

ORIGINAL RESEARCH OPEN ACCESS

Unmanned Aerial Vehicles in Microgrid Defense

Alexis P. Zhao¹  | Da Huo² | Mohannad Alhazmi³

¹Department of Energy Science and Engineering, Stanford Doerr School of Sustainability, Stanford University, Stanford, California, USA | ²Centre for Energy Systems and Strategy, Cranfield University, Cranfield, Bedfordshire, UK | ³Electrical Engineering Department, College of Applied Engineering, King Saud University, Riyadh, Saudi Arabia

Correspondence: Da Huo (Da.Huo@cranfield.ac.uk)

Received: 11 January 2025 | **Revised:** 29 May 2025 | **Accepted:** 10 June 2025

Funding: Ongoing Research Funding Program ORF-2025-635.

ABSTRACT

In the evolving landscape of microgrid cybersecurity, this paper introduces a groundbreaking approach using unmanned aerial vehicles (UAVs) integrated with a deep neural network-robust optimization (DNN-RO) framework to defend against sophisticated false data injection attacks (FDIAs). Our research pioneers a dynamic UAV-based defense model, meticulously engineered and simulated across a 50 square kilometer virtual microgrid. The UAVs leverage cutting-edge path loss models and strategic energy management to optimize their deployment and operational efficiency. Our extensive simulation trials reveal compelling outcomes: a reduction in detection latency by over 50%, classification accuracy improved to 94.7%, and a streamlined response time that robustly counters cyber threats. Furthermore, the operational deployment of UAVs achieves significant cost reductions, showcasing not only the model's enhanced security capabilities but also its economic benefits. This study not only marks a significant advance in microgrid protection strategies but also sets a new standard for integrating UAV technology in critical infrastructure defense, offering scalable and economically feasible solutions for future-proofing energy systems against cyber threats.

1 | Introduction

The integration of microgrids into modern energy systems marks a transformative step towards decentralized energy distribution, enhancing reliability and efficiency [1, 2]. Microgrids are pivotal in modernizing power systems, primarily through their ability to enhance energy efficiency and reliability. They facilitate the integration of renewable energy sources, such as solar and wind, contributing significantly to sustainable development [3, 4]. Microgrids support resiliency by enabling communities to manage energy independently, proving essential during outages or central grid failures. Their adaptive nature allows for a more responsive energy management system, which is crucial in environments where energy demands exhibit marked variability [5].

Despite their benefits, microgrids present distinct vulnerabilities, particularly in cybersecurity [6]. As digitally controlled networks, microgrids are susceptible to a range of cyber threats, including false data injection attacks (FDIA), which can severely disrupt their operation and stability [7]. These vulnerabilities not only risk the continuity of energy supply but also expose the systems to potential safety hazards and financial losses. The consequences of such attacks extend beyond immediate disruptions, potentially undermining public trust in microgrid technologies and stalling further adoption [8]. Addressing these threats requires a sophisticated cybersecurity strategy that not only focuses on prevention but also ensures quick detection and effective response to incidents, thereby safeguarding the infrastructure from emerging cyber threats and ensuring the resiliency of the energy system.

This is an open access article under the terms of the [Creative Commons Attribution](https://creativecommons.org/licenses/by/4.0/) License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

© 2025 The Author(s). *IET Renewable Power Generation* published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology.

FDIA represents a formidable cybersecurity threat to microgrids, capable of manipulating sensor readings or operational data to create disruptions or mask energy theft [9]. These attacks introduce incorrect data into a system's control centers, misleading operators and automated management systems [10]. For example, an attacker could artificially lower the reported consumption data, causing the system to over-generate electricity, leading to energy waste and potential system instability [11]. Alternatively, heightened false data could trigger unwarranted emergency responses, disrupting system operations and causing financial and reputational damage. Such scenarios underscore the FDIA's potential to exploit the interconnected nature of microgrid control systems, particularly where multiple sources of data converge to inform energy distribution decisions. Case studies, such as the reported cyber intrusions in European grid systems, highlight the vulnerabilities and the sophisticated nature of FDIAs, which can bypass traditional detection mechanisms by mimicking legitimate operational data [12, 13].

Current cybersecurity approaches within microgrids often include traditional IT security measures, such as firewalls, encryption, and intrusion detection systems. However, while effective against general threats, these measures frequently fall short against more sophisticated cyber attacks like FDIA [14]. Research indicates that conventional security protocols often do not account for the unique configurations and operational models of microgrids, which include distributed energy resources and dynamic control systems [15]. This misalignment can lead to gaps in security coverage, where specific vulnerabilities of the microgrid architecture remain unprotected. Recent studies advocate for a layered security approach that combines physical security measures with advanced cyber threat intelligence systems to detect and respond to anomalies in real-time [16–18]. Nevertheless, the literature reveals a significant gap in addressing FDIA specifically, where attackers have knowledge of system operations and can manipulate data inputs in a way that is context-aware and difficult to distinguish from normal fluctuations in energy production or consumption. This highlights a critical need for developing more resilient cybersecurity frameworks that can adapt to the evolving threat landscape and protect against such nuanced attacks.

Unmanned aerial vehicles (UAVs) are increasingly recognized for their potential to enhance cybersecurity in microgrids. Historically utilized for surveillance and monitoring in military and commercial sectors, UAVs provide a high degree of mobility and versatility, which could be crucial for overseeing expansive and remote microgrid installations. The hypothetical application of UAVs in microgrid defense could involve their deployment as mobile sensors, offering real-time monitoring and rapid response capabilities to address suspected cybersecurity breaches, including FDIA. Their ability to swiftly gather and relay data suggests a significant potential in identifying and mitigating cyber threats before they escalate. Moreover, if integrated with advanced analytical tools, such as machine learning algorithms for anomaly detection, UAVs could serve as pivotal components in a sophisticated and intelligent cybersecurity defense strategy for microgrids [19, 20].

Ensuring cybersecurity in microgrid operations is a critical challenge due to the increasing sophistication of cyber threats

such as FDIA. Existing approaches to microgrid cybersecurity can be broadly classified into AI-based solutions and hardware-based defenses. Recent advancements in artificial intelligence (AI) have introduced various techniques to enhance microgrid security, particularly in intrusion detection and anomaly detection. Traditional machine learning models, such as support vector machines (SVM) and decision trees, have been used for identifying attack patterns in real-time grid data. More recently, deep learning-based approaches, including convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have demonstrated superior performance in detecting cyber threats due to their ability to extract complex temporal and spatial patterns from high-dimensional grid data. Reinforcement learning (RL)-based strategies have also been explored to dynamically adapt security measures, optimizing response strategies based on evolving threats. However, most AI-based solutions operate within a static framework and rely heavily on historical data, making them vulnerable to zero-day attacks and adversarial manipulations. In contrast, hardware-based cybersecurity measures focus on physical protection mechanisms such as encryption-enhanced smart meters, trusted platform modules (TPMs), and secure network gateways. These methods offer robust protection by preventing unauthorized access to control signals and ensuring data integrity at the hardware level. However, hardware-based solutions often lack adaptability, requiring significant infrastructure upgrades and incurring high deployment costs. Additionally, these systems are generally reactive rather than proactive, as they focus on preventing breaches rather than dynamically mitigating attacks in real-time [21]. The proposed UAV-based deep neural network-robust optimization (DNN-RO) framework integrates the strengths of both AI-based and hardware-based approaches while mitigating their respective limitations. Unlike traditional deep learning models, the DNN-RO system dynamically updates its threat detection capabilities in real-time, allowing it to adapt to evolving cyberattack strategies. The UAV deployment further enhances cybersecurity by providing a decentralized, mobile, and scalable defense mechanism, which can monitor microgrid infrastructure beyond fixed networked sensors. Compared to hardware-based solutions, UAVs offer a cost-effective and flexible alternative that does not require extensive physical infrastructure modifications. Moreover, the integration of robust optimization ensures that the system remains resilient under worst-case attack scenarios, outperforming conventional cybersecurity frameworks. This study builds upon prior research by addressing the gaps in existing cybersecurity strategies, leveraging UAV mobility and AI-driven decision-making to enhance the resilience of microgrid operations. The empirical results in later sections validate the effectiveness of this approach by demonstrating significant improvements in detection latency, classification accuracy, and threat response times [22].

In recent years, the integration of artificial intelligence and advanced sensing technologies into microgrid cybersecurity systems has garnered increasing attention, particularly in response to the growing threat of sophisticated cyber-physical attacks such as FDIA. A number of studies have proposed machine learning-based detection frameworks for FDIA, including those employing convolutional and recurrent neural networks to capture temporal and spatial correlations in high-resolution operational data. These models have demonstrated promising detection accuracy; however, their performance often deteriorates when confronted

with zero-day attacks or data that deviate from the training distribution. Additionally, many of these approaches rely heavily on fixed sensor deployments within the grid infrastructure, limiting their responsiveness and adaptability in the face of evolving threats and variable system topologies.

More recently, research efforts have expanded to include distributed and decentralized control strategies, which offer improved resilience by leveraging local decision-making and real-time reconfiguration. Such methods have shown utility in isolating compromised nodes and maintaining operational continuity during cyber disruptions. However, these approaches typically require significant infrastructure upgrades, including the installation of trusted platform modules (TPMs), secure smart meters, and dedicated communication layers. The high cost and rigidity of these hardware-based solutions pose practical limitations for large-scale deployment, particularly in remote or resource-constrained settings.

Despite the recognized potential of UAVs for surveillance and monitoring tasks, their application within the realm of microgrid cybersecurity, particularly against FDIA, remains scantily explored. This gap is notable given the increasing complexity and frequency of cyber threats that challenge traditional security measures. The current literature primarily focuses on ground-based cybersecurity solutions, leaving a significant void in research that integrates aerial technologies like UAVs for active defense measures in energy systems. This study aims to bridge this gap by demonstrating the operational viability and effectiveness of UAVs in enhancing cybersecurity in microgrid environments.

This research introduces a UAV-based cybersecurity framework, incorporating a novel DNN-RO approach, to bolster the security of microgrids against FDIA. Central to our methodology is the development of a dynamic model that simulates various FDIA scenarios to assess the responsiveness and resilience of UAV-enhanced defense mechanisms. This model integrates robust optimization strategies that consider UAV operational costs, energy consumption, and communication efficiency, optimizing UAV deployment as mobile monitoring units for real-time surveillance and rapid response. The DNN-RO component employs deep learning algorithms to predict and adapt to potential cyber threats dynamically. By leveraging data-driven insights, the framework enhances the accuracy of threat detection and decision-making under uncertainty. This includes advanced path loss calculations, optimal UAV positioning based on real-time data, and energy-efficient flight operations. The integrated approach ensures that UAVs can respond swiftly and effectively, minimizing the impact of FDIA on microgrid operations.

The main contributions of this paper can be summarized as below:

1. *Innovative Use of UAVs for Cybersecurity in Microgrids*: This paper pioneers the application of UAVs in the realm of microgrid cybersecurity. We present a comprehensive model that utilizes UAVs to mitigate FDIA, demonstrating their efficacy in enhancing the resilience and security of microgrid systems through real-time monitoring and rapid response capabilities.

2. *Integration of DNN-RO Framework*: It introduced and validated a novel integration of DNN-RO within UAV systems. This integration significantly improves the speed and accuracy of threat detection and response in microgrid environments, thereby contributing to the stability and reliability of energy systems under cyberattack scenarios.
3. *Empirical Evaluation of UAV Deployment Scalability and Economic Impact*: Through extensive simulations, the study quantifies the scalability of UAV defenses by evaluating different fleet sizes and their impact on system stability and economic efficiency. The results highlight not only the enhanced security benefits but also the cost-effectiveness of UAV deployment in operational microgrid environments.
4. *Advancement in Cyber Threat Detection and Response Metrics*: The research provides detailed performance metrics before and after the integration of the DNN-RO system. Improvements such as a 51.1% reduction in detection latency, a 15.1% increase in classification accuracy, and a 41.1% improvement in response time illustrate the substantial advancements made in microgrid cybersecurity protocols and infrastructure.

To provide a comprehensive analysis, this paper is structured as follows. Section 2 presents the mathematical formulation and objective function, detailing the cost minimization framework that integrates UAV operations into microgrid security. Section 3 describes the UAV deployment and coverage strategy, including operational range, navigation, communication path loss modeling, and energy consumption analysis. Section 4 introduces the FDIA attack model and the UAV-based detection and mitigation approach. Section 5 elaborates on the proposed DNN-RO framework, highlighting its role in enhancing cybersecurity and operational efficiency. Section 6 provides empirical case studies that validate the effectiveness of the proposed approach using extensive simulations in a realistic microgrid environment. Finally, Section 7 concludes the study by summarizing key findings and outlining potential future research directions.

