j^{\text{cap}}} \right) + \mu_u \cdot \left(\frac{\Psi_{u,t}^{\text{bat}}}{\Psi_u^{\text{max}}} \right) \right] \quad (2)$$

Equation (2) represents the relationship between UAV power usage and attack duration, incorporating multiple energy-intensive components such as flight $\Xi_{u,t}^{\text{flight}}$ and hovering $\Pi_{u,t}^{\text{hover}}$, normalized against their respective constraints Γ_u^{max} and Θ_u^{max} . The attack execution power $\Lambda_{u,j,t}^{\text{attack}}$ is constrained by system capacity Λ_j^{cap} , while the battery discharge rate $\Psi_{u,t}^{\text{bat}}$ must remain within the UAV's allowable operational range Ψ_u^{max} . This function ensures an optimal trade-off between sustained attack effectiveness and UAV power efficiency.

$$\max_{\Upsilon} \sum_{t=1}^T \sum_{u \in \mathcal{U}} \left[\eta_u \cdot \left(\frac{\Upsilon_{u,t}^{\text{attack}}}{\Phi_u^{\text{max}}} \right) + \omega_u \cdot \left(\frac{\Theta_{u,t}^{\text{maneuver}}}{\Theta_u^{\text{max}}} \right) \right] - \sum_{t=1}^T \sum_{u \in \mathcal{U}} \left[\chi_u \cdot \left(\frac{\Delta_{u,t}^{\text{bat}}}{\Delta_u^{\text{max}}} \right) + \tau_u \cdot \left(\frac{\Xi_{u,t}^{\text{recharge}}}{\Xi_u^{\text{max}}} \right) \right] \quad (3)$$

Equation (3) establishes a time-constraint model ensuring prolonged attack without early termination, balancing sustained interference duration $\Upsilon_{u,t}^{\text{attack}}$ and efficient UAV maneuvers $\Theta_{u,t}^{\text{maneuver}}$ with energy constraints. The UAV's battery discharge rate $\Delta_{u,t}^{\text{bat}}$ and recharging cycles $\Xi_{u,t}^{\text{recharge}}$ are optimized to maintain attack persistence.

$$\max_{\Omega} \sum_{t=1}^T \sum_{u \in \mathcal{U}} \left[\lambda_u \cdot \left(\frac{\Omega_{u,t}^{\text{traj}}}{\Omega_u^{\text{max}}} \right) + \nu_u \cdot \left(\frac{\Pi_{u,t}^{\text{recharge}}}{\Pi_u^{\text{max}}} \right) \right] - \sum_{t=1}^T \sum_{u \in \mathcal{U}} \left[\xi_u \cdot \left(\frac{\Psi_{u,t}^{\text{drain}}}{\Psi_u^{\text{max}}} \right) + \delta_u \cdot \left(\frac{\Lambda_{u,t}^{\text{exec}}}{\Lambda_u^{\text{cap}}} \right) \right] \quad (4)$$

Equation (4) represents the attack duration as a function of UAV trajectory and recharging constraints. The UAV's flight path $\Omega_{u,t}^{\text{traj}}$ and recharging strategy $\Pi_{u,t}^{\text{recharge}}$ are optimized to sustain prolonged engagement, ensuring that energy depletion $\Psi_{u,t}^{\text{drain}}$ and execution power $\Lambda_{u,t}^{\text{exec}}$ remain within feasible limits. This formulation is inherently

UAV-specific and cannot be trivially applied to static or ground-based attack devices. It incorporates aerial maneuverability, battery-constrained endurance, altitude-dependent energy use, and three-dimensional trajectory dynamics that uniquely define UAV operational behavior. These constraints induce complex trade-offs between stealth, spatial reachability, and sustained interference power, all of which are optimized jointly in our multi-objective framework. If the attacker were a static or low-mobility device, such trajectory-energy coupling and flight-constrained planning would become irrelevant, fundamentally altering the problem structure. Thus, the UAV's flight characteristics are not peripheral but central to the architecture of the proposed model.

$$\max_{\Delta} \sum_{t=1}^T \sum_{n \in \mathcal{N}} \left[\alpha_n \cdot \left(\frac{\Delta_{n,t}^{\text{power}}}{\Delta_n^{\text{max}}} \right) + \gamma_n \cdot \left(\frac{\Xi_{n,t}^{\text{voltage}}}{\Xi_n^{\text{max}}} \right) \right] \quad (5)$$

Equation (5) defines power flow deviation caused by false data injection, where manipulated power data $\Delta_{n,t}^{\text{power}}$ and voltage anomalies $\Xi_{n,t}^{\text{voltage}}$ disrupt the microgrid's stability. Importantly, the coefficients α_n and γ_n in this objective function are not uniform—they are designed to reflect the criticality of each node n based on its role in the network. Nodes that are topologically central or have higher power exchange are assigned larger weights, ensuring that UAVs are guided toward more impactful targets. This allows the optimization to prioritize spatial positions where disruption effects are amplified, thereby linking UAV trajectory decisions to node-specific vulnerability. Furthermore, the upper bound Δ_{max} is set to 5%, consistent with standard microgrid voltage deviation tolerance levels. This ensures that the modeled attack remains within plausible operational thresholds while still inducing observable system impact.

$$\max_{\Phi} \sum_{t=1}^T \sum_{n \in \mathcal{N}} \left[\rho_n \cdot \left(\frac{\Phi_{n,t}^{\text{data}}}{\Phi_n^{\text{max}}} \right) + \sigma_n \cdot \left(\frac{\Theta_{n,t}^{\text{freq}}}{\Theta_n^{\text{max}}} \right) \right] \quad (6)$$

Equation (6) represents the impact of data manipulation on microgrid stability, balancing injected false data $\Phi_{n,t}^{\text{data}}$ and frequency anomalies $\Theta_{n,t}^{\text{freq}}$.

$$\max_{\Gamma} \sum_{t=1}^T \sum_{m \in \mathcal{M}} \left[\epsilon_m \cdot \left(\frac{\Gamma_{m,t}^{\text{cost}}}{\Gamma_m^{\text{max}}} \right) + \lambda_m \cdot \left(\frac{\Psi_{m,t}^{\text{loss}}}{\Psi_m^{\text{max}}} \right) \right] \quad (7)$$

Equation (7) captures the economic cost function representing increased operational expenses due to an attack, where microgrid operational costs $\Gamma_{m,t}^{\text{cost}}$ and power loss $\Psi_{m,t}^{\text{loss}}$ contribute to financial burdens.

$$\max_{\Omega} \sum_{t=1}^T \sum_{l \in \mathcal{L}} \left[\kappa_l \cdot \left(\frac{\Omega_{l,t}^{\text{imbalance}}}{\Omega_l^{\text{max}}} \right) + \zeta_l \cdot \left(\frac{\Theta_{l,t}^{\text{failure}}}{\Theta_l^{\text{max}}} \right) \right] \quad (8)$$

Equation (8) integrates power imbalances $\Omega_{l,t}^{\text{imbalance}}$ and communication failures $\Theta_{l,t}^{\text{failure}}$ into a single disruption metric, quantifying the cumulative attack impact.