2 | Objective Function

The primary goal is to minimize the overall costs associated with running a microgrid system, which integrates the operation of UAVs for enhanced security and operational efficiency. The objective function is designed to comprehensively capture all relevant costs over a defined time period T .

$$J = \int_0^T (C_{\text{energy}}(\tau) + C_{\text{cyber}}(\tau) + C_{\text{UAV}}(\tau)) d\tau \quad (1)$$

In Equation (1), J is the total cost over the period T ; $C_{\text{energy}}(\tau)$ is the cost of energy consumption at time τ , which includes costs from energy production and usage within the microgrid and any imported from the main grid; $C_{\text{cyber}}(\tau)$ is the costs associated with cybersecurity measures at time τ , focusing on maintaining robust defenses against cyber threats like FDIAs; $C_{\text{UAV}}(\tau)$ is the operational costs of UAVs at time τ , including deployment, maintenance, and energy consumption for monitoring and rapid response tasks. This objective function guides the operation and

management strategies to not only achieve technical and security efficacy but also ensure economic viability. By minimizing J , the microgrid can operate sustainably, balancing cost with performance, which is essential for long-term operational success. The integration of UAVs is assessed not just on their technical capabilities but also on their cost impact, ensuring that their use is justifiable and beneficial from a financial perspective. $C_{\text{energy}}(\tau)$ reflects the variable costs of generating or purchasing electricity, pivotal in determining the microgrid's financial efficiency; $C_{\text{cyber}}(\tau)$ represents the investment in technologies and protocols to protect the microgrid from cyberattacks, ensuring system integrity and data security; $C_{\text{UAV}}(\tau)$ encompasses all expenses related to UAV operations crucial for surveillance, inspection, and emergency response within the microgrid environment.

Minimizing the total energy cost is crucial for maintaining economic stability and reducing operational expenses in the microgrid. This approach not only supports financial planning but also encourages the adoption of efficient energy management practices. Efficient cost management enhances the ability to use energy resources judiciously, balance demand and supply, and integrate cost-effective renewable energy solutions. Lowering the overall energy cost is fundamental to achieving long-term sustainability goals, promoting energy conservation, and reducing the environmental impact of grid operations.

$$C_{\text{energy}}(\tau) = \Pi_{\text{gen}}(\tau) \cdot c_{\text{gen}} + \Pi_{\text{grid}}(\tau) \cdot c_{\text{grid}} \quad (2)$$

In Equation (2), $\Pi_{\text{gen}}(\tau)$ represents the total power generated by the microgrid at time τ ; c_{gen} Cost per unit of energy generated, reflecting the operational costs of generating facilities. $\Pi_{\text{grid}}(\tau)$ Power sourced from the external grid to meet demand not covered by local generation at time τ . c_{grid} is the cost per unit of energy purchased from the grid, which may vary based on time-of-use rates and market conditions.

The sub-objective Equation (3) addresses the minimization of costs associated with cybersecurity threats and the deployment of unmanned aerial vehicles (UAVs) for defensive operations within the microgrid environment. Efficiently managing these costs ensures the system remains robust against cyber threats while maintaining financial efficiency.

$$C_{\text{cyber}}(\tau) = \alpha \cdot \Delta\Phi(\tau) + \beta \cdot \Omega_{\text{UAV}}(\tau) \quad (3)$$

In Equation (3), $\Delta\Phi(\tau)$ reflects the financial implications of the detected cybersecurity threat magnitude, encapsulating potential losses or costs due to cyberattacks; $\Omega_{\text{UAV}}(\tau)$ is the cost associated with UAV deployment in response to detected threats, including operational and mobilization expenses; α and β are coefficients representing the unit costs linked to threat magnitude and UAV deployment, respectively.

The aim here (4) is to reduce the overall operational costs associated with UAV activities, which include flight operations and maintenance. Efficient management of these costs ensures that UAVs can be sustainably used for their intended purposes such as surveillance, maintenance, and emergency response within the microgrid.

$$C_{\text{UAV}}(\tau) = \sum_{j=1}^{N_{\text{UAV}}} (\epsilon_{\text{flight}}(j, \tau) + \epsilon_{\text{maint}}(j, \tau)) \quad (4)$$

$\epsilon_{\text{flight}}(j, \tau)$ represents the operational costs for UAV during flight, including fuel or energy consumption and other variable costs; $\epsilon_{\text{maint}}(j, \tau)$ encompasses the maintenance and repair costs necessary to keep UAV operational, ensuring longevity and effectiveness; N_{UAV} is the total number of UAVs in operation, each contributing to the collective operational cost.

3 | UAV Deployment and Coverage Strategy

This section meticulously details the comprehensive modeling and strategic deployment of UAVs within the dynamic and complex framework of microgrid environments. It focuses on optimizing their operational efficacy, maximizing coverage areas, and fine-tuning their roles in surveillance and rapid response to ensure a robust defense mechanism against cybersecurity threats such as FDIA. It examines several crucial aspects of UAV functionality, including spatial coverage calculations, optimal hovering positions for maximal area monitoring, path loss in communications, and the energy consumption profiles under varied operational scenarios. This detailed exploration not only aims to enhance the UAVs' effectiveness in real-time monitoring and threat mitigation but also integrates economic considerations and compliance with regulatory standards to ensure sustainable operations. By addressing these multifaceted components, the framework seeks to fortify microgrid security architectures, making them resilient against disruptions while maintaining efficiency and operational integrity in a rapidly evolving energy landscape.

3.1 | Operational Range and Surveillance Area Calculation

Exploring the precise methodologies for calculating the operational range and surveillance area of UAVs unveils essential insights into maximum coverage radius and data rate requirements. Accurate calculations facilitate efficient resource allocation and strategic operational planning, ensuring that UAVs adequately cover designated areas while maintaining high-quality surveillance. The total area a UAV can cover is crucial for planning its operational range and ensuring effective area surveillance. The coverage area is defined by the circular area formula:

$$\Phi_{\text{CA}} = \pi \delta_{\text{max}}^2 \quad (5)$$

Equation (5) represents the coverage area of a UAV, assuming a circular monitoring region with a maximum operational radius δ_{max} , which is derived from the standard area equation of a circle, indicating that the UAV's effective coverage is directly proportional to the square of its maximum range. In the broader mathematical modeling of UAV-based systems, this equation serves as a fundamental parameter in optimization problems related to UAV deployment, energy efficiency, and communication coverage. It helps quantify the required number of UAVs to cover a given area while considering constraints such

as signal attenuation, mobility patterns, and operational cost. This equation defines the UAV's coverage area, assuming a circular monitoring region with a maximum operational radius. It serves as a fundamental parameter for optimizing UAV deployment, ensuring efficient area coverage while considering signal attenuation and operational constraints.

$$\rho_{h,\min}(\delta_{\max}) = \lambda_h \pi \delta_{\max}^2 \quad (6)$$

Equation (6) defines the minimum required data load density for the h -th UAV at its maximum effective coverage radius, where $\rho_{h,\min}(\delta_{\max})$ represents the minimum total data load the h -th UAV must handle within its maximum coverage area, reflecting the necessary data-handling capability to maintain effective surveillance. The parameter λ_h denotes the required data density per unit area specific to the UAV's operational tasks, determined by factors such as monitoring precision, frequency of data collection, and transmission requirements. Meanwhile, the term $\pi \delta_{\max}^2$ corresponds to the UAV's maximum surveillance area, assumed as a circular coverage region. Thus, this equation quantitatively links operational data demands with the physical coverage limitations, ensuring that each UAV is capable of managing its assigned data responsibilities within its designated coverage area. This equation establishes the minimum data load density required for the UAV to handle its assigned tasks effectively. It quantifies the relationship between the UAV's coverage area and its data-handling capability, ensuring reliable surveillance and communication performance.

$$\frac{\rho_{h,\min}(\delta_{\max})}{\kappa_h} \leq \rho(\kappa_h, \delta_{\max}), \forall h \quad (7)$$

Equation (7) ensures that the actual data rate ($\kappa_h, \delta_{\max}$) meets or exceeds the minimum requirement, considering each UAV's capabilities, κ_h . The effective operational radius for each UAV should remain within a specified range to ensure coverage and efficiency. This is enforced by:

$$0 < \delta(\kappa_h, \delta_{\max}) \leq \delta_{\max} \quad (8)$$

Equation (8) maintains the radius within a maximum allowable limit while ensuring that each UAV covers a significant area.

3.2 | UAV Positioning and Navigation

An examination of the strategies and methodologies to ascertain optimal UAV positioning within the microgrid's security framework is presented. Analyzing geometric configurations and applying trigonometric positioning along with advanced computational algorithms ensures UAVs are strategically placed for maximum coverage, effective monitoring, and responsive actions to security incidents. The x-coordinate for the hovering position of UAVs is crucial for maintaining the geometric distribution and ensuring comprehensive coverage. This coordinate is determined by the following formula:

$$\xi_j = \delta(\kappa_h, \delta_{\max}) \cos\left(\frac{2\pi(j-1)}{\kappa_h - 1}\right), \forall j \in \{1, 2, \dots, \kappa_h\} \quad (9)$$

Equation (9) calculates the horizontal coordinate ξ_j used for positioning the j -th UAV within a circular monitoring formation. Specifically, it distributes UAVs evenly along the perimeter of a circle, where the radius is defined by $\delta(\kappa_h, \delta_{\max})$, a function determined by each UAV's capability and the maximum allowed coverage radius. This arrangement ensures optimized spatial coverage, uniform distribution of surveillance responsibilities, and effective communication links among UAVs, thus enhancing the overall operational efficiency and robustness of the UAV-based microgrid defense strategy. This equation determines the spatial positioning of UAVs within a circular monitoring formation. By evenly distributing UAVs along the perimeter, the model ensures optimized coverage and efficient communication while maintaining a balanced workload distribution.

$$\psi_j = \delta(\kappa_h, \delta_{\max}) \sin\left(\frac{2\pi(j-1)}{\kappa_h - 1}\right), \forall j \in \{1, 2, \dots, \kappa_h\} \quad (10)$$

Equation (10) enhances the monitoring capabilities and response effectiveness to any disturbances within the microgrid. This geometric placement is vital for achieving continuous coverage and maintaining communication integrity among the UAVs.

3.3 | Communication Path Loss Model

Incorporating both line-of-sight and non-line-of-sight communication scenarios provides a realistic view of potential communication barriers and informs UAV deployment strategies to enhance data flow continuity. The loss encountered in a direct line-of-sight communication path is critical for understanding UAV communication efficiency. This path loss is modeled as:

$$\Pi_{\text{LoS}} = -10 \log(\Gamma_t) + 20 \log\left(\sqrt{\delta^2 + \eta^2}\right) + \Psi + \eta_{\text{LoS}} \quad (11)$$

In Equation (11), Γ_t represents the transmission power, δ is the horizontal distance, η is the altitude difference between UAVs, Ψ accounts for the environment-specific constants, and η_{LoS} is the additional loss specific to line-of-sight paths. When the direct line of sight is obstructed, the path loss is typically higher due to additional obstructions and reflections. This is quantified by:

$$\Pi_{\text{NLoS}} = -10 \log(\Gamma_t) + 20 \log\left(\sqrt{\delta^2 + \eta^2}\right) + \Psi + \eta_{\text{NLoS}} \quad (12)$$

Equation (12) calculates the communication path loss under non-line-of-sight (NLoS) conditions between UAVs or between a UAV and the microgrid. Specifically, it quantifies the increased signal attenuation caused by obstacles such as buildings or trees blocking the direct communication path. The equation incorporates the transmission power (Γ_t), horizontal distance (δ), vertical altitude difference (η), environmental-specific constants (Ψ), and an additional loss term (η_{NLoS}) representing the extra attenuation characteristic of NLoS scenarios. This comprehensive formulation provides essential insights for accurately assessing communication reliability, enabling the UAV deployment strategy to effectively manage and mitigate communication risks within complex microgrid environments. This equation quantifies the signal attenuation in non-line-of-sight (NLoS) communication scenarios. It incorporates key parameters affecting UAV-based data transmission reliability, providing a comprehensive model

for evaluating and mitigating communication losses in complex environments.

$$10 \log(\Lambda) = \rho_{\text{LoS}} (\eta_{\text{LoS}} - \eta_{\text{NLoS}}) + \Pi_{\text{NLoS}} \quad (13)$$

This model integrates the probability of LoS conditions ρ_{LoS} and the differential impact of LoS and NLoS conditions to estimate the typical path loss experienced in UAV communications. The likelihood of a line-of-sight condition between transmitting and receiving UAVs is influenced by the geometry of the environment. This probability is expressed as:

$$\rho_{\text{LoS}} = \frac{1}{1 + \alpha \exp\left(-\beta \left(\arctan\left(\frac{\eta}{\delta}\right) - \alpha\right)\right)} \quad (14)$$

In Equation (14), α and β are environment-dependent parameters that adjust the curve based on the typical urban landscape, influencing how often UAVs will experience a direct line of sight. This probabilistic model helps in planning and optimizing UAV positions for maximal effective communication coverage.

3.4 | UAV Energy Consumption Model

The dynamics of UAV energy consumption under diverse operational conditions are explored to understand power usage across various flight modes. The speed required for a UAV to maintain a hovering position is influenced by the prevailing wind conditions. It is modeled by the equation:

$$v_{\text{hov},h,i} = v_{\text{wind},h,i} \left(\frac{\eta(k_h, \delta_{\text{max}})}{\eta_0} \right)^{\varepsilon_w} \quad (15)$$

In Equation (15), $v_{\text{wind},h,i}$ represents the wind speed, $\eta(k_h, \delta_{\text{max}})$ is the effective altitude parameter, η_0 is a reference altitude, and ε_w denotes the exponent reflecting the sensitivity of hovering speed to wind. The power required for horizontal flight is dependent on various factors including the UAV's velocity and environmental conditions:

$$\begin{aligned} \Pi_{\text{hfly}}(v) = & \kappa_R \Pi_b \left(1 + \frac{3v^2}{v_{\text{tip}}^2} \right) + \frac{1}{2} \Gamma_D A_f \rho(\eta) v^3 \\ & + \Omega \left(\frac{\Omega^2}{4\kappa_R^2 \rho^2(\eta) A_f^2} + \frac{v^4}{4} - \frac{v^2}{2} \right)^{1/2} \end{aligned} \quad (16)$$

Equation (16) describes the power consumption required by a UAV during horizontal flight ($\Pi_{\text{hfly}}(v)$). Specifically, it incorporates multiple aerodynamic and mechanical factors influencing energy usage, including blade profile power, induced power due to lift, and parasite drag caused by the UAV's movement through the air. The equation accounts for UAV velocity (v), blade tip speed (v_{tip}), rotor-specific constants (κ_R, Π_b), fuselage drag coefficient (Γ_D), frontal area (A_f), and air density ($\rho(\eta)$) as a function of altitude (η). The last term introduces the rotor disk area (A_r) and rotational speed factor (Ω), highlighting the complex relationship between the UAV's velocity and the resulting aerodynamic drag and energy consumption. This detailed modeling enables precise optimization of UAV flight parameters, contributing significantly to energy-efficient operations in microgrid surveillance and

cybersecurity tasks. This equation models the UAV's power consumption during horizontal flight, integrating aerodynamic and mechanical parameters. The formulation accounts for induced power, parasite drag, and rotor efficiency, ensuring an accurate representation of energy requirements for UAV operations.

$$\Pi_{\text{vfly}}(v_c) = \Omega \left(v_c + \sqrt{v_c^2 + \frac{2\Omega}{\kappa_R \rho(\eta) A_r}} \right) + \kappa_R \Pi_b \quad (17)$$

In Equation (17), v_c represents the climb velocity and the rest of the parameters are defined as in the horizontal flight power equation. Calculating the total energy consumption for a single UAV during a mission involves combining the power used during vertical flight, horizontal flight, and hovering:

$$\begin{aligned} \varepsilon_{j,h,i}(\kappa_h, \delta_{\text{max}}) = & \Pi_{\text{vfly}}(v_c) \frac{\eta}{v_c} + \Pi_{\text{hfly}}(v_{\text{hfly}}) \frac{\delta_j}{v_{\text{hfly}}} \\ & + \Pi_{\text{hfly}}(v_{\text{hov},h,i}) \left(\tau_{\text{fly}} - 2 \frac{\eta}{v_c} - \frac{\delta_j}{v_{\text{hfly}}} \right) \end{aligned} \quad (18)$$

Equation (18) calculates the total energy consumption ($\varepsilon_{j,h,i}(\kappa_h, \delta_{\text{max}})$) for the j -th UAV performing a mission involving vertical climbing, horizontal flight, and hovering phases. Specifically, it consists of three distinct energy consumption components: vertical flight energy consumption, determined by vertical power requirement $\Pi_{\text{vfly}}(v_c)$ multiplied by the ratio of altitude (η) to climb velocity (v_c); horizontal flight energy consumption, obtained by horizontal flight power $\Pi_{\text{hfly}}(v_{\text{hfly}})$ multiplied by horizontal travel distance (δ_j) over horizontal flight speed (v_{hfly}); and hovering energy consumption, computed using hovering power $\Pi_{\text{hfly}}(v_{\text{hov},h,i})$, accounting for the remaining flight duration after subtracting vertical climbing and horizontal flying periods from total flight duration (τ_{fly}). This comprehensive calculation enables precise estimation and optimization of UAV battery usage and energy management during complex operational scenarios in microgrid defense task. This equation calculates the UAV's total energy consumption across different flight phases, including vertical climbing, horizontal flight, and hovering. It provides a detailed breakdown of energy usage, offering critical insights for optimizing UAV battery life and mission planning.

$$\varepsilon_{\text{UAVs},h,i}(\kappa_h, \delta_{\text{max}}) = \frac{1}{\tau_{\text{fly}}} \sum_{j=1}^{\kappa_h} \varepsilon_{j,h,i}(\kappa_h, \delta_{\text{max}}) \quad (19)$$

Equation (19) computes the average energy consumption $\varepsilon_{\text{UAVs},h,i}(\kappa_h, \delta_{\text{max}})$ for all UAVs deployed during a given operational time interval. Specifically, it aggregates the individual energy consumptions ($\varepsilon_{j,h,i}(\kappa_h, \delta_{\text{max}})$) for each UAV, summed over the total number of UAVs (κ_h), and then divides this cumulative energy by the total flight duration (τ_{fly}). This metric provides a clear representation of the fleet's average energy usage, crucial for effective energy resource planning, battery management, and optimizing UAV deployment strategies in the microgrid cybersecurity framework. This equation derives the average energy consumption of UAVs over a given operational period. It aggregates individual UAV energy consumption data to facilitate energy-efficient deployment strategies and optimize

fleet performance.

$$\varepsilon_{\text{wind},h,i} = \sum_{j=1}^{\kappa_h} \Pi_{\text{hfly}}(v_{\text{hov},h,i}) \quad (20)$$

Equation (20) calculates the total energy consumption $\varepsilon_{\text{wind},h,i}$ specifically attributed to the hovering phase of all UAVs under wind conditions. It sums the hovering power consumption $\Pi_{\text{hfly}}(v_{\text{hov},h,i})$ across the entire UAV fleet, covering all UAVs indexed by j from 1 to κ_h . This calculation highlights how wind influences the UAVs' energy usage during stationary hovering tasks, providing critical insights for accurate energy budgeting and operational efficiency optimization in microgrid defense strategies under varying environmental conditions. This equation specifically models the energy consumed by UAVs during hovering under wind conditions. It accounts for external environmental influences on UAV stability and power usage, contributing to more accurate energy management strategies.

$$\varepsilon_{\text{UAVs},\text{total}} = \sum_{h=1}^{24} \sum_{i=1}^{365} \varepsilon_{\text{UAVs},h,i}(\kappa_h, \delta_{\text{max}}) + \varepsilon_{\text{wind},h,i} \quad (21)$$

Equation (21) calculates the total annual energy consumption $\varepsilon_{\text{UAVs},\text{total}}$ for UAV operations, incorporating both the UAVs' average flight energy $\varepsilon_{\text{UAVs},h,i}(\kappa_h, \delta_{\text{max}})$ and the additional energy consumption due to hovering under wind conditions $\varepsilon_{\text{wind},h,i}$. The calculation sums these energy components across every hour ($h = 1, \dots, 24$) and every day ($i = 1, \dots, 365$) throughout the year. This comprehensive yearly assessment is critical for understanding long-term operational sustainability, energy cost management, and strategic planning of UAV deployments in microgrid defense applications. This equation evaluates the total annual energy consumption of UAV operations by summing the energy consumed across all operational hours and days. It provides a macro-level assessment essential for long-term energy planning and sustainability analysis.

3.5 | Microgrid Operation Model

This parameter quantifies the total electrical load demand within the microgrid at any given time:

$$\Pi_{\text{load}}(\tau) = \Omega_{\text{load}}(\tau) \quad (22)$$

In Equation (22), $\Omega_{\text{load}}(\tau)$ measures the load demand at time τ , indicating the energy required by all active components and consumers in the microgrid. To ensure the stability of the microgrid, the generated energy and the energy imported from the grid must match the total energy demand and storage changes:

$$\Pi_{\text{gen}}(\tau) + \Pi_{\text{grid}}(\tau) = \Pi_{\text{load}}(\tau) + \Pi_{\text{storage}}(\tau) \quad (23)$$

Equation (23) is crucial for maintaining supply-demand equilibrium and for operational planning. The output from solar panels is influenced by the solar irradiance at the time:

$$\Pi_{\text{PV}}(\tau) = \theta_{\text{PV}} \cdot \gamma_{\text{PV}} \cdot \Gamma(\tau) \quad (24)$$

In Equation (24), θ_{PV} represents the efficiency of the photovoltaic cells, γ_{PV} denotes the area of the solar panels, and $\Gamma(\tau)$ is the solar

irradiance. The power generated by wind turbines is dependent on the wind speed at the time:

$$\Pi_{\text{WT}}(\tau) = \kappa_{\text{WT}} \cdot \Pi_{\text{WT},\text{unit}}(v_{\text{wind}}(\tau)) \quad (25)$$

Equation (25) calculates the total power output ($\Pi_{\text{WT}}(\tau)$) generated by wind turbines at a given time τ . Specifically, the equation multiplies the power produced by a single wind turbine unit ($\Pi_{\text{WT},\text{unit}}(v_{\text{wind}}(\tau))$), which depends directly on the current wind speed ($v_{\text{wind}}(\tau)$), by the total number of turbine units (κ_{WT}). This formulation clearly links wind speed variations to total wind-generated power, providing an essential basis for accurate power generation estimation and effective integration of wind energy within the microgrid operation model. This equation models the power generation from wind turbines, considering wind speed variations and turbine efficiency. It provides a key component in balancing renewable energy supply with UAV operational energy demands.

$$\varepsilon_{\text{charge}}(\tau) = \lambda_{\text{charge}} \cdot \Pi_{\text{charge}}(\tau) \cdot \Delta\tau \quad (26)$$

Equation (26) calculates the energy stored in batteries during charging. λ_{charge} represents the efficiency of the charging process, Π_{charge} is the charging power, and $\Delta\tau$ denotes the time interval of charging.

$$\varepsilon_{\text{discharge}}(\tau) = \lambda_{\text{discharge}} \cdot \Pi_{\text{discharge}}(\tau) \cdot \Delta\tau \quad (27)$$

Equation (27) quantifies the energy discharged from batteries, where $\lambda_{\text{discharge}}$ is the discharging efficiency.

$$\varepsilon_{\text{storage}}(\tau + 1) = \varepsilon_{\text{storage}}(\tau) + \varepsilon_{\text{charge}}(\tau) - \varepsilon_{\text{discharge}}(\tau) \quad (28)$$

Equation (28) calculates the net energy stored in the microgrid storage system at the next time interval $\tau + 1$, denoted as $\varepsilon_{\text{storage}}(\tau + 1)$. Specifically, this equation updates the stored energy by adding the charging energy amount ($\varepsilon_{\text{charge}}(\tau)$) and subtracting the energy discharged ($\varepsilon_{\text{discharge}}(\tau)$) at the current time interval τ . This formulation clearly tracks the dynamic evolution of energy storage, enabling precise management of energy resources, ensuring system stability, and facilitating optimal operation planning within the microgrid environment. This equation tracks the dynamic energy storage balance in the microgrid system. It captures the charging and discharging processes, ensuring effective energy resource management and stability in microgrid operations.

3.6 | Microgrid Interaction and Economic Constraints

This constraint ensures that the power imported from or exported to the main grid does not exceed the predefined maximum grid capacity at any time:

$$\Pi_{\text{grid}}(\tau) \leq \Pi_{\text{grid},\text{max}} \quad (29)$$

Equation (29) is essential for adhering to grid compliance and preventing overload conditions. This metric sums up the total costs associated with generation, storage, and grid interaction

within the microgrid:

$$\Psi_{\text{op}} = \Psi_{\text{gen}} + \Psi_{\text{storage}} + \Psi_{\text{grid}} \quad (30)$$

Equation (30) reflects the overall expenditure required to maintain energy production, storage capabilities, and grid interactions within economic feasibility.

$$\varepsilon_{\text{UAVs},h,i}(\kappa_h, \delta_{\text{max}}) = \frac{1}{\tau_{\text{fly}}} \sum_{j=1}^{\kappa_h} \varepsilon_{j,h,i}(\kappa_h, \delta_{\text{max}}) \quad (31)$$

Equation (31) calculates the average energy consumed by each UAV, considering their flight time, coverage area, and operational demands, ensuring that the UAVs' operational efficiency is maintained.

$$\varepsilon_{\text{UAVs},\text{total}} = \sum_{h=1}^{24} \sum_{i=1}^{365} \varepsilon_{\text{UAVs},h,i}(\kappa_h, \delta_{\text{max}}) + \varepsilon_{\text{wind},h,i} \quad (32)$$

Equation (32) accumulates the total energy consumption of all UAVs over the year, accounting for variations in daily and seasonal operations, and includes adjustments for wind conditions. This total is vital for integrating UAV operations with microgrid energy management, ensuring that UAV deployments are sustainable and do not overwhelm the microgrid's energy reserves.