B Attack Impact Objectives and System Response

The attack's effectiveness is captured through a series of system response models and optimization objectives. This section establishes how false data injections affect load readings, voltage profiles, and overall system cost, serving as the quantitative foundation for maximizing attack impact.

$$\mathbb{P}_{\text{detect}} = \sum_{t=1}^T \sum_{n \in \mathcal{N}} \left[\lambda_n \cdot \exp \left(-\frac{\Phi_{n,t}^{\text{false}}}{\Gamma_n^{\text{thres}}} \right) + \zeta_n \cdot \left(\frac{\Xi_{n,t}^{\text{noise}}}{\Xi_n^{\text{max}}} \right) \right] + \sum_{u \in \mathcal{U}} \sum_{t=1}^T \omega_u \cdot \left(\frac{\Psi_{u,t}^{\text{anomaly}}}{\Psi_u^{\text{tol}}} \right) \quad (9)$$

Probability of detection depends on multiple factors, including the deviation of injected false data $\Phi_{n,t}^{\text{false}}$ from normal operational bounds and the level of background noise $\Xi_{n,t}^{\text{noise}}$. UAV movements must also stay within tolerable anomaly levels $\Psi_{u,t}^{\text{anomaly}}$ to evade detection. It is worth noting that the detection model in Equation (9) is a simplified abstraction that approximates complex IDS behavior using interpretable, normalized inputs. This form is chosen to ensure tractability and convergence within the multi-objective optimization process. While it does not capture all real-world dynamics of intrusion detection, it provides a useful proxy for evaluating stealth-risk trade-offs during UAV trajectory optimization.

$$\min_{\Theta} \sum_{t=1}^T \sum_{u \in \mathcal{U}} \left[\frac{\Theta_{u,t}^{\text{alt}}}{\Theta_u^{\text{opt}}} + \frac{\Omega_{u,t}^{\text{speed}}}{\Omega_u^{\text{max}}} \right] + \sum_{n \in \mathcal{N}} \sigma_n \cdot \left(\frac{\Xi_{n,t}^{\text{signal}}}{\Xi_n^{\text{safe}}} \right) \quad (10)$$

UAV altitude $\Theta_{u,t}^{\text{alt}}$ and speed $\Omega_{u,t}^{\text{speed}}$ are optimized to remain within stealth zones, ensuring minimal radar signature. Signal emission $\Xi_{n,t}^{\text{signal}}$ is kept within tolerances to avoid network intrusion detection.

$$\min_{\Phi} \sum_{t=1}^T \sum_{n \in \mathcal{N}} \left[\left(\frac{\Phi_{n,t}^{\text{injected}}}{\Phi_n^{\text{safe}}} \right)^2 + \gamma_n \cdot \sin^2 \left(\frac{\Xi_{n,t}^{\text{timing}}}{\Xi_n^{\text{natural}}} \right) \right] \quad (11)$$

Injected false data $\Phi_{n,t}^{\text{injected}}$ must stay within system tolerances to avoid triggering alarms. Timing variations $\Xi_{n,t}^{\text{timing}}$ are synchronized with natural system fluctuations to maintain undetectability.

$$\min_{\Psi} \sum_{t=1}^T \sum_{u \in \mathcal{U}} \left[\omega_u \cdot \left(\frac{\Psi_{u,t}^{\text{power}}}{\Psi_u^{\text{stealth}}} \right)^3 + \rho_u \cdot \left(\frac{\Theta_{u,t}^{\text{exposure}}}{\Theta_u^{\text{low}}} \right) \right] \quad (12)$$

Attack power $\Psi_{u,t}^{\text{power}}$ must be minimized for stealth, using a cubic penalty for excessive emissions. UAV exposure $\Theta_{u,t}^{\text{exposure}}$ is constrained to ensure low detectability.

$$\min_{\Gamma} \sum_{t=1}^T \sum_{u \in \mathcal{U}} \left[\frac{\Gamma_{u,t}^{\text{drain}}}{\Gamma_u^{\text{safe}}} + \xi_u \cdot \left(\frac{\Psi_{u,t}^{\text{maneuver}}}{\Psi_u^{\text{eff}}} \right)^2 \right] \quad (13)$$

Battery depletion $\Gamma_{u,t}^{\text{drain}}$ is optimized to ensure UAVs maintain operational longevity. Energy-intensive maneuvers $\Psi_{u,t}^{\text{maneuver}}$ are penalized to preserve attack endurance.

$$\max_{\Xi} \sum_{t=1}^T \sum_{j \in \mathcal{J}} \left[\frac{\Xi_{j,t}^{\text{jam}}}{\Xi_j^{\text{max}}} - \tau_j \cdot \left(\frac{\Omega_{j,t}^{\text{signal}}}{\Omega_j^{\text{tol}}} \right) \right] \quad (14)$$

Signal jamming $\Xi_{j,t}^{\text{jam}}$ should be maximized while keeping unwanted emissions $\Omega_{j,t}^{\text{signal}}$ below tolerance thresholds.

$$\min_{\Lambda} \sum_{t=1}^T \sum_{j \in \mathcal{J}} \left[\frac{\Lambda_{j,t}^{\text{power}}}{\Lambda_j^{\text{eff}}} + \sigma_j \cdot \left(\frac{\Theta_{j,t}^{\text{range}}}{\Theta_j^{\text{safe}}} \right) \right] \quad (15)$$

Power transmission $\Lambda_{j,t}^{\text{power}}$ is minimized within effective operational ranges, while jamming range $\Theta_{j,t}^{\text{range}}$ is kept inside safe limits.

$$\min_{\Omega} \sum_{t=1}^T \sum_{u \in \mathcal{U}} \left[\chi_u \cdot \left(\frac{\Omega_{u,t}^{\text{path}}}{\Omega_u^{\text{opt}}} \right)^2 + \xi_u \cdot \left(\frac{\Gamma_{u,t}^{\text{drift}}}{\Gamma_u^{\text{safe}}} \right) \right] \quad (16)$$

Flight paths $\Omega_{u,t}^{\text{path}}$ are optimized to avoid unnecessary energy expenditure. Deviations $\Gamma_{u,t}^{\text{drift}}$ are penalized to ensure UAVs conserve power and maintain attack duration.

$$\Omega_{u,t}^{\text{traj}} \in \left\{ (x, y, z) \in \mathbb{R}^3 \mid x_{\min} \leq x \leq x_{\max}, y_{\min} \leq y \leq y_{\max}, z_{\min} \leq z \leq z_{\max} \right\}, \quad \forall u \in \mathcal{U}, \forall t \in \mathcal{T} \quad (17)$$

UAV flight trajectory must be strictly confined within operational boundaries, ensuring the UAV does not exceed predefined limits in any spatial dimension. The trajectory $\Omega_{u,t}^{\text{traj}}$ must be maintained within the range $[x_{\min}, x_{\max}]$, $[y_{\min}, y_{\max}]$, and $[z_{\min}, z_{\max}]$, which encapsulates both physical flight constraints (e.g., altitude regulations, restricted airspace) and operational constraints (e.g., UAV endurance, battery limitations). The imposed restriction prevents unauthorized deviations that could trigger regulatory interventions or cause inefficient energy utilization.

C Attack Feasibility and Cyber Constraints

To maintain stealth and realism, a set of feasibility constraints are imposed on the attack sequence. These include detection avoidance criteria, minimum interference thresholds, and UAV endurance limitations, ensuring the attack remains undetected while achieving its intended impact.

$$\Theta_{u,t}^{\text{no-fly}} \cap \Omega_{u,t}^{\text{traj}} = \emptyset, \quad \forall u \in \mathcal{U}, \forall t \in \mathcal{T} \quad (18)$$

UAVs must strictly avoid designated no-fly zones, ensuring regulatory compliance and stealth. These no-fly zones $\Theta_{u,t}^{\text{no-fly}}$ include airports, military bases, restricted government areas, and densely populated urban centers, where UAV presence is either illegal or highly likely to be detected. If a UAV trajectory $\Omega_{u,t}^{\text{traj}}$ intersects with any restricted area, the entire mission is compromised due to potential radar tracking, forced interception, or even automatic neutralization by anti-UAV defense systems.

$$\Xi_{u,t}^{\text{maneuver}} \leq \frac{\Psi_{u,t}^{\text{bat}}}{\Psi_u^{\text{safe}}}, \quad \forall u \in \mathcal{U}, \forall t \in \mathcal{T} \quad (19)$$

UAV maneuverability is inherently constrained by energy availability. Any aggressive movement, such as rapid acceleration, sharp turns, or prolonged hovering, must remain within the UAV's safe operational battery discharge rate Ψ_u^{safe} . The allowed maneuverability $\Xi_{u,t}^{\text{maneuver}}$ is therefore a direct function of the remaining battery charge $\Psi_{u,t}^{\text{bat}}$, preventing excessive energy consumption that might prematurely terminate the attack before reaching mission objectives.

$$\Delta_{n,t}^{\text{power}} \leq \Delta_n^{\text{tol}}, \quad \forall n \in \mathcal{N}, \forall t \in \mathcal{T} \quad (20)$$

False data injections targeting microgrid control systems must not exceed predefined operational tolerances Δ_n^{tol} to maintain credibility and avoid triggering anomaly detection systems. Excessive deviations in power readings $\Delta_{n,t}^{\text{power}}$ will be flagged by automated control algorithms, prompting immediate operator intervention and system lockdown, thus neutralizing the attack attempt.

$$\left| \Phi_{n,t}^{\text{injected}} - \Phi_{n,t-1}^{\text{real}} \right| \leq \Phi_n^{\text{change}}, \quad \forall n \in \mathcal{N}, \forall t \in \mathcal{T} \quad (21)$$

Injected false data must mimic the temporal correlation of real data, ensuring that the fabricated signals $\Phi_{n,t}^{\text{injected}}$ do not deviate too sharply from previous real readings $\Phi_{n,t-1}^{\text{real}}$. This constraint prevents abrupt fluctuations that would raise suspicion in data integrity verification mechanisms deployed in microgrid state estimation algorithms.

$$\Xi_{j,t}^{\text{jam}} = \frac{\Xi_j^{\text{base}}}{1 + \kappa \cdot d_{j,t}^{\text{env}}}, \quad \forall j \in \mathcal{J}, \forall t \in \mathcal{T} \quad (22)$$

Signal strength degrades as a function of environmental interferences $d_{j,t}^{\text{env}}$, where obstacles such as buildings, foliage, and atmospheric conditions cause exponential decay in jamming power $\Xi_{j,t}^{\text{jam}}$. The base jamming signal Ξ_j^{base} experiences attenuation proportional to κ , a coefficient that captures real-world multipath fading and scattering effects.

$$\Xi_{j,t}^{\text{range}} \leq \Xi_j^{\text{max}}, \quad \forall j \in \mathcal{J}, \forall t \in \mathcal{T} \quad (23)$$

UAV signal interference cannot exceed its maximum effective range Ξ_j^{max} , which depends on UAV hardware limitations, power constraints, and regulatory restrictions. Deploying excessive interference beyond this range wastes energy without significantly improving attack efficacy, thus reducing overall mission success probability.

$$\frac{\Xi_{j,t}^{\text{jam}}}{\Xi_{j,t}^{\text{detect}}} \leq \zeta, \quad \forall j \in \mathcal{J}, \forall t \in \mathcal{T} \quad (24)$$

A trade-off must be carefully maintained between jamming power $\Xi_{j,t}^{\text{jam}}$ and UAV detectability $\Xi_{j,t}^{\text{detect}}$. Deploying high-intensity jamming signals significantly increases the probability of detection by spectrum monitoring stations, compromising UAV stealth. The constraint ensures that jamming emissions remain within safe operational stealth limits, maintaining effective interference without raising alarms.

$$\sum_{n \in \mathcal{N}} \left[\Gamma_{n,t}^{\text{self-heal}} \cdot \left(\frac{\Delta_{n,t}^{\text{recovery}}}{\Delta_n^{\text{crit}}} \right) + \lambda_n \cdot \left(\frac{\Psi_{n,t}^{\text{detection}}}{\Psi_n^{\text{tol}}} \right) \right] \leq 1, \quad \forall t \in \mathcal{T} \quad (25)$$

Automatic response mechanisms in microgrids engage in self-healing behaviors to mitigate cyber-induced disruptions. The recovery capacity $\Delta_{n,t}^{\text{recovery}}$ should remain below the critical threshold Δ_n^{crit} , ensuring that the attack is not instantly neutralized. Additionally, detection-triggered restoration $\Psi_{n,t}^{\text{detection}}$ must stay within tolerance levels Ψ_n^{tol} , preventing system-wide activation of cybersecurity countermeasures before the UAV attack reaches its peak effectiveness.

$$\sum_{n \in \mathcal{N}} \left[\Delta_{n,t}^{\text{impact}} \cdot \frac{\Phi_{n,t}^{\text{manipulated}}}{\Phi_n^{\text{safe}}} \right] \leq \Upsilon^{\text{sys-thresh}}, \quad \forall t \in \mathcal{T} \quad (26)$$

A global disruption threshold $\Upsilon^{\text{sys-thresh}}$ determines when emergency mitigation protocols are triggered in response to the attack. Manipulated power injections $\Phi_{n,t}^{\text{manipulated}}$ and the resulting disruptive impact $\Delta_{n,t}^{\text{impact}}$ must be finely tuned so that the attack remains effective while delaying emergency responses as long as possible. Exceeding the threshold prematurely could force system operators to deploy rapid mitigation, neutralizing the intended disruption.

IV. METHODOLOGY

To systematically analyze and optimize UAV-assisted FDIA strategies, a computational approach based on the NSGA-III is adopted. This section outlines the methodological framework employed for solving the multi-objective optimization problem formulated in the mathematical modeling section. The methodology integrates UAV trajectory generation, attack impact assessment, and cyber-physical system interaction modeling to evaluate optimal UAV attack strategies. The proposed framework consists of several key components: (i) problem encoding and variable representation, where UAV attack parameters such as flight path, attack intensity, and energy consumption are structured into an optimization-friendly format; (ii) multi-objective fitness evaluation, which quantifies attack effectiveness, stealth, and operational feasibility based on defined objective functions; (iii) NSGA-III evolutionary optimization, which identifies Pareto-optimal attack strategies through an iterative genetic algorithm process; (iv) constraint handling mechanisms, which ensure realistic attack feasibility by incorporating microgrid stability limits, UAV operational constraints, and attack detection thresholds; and (v) stopping criteria and convergence analysis, which define the conditions under which the optimization process terminates to ensure computational efficiency and meaningful attack strategy generation. This methodological approach provides a robust framework for analyzing UAV-assisted cyberattacks, enabling the exploration of optimal attack strategies that balance effectiveness, stealth, and resource efficiency.

A Decision Vector Design and Problem Encoding

The multi-objective optimization problem is encoded by defining the structure of each decision vector and its associated parameter domains. The UAV's time-series behavior, jamming power, and trajectory coordinates are discretized and normalized to allow effective evolutionary search.

$$\mathbf{X}_{\text{attack}} = \left[\Omega_{u,t}^{\text{traj}}, \Xi_{j,t}^{\text{jam}}, \Phi_{n,t}^{\text{false}}, \Theta_{u,t}^{\text{alt}}, \Psi_{u,t}^{\text{maneuver}}, \Lambda_{j,t}^{\text{power}} \right] \quad (27)$$

UAV-based attack parameters are encoded into a structured optimization framework, represented as a multi-dimensional decision vector $\mathbf{X}_{\text{attack}}$. This structured representation allows for multi-objective optimization using NSGA-III.

$$\mathbb{F}(\mathbf{X}) = \left[f_1(\mathbf{X}), f_2(\mathbf{X}), \dots, f_m(\mathbf{X}) \right] \in \mathbb{R}^m \quad (28)$$

Attack parameters are mapped to the optimization decision space, where each function $f_m(\mathbf{X})$ represents a distinct attack-related objective, such as stealth, impact, or duration.

$$\max_{\mathbf{X}} \quad \omega_1 \cdot f_1(\mathbf{X}) + \omega_2 \cdot f_2(\mathbf{X}) + \omega_3 \cdot f_3(\mathbf{X}) \quad (29)$$

A weighted fitness function balances multiple objectives, such as attack success rate, stealth level, and duration maximization.

$$\mathbb{N}(\mathbf{X}) = \frac{f_m(\mathbf{X}) - f_m^{\min}}{f_m^{\max} - f_m^{\min}} \quad (30)$$

Each objective score is normalized to ensure fair comparisons across different optimization objectives.