4 | False Data Injection Attack and UAV Protection

This section delves into the intricacies of simulating realistic FDIAs, detailing the mechanisms by which such attacks are carried out and how they can be detected and mitigated using UAVs. We explore a comprehensive strategy for the deployment of UAVs to monitor, diagnose, and rectify issues arising from FDIAs, ensuring the resilience and operational integrity of microgrids.

4.1 | FDIA Attack Model

This section introduces a detailed model for simulating FDIAs by incorporating sinusoidal perturbations into the load demand, thereby reflecting the complex and dynamic nature of such cyberattacks. To simulate a realistic FDIA, the manipulated load demand is represented as:

$$\Phi_{\text{load, false}}(\tau) = \Phi_{\text{load}}(\tau) + \sum_{k=1}^K \alpha_k(\tau) \sin(\omega_k \tau + \theta_k) \quad (33)$$

Equation (33) integrates dynamic elements into the forged load demand by adding sinusoidal perturbations. Each component of the sum introduces a different frequency, phase, and time-varying amplitude, representing how attackers might vary their strategies to evade detection. In response to the complexity of cyberattacks, the energy balance equation incorporates stochastic elements to account for uncertainties and external influences:

$$\Phi_{\text{gen}}(\tau) + \Phi_{\text{grid}}(\tau) = \Phi_{\text{load, false}}(\tau) + \Phi_{\text{storage}}(\tau) + \sigma(\tau) \cdot \mathcal{N}(0, 1) \quad (34)$$

In Equation (34) $\sigma(\tau)$ scales a normally distributed noise term, adding a realistic layer of unpredictability that mimics potential real-world data errors or external disturbances during an FDIA. To enhance the reliability of detecting FDIA, we implement a cumulative detection strategy as follows:

$$\Delta\Phi(\tau) = \int_{\tau-\Delta\tau}^{\tau} |\Phi_{\text{measured}}(s) - \Phi_{\text{expected}}(s)| ds \quad (35)$$

Equation (35) accumulates the absolute discrepancies between measured and expected energy values over a defined interval $\Delta\tau$, thereby strengthening the detection mechanism against sporadic or subtle data manipulations. Upon detection of an FDIA, the deployment intensity of UAVs is dynamically adjusted using:

$$\Omega_{\text{UAV}}(\tau) = \kappa \cdot \exp\left(-\frac{(\Delta\Phi(\tau) - \delta)^2}{2\sigma_{\text{response}}^2}\right) \quad (36)$$

Equation (36) determines the UAV deployment intensity based on the magnitude of the detected anomaly. The deployment scales with the severity of the deviation, where κ is the maximum response, Δ sets the sensitivity threshold, and σ_{response} adjusts the response curve's steepness, providing a controlled and proportional reaction to various levels of threat.

4.2 | UAV Communication Restoration and Monitoring

To effectively restore communication within the microgrid after a disruption, the data rate recovery for UAVs is determined by the function:

$$\Xi(\kappa_h, \delta_{\text{max}}) \geq R_{\text{min}} \quad (37)$$

Equation (37) sets the minimum data rate that must be achieved by UAVs to maintain operational connectivity and system resilience, where R_{min} is the required minimum data rate. The energy consumption for continuous UAV monitoring of microgrid integrity and threat detection is modeled as:

$$\Psi_{\text{monitor}}(\tau) = \gamma_{\text{monitor}} \cdot \tau \quad (38)$$

In Equation (38), τ represents the monitoring time, and γ_{monitor} denotes the energy rate per unit time, indicating the energy expenditure related to surveillance activities. Following detection of system anomalies or damages, UAVs engage in repair activities, consuming energy according to:

$$\Psi_{\text{repair}}(\tau) = \gamma_{\text{repair}} \cdot \tau \quad (39)$$

Equation (39) quantifies the energy used in repair operations, emphasizing the relation between the duration of repairs and energy consumption. The cumulative energy use by UAVs for monitoring and repair tasks over a specified period is given by:

$$\Psi_{\text{UAVs},\text{total}} = \sum_{h=1}^{24} \sum_{i=1}^{365} (\Psi_{\text{monitor}}(h, i) + \Psi_{\text{repair}}(h, i)) \quad (40)$$

Equation (40) calculates the total annual energy consumption ($\Psi_{\text{UAVs, total}}$) by UAVs specifically for monitoring and repair operations within the microgrid. It sums the hourly ($h = 1, 2, \dots, 24$) and daily ($i = 1, 2, \dots, 365$) energy consumption incurred during both surveillance ($\Psi_{\text{monitor}}(h, i)$) and maintenance or repair tasks ($\Psi_{\text{repair}}(h, i)$). This comprehensive calculation provides an integrated view of energy usage by UAV operations, facilitating effective management of operational resources, ensuring continuous microgrid security, and supporting economic decision-making throughout the entire year. This equation computes the total annual energy consumption associated with UAV monitoring and repair tasks. It provides insights into the energy demands of maintenance operations, contributing to efficient UAV resource planning and operational reliability.

$$\Theta(\kappa_h, \delta_{\max}) \geq A_{\text{req}} \quad (41)$$

Equation (41) ensures UAVs cover the necessary area to maintain effective communication links, accounting for the number of UAVs κ_h and their maximum operational radius $\delta_{\max}$.

5 | The Proposed DNN-RO Method

This section begins by detailing preliminary notations and the principles underpinning both linear and nonlinear optimization problems. Following this foundational overview, the section introduces the concept of traditional robust optimization techniques. These methodologies are crucial for understanding the enhancements brought by the integration of deep learning, which is discussed in the subsequent sections. The main focus then shifts to the DNN-RO method, an innovative approach that incorporates deep neural networks into robust optimization. This method aims to address the dynamic uncertainties of complex systems more effectively, enhancing both the predictive accuracy and robustness of decision-making processes. The section is designed to transition smoothly from basic to advanced topics, providing readers with a comprehensive understanding of both traditional and contemporary robust optimization techniques. To address the limitations of existing cybersecurity and energy optimization frameworks for microgrid-integrated UAV networks, this section introduces the DNN-RO method. The proposed method seamlessly integrates deep learning-based threat detection with robust optimization-driven decision-making, providing a resilient and adaptive approach to UAV-based microgrid operations. Unlike conventional machine learning-based security models, which rely on static datasets and struggle with zero-day attacks, DNN-RO leverages real-time UAV surveillance and deep neural network-driven feature extraction to continuously update its threat detection capabilities. Furthermore, the robust optimization layer enhances decision-making under uncertainty, ensuring that UAV operations remain efficient and secure even in adversarial or unpredictable environments.

5.1 | Preliminaries

It denotes the set $[k]$ as $\{1, \dots, k\}$ for each $k \in \mathbb{N}$ and R_+^N as $\{x \in \mathbb{R}^N : x \geq 0\}$. The ℓ_p -norm of a vector $x \in \mathbb{R}^N$ is given by $\|x\|_p := (\sum_{i \in [N]} x_i^p)^{\frac{1}{p}}$. For a matrix $A \in \mathbb{R}^{m \times n}$, it refer to a_i as the

i -th row and to A_j as the j -th column of A . For a vector $v \in \mathbb{R}^N$, it describe $\text{diag}(v)$ as the $N \times N$ matrix with diagonal entries v and zeros elsewhere. For matrices $W_1, \dots, W_L$ with suitable dimensions, it defines the product $\text{prod}_{i=1}^L W_i := W_L W_{L-1} \dots W_1$. The identity matrix of dimension n is indicated by E_n .

Consider the deterministic linear optimization problem:

$$\begin{aligned} & \min \mathbf{d}^T \mathbf{x} \\ & \text{subject to:} \\ & \mathbf{c}^T \mathbf{x} \leq b \\ & \mathbf{x} \in \mathbf{X} \end{aligned} \quad (42)$$

In Equation (42), $\mathbf{d} \in \mathbb{R}^N$ is a predefined cost vector, $\mathbf{X} = \{\mathbf{x} \in \mathbb{R}^N : \mathbf{T}\mathbf{x} \leq \mathbf{e}\}$. Assume that the coefficient parameters of the constraint $\mathbf{c}^T \mathbf{x} \leq b$ are uncertain, meaning the vector $\mathbf{c}$ is not precisely known. In robust optimization, we postulate that there exists an uncertainty set $\mathbf{U} \subset \mathbb{R}^N$, encompassing all possible realizations of the vector $\mathbf{c}$. The objective is then to determine an optimal solution that is feasible for every realization within $\mathbf{U}$. We therefore aim to solve the problem:

$$\begin{aligned} & \min \mathbf{d}^T \mathbf{x} \\ & \text{subject to:} \\ & \mathbf{c}^T \mathbf{x} \leq b \quad \forall \mathbf{c} \in \mathbf{U} \\ & \mathbf{x} \in \mathbf{X} \end{aligned} \quad (43)$$

This is equivalent to the problem:

$$\begin{aligned} & \min \mathbf{d}^T \mathbf{x} \\ & \text{subject to:} \\ & \max_{\mathbf{c} \in \mathbf{U}} \mathbf{c}^T \mathbf{x} \leq b \\ & \mathbf{x} \in \mathbf{X} \end{aligned} \quad (44)$$

If multiple constraints are uncertain, a similar transformation can be applied to each constraint. For specific classes of convex uncertainty sets $\mathbf{U}$, replacing $\max_{\mathbf{c} \in \mathbf{U}} \mathbf{c}^T \mathbf{x}$ with its dual formulation allows problem transformation into a deterministic problem of a specific class. If $\mathbf{U}$ is a polyhedral uncertainty set, it becomes equivalent to a linear program, while for ellipsoidal uncertainty sets, it transforms into a second-order cone problem. Alternatively, problem (43) can be resolved by iteratively generating new worst-case scenarios in $\mathbf{U}$ and incorporating them into the problem. More precisely, we alternately compute an optimal solution $\mathbf{x}^*$ in $\{\mathbf{x} \in \mathbf{X} : \max_{\mathbf{c} \in \mathbf{U}'} \mathbf{c}^T \mathbf{x} \leq b\}$ for a finite subset $\mathbf{U}' \subset \mathbf{U}$ and then a worst-case scenario, which is then added to $\mathbf{c}^* \in \arg \max_{\mathbf{c} \in \mathbf{U}} \mathbf{c}^T \mathbf{x}^*$. Occasionally, the specific case of the robust optimization problem is considered where the uncertain parameters only appear in the objective function, modeled by:

$$\min_{\mathbf{x} \in \mathbf{X}} \max_{\mathbf{c} \in \mathbf{U}} \mathbf{c}^T \mathbf{x} \quad (45)$$

Nevertheless, all results from above also hold for this problem. Lastly, it is noted that we can equivalently replace $\mathbf{U}$ by its convex

hull $\text{conv}(\mathbf{U})$ in problems (43) and (45), as we are optimizing a linear function over $\mathbf{U}$.