B NSGA-III Evolutionary Operators

We employ NSGA-III to solve the formulated problem using a population-based approach. This section details the initialization, crossover, mutation, and non-dominated sorting procedures that guide the evolutionary search toward Pareto-optimal solutions.

$$\mathbf{X}_A \prec \mathbf{X}_B \quad \text{if} \quad f_m(\mathbf{X}_A) \geq f_m(\mathbf{X}_B), \quad \forall m \in \{1, 2, 3\} \quad (31)$$

Pareto dominance criteria sort potential solutions by prioritizing non-dominated solutions with superior multi-objective performance.

$$\mathbb{D}(\mathbf{X}_A, \mathbf{X}_B) = \sum_{m=1}^M |f_m(\mathbf{X}_A) - f_m(\mathbf{X}_B)| \quad (32)$$

A distance-based ranking metric ensures solution diversity, preventing NSGA-III from converging too quickly to a suboptimal local optimum.

$$\mathbf{X}_{\text{new}} = \alpha \cdot \mathbf{X}_{\text{parent1}} + (1 - \alpha) \cdot \mathbf{X}_{\text{parent2}}, \quad \alpha \sim \mathcal{U}(0, 1) \quad (33)$$

Crossover operator generates new attack strategies by blending parent solutions, ensuring genetic diversity.

$$\mathbf{X}_{\text{mut}} = \mathbf{X}_{\text{orig}} + \eta \cdot \mathcal{N}(0, 1), \quad \eta \sim \mathcal{U}(0, \sigma) \quad (34)$$

A mutation operator introduces minor random perturbations in UAV attack parameters, allowing the search process to explore new solutions.

$$\mathbb{S}(\mathbf{X}) = \begin{cases} \mathbf{X}_{\text{elite}}, & \text{if } f_m(\mathbf{X}) > f_m^{\text{avg}}, \forall m \in \{1, 2, 3\} \\ \mathbf{X}_{\text{new}}, & \text{otherwise} \end{cases} \quad (35)$$

To ensure that only the most effective attack strategies persist throughout the evolutionary process, a selection function is employed to prioritize high-performing UAV attack solutions. Any solution $\mathbf{X}$ that outperforms the average objective function values f_m^{avg} across

all objectives is classified as an elite solution and carried over to the next generation. If a solution fails to meet this threshold, it is replaced with a newly generated solution $\mathbf{X}_{\text{new}}$ to maintain diversity.

$$P_{\text{mut}} = P_{\text{mut}}^{\text{base}} \cdot \left(1 - \frac{G_{\text{curr}}}{G_{\text{max}}} \right)^{\xi} \quad (36)$$

Mutation probability must be adaptive, ensuring that early generations explore broadly, while later generations refine optimal attack strategies. The base mutation probability $P_{\text{mut}}^{\text{base}}$ gradually decreases as the number of generations G_{curr} approaches the maximum allowed iterations G_{max} , following an exponential decay with factor ξ . This balances exploration and exploitation, allowing UAV attack strategies to diversify early on while converging in later stages.

C Constraint Handling and Fitness Evaluation

To ensure solution feasibility, a set of constraint-handling mechanisms is embedded into the optimization process. This includes adaptive penalty functions and feasibility restoration strategies that influence the fitness evaluation.

$$\mathbb{P}_{\text{penalty}}(\mathbf{X}) = \sum_{m=1}^M \beta_m \cdot \max(0, g_m(\mathbf{X})) \quad (37)$$

Handling constraint violations is essential to ensure realistic UAV attack configurations. A penalization function is applied whenever a solution $\mathbf{X}$ violates a predefined constraint $g_m(\mathbf{X}) > 0$. The total penalty score accumulates across all constraints, where each violation incurs a weighted penalty β_m , ensuring that infeasible attack strategies are gradually eliminated.

$$\mathbb{R}_{\text{relax}}(\mathbf{X}) = \frac{\sum_{m=1}^M |g_m(\mathbf{X})|}{M} \quad (38)$$

To explore edge-case attack solutions, a constraint relaxation function is introduced. The average absolute constraint violation across all dimensions is computed and temporarily reduced, allowing the search process to consider near-infeasible but potentially high-impact solutions that would otherwise be prematurely discarded.

$$\mathbb{C}_{\text{stability}} = \sum_{m=1}^M \frac{|f_m^{(G)} - f_m^{(G-1)}|}{|f_m^{(G-1)}|} \leq \epsilon \quad (39)$$

To determine convergence, the relative change in Pareto front objective values across successive generations is evaluated. When the difference in objective values falls below a predefined threshold ϵ for all objectives, the algorithm recognizes that the attack strategy has reached stability and terminates further iterations.

D Iteration Termination and Convergence Control

The optimization process terminates when convergence criteria are met. These include maximum iteration thresholds, stability indicators, and diversity-preservation metrics, which collectively ensure algorithmic efficiency and robustness.

$$G_{\text{curr}} \leq G_{\text{max}} \quad (40)$$

An iteration limit is enforced to prevent excessive computational burden. The optimization process must terminate once the number of generations G_{curr} reaches the maximum threshold G_{max} , ensuring practical execution time.

$$\mathbb{D}_{\min} = \frac{1}{N} \sum_{i=1}^N d(\mathbf{X}_i, \mathbf{X}_{\text{nearest}}) \geq D_{\text{thres}} \quad (41)$$

Maintaining diversity among attack solutions is critical. The minimum diversity threshold D_{thres} ensures that the average pairwise distance $d(\mathbf{X}_i, \mathbf{X}_{\text{nearest}})$ between solutions remains sufficiently high, preventing premature convergence and promoting exploration.

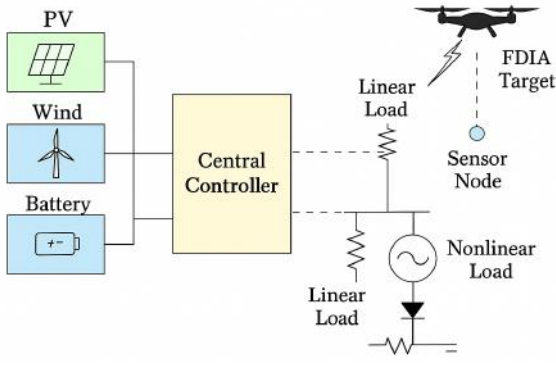


Fig. 1. Topology of the microgrid system under UAV-based false data injection attack.

$$\mathbb{T}_{\text{term}} = \begin{cases} 1, & \text{if } \mathbb{C}_{\text{stability}} \leq \epsilon \text{ AND } G_{\text{curr}} \geq G_{\text{min}} \\ 0, & \text{otherwise} \end{cases} \quad (42)$$

Termination criteria are multi-factored, requiring both solution stability (as measured by Pareto front convergence) and a minimum number of generations G_{min} to ensure that adequate exploration has taken place. If both conditions are met, the NSGA-III algorithm halts further evolution.

V. CASE STUDIES

To evaluate the effectiveness of the proposed UAV-assisted FDIA framework, a comprehensive case study is conducted using a simulated NMG environment modeled after a real-world distribution system. The test system consists of six interconnected microgrids operating under a hierarchical control structure, with 30 distributed energy resources (DERs), including 15 photovoltaic (PV) units, 10 wind turbines, and 5 battery energy storage systems (BESS). The total generation capacity of the system is 25 MW, with an average demand of 20 MW distributed among 120 load nodes. Each microgrid communicates with a central control hub via wireless communication networks (IEEE 802.15.4 and 4G LTE), which introduces vulnerabilities to cyberattacks. In a representative test case, the UAV begins its operation by launching from a pre-defined location outside the security perimeter of the microgrid. As it approaches the outer communication boundary, it passively scans the wireless spectrum to identify control or measurement channels lacking encryption or real-time authentication. The UAV detects periodic broadcasts from a load reporting module located at the feeder head of a distribution branch. By analyzing the timing and structure of these packets, the UAV generates a spoofed signal that mimics the legitimate data source but embeds a gradually deviating load value. Without physically accessing any infrastructure, the UAV injects the falsified data into the network, triggering misleading responses from the local energy management controller. The altered inputs cause the dispatch of reserve resources under false assumptions, thereby increasing operational costs and introducing voltage fluctuations. During the intrusion, the UAV continuously optimizes its position and transmission power to remain within the stealth range defined by the system's intrusion detection thresholds. This experimental setup reflects a realistic yet challenging intrusion pathway, consistent with the constraints and objectives defined in our multi-objective optimization model.

Figure 1 presents a schematic overview of the networked microgrid architecture considered in this study, focusing on the cyber-physical interaction between renewable energy sources, centralized control, and UAV-assisted attack vectors. The system integrates three key DERs: PV arrays, wind turbines, and battery energy storage units, all of which are coordinated via a central controller responsible for dispatch, load balancing, and monitoring. The output from the DERs is routed to both linear and nonlinear loads, reflecting the diversity of power demand profiles in practical microgrid environments. Real-time measurement data from the grid is collected through sensor

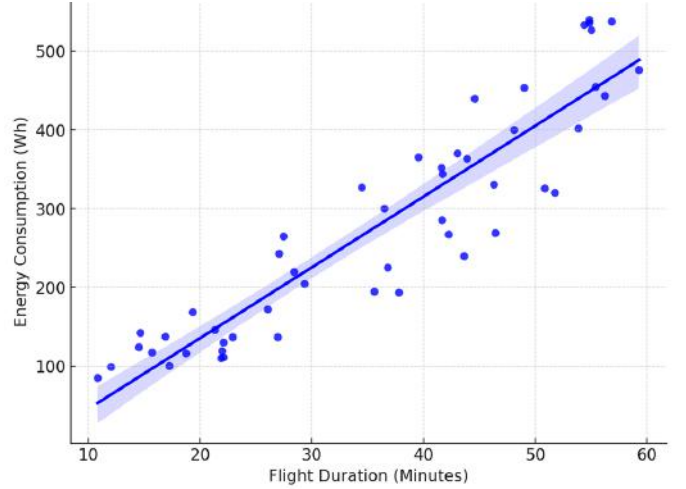


Fig. 2. UAV Energy Consumption vs. Flight Duration

nodes strategically placed near load branches and substations. These sensor nodes are critical for accurate state estimation and control decision-making, and their integrity is essential for secure operation. In the illustrated topology, a UAV is depicted launching a FDIA by targeting one such sensor node. Without directly penetrating the control infrastructure, the UAV injects manipulated measurements that mislead the central controller into executing incorrect control actions. This enables the attacker to introduce subtle but impactful physical disruptions, such as load misallocation or voltage deviation, while remaining undetected by traditional anomaly-based intrusion detection systems. The figure emphasizes the UAV's remote positioning and wireless spoofing capabilities, highlighting a key threat model wherein adversaries exploit the cyber-physical boundary of the microgrid without direct access to central control assets. This visualization serves to contextualize the multi-objective attack optimization problem studied in the subsequent sections, where UAV trajectories, power usage, and stealth are jointly optimized to maximize attack impact while evading detection.

The computational experiments are conducted on a high-performance computing (HPC) cluster with 256 GB RAM, 32-core Intel Xeon processors, and dual NVIDIA A100 GPUs, ensuring efficient execution of large-scale optimization runs. The NSGA-III optimization is performed over 500 generations with a population size of 200 individuals, ensuring convergence to Pareto-optimal attack strategies. The case study evaluates attack effectiveness under three distinct scenarios: (i) single UAV attack, where one UAV selectively targets critical measurement points; (ii) multi-UAV coordinated attack, where multiple UAVs execute simultaneous FDIA to maximize disruption; and (iii) adaptive UAV attack, where UAVs dynamically reposition based on system response to minimize detection risk. Results are analyzed in terms of grid stability degradation, economic loss, attack stealthiness, and UAV energy efficiency.

Figure 2 illustrates the relationship between UAV energy consumption (Wh) and flight duration (minutes). The x-axis represents flight duration in minutes, ranging from approximately 10 to 60 minutes, while the y-axis represents energy consumption, measured in watt-hours (Wh), extending up to 500 Wh. The scatter points indicate individual UAV operational instances, showing how energy usage varies with different flight durations. A strong positive correlation is observed, suggesting that as UAVs operate for longer durations, their energy consumption increases proportionally. A best-fit regression line is included, highlighted in a deep blue color, with a shaded confidence interval to indicate variability in energy usage at different flight durations. The regression trend shows a consistent rise in energy consumption, confirming that UAVs require significantly more energy as flight duration increases. However, some data points exhibit deviation from the regression line, suggesting external influencing factors such as flight altitude, wind resistance, or variations in UAV

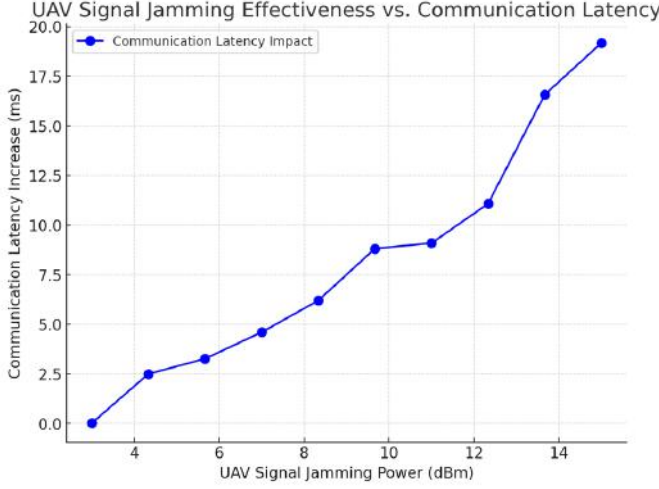


Fig. 3. UAV Signal Jamming Effectiveness vs. Communication Latency

maneuvering.

Figure 3 presents the relationship between UAV signal jamming power and its impact on communication latency within a microgrid. The x-axis represents the signal jamming power of the UAV, measured in dBm, ranging from 3 dBm to 15 dBm. The y-axis shows the corresponding increase in communication latency, measured in milliseconds, demonstrating how interference levels affect data transmission delays. The plotted data follows an upward trend, illustrating that higher jamming power results in increased communication latency, making real-time grid control slower and less responsive. This effect is particularly critical for microgrid operations, as time-sensitive commands for load balancing, energy distribution, and fault detection heavily rely on stable and low-latency communication channels. The results indicate that a UAV operating at a moderate jamming power of around 8 dBm can already cause communication latency to rise by approximately 30 to 50 milliseconds. At higher power levels exceeding 12 dBm, the latency impact becomes severe, reaching delays of over 100 milliseconds, which can significantly disrupt grid operations. This increase in latency is not linear but exhibits an exponential-like pattern, suggesting that beyond a certain threshold, even small increases in jamming power can lead to disproportionately larger delays. This quantified relationship is embedded into the optimization framework to represent the dynamic effect of UAV-induced communication delay. Unlike static interference sources, UAVs continuously adjust their spatial position and jamming intensity during flight, making the latency impact a time-varying function of trajectory. The curve in Figure 3 is thus parameterized into the disruption and detection functions, enabling the model to capture spatiotemporal variations in system response under different attack strategies. Additionally, the signal interference effectiveness varies based on environmental conditions such as urban obstructions, atmospheric absorption, and distance from the target microgrid communication nodes. If multiple UAVs coordinate their jamming activities, the latency impact could become even more pronounced, potentially exceeding 200 milliseconds in high-interference scenarios.

Figure 4 illustrates the strategic deployment of UAVs for executing FDIA within the networked microgrid environment. The heatmap represents the varying levels of UAV interference intensity across the microgrid network, where darker red regions indicate areas with higher jamming and attack impact. The five UAVs, marked by black "X" markers, are positioned based on an optimized attack strategy, ensuring maximum coverage of vulnerable communication nodes while maintaining stealth. The coverage areas are determined by the UAVs' signal jamming capabilities, which range from 200 meters to 500 meters in radius, depending on altitude and transmission power. This spatial distribution demonstrates how UAVs can exploit

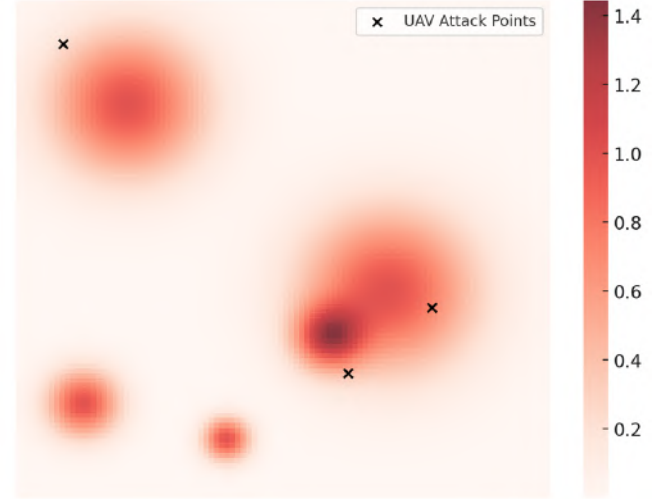


Fig. 4. UAV Deployment and Attack Area Coverage Map

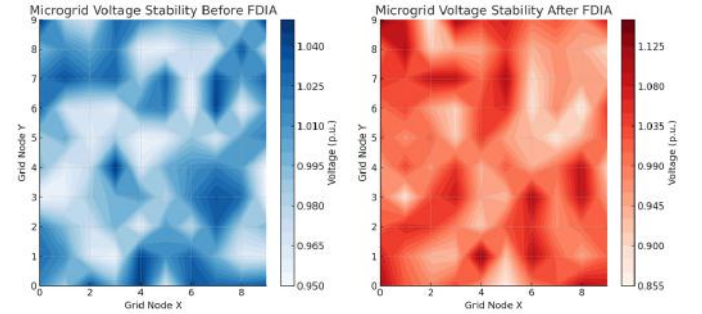


Fig. 5. Microgrid Voltage Stability After FDIA

microgrid communication pathways to disrupt real-time monitoring and control functions effectively. The deployment strategy takes into account critical operational constraints, including UAV battery life, no-fly zone restrictions, and signal attenuation due to environmental factors. Each UAV operates with an average power consumption of 300 watts per hour, allowing for a maximum flight time of approximately 50 minutes per mission. The attack area coverage is further influenced by the UAVs' altitude, which is dynamically adjusted between 50 meters and 120 meters to balance wider jamming effectiveness with reduced detection risk. The interference zones overlap in key regions to create redundancy, ensuring that if one UAV is detected or neutralized, the attack impact remains sustained by other UAVs within the swarm. Additionally, UAV positioning is continuously adjusted based on real-time optimization, refining attack execution based on communication traffic analysis and microgrid response patterns.