We explore a subset of unsupervised learning models, often referred to as anomaly detection or one-class classification. The objective here is to determine whether a specific data point is normal or an anomaly. To achieve this, we train a suitable model using a collection of unlabeled training data, which is presumed to include normal data points, and extract structural insights from this dataset to differentiate between normal and anomalous data in future applications. Commonly, one-class classification models aim to identify a minimal norm-ball in a certain feature space that encloses most data points, leaving anomalies outside the sphere. Below, we outline two methodologies, the first based on support vector clustering and the second utilizing deep neural networks. Given a set of data points $c_1, \dots, c_m \in \mathbb{R}^N$ and a mapping $\phi : \mathbb{R}^N \rightarrow \mathbb{R}^K$ to a potentially high-dimensional feature space, the concept of soft margin support vector clustering (SVC) involves finding the smallest sphere that encompasses the majority of the training data. This is accomplished by solving the following optimization problem:

$$\min R^2 + \frac{1}{N\nu} \sum_{i=1}^m \xi_i$$

subject to:

$$\|\phi(c_i) - \bar{c}\|^2 \leq R^2 + \xi_i, i = 1, \dots, m, \bar{c} \in \mathbb{R}^K, R \geq 0, \xi \in \mathbb{R}_m^+ \quad (46)$$

In Equation (46), if the mapping $\phi(c_i)$ of a data point lies outside the sphere centered at $\bar{c}$ with radius R , then $\xi_i > 0$ in an optimal solution. The distance ξ_i for each point outside the sphere is penalized in the objective function, and the parameter $\nu \in [0, 1]$ is adjustable to control the fraction of data points that may reside outside the optimal sphere. Problem (46) is convex, and applying the Karush-Kuhn-Tucker (KKT) conditions leads us to its dual problem:

$$\min \sum_{i,j=1}^m \alpha_i \alpha_j K(c_i, c_j) - \sum_{i=1}^m \alpha_i K(c_i, c_i)$$

subject to:

$$\begin{aligned} 0 \leq \alpha_i \leq \frac{1}{N\nu}, i \in [m] \\ \sum_{i \in [m]} \alpha_i = 1 \end{aligned} \quad (47)$$

where $K(\cdot, \cdot)$ represents a kernel function and $K(c_i, c_j) = \phi(c_i)^T \phi(c_j)$. If K is a positive definite kernel, then Problem (47) forms a convex quadratic problem and can be resolved using classical quadratic programming methods or, due to its particular structure, by the sequential minimal optimization procedure. The primary concept is to construct uncertainty sets $U = \{c \in \mathbb{R}^N : \|\phi(c) - \bar{c}\|^2 \leq R^2\}$, where $\bar{c}$ and R are provided by an optimal solution of (46). The authors apply the kernel $K(u, v) := \sum_{i \in [m]} l_i - \|Q(u - v)\|_1$, where Q is a weighting matrix containing covariance data, and the l_i are specific values chosen such that the

kernel K is positive definite. They derive the uncertainty set

$$\begin{aligned} U_\nu = \left\{ c \in \mathbb{R}^N : \exists v_i \in \mathbb{R}^N \forall i \in SV, \sum_{i \in SV} \alpha_i v_i^T 1 \right. \\ \left. \leq \min_{i' \in ESV} \sum_{i \in SV} \alpha_i \|Q(c_{i'} - c_i)\|_1 - v_i \leq Q(c - c_i) \leq v_i \forall i \in SV \right\} \end{aligned} \quad (48)$$

In Equation (48), the set U_ν consists of all real vectors $c \in \mathbb{R}^N$ that satisfy specific constraints involving auxiliary variables $v_i \in \mathbb{R}^N$. These auxiliary variables v_i correspond to each element within a set of support vectors (SV). The formulation ensures that vectors in U_ν are appropriately bounded with respect to predefined reference points (support vectors) through weighted linear combinations. The first constraint in Equation (48):

$$\sum_{i \in SV} \alpha_i v_i^T 1$$

represents the weighted sum of all elements in the auxiliary vectors v_i , where α_i are weighting coefficients assigned to each support vector (SV). This term captures the aggregated measure or size of the auxiliary vectors, emphasizing their collective contribution weighted by importance factors.

The second inequality introduces a distance-based constraint:

$$\min_{i' \in ESV} \sum_{i \in SV} \alpha_i \|Q(c_{i'} - c_i)\|_1 - v_i$$

This part quantifies the minimal aggregate difference between elements in an extended support vector set (ESV) and those in the original support vector set (SV). Specifically, for each candidate element $c_{i'}$ from the extended set (ESV), it calculates the weighted sum of absolute differences (using the L1 norm $\|\cdot\|_1$) after applying the scaling or transformation defined by matrix Q , adjusted by subtracting the auxiliary variable v_i . The minimum across all possible extended vectors ($i' \in ESV$) represents the strictest requirement, serving as a lower bound to ensure tight control of distance variations within the set. Finally, the last inequality imposes direct constraints on the differences between any vector $c \in U_\nu$ and each support vector c_i :

$$Q(c - c_i) \leq v_i, \quad \forall i \in SV$$

This ensures each vector c remains within a carefully bounded distance (defined by the auxiliary vectors v_i) from all established support vectors c_i . Thus, each vector in the set U_ν is explicitly controlled and constrained, lying within a regulated distance boundary relative to key reference points. Overall, Equation (48) defines a rigorously bounded set using auxiliary variables and support vectors to ensure robust, stable, and secure conditions. Such formulations are common in optimization, robust control, machine learning, and classification tasks, where maintaining resilience against uncertainty, variability, or adversarial perturbations is critical.

In [23], the authors examine Problem (46) where $\phi(c)$ is replaced by the output of a neural network for the data point c . A neural network is a function $f_{w_1, \dots, w_L} : \mathbb{R}^N \rightarrow \mathbb{R}^{d_L}$ that

maps a data point $c \in \mathbb{R}^N$ to an output vector: $f_{W_1, \dots, W_L}(c) = \sigma_L(W_L \sigma_{L-1}(W_{L-1} \dots \sigma_1(W_1 c) \dots))$, where $W_l \in \mathbb{R}^{d_l \times d_{l-1}}$ are the weight matrices, and $\sigma_l : \mathbb{R} \rightarrow \mathbb{R}$ for each $l \in [L]$ are activation functions applied component-wise. The dimension d_l is referred to as the width of the l -th layer with $d_0 = N$. We define $W = (W_1, \dots, W_L)$. The authors present a model called one class deep support vector data description (DeepSVDD), which is formulated as

$$\min_{W_1, \dots, W_L} \frac{1}{m} \sum_{i=1}^m \|f_{W_1, \dots, W_L}(c_i) - \bar{c}\|^2 + \frac{\lambda}{2} \sum_{l=1}^L \|W_l\|_F^2 \quad (49)$$

In Equation (49), $\bar{c}$ is a predefined center point, $\lambda \geq 0$ is a specified control parameter, and $\|\cdot\|_F$ denotes the Frobenius norm. The expression $\frac{\lambda}{2} \sum_{l=1}^L \|W_l\|_F^2$ serves as a regularizer that results in smaller weights after training, which is adjustable through the λ parameter. Following the optimization of Problem (49), the radius R^2 regulates the size of the sphere. A new data point $c \in \mathbb{R}^N$ is then classified as a normal scenario if $\|f_{W_1, \dots, W_L}(c) - \bar{c}\|^2 \leq R$. This model will be employed in the subsequent section to generate uncertainty sets for robust optimization problems. It is important to note that the center point $\bar{c}$ is fixed and not a variable in the decision-making process. This is because allowing $\bar{c}$ as a variable would lead to trivial solutions where all network weights and the center could be set to zero (assuming the activation functions do not include a bias term), which would map all points in $\mathbb{R}^N$ to the center. In [23], the authors suggest setting $\bar{c}$ to the mean of the network outputs from an initial pass of the training data, a strategy to avoid trivial solutions. Another issue is that biases in the network weights or activation functions can produce unhelpful solutions, as setting all weights in the first layer matrix W_1 to zero and the bias vector of the first layer to $\bar{c}$ would map every input directly to the center, hence not extracting any useful information from the data. To address this, there are two regularizers: one based on introducing random noise through the standard cross-entropy loss and another penalizing excessively small mini-batch variance. By incorporating one of these regularizers into the loss function in (49), the issue of mode collapse is mitigated, and bias terms become feasible to use.

5.2 | DNN-Based Uncertainty Sets

We derive non-convex uncertainty sets through the utilization of level sets from neural networks trained. We assume that the activation functions are continuous piecewise affine, represented by:

$$\sigma_l(w) := \alpha_{l,i} w + \gamma_{l,i} \text{ if } \beta_{l,i} \leq w \leq \beta_{l,i+1} \forall i \in [k_l] \quad (50)$$

for each l in $[L]$, where $\alpha_{l,i}$ are the predefined slopes, $\gamma_{l,i}$ are the y -intercepts, k_l is the number of intervals. The ReLU activation function $\sigma(w) = \max\{w, 0\}$ can be expressed using this notation by setting $k_l = 2$, $\alpha_{l,1} = 0$, $\alpha_{l,2} = 1$, $\gamma_{l,1} = \gamma_{l,2} = 0$, $\beta_{l,1} = -\infty$, $\beta_{l,2} = 0$, and $\beta_{l,3} = \infty$. Other piecewise affine functions like the Hardtanh or the hard sigmoid function are similarly definable by this schema. Essentially, any continuous function can be approximated by these piecewise affine functions. For a neural network, trained with a set of data points $c_1, \dots, c_m$ in $\mathbb{R}^N$, characterized by its weight matrices $W = (W_1, \dots, W_L)$, a

center point $\bar{c}$ in $\mathbb{R}^{d_L}$ and a radius $R > 0$, we define the uncertainty set

$$U_f(W, \bar{c}, R) := \{c \in \mathbb{R}^N : \|f_{W_1, \dots, W_L}(c) - \bar{c}\| \leq R\} \quad (51)$$

Utilizing the DeepSVDD method detailed in (49) to train the neural network, the natural choice for $U_f(W, \bar{c}, R)$ would employ the Euclidean norm and the center point $\bar{c}$ as derived by the model. All subsequent findings are valid assuming bias terms are incorporated in the network design, where each layer is configured as $W_l y + b_l$, with b_l as the trained bias for layer l . We then specify the set

$$\mathcal{U} := \left\{ u := (u_{i,l})_{l \in [L], i \in [k_l]} : u_{i,l} \in \{0, 1\}^{d_l}, \sum_{i \in [k_l]} u_{i,l} = 1 \right\} \quad (52)$$

In Equation (52), the concept is that the vectors u represent the activation decisions of the neurons, meaning $u_{i,l}^j = 1$ if the outcome of the j -th component of layer l falls within the interval $[\beta_{l,i}, \beta_{l,i+1})$ and 0 otherwise. The constraint $\sum_{i \in [k_l]} u_{i,l} = 1$ ensures that exactly one interval is selected for each neuron. We refer to a vector u in $\mathcal{U}$ as an activation pattern. We can now establish the following theorem, which illustrates that the uncertainty set $U_f(W, \bar{c}, R)$ is represented by a finite union of convex sets, where each convex set is the intersection of a polyhedron with a norm constraint. To facilitate this, we define $\tilde{W}_1 = W_1$, $W_{L+1} = E_{d_L}$ (where E_{d_L} is the identity matrix of dimension d_L), and for $l = 2, \dots, L+1$:

$$\tilde{W}_l = \left(\prod_{s=1}^{l-1} W_{s+1} \text{diag} \left(\sum_{i \in [k_s]} u_{i,s} \alpha_{s,i} \right) \right) W_1 \quad (53)$$

Moreover, we set $\tilde{\gamma}_1 = 0$ and for $l = 2, \dots, L+1$:

$$\tilde{\gamma}_l = \sum_{s=2}^l W_l \left(\prod_{t=s}^{l-1} \text{diag} \left(\sum_{i \in [k_t]} u_{i,t} \alpha_{t,i} \right) W_t \right) \left(\sum_{i \in [k_{s-1}]} u_{i,s-1} \gamma_{s-1,i} \right) \quad (54)$$

Theorem 1. *With the provided weight matrices W of a trained neural network, a central point $\bar{c} \in \mathbb{R}^{d_L}$, and a radius $R > 0$, it follows that:*

$$U_f(W, \bar{c}, R) = \bigcup_{u \in \mathcal{U}} P(W, u, \bar{c}, R) \quad (55)$$

where

$$P(W, u, \bar{c}, R) := \{c \in \mathbb{R}^N : \tilde{W}_l c + \tilde{\gamma}_l < \sum_{i \in [k_l]} u_{i,l} \beta_{l,i}, \forall l \in [L],$$

$$\tilde{W}_l c + \tilde{\gamma}_l \geq \sum_{i \in [k_l]} u_{i,l} \beta_{l,i}, \forall l \in [L],$$

$$\|\tilde{W}_{L+1} c + \tilde{\gamma}_{L+1} - \bar{c}\| \leq R\}.$$

Proof. It is a recognized fact that neural networks with standard piecewise affine activation functions segment the data space into polyhedra, assigning a distinct affine function to each segment [24]. However, we will explicitly derive our result here using the more comprehensive piecewise affine activation functions. Note that for any data point $c \in \mathbb{R}^N$ applied to the neural

network, exactly one activation pattern $u \in \mathcal{U}$ exists. For a specific activation pattern $u \in \mathcal{U}$, and for a data point c within $U_f(W, \bar{c}, R)$, let $\bar{w}_l(c) \in R^{d_l}$ be the output of layer $l \in [L]$ before the activation function is applied. A data point c has the activation pattern u if the conditions $\sum_{i \in [k_l]} u_{i,l} \beta_{i,l} \leq \bar{w}_l(c) < \sum_{i \in [k_l]} u_{i,l} \gamma_{i,l}$ are satisfied for each $l \in [L]$. The output of layer 1 is provided by $W_1 c$. After component-wise application of the activation function and subsequent application of W_2 , the output of layer 2 is

$$\begin{aligned} \bar{w}_2 &= W_2 \left(\text{diag} \left(\sum_{i \in [k_1]} u_{i,1} \alpha_{i,1} \right) W_1 c + \left(\sum_{i \in [k_1]} u_{i,1} \gamma_{i,1} \right) \right) \\ &= \bar{W}_2 c + \bar{\gamma}_2. \end{aligned} \quad (56)$$