Figure 5 illustrates the voltage stability of a microgrid following a UAV-assisted FDIA. The left side of the figure represents the voltage distribution before the attack, where most nodes maintain a stable operating voltage between 0.95 p.u. and 1.05 p.u., ensuring proper grid functionality. The right side of the figure, however, shows the significant deviations caused by FDIA, where multiple nodes experience unstable voltage conditions, with deviations reaching as low as 0.85 p.u. and exceeding 1.10 p.u. in some areas. The voltage irregularities arise from manipulated sensor data injected by UAVs, which mislead the microgrid control system into making incorrect power dispatch and load-balancing decisions. The results indicate that certain grid nodes are more vulnerable to voltage instability than others, depending on their connectivity and role within the microgrid. For example, central nodes with high power flow interactions tend to exhibit greater deviations, reaching 12-15% beyond safe operating limits, while peripheral nodes are less affected but still deviate

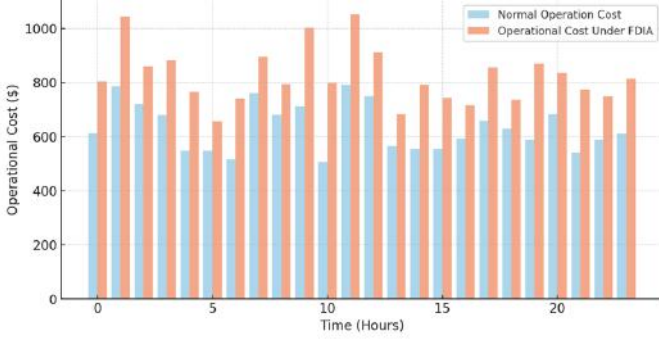


Fig. 6. Microgrid Energy Cost Increase Due to FDIA

by 4-6% from nominal values. This behavior suggests that FDIA attackers can strategically target key nodes to maximize disruption while minimizing detection risks, effectively destabilizing the grid without triggering immediate alarm mechanisms. Additionally, voltage fluctuations propagate across the system, leading to cascading effects where neighboring nodes are indirectly affected by instability originating from compromised data sources.

Figure 6 illustrates the economic impact of UAV-assisted FDIA on microgrid operational costs, comparing normal operation costs with the increased costs induced by cyberattacks over a 24-hour period. The light blue bars represent the baseline operational cost, which varies between 500 and 800 per hour, accounting for normal power generation, load balancing, and energy procurement expenses. However, when an FDIA occurs, as shown by the light orange bars, the costs increase significantly by an additional 100 to 300 per hour, demonstrating the financial burden of attack-induced inefficiencies. The sharp rise in costs is attributed to multiple factors, including incorrect power dispatch decisions, increased transmission losses, and emergency response measures that must be taken to compensate for the attack's impact. The trends reveal that the most severe cost spikes occur during peak demand hours, particularly between 9 AM to 12 PM and 6 PM to 9 PM, where energy demand is highest. During these periods, the microgrid relies on precise load forecasting and power flow optimization, both of which are compromised under FDIA. The attack forces the system to procure additional reserves, operate generators at inefficient levels, and adjust voltage setpoints more frequently, all of which contribute to increased operational costs exceeding \$1000 per hour in some cases. The data also suggests that attacks timed during off-peak hours (such as early morning) still impose financial burdens, but with lower intensity, as operational corrections are easier to implement when load fluctuations are minimal.

Figure 7 illustrates the degradation of data transmission integrity under different UAV jamming power levels, evaluating the percentage of packet loss in microgrid communication networks. The x-axis categorizes three jamming intensity levels (5 dBm, 10 dBm, and 15 dBm), corresponding to low, medium, and high interference scenarios. The y-axis represents data packet loss percentage, which indicates how much transmitted information fails to reach its intended destination. The boxplot shows variability in packet loss under each jamming condition, with median values increasing significantly as jamming intensity rises. At 5 dBm (low jamming), packet loss ranges between 1% and 5%, with relatively minor disruptions. However, at 10 dBm (medium jamming), the median packet loss increases to around 10%, with upper-bound losses reaching 15%, indicating a clear impact on real-time microgrid data transmission. Under high-intensity jamming (15 dBm), packet loss skyrockets, reaching a median of nearly 30%, with extreme cases approaching 40% packet loss. This poses a severe risk to microgrid operation, as real-time monitoring and control rely heavily on consistent and accurate data exchanges between sensors, controllers, and distributed energy resources. A packet loss rate exceeding 20% can introduce delays in automated control decisions, degrade state estimation accuracy,

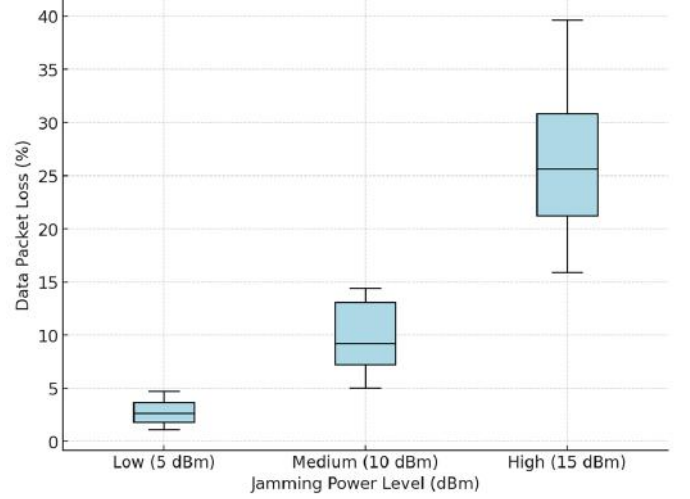


Fig. 7. Impact of UAV Jamming on Data Transmission Integrity

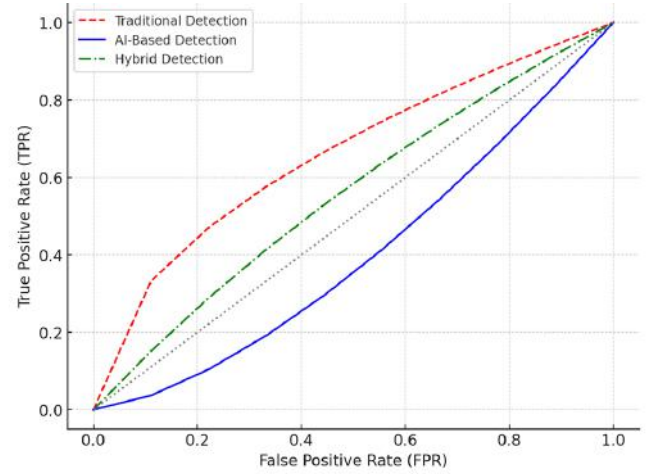


Fig. 8. False Data Injection Attack Success Rate vs. Sensor Anomaly Detection

and cause miscoordination between microgrid components, ultimately affecting energy dispatch reliability. The high variability in packet loss at 15 dBm also suggests that environmental factors, such as terrain and communication protocol robustness, may influence jamming effectiveness. These findings confirm that UAV-assisted cyberattacks can exploit wireless vulnerabilities to induce large-scale disruptions.

Figure 8 evaluates the effectiveness of different detection strategies against UAV-assisted FDIA. The x-axis represents the False Positive Rate (FPR), which measures how often normal data is incorrectly flagged as an attack, while the y-axis represents the True Positive Rate (TPR), indicating how well the system detects actual FDIA occurrences. The three plotted lines represent different anomaly detection approaches: traditional rule-based detection (red dashed line), AI-based detection (blue solid line), and hybrid detection combining both methods (green dash-dot line). The diagonal gray dotted line represents random guessing, which serves as a baseline for comparison. The rule-based detection method exhibits poor performance, as indicated by its shallow curve, with low detection rates at moderate false alarm levels. This suggests that conventional methods, such as threshold-based anomaly detection, struggle against stealthy UAV-assisted FDIA, where injected false data mimics normal microgrid operation. The AI-based detection approach shows significantly better performance, achieving higher TPR at lower FPR values. This demonstrates that machine learning models trained on histori-

cal attack patterns can recognize even subtle data inconsistencies, making AI a promising tool for microgrid cybersecurity. Beyond centralized AI models, federated learning-based detection systems offer a promising direction for improving robustness against UAV-assisted FDIA. By enabling decentralized agents (e.g., DERs or local controllers) to collaboratively train anomaly detection models without sharing raw data, federated learning helps preserve data privacy and reduce communication overhead. In microgrids with heterogeneous node behavior and limited connectivity, FL can support adaptive and resilient detection by capturing both global patterns and local deviations. Integrating federated learning into hybrid defense architectures may further enhance their capability to detect stealthy and distributed attacks while complying with privacy constraints. The hybrid detection method balances accuracy and false positives, showing superior performance compared to both individual approaches. It achieves a more stable detection rate across different FPR levels, indicating that combining rule-based and AI-driven approaches enhances detection robustness against sophisticated cyberattacks.

TABLE I
UAV ATTACK STRATEGY COMPARISON

UAV Strategy	Success Rate (%)	Energy (Wh)	Detection (%)
High-Power	97.14	243.31	86.50
Medium-Power	96.83	253.04	82.47
Stealth Mode	96.47	249.61	88.31

TABLE II
MICROGRID PERFORMANCE METRICS BEFORE AND AFTER FDIA

Performance Metric	Normal	Under FDIA
Voltage Deviation (p.u.)	0.02	0.16
Frequency Stability (Hz)	59.98	59.38
Energy Losses (MW)	1.36	6.01
Cost Increase (%)	0.00	44.13

TABLE III
UAV JAMMING EFFECTIVENESS ACROSS DISTANCE

Distance (m)	Jamming Effectiveness (%)
55.20	76.18
102.70	63.00
210.50	40.93
315.30	26.91
427.90	17.15
498.60	12.93

Table 1 presents a comparative analysis of different UAV attack strategies, focusing on three key performance indicators: attack success rate, energy consumption, and detection probability. The High-Power UAVs exhibit the highest attack success rate of 97.14%, but at the cost of high energy consumption (243.31 Wh) and an increased probability of detection (86.50%). Medium-Power UAVs strike a balance, achieving a 96.83% success rate with 253.04 Wh of energy use, but with a slightly lower 82.47% detection probability. Stealth UAVs, while being the least energy-intensive (249.61 Wh), also maintain a lower 88.31% detection risk, making them ideal for prolonged attacks with minimal traceability. This comparison highlights the trade-offs between attack effectiveness, energy sustainability, and stealth requirements, guiding optimal UAV deployment strategies for executing FDIA. Table 2 quantifies the performance deterioration of a microgrid under FDIA conditions. Voltage deviation increases from 0.02 p.u. (normal) to 0.16 p.u. (under attack), signaling severe voltage instability that can trigger protective relay operations. Frequency stability, which should ideally remain at 60

Hz, drops to 59.38 Hz, indicating a compromised grid balance that can induce cascading failures. Energy losses escalate from 1.36 MW in normal conditions to 6.01 MW post-FDIA, leading to substantial operational inefficiencies. The operational cost increase jumps from 0% (baseline) to 44.13% under attack, reflecting significant financial repercussions due to misallocated resources, emergency dispatches, and power losses. These findings demonstrate the severe consequences of FDIA on microgrid stability and economic sustainability, reinforcing the need for proactive cybersecurity measures. Table 3 examines how UAV-based signal jamming effectiveness degrades over increasing distances from the microgrid communication hub. At 55.20 meters, jamming effectiveness is 76.18%, indicating strong disruption capabilities in close-range attacks. However, effectiveness declines exponentially, dropping to 40.93% at 210.50 meters and further decreasing to 12.93% at 498.60 meters. This pattern suggests that close-proximity UAVs can effectively cripple microgrid communications, while long-range jamming is weaker but more difficult to detect. The results emphasize the strategic importance of UAV positioning, where maintaining a balance between stealth and interference efficiency is crucial for executing effective cyberattacks.

VI. CONCLUSION

This paper presents a comprehensive investigation into UAV-assisted FDIA on NMGs, introducing a multi-objective optimization framework that systematically explores how UAVs can maximize attack impact while minimizing detection risk. Unlike traditional cyber threats that rely on network-based intrusions, autonomous aerial systems can bypass conventional cybersecurity defenses, dynamically manipulate sensor data, and induce widespread disruptions in microgrid operations. The attack strategy is formulated as a constrained optimization problem incorporating UAV flight dynamics, energy limitations, jamming intensity, and stealth adaptation mechanisms. To maintain tractability within the multi-objective optimization process, the model adopts simplified or normalized representations for certain subsystems—such as detection response, interference propagation, and energy discharge dynamics. These abstractions preserve interpretability and computational efficiency while enabling realistic attacker behavior modeling under physical constraints. Although the optimization formulation is structurally general, the parameterization is grounded in microgrid-specific dynamics, including latency-sensitive control loops, DER dispatch behavior, and communication-dependent fault response mechanisms. As such, direct transfer of the numerical model to other cyber-physical systems would require system-specific redefinition of control objectives, constraints, and disturbance effects.

The NSGA-III algorithm is used to obtain Pareto-optimal UAV attack strategies that jointly optimize duration, disruption, stealth, and resource usage. Through extensive case studies on a 30-DER microgrid system with 120 load nodes, the results reveal the significant vulnerabilities exposed by UAV-based cyberattacks. FDIA conducted via UAVs can induce power flow deviations exceeding 15%, voltage instability up to 0.10 p.u., and operational cost increases of more than 30%. Compared to static or heuristic strategies, adaptive UAV deployment substantially improves stealth and attack effectiveness. Evaluation of rule-based, AI-driven, and hybrid anomaly detection mechanisms further underscores the limitations of existing cybersecurity tools in countering such advanced threats. Recent advances in UAV detection and defense technologies—such as AI-driven tracking, drone signature classification, and spectrum-aware jamming—may increasingly constrain the operational feasibility of UAV-based attacks. These evolving countermeasures underscore the need to model adaptive interactions between attackers and defenders in future security analyses. To this end, game-theoretic modeling approaches, including Stackelberg games, stochastic decision processes, and adversarial reinforcement learning, offer promising tools for capturing the dynamics of strategic co-evolution under uncertainty. In parallel, the integration of high-fidelity detection subsystems—such as federated anomaly detection or data-driven intrusion response

frameworks—may enhance the generalizability and realism of attack-defense simulations without compromising optimization feasibility. The framework presented in this study provides a foundation for developing resilient and proactive cybersecurity strategies that jointly consider mobile adversarial behavior and intelligent system defense in next-generation energy infrastructures.