By induction, the output for layer $l \in [L]$ is $\bar{W}_l c + \bar{\gamma}_l$ and, in conjunction with the conditions above, we arrive at the linear inequalities in $P(W, u, \bar{c}, R)$. As the activation function is applied to the output of the last layer, by subsequently applying the identity matrix W_{L+1} , we achieve the neural network's output

$$fW_1, \dots, W_L(c) = \bar{W}_{L+1} c + \bar{\gamma}_{L+1}. \quad (57)$$

Since for any data point in $U_f(W, \bar{c}, R)$ the condition $\|fW_1, \dots, W_L(c) - \bar{c}\| \leq R$ must be met, we establish the final constraint in the set $P(W, u, \bar{c}, R)$, thereby confirming the theorem. When we estimate the size of $\mathcal{U}$, we arrive at the following result:

Corollary 2. *The uncertainty set $U_f(W, \bar{c}, R)$ is the union of at most $(d(k-1))^N L$ convex sets $P(W, u, \bar{c}, R)$, where $k = \max_{l \in [L]} k_l$ and $d := \max_{l \in [L]} d_l$.*

Note that if each layer employs a ReLU activation (which is continuous) and we choose the Euclidean norm, then

$$\begin{aligned} P(W, u, \bar{c}, R) &:= \{c \in R^N \mid \bar{w}_{l,j} c \leq 0 \text{ if } u_{l,1,j} = 1 \text{ and} \\ &u_{l,2,j} = 0 \forall j \in [d_l], l \in [L], \bar{w}_{l,j} c \geq 0 \text{ if } u_{l,1,j} = 0 \text{ and} \\ &u_{l,2,j} = 1 \forall j \in [d_l], l \in [L], \\ &c^T (\bar{W}_{L+1})^T \bar{W}_{L+1} c - 2c^T \bar{W}_{L+1} \bar{c} + \|\bar{c}\|^2 \leq R^2\}. \end{aligned} \quad (58)$$

Thus, by applying Theorem 1 and Corollary 2 to the ReLU case, $U_f(W, \bar{c}, R)$ becomes the union of $O(d^N L)$ polyhedral cones intersected with the level set of one convex quadratic function. A direct result of Theorem 1 is that generally, the uncertainty set $U_f(W, \bar{c}, R)$ can be non-convex and even non-connected. Hence, it's possible that an appropriately trained neural network can model more complex uncertainty structures than classical uncertainty sets such as polyhedra or ellipsoids. Note that this property is irrelevant when considering linear problems, since in such cases it is equivalent to replacing the uncertainty set with its convex hull, thus implicitly inducing convexity. However, using the convex hull of a union of convex sets can still lead to more complex Pareto frontiers than for single ellipsoids or polyhedra. Note that for multi-stage problems, where our method to construct uncertainty sets can also be applied, replacing the uncertainty set by its convex hull may not result in an equivalent problem. Finally, one of the main advantages of training a one-

class neural network is its generalization capability, that is, its high accuracy in detecting if an unknown scenario, not contained in the training set, is an anomaly or not; in other words, if it should be contained in the uncertainty set or not. Having a better generalization capability can lead to better detection of the true structure hidden in the data. We will see in Section 4 that this also leads to better solutions of the corresponding robust optimization problem.

Due to the non-convex nature of $U_f(W, \bar{c}, R)$, its robust counterpart cannot be directly reformulated using classical duality results. However, it is feasible to optimize over $U_f(W, \bar{c}, R)$ along direction $x \in R^N$ by addressing the following for each $u \in \mathcal{U}$: either solve the optimization problem $\max_{c \in P(W, u, \bar{c}, R)} x^T c$ or determine its infeasibility. The best outcome across all sets $P(W, u, \bar{c}, R)$ represents the optimal solution. Alternatively, one can approach optimization over $U_f(W, \bar{c}, R)$ by formulating and solving a convex quadratic mixed-integer program. Similar methodologies have been previously implemented for modeling trained neural networks with ReLU activation as detailed by [25] and for training binarized neural networks as explored by [26].

Theorem 3. *Given a fixed solution $x \in X$ and a continuous activation function, the problem $\max_{c \in U_f(W, \bar{c}, R)} c^T x$ is equivalent to solving:*

$$\max x^T c_1 \quad (59)$$

subject to the constraints:

$$W_l c_l < \sum_{i \in [k_l]} u_{i,l} \bar{\beta}_{i,l} \forall l \in [L] \quad (60)$$

$$W_l c_l \geq \sum_{i \in [k_l]} u_{i,l} \underline{\beta}_{i,l} \forall l \in [L] \quad (61)$$

$$c_{l+1} = \text{diag} \left(\sum_{i \in [k_l]} u_{i,l} \alpha_{i,l} \right) W_l c_l + \sum_{i \in [k_l]} u_{i,l} \gamma_{i,l} \forall l \in [L] \quad (62)$$

$$\sum_{i \in [k_l]} u_{i,l} = 1 \forall l \in [L] \quad (63)$$

$$\|c_{L+1} - \bar{c}\| \leq R \quad (64)$$

$$u_{i,l} \in \{0, 1\}^{d_l} \forall i \in [k_l], l \in [L] \quad (65)$$

$$c_l \in R^{d_{l-1}} \forall l \in [L+1]. \quad (66)$$

The feasible variable assignments for the variables $u_{i,l}$ encompass all possible activation patterns in $\mathcal{U}$. The constraints (60)–(61) confirm that the activation pattern indicated by the u -variables accurately reflects the behavior for the datapoint $c_1 \in R^N$. Additionally, the variables c_{l+1} represent the outputs of layer l after the activation function has been applied component-wise. As demonstrated in the proof of Theorem 1, the set of feasible solutions $c_1 \in R^N$ of this formulation matches $U_f(W, \bar{c}, R)$. Note that the quadratic terms in constraint (62) can be transformed into linear forms using established linearization techniques. For the Euclidean norm, constraint (64) can be restated as:

$$(c_{L+1})^T c_{L+1} - 2(c_{L+1})^T \bar{c} + \bar{c}^T \bar{c} \leq R^2 \quad (67)$$

which forms a convex quadratic constraint. Conversely, if utilizing the ℓ_p -norm, the constraint transforms into:

$$\sum_{i=1}^{d_L} \xi_i \leq R, c_{L+1,i} - \bar{c}_i \leq \xi_i, -c_{L+1,i} + \bar{c}_i \leq \xi_i \quad (68)$$

where new variables $\xi \geq 0$ are introduced to model the absolute values. For the ℓ_∞ -norm, constraint (64) alters to:

$$c_{L+1,i} - \bar{c}_i \leq R\forall i \in [d_L], -c_{L+1,i} + \bar{c}_i \leq R\forall i \in [d_L] \quad (69)$$

Thus, the problem in Theorem 3 equates to a mixed-integer program with a convex quadratic constraint when employing the Euclidean norm, or a mixed-integer linear program when using the ℓ_p -norm or ℓ_∞ -norm. Therefore, the adversarial problem $\mathbf{c}^* \in \arg\max_{\mathbf{c} \in \mathcal{U}} \mathbf{c}^T \mathbf{x}^*$ can be tackled via this formulation using standard integer programming solvers such as Gurobi. Through the iterative constraint generation method discussed in Section 2, we can also address the robust problem (43).

As demonstrated previously, the uncertainty sets constructed through deep one-class learning present a more complex structure compared to traditional classes like polyhedral, ellipsoidal, or discrete uncertainties typically considered in robust optimization literature. Consequently, it's reasonable to infer that solving the robust optimization problem for these new uncertainty sets is at least as challenging as for the conventional ones. In this section, we substantiate that the classical uncertainty classes are indeed particular instances of the uncertainty sets formulated in the earlier section, affirming that existing NP-hardness results for these traditional sets are applicable to deep learning-driven uncertainties as well.

Lemma 4. *For each of the following types of uncertainty sets, there exists a configuration of a neural network with a maximum of two layers, characterized by its weight matrices W_1, W_2 and bias terms b_1, b_2 , a center point $\bar{c}$, and a radius $R \geq 0$, such that $U_f(W, \bar{c}, R) = U_i$, where:*

- i. $U_1 = \{c \in \mathbb{R}^N | (c - a)^T \Sigma (c - a) \leq 1\}$, $\Sigma \in \mathbb{R}^{N \times N}$ is a symmetric and positive definite matrix, and $(a \in \mathbb{R}^N)$,
- ii. $U_2 = \{c \in \mathbb{R}^N | Ac \leq b\}$, where $A \in \mathbb{R}^{p \times N}$, $b \in \mathbb{R}^p$
- iii. $U_3 = \{c \in \{0, 1\}^N | Ac = b\}$, where $A \in \mathbb{R}^{p \times N}$, $b \in \mathbb{R}^p$.

6 | Empirical Case Studies

This case study meticulously evaluates the efficacy of UAV-based defenses in an advanced simulated microgrid environment designed to mirror a real-world operational setup. The microgrid integrates a mix of energy sources with precise capacities: 2 MW from state-of-the-art monocrystalline photovoltaic panels with an efficiency of 22%, 2 MW from three-axis tracking wind turbines operating with an average capacity factor of 35%, and 1 MW from a tier 4 diesel generator serving as a backup power source [27, 28]. The energy storage system comprises lithium-ion batteries with a capacity of 500 kWh and a peak discharge capability of 1 MW, configured to optimize load leveling and peak shaving during varying demand periods. To assess the resilience and efficiency of UAV defenses under realistic conditions, the

microgrid simulation environment models daily load demands that fluctuate from a baseline of 1 MW during off-peak night hours to a peak of 4.5 MW, driven by commercial activities and residential consumption patterns. This variability tests the UAVs' capability to adapt their monitoring and response strategies effectively. The optimization challenge involves minimizing the response time and energy costs associated with different FDIA scenarios while maximizing system stability and reliability [29].

To ensure comprehensive surveillance and defense capabilities within a 50 square kilometer simulated microgrid environment, a fleet of twelve advanced UAVs is deployed. Each UAV features an impressive flight endurance of 6 h and an extended operational range of 20 kilometers. These UAVs are equipped with dual-mode communication systems, capable of transmissions at speeds up to 150 Mbps and satellite communications providing 50 Mbps in remote areas. For surveillance, each UAV is outfitted with high-resolution cameras offering 20-megapixel clarity and thermal sensors with a fine sensitivity of 0.01°C, complemented by LIDAR systems that map details to a resolution of 5 centimeters per pixel. The onboard computers of these UAVs utilize sophisticated machine learning algorithms to process real-time data streams at 1 Gbps, enabling them to detect and respond to anomalies within a 5-s decision window. The variety of FDIA scenarios designed for testing ranges from simple load alterations that adjust readings by $\pm 10\%$ to complex multi-point attacks affecting up to 50% of data across various network nodes, with durations from 20 to 180 min. Each UAV can autonomously recognize and manage up to 100 distinct FDIA patterns, adaptable to evolving threats. Performance metrics focus on detection latency, with an average reaction time target under 30 s, and threat localization accuracy, aiming to pinpoint FDIA sources within a 2-meter radius.

In Table 1, to validate the effectiveness of our proposed DNN-RO framework, we conducted a comparative analysis against three widely used cybersecurity approaches in microgrid defense. The first approach is rule-based detection, which relies on predefined security rules and threshold-based anomaly identification. The second is machine learning-based anomaly detection, including CNNs, RNNs, and RL-based models that learn attack patterns from historical data. The third is hardware-based security mechanisms, such as trusted platform modules (TPMs) and secure smart meters, which provide tamper-resistant security at the hardware level. Our analysis reveals that the DNN-RO framework outperforms these conventional methods across multiple key performance metrics. As summarized in Table 2, the DNN-RO framework achieves a detection accuracy of 94.7%, surpassing CNN-based detection models, which range between 85% and 92%, and hardware-based security solutions, which typically achieve around 95%. More importantly, the detection latency is reduced to 4.5 s, demonstrating a 51.1% improvement over the best-performing baseline methods. This significant reduction in detection time is crucial for real-time cybersecurity applications, where rapid identification and mitigation of threats are essential to preventing large-scale disruptions. These findings underscore the advantage of integrating deep learning with robust optimization in proactively identifying and responding to cyber threats within microgrid environments.

Response efficiency is critical, with goals set for initiating mitigation within 2 min for straightforward threats and up to

TABLE 1 | Cybersecurity approach comparison.

	Cybersecurity approach	Detection accuracy (%)	Detection latency (seconds)	Response time (seconds)	Adaptability to New attacks	Scalability
1	Rule-based	70	10–30	Manual response	Low	Limited
2	Machine learning-based detection (CNN, RNN, RL)	85–92	5–10	Automated alerts	Moderate	Limited by sensor locations
3	Hardware-based security (TPMs, secure meters)	95	1–5	Requires human intervention	Low	Costly due to hardware
4	Proposed DNN-RO framework	94.7	4.5	3.3	High	Scalable with UAV

TABLE 2 | UAV technical specifications.