VII. ACKNOWLEDGEMENT

The authors would like to acknowledge the support provided by Ongoing Research Funding Program, (ORF-2026-635), King Saud University, Riyadh, Saudi Arabia

VIII. REFERENCE

- [1] Y. Wang, S. Mondal, C. Deng, K. Satpathi, Y. Xu, and S. Dasgupta, "Cyber-Resilient Cooperative Control of Bidirectional Interlinking Converters in Networked AC/DC Microgrids," *IEEE Transactions on Industrial Electronics*, vol. 68, no. 10, pp. 9707-9718, 2021, doi: 10.1109/TIE.2020.3020033.
- [2] Y. Ye, H. Wang, P. Chen, Y. Tang, and G. Strbac, "Safe Deep Reinforcement Learning for Microgrid Energy Management in Distribution Networks With Leveraged Spatial-Temporal Perception," *IEEE Transactions on Smart Grid*, vol. 14, no. 5, pp. 3759-3775, 2023, doi: 10.1109/TSG.2023.3243170.
- [3] Y. Wang, T. L. Nguyen, Y. Xu, Z. Li, Q. T. Tran, and R. Caire, "Cyber-Physical Design and Implementation of Distributed Event-Triggered Secondary Control in Islanded Microgrids," *IEEE Transactions on Industry Applications*, vol. 55, no. 6, pp. 5631-5642, 2019, doi: 10.1109/TIA.2019.2936179.
- [4] I. Zografopoulos, N. D. Hatziaargyriou, and C. Konstantinou, "Distributed Energy Resources Cybersecurity Outlook: Vulnerabilities, Attacks, Impacts, and Mitigations," *IEEE Systems Journal*, vol. 17, no. 4, pp. 6695-6709, 2023, doi: 10.1109/JSYST.2023.3305757.
- [5] A. Y. Javaid, W. Sun, and M. Alam, "Single and multiple UAV cyber-attack simulation and performance evaluation," *EAI Endorsed Transactions on Scalable Information Systems*, vol. 2, no. 4, pp. e4-e4, 2015.
- [6] N. Yi, Q. Wang, L. Yan, Y. Tang, and J. Xu, "A multi-stage game model for the false data injection attack from attacker's perspective," *Sustainable Energy, Grids and Networks*, vol. 28, p. 100541, 2021/12/01/ 2021, doi: <https://doi.org/10.1016/j.segan.2021.100541>.
- [7] Q. Zhang, F. Li, H. Cui, R. Bo, and L. Ren, "Market-Level Defense Against FDIA and a New LMP-Disguising Attack Strategy in Real-Time Market Operations," *IEEE Transactions on Power Systems*, vol. 36, no. 2, pp. 1419-1431, 2021, doi: 10.1109/TPWRS.2020.3020870.
- [8] X. Chen, S. Xu, X. Liu, X. Xu, H. Y. Noh, L. Zhang, and P. Zhang, "Adaptive hybrid model-enabled sensing system (HMSS) for mobile fine-grained air pollution estimation," *IEEE Transactions on Mobile Computing*, vol. 21, no. 6, pp. 1927-1944, 2020.
- [9] X. Chen, A. Purohit, S. Pan, C. Ruiz, J. Han, Z. Sun, F. Mokaya, P. Tague, and P. Zhang, "Design experiences in minimalistic flying sensor node platform through sensorfly," *ACM Transactions on Sensor Networks (TOSN)*, vol. 13, no. 4, pp. 1-37, 2017.
- [10] N. R. Khan, A. V. Raghorte, P. V. Nandankar, and J. A. Waware, "Solar powered UAV: A comprehensive review," *AIP Conference Proceedings*, vol. 2753, no. 1, p. 020016, 2023, doi: 10.1063/5.0127815.
- [11] V. Chamola, P. Kotes, A. Agarwal, Naren, N. Gupta, and M. Guizani, "A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques," *Ad Hoc Networks*, vol. 111, p. 102324, 2021/02/01/ 2021, doi: <https://doi.org/10.1016/j.adhoc.2020.102324>.
- [12] R. Puchalski and W. Giernacki, "UAV Fault Detection Methods, State-of-the-Art," *Drones*, vol. 6, no. 11, doi: 10.3390/drones6110330.
- [13] C. Kaura, N. Sindhwani, and A. Chaudhary, "Analysing the impact of cyber-threat to ICS and SCADA systems," in *2022 International Mobile and Embedded Technology Conference (MECON)*, 2022: IEEE, pp. 466-470.
- [14] K. Boakye-Boateng, A. A. Ghorbani, and A. H. Lashkari, "Implementation of a Trust-Based Framework for Substation Defense in the Smart Grid," *Smart Cities*, vol. 7, no. 1, pp. 99-140, doi: 10.3390/smartcities7010005.
- [15] A. P. Zhao, Q. Zhang, M. Alhazmi, P. J.-H. Hu, S. Zhang, and X. Yan, "AI for science: Covert cyberattacks on energy storage systems," *Journal of Energy Storage*, vol. 99, p. 112835, 2024/10/01/ 2024, doi: <https://doi.org/10.1016/j.est.2024.112835>.
- [16] A. P. Zhao, S. Li, Z. Cao, P. J.-H. Hu, J. Wang, Y. Xiang, D. Xie, and X. Lu, "AI for science: Predicting infectious diseases," *Journal of Safety Science and Resilience*, vol. 5, no. 2, pp. 130-146, 2024/06/01/ 2024, doi: <https://doi.org/10.1016/j.jnlssr.2024.02.002>.
- [17] Y. Qin, M. A. Kishk, and M.-S. Alouini, "Performance Analysis of Charging Infrastructure Sharing in UAV and EV-involved Networks," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 3, pp. 3973-3988, 2022.
- [18] B. Ly and R. Ly, "Cybersecurity in unmanned aerial vehicles (UAVs)," *Journal of cyber security technology*, vol. 5, no. 2, pp. 120-137, 2021.
- [19] X. Zhang and K. Chandramouli, "Critical Infrastructure Security Against Drone Attacks Using Visual Analytics," in *Computer Vision Systems*, Cham, D. Tzovaras, D. Giakoumis, M. Vincze, and A. Argyros, Eds., 2019// 2019: Springer International Publishing, pp. 713-722.
- [20] A. Trotta, M. D. Felice, F. Montori, K. R. Chowdhury, and L. Bononi, "Joint Coverage, Connectivity, and Charging Strategies for Distributed UAV Networks," *IEEE Transactions on Robotics*, vol. 34, no. 4, pp. 883-900, 2018, doi: 10.1109/TRO.2018.2839087.
- [21] T. Han and Y. Xu, "Topology-Based Stabilization of Islanded Microgrids With Multiple Tie Switches Under Operational Variations: A Neural Control Approach," *IEEE Transactions on Power Systems*, pp. 1-14, 2024, doi: 10.1109/TPWRS.2024.3422453.
- [22] Y. Xia, Q. Xu, J. Fang, and F. Li, "Non-Iterative Decentralized Peer-to-Peer Market Clearing in Multi-Microgrid Systems via Model Substitution and Network Reduction," *IEEE Transactions on Power Systems*, vol. 39, no. 2, pp. 2922-2935, 2024, doi: 10.1109/TPWRS.2023.3301447.
- [23] X. Chen, Y. Liang, H. Xu, J. Wu, and M. Liu, "DDL: Empowering Delivery Drones With Large-Scale Urban Sensing Capability," *IEEE J. Sel. Topics Signal Process.*, vol. 18, no. 3, pp. 502-515, Apr. 2024, doi: 10.1109/JSTSP.2024.3427371.
- [24] P. Zhao, S. Li, Z. Cao, P. J. H. Hu, C. Gu, X. Yan, D. Huo, T. Luo, and Z. Wang, "Socially Governed Energy Hub Trading Enabled by Blockchain-Based Transactions," *IEEE Transactions on Computational Social Systems*, pp. 1-16, 2023, doi: 10.1109/TCSS.2023.3308608.
- [25] H. Wang, Z. Yang, M. Fu, and Y. Gu, "TransformLoc: Transforming MAVs into Mobile Localization Infrastructures in Heterogeneous Swarms," in *IEEE INFOCOM 2024 - IEEE Conference on Computer Communications*, Vancouver, BC, Canada, 2024, pp. 1101-1110, doi: 10.1109/INFOCOM52122.2024.10621375.
- [26] M. Adil, H. Song, S. Mastorakis, H. Abulkasim, A. Farouk, and Z. Jin, "UAV-Assisted IoT Applications, Cybersecurity Threats, AI-Enabled Solutions, Open Challenges With Future Research Directions," *IEEE Transactions on Intelligent Vehicles*, vol. 9, no. 4, pp. 4583-4605, 2024, doi: 10.1109/TIV.2023.3309548.



DSSPACE

<https://dspace.org/>

Unmanned aerial vehicle-based cyberattacks on microgrids

Zhao, Alexis P.; Li, Shuangqi; Li, Zhengmao; Ma, Zixiao; Huo, Da ...

2026-04

Institute of Electrical and Electronics Engineers (IEEE)

<https://doi.org/10.1109/tia.2025.3618810>

Zhao AP, Li S, Li Z, et al., (2026) Unmanned aerial vehicle-based cyberattacks on microgrids. IEEE Transactions on Industry Applications, Volume 62, Issue 2, March-April 2026, pp. 3212-3225