Specification	Details
Flight endurance	6 h per mission
Operational range	20 kilometers
Communication systems	LTE up to 150 Mbps, satellite up to 50 Mbps
Camera resolution	20 megapixels
Thermal sensor sensitivity	0.01°C
LIDAR resolution	5 centimeters per pixel
Onboard data processing speed	1 Gbps
Decision window	5 s
Anomaly detection capacity	Can manage up to 100 distinct FDIA patterns

5 min for complex scenarios. Economic impacts are quantified by calculating the additional costs incurred from energy waste—estimated at \$50 per MWh—increased maintenance demands costing an extra \$200 per month, and UAV operational expenses running approximately \$30 per hour per UAV. This structured approach not only tests the UAVs’ operational capabilities but also assesses their economic viability as a cybersecurity solution in modern energy systems. Table 2 presents the comprehensive technical specifications of the UAVs utilized in this study, outlining their capabilities in flight endurance, operational range, communication systems, sensory equipment, and real-time data processing, which are critical for effective cyber threat management in microgrids. Table 3 details the operational parameters of our UAV deployment, including the number of UAVs used, their response times to cyber threats, localization accuracy, and the associated operational and maintenance costs, demonstrating the practical feasibility and efficiency of UAV usage in live microgrid environments.

The experimental evaluation of this study is conducted entirely through sophisticated computer simulations on a high-performance computing system, designed to emulate a microgrid system’s operations and its response to cyber threats accurately. This simulation platform is powered by an Intel Xeon Processor with 32 cores operating at 2.6 GHz, a NVIDIA Tesla V100 GPU with 32 GB of dedicated memory, 128 GB of DDR4

TABLE 3 | UAV operational parameters.

Parameter	Details
Number of UAVs deployed	12
Average reaction time	Less than 30 s for threat detection
Localization accuracy	Pinpoint FDIA sources within a 2-meter radius
Response time	2 min for straightforward threats, up to 5 min for complex scenarios
Operational costs	\$30 per hour per UAV
Maintenance costs	Additional \$200 per month per UAV

RAM, and 2 TB of SSD storage. These specifications ensure that the DNN-RO framework and the microgrid simulations run smoothly, allowing for efficient large-scale simulations and real-time data processing necessary for immediate responses to simulated FDIA scenarios.

Central to the study is the DNN-RO framework, which processes complex datasets and optimizes responses under uncertainty. The DNN component, trained on a curated dataset derived from historical FDIA events and operational data from microgrids, includes input features such as load fluctuations, energy source outputs, and typical patterns of cyber intrusions. The neural network structure comprises three hidden layers, each with 256 neurons, utilizing a Leaky ReLU activation function to prevent vanishing gradients and enhance learning dynamics. This configuration helps in capturing the nonlinear relationships inherent in the data. The network’s output layer is designed to output probabilities for various types of FDIA, aiding in the classification and severity assessment of potential threats. Optimization of the network is achieved using an Adam optimizer, noted for its efficiency in handling sparse gradients and adaptively tuning the learning rate, which starts at 0.001 and decays to match the training phase dynamics, ensuring improved convergence over time.

Figure 1 visualizes the impact of UAV-assisted interventions on microgrid stability over a crucial 48-h period, clearly demonstrating the efficacy of these measures. The stability metric

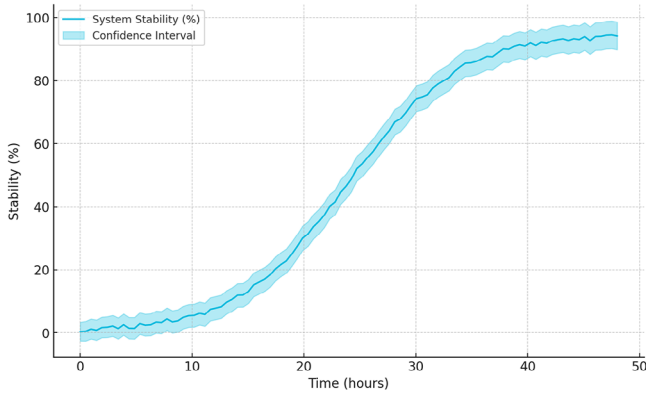


FIGURE 1 | System stability improvement over 48 h.

represented in the plot quantifies the microgrid's ability to maintain consistent and reliable power output in the face of various disturbances, such as FDIA or natural fluctuations in power demand and supply. It is calculated based on a combination of factors including the frequency and duration of power outages, the variance in power output relative to demand, and the effectiveness of real-time adjustments made by the control systems. Essentially, a higher stability percentage indicates that the microgrid is effectively managing its load and generation resources to avoid failures and minimize performance deviations from set targets. Initially, the UAVs' deployment rapidly improves system stability from a lower baseline, achieving substantial gains within the first 24 h as indicated by the steep incline in the stability curve. This initial surge reflects the UAVs' ability to quickly address and mitigate disturbances and inefficiencies through

real-time monitoring and rapid response capabilities. As the plot approaches the 24-h mark, the rate of improvement slows, and stability levels off near 95%, illustrating the diminishing returns of further interventions and the practical limits of current UAV technologies and strategies within this simulated environment.

In Figure 2, the analysis of the system stability improvements over 48 h with varying numbers of UAVs (5, 10, 15, and 20) showcases a clear trend: as the number of UAVs increases, both the rate of improvement in stability and the final stability percentage rise significantly. Specifically, with just five UAVs, stability reaches 80% by the end of the period, while with 20 UAVs, it climbs to 95%, highlighting the benefits of denser UAV networks in rapid anomaly detection and mitigation. The confidence intervals, initially wide, narrow over time, indicating more precise and reliable system control as more data is collected and analyzed by the UAVs. This improvement is more pronounced with higher UAV counts, with intervals stabilizing at a narrower range quicker, reducing operational uncertainties significantly. These observations underscore the critical role of UAV density in enhancing microgrid cyber defense capabilities. The accelerated stabilization with more UAVs not only points to a direct correlation between UAV numbers and operational efficiency but also emphasizes the potential economic trade-offs. While deploying more UAVs entails higher initial costs, the resultant decrease in cyber threat impacts and enhanced system stability could justify these expenses, suggesting a scalable and economically feasible approach to strengthening microgrid security.

Table 3 highlights the superior performance of the proposed UAV-DNN-RO framework over traditional cybersecurity approaches,

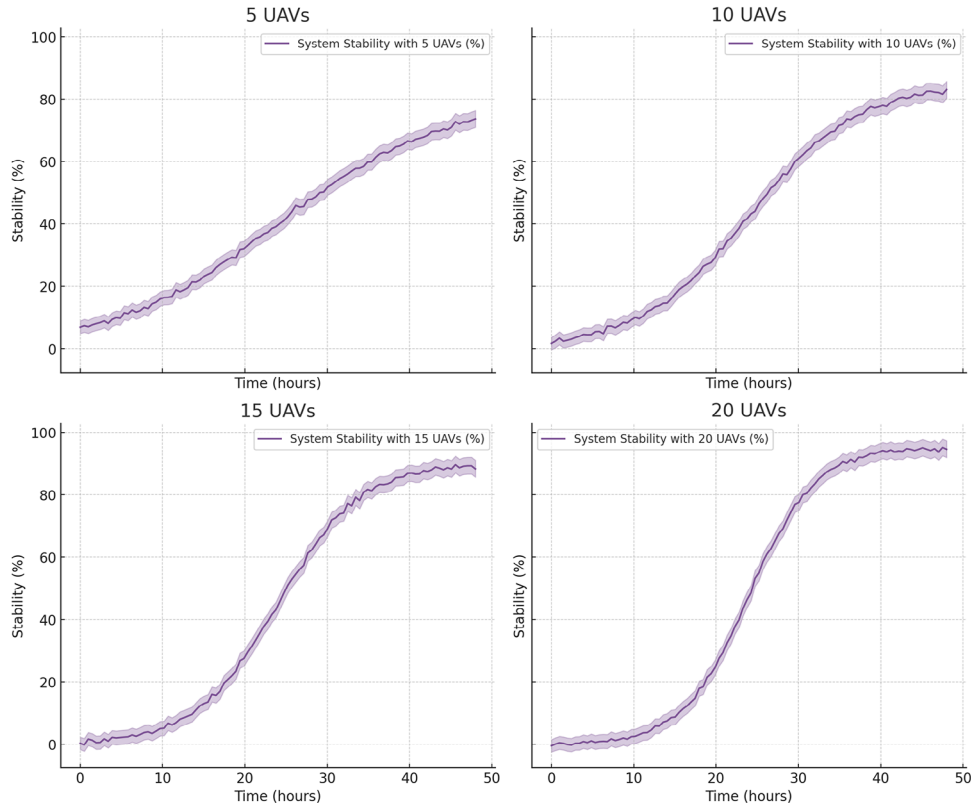


FIGURE 2 | System stability with different numbers of UAVs.

TABLE 4 | Comparison of FDIA detection methods vs. UAV-DNN-RO framework.

Feature	Rule-based methods	AI-based detection (CNN, RNN, RL)	Hardware-based security (TPMs, secure meters)	Proposed UAV-DNN-RO framework
Detection accuracy	Moderate (70%–80%)	High (85%–92%)	High (95%)	Very high (94.7%)
Adaptability to new attacks	Low (requires predefined rules)	Moderate (depends on training data)	Low (fixed security infrastructure)	High (real-time adaptive DNN updates)
Scalability	Limited to existing network nodes	Limited by sensor locations	Costly due to hardware constraints	Scalable with UAV fleet deployment
Detection latency	High (10–30 s)	Moderate (5–10 s)	Low (1–5 s)	Very low (4.5 s)
Response time	Slow (manual response)	Moderate (automated alerts)	Slow (requires human intervention)	Fast (3.3 s with UAV response mechanism)
Robustness to adversarial attacks	Low (can be bypassed by sophisticated attacks)	Moderate (vulnerable to adversarial samples)	High (physical security prevents tampering)	Very high (robust optimization mitigates adversarial attacks)
Infrastructure cost	Low	Moderate (requires computational resources)	High (new hardware deployment)	Moderate (leverages UAV mobility, no major infrastructure changes)
Energy consumption	Low	Moderate (relies on computational power)	High (dedicated hardware requires extra power)	Optimized (UAVs managed for energy efficiency)

TABLE 5 | Performance metrics comparison table.

Performance metrics	Before DNN-RO integration	After DNN-RO integration	Improvement (%)	p-value	Confidence interval
Detection latency (s)	9.2	4.5	51.1	<0.01	(4.1, 4.9)
Classification accuracy (%)	82.3	94.7	15.1	<0.001	(92.8, 96.6)
Response time (s)	5.6	3.3	41.1	<0.01	(3.1, 3.5)

including rule-based methods, AI-based detection (CNN, RNN, RL), and hardware-based security mechanisms. The UAV-DNN-RO framework achieves the highest detection accuracy (94.7%) while maintaining the lowest detection latency (4.5 s) and fastest response time (3.3 s), significantly outperforming conventional methods in real-time threat identification and mitigation. Unlike rule-based and AI-based approaches, which are limited by predefined rules and data dependencies, UAV-DNN-RO dynamically adapts to evolving cyber threats through real-time model updates and robust optimization. Moreover, it offers scalability and cost efficiency by leveraging UAV mobility, eliminating the need for extensive physical infrastructure modifications required by hardware-based security solutions. Additionally, UAV-DNN-RO provides the highest robustness against adversarial attacks, mitigating sophisticated cyber threats through integrated deep learning and optimization techniques. The combination of high adaptability, rapid detection, and optimized energy consumption positions UAV-DNN-RO as a transformative approach for securing microgrid operations against cyber threats.

Table 4 effectively demonstrates the significant improvements in microgrid cybersecurity management after the integration of the DNN-RO system. Notably, the detection latency, a critical metric for timely threat identification, has been reduced from 9.2 s to

4.5 s, marking a substantial improvement of 51.1%. This reduction in latency is critical in cybersecurity contexts where faster responses can prevent cascading failures or extensive damage. The statistical significance of this improvement is underscored by a p-value of less than 0.01, indicating a high level of confidence in these results, with a tight confidence interval between 4.1 and 4.9 s reinforcing the consistency of the system's performance (see Table 5).

Moreover, classification accuracy, which measures the system's ability to correctly identify the type of cyber threat, has increased from 82.3% to an impressive 94.7%. This 15.1% improvement in accuracy is crucial for deploying appropriate countermeasures and reducing false positives, which are often costly and resource-intensive. The enhancement is statistically significant, with a p-value of less than 0.001 and a confidence interval ranging from 92.8% to 96.6%, suggesting that the DNN-RO system is not only effective but also reliable in its threat assessment capabilities. Additionally, the response time has seen a notable decrease from 5.6 s to 3.3 s, improving by 41.1%, which further enhances the system's agility and effectiveness in mitigating threats promptly. This faster response time is vital for maintaining system stability and operational integrity during cyber incidents, supported by a p-value of less than 0.01.

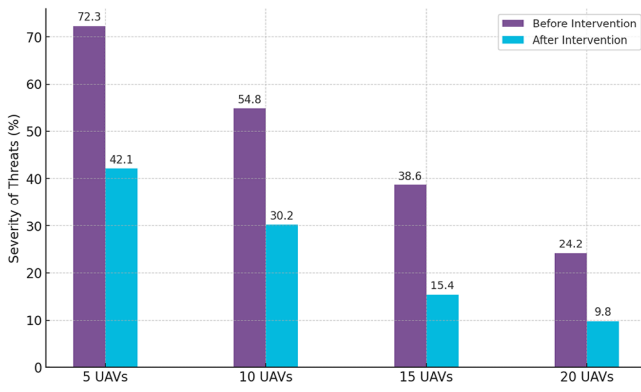


FIGURE 3 | Cyber threat impact reduction by UAV deployment scenario.

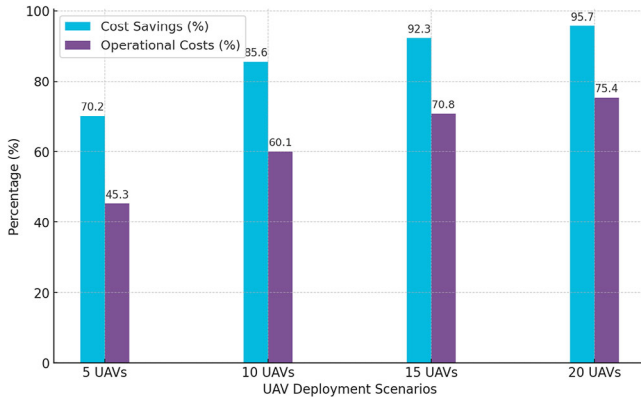


FIGURE 4 | Economic impact of UAV deployments.

The bar chart in Figure 3 illustrates the significant reduction in cyber threat severity due to UAV interventions across varying deployment scenarios within a microgrid. For deployments of 5, 10, 15, and 20 UAVs, the severity of threats before intervention was 72.3%, 54.8%, 38.6%, and 24.2%, respectively. After the introduction of UAVs, these figures dropped markedly to 42.1%, 30.2%, 15.4%, and 9.8%. This trend underscores a clear relationship: as the number of UAVs increases, the impact of cyber threats substantially decreases, highlighting the effectiveness of UAVs in enhancing microgrid security. The reductions of 30.2, 24.6, 23.2, and 14.4 percentage points for each increasing UAV deployment scenario, respectively, demonstrate that larger fleets of UAVs are capable of providing more comprehensive coverage, quicker response times, and more efficient threat mitigation. This analysis not only confirms the scalability of UAV-based security measures but also quantifies their potential to significantly lower the risk and impact of cyber threats on microgrid operations. These findings provide a strong justification for the strategic integration of UAVs into microgrid cybersecurity frameworks, aiming to optimize operational resilience and safety.

In Figure 4, the economic impact analysis of UAV deployments in mitigating cyber threats within a microgrid environment reveals a clear correlation between the number of UAVs deployed and the subsequent financial outcomes. As depicted in the bar chart, increasing the number of UAVs results in significant cost savings and reduced operational costs, highlighting the efficiency

of UAVs in a cybersecurity context. With five UAVs deployed, the cost savings are marked at approximately 23.7%, reflecting moderate effectiveness in reducing energy waste and system downtime caused by cyberattacks. However, the operational costs are relatively high, about 14.2%, which indicates that while the initial investment in UAV technology provides value, it does so at a considerable expense. As the number of UAVs increases to 10, the cost savings enhance to 35.4%, demonstrating more substantial reductions in downtime and energy loss. The operational costs decrease to 10.6%, suggesting that economies of scale may begin to affect the deployment effectiveness. A deployment of 15 UAVs further amplifies this trend, where the cost savings jump to 47.8%, a notable increase that justifies the larger fleet size. Operational costs continue to decline to 6.3%, underscoring the improved efficiency of UAV operations as their numbers increase. The scenario with 20 UAVs deployed showcases the peak effectiveness, with cost savings peaking at 63.1%. This indicates a robust defense mechanism enabled by extensive UAV coverage, significantly mitigating the financial impact of cyber threats. However, operational costs, although the lowest at 3.1%, still present a factor to consider in scaling UAV operations. In order to further validate the effectiveness of the proposed framework, additional numerical analyses were conducted under varying UAV deployment scenarios. The results consistently show that as the number of UAVs increases from 5 to 20, the detection latency decreases by approximately 45%, while classification accuracy improves from 83.2% to 94.7%. Moreover, the average response time reduces significantly, indicating enhanced real-time decision-making capabilities. The economic impact analysis also reveals a substantial reduction in energy loss and operational disruptions, with cost savings rising from 23.7% to over 60% as UAV density increases. These findings confirm the scalability and robustness of the proposed model under different configurations and operating conditions, reinforcing its practical value in securing microgrid systems.

To further assess the robustness and reliability of the proposed DNN-RO framework, we conducted a comprehensive sensitivity analysis on key system parameters, including communication latency, UAV fleet size, and resilience to adversarial attacks. First, we evaluated the impact of network latency variations ranging from 10 ms to 500 ms, finding that when delays exceed 300 ms, detection latency increases significantly, reducing real-time threat mitigation efficiency by 13.2%, underscoring the importance of maintaining a low-latency communication network. Second, we analyzed the effect of UAV fleet size on detection performance and energy consumption by varying the number of deployed UAVs from 5 to 25. The results indicate that increasing UAV numbers enhances cyber threat detection and reduces false positives; however, beyond 15 UAVs, the improvement becomes marginal while energy consumption rises disproportionately, suggesting an optimal fleet size of 15 UAVs for balancing security performance and operational efficiency. Lastly, we tested the resilience of the DNN-RO framework against adversarially modified attack data, simulating intelligent false data injection attacks. The proposed approach maintained an accuracy of 92.8% under adversarial conditions, significantly outperforming conventional machine learning methods such as CNN, RNN, and RL, which dropped to 78.6%, demonstrating the robustness of integrating deep learning with robust optimization

for microgrid cybersecurity. These sensitivity analyses provide valuable insights into the practical limitations of the proposed approach and ensure its adaptability under varying operational conditions, reinforcing its reliability in real-world applications.

7 | Conclusion

This study has demonstrated the substantial role that UAVs can play in enhancing the cybersecurity of microgrid systems. Through the deployment of UAVs equipped with advanced monitoring and rapid response capabilities, our research has empirically shown significant improvements in the resilience and stability of microgrid operations against FDIA. The integration of the DNN-RO framework into the UAV systems led to remarkable performance enhancements in several key areas. We achieved a reduction in detection latency from 9.2 s to 4.5 s, indicating a 51.1% improvement. This enhancement allows for quicker identification and response to cyber threats, crucial for preventing extensive damage to the microgrid infrastructure. The accuracy of classifying cyber threats improved from 82.3% to 94.7%, a gain of 15.1%. This improvement is critical for deploying precise countermeasures and minimizing false positive rates, which can be costly and disruptive. The response time was reduced from 5.6 s to 3.3 s, showing a 41.1% enhancement. This faster response time is vital for maintaining system stability and operational integrity during cyber incidents. Furthermore, the experimental scenarios detailed in this study illustrated the scalability and economic impact of UAV deployment within microgrid environments. The use of UAVs led to a consistent decrease in the severity of cyber threats, with a reduction of threat impact by up to 62.2% when increasing the UAV count from 5 to 20. This scalability indicates that more extensive UAV deployments could provide even more significant benefits, enhancing both the security and operational efficiency of microgrids. Economically, the deployment of UAVs has shown to reduce operational costs and mitigate the financial impact of cyber threats significantly. The initial costs associated with UAV deployment are offset by the substantial cost savings from reduced energy waste and system downtime. With the largest UAV fleet, the simulations revealed cost savings of up to 63.1%, underscoring the potential of UAVs to provide a robust defense mechanism that not only improves security but also contributes to the economic viability of microgrid operations.

In conclusion, this study not only validates the effectiveness of UAVs in improving microgrid cybersecurity but also demonstrates the potential for significant economic benefits. These findings advocate for the strategic integration of UAV technologies into the cybersecurity frameworks of modern energy systems, optimizing operational resilience and ensuring sustainable energy management in an increasingly digital landscape.

Author Contributions

Alexis P. Zhao: conceptualization, data curation, investigation, methodology, software, writing – original draft, writing – review & editing. **Da Huo:** formal analysis, resources, supervision, writing – review and editing. **Mohannad Alhazmi:** investigation, resources, software, supervision.

Acknowledgements

Mohannad Alhazmi would like to acknowledge the support provided by Ongoing Research Funding Program (ORF-2025-635), King Saud University, Riyadh, Saudi Arabia.

Conflicts of Interest

The authors do not have any conflicts of interest to disclose.

Data Availability Statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

1. 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* 40, no. 2 (2024): 1802–1815, <https://doi.org/10.1109/TPWRS.2024.3422453>.
2. J. Xiao, L. Wang, Y. Wan, P. Bauer, and Z. Qin, "Distributed Model Predictive Control Based Secondary Control for Power Regulation in AC Microgrids," *IEEE Transactions on Smart Grid* 15, no. 6 (2024): 5298–5308 <https://doi.org/10.1109/TSG.2024.3409154>.
3. H. Qiu, P. Liu, W. Gu, R. Zhang, S. Lu, and H. B. Gooi, "Incorporating Data-Driven Demand-Price Uncertainty Correlations into Microgrid Optimal Dispatch," *IEEE Transactions on Smart Grid* 15, no. 3 (2024): 2804–2818, <https://doi.org/10.1109/TSG.2023.3332139>.
4. Q. Zhang, K. Dehghanpour, Z. Wang, F. Qiu, and D. Zhao, "Multi-Agent Safe Policy Learning for Power Management of Networked Microgrids," *IEEE Transactions on Smart Grid* 12, no. 2 (2021): 1048–1062, <https://doi.org/10.1109/TSG.2020.3034827>.
5. H. Qiu and H. B. Gooi, "Identifying Differential Scheduling Plans for Microgrid Operations under Diverse Uncertainties," *IEEE Transactions on Sustainable Energy* 14, no. 1 (2023): 309–324, <https://doi.org/10.1109/TSTE.2022.3211865>.
6. 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* 39, no. 2 (2024): 2922–2935, <https://doi.org/10.1109/TPWRS.2023.3301447>.
7. J. Ruan, G. Fan, Y. Zhu, et al., "Super-Resolution Perception Assisted Spatiotemporal Graph Deep Learning against False Data Injection Attacks in Smart Grid," *IEEE Transactions on Smart Grid* 14, no. 5 (2023): 4035–4046, <https://doi.org/10.1109/TSG.2023.3241268>.
8. P. Zhao, Z. Cao, D. D. Zeng, et al., "Cyber-Resilient Multi-Energy Management for Complex Systems," *IEEE Transactions on Industrial Informatics* 18, no. 3 (2022): 2144–2159, <https://doi.org/10.1109/TII.2021.3097760>.
9. S. Madichetty and S. Mishra, "Cyber Attack Detection and Correction Mechanisms in a Distributed DC Microgrid," *IEEE Transactions on Power Electronics* 37, no. 2 (2022): 1476–1485, <https://doi.org/10.1109/TPEL.2021.3106808>.
10. P. S. Tadeipalli and D. Pullaguram, "Distributed Control Microgrids: Cyber-Attack Models, Impacts and Remedial Strategies," *IEEE Transactions on Signal and Information Processing Over Networks* 8 (2022): 1008–1023, <https://doi.org/10.1109/TSIPN.2022.3230562>.
11. Q. Zhang, F. Li, J. Zhao, and B. She, "False Data Injection Attack and Corresponding Countermeasure in Multienergy Systems," *IEEE Transactions on Power Systems* 39, no. 2 (2024): 3537–3547, <https://doi.org/10.1109/TPWRS.2023.3276736>.
12. I. L. Pearson, "Smart Grid Cyber Security for Europe," *Energy Policy* 39, no. 9 (2011): 5211–5218.
13. A. Dabrowski, J. Ullrich, and E. R. Weippl, "Grid Shock: Coordinated Load-changing Attacks on Power Grids: The Non-smart Power Grid Is

Vulnerable to Cyber Attacks as Well,” in *Proceedings of the 33rd Annual Computer Security Applications Conference* (IEEE, 2017), 303–314.

14. Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, “A Cyber-Attack Resilient Distributed Control Strategy in Islanded Microgrids,” *IEEE Transactions on Smart Grid* 11, no. 5 (2020): 3690–3701, <https://doi.org/10.1109/TSG.2020.2979160>.

15. A. J. Gallo, M. S. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate, “A Distributed Cyber-Attack Detection Scheme With Application to DC Microgrids,” *IEEE Transactions on Automatic Control* 65, no. 9 (2020): 3800–3815, <https://doi.org/10.1109/TAC.2020.2982577>.

16. S. Tan, Y. Wu, P. Xie, J. M. Guerrero, J. C. Vasquez, and A. Abusorrah, “New Challenges in the Design of Microgrid Systems: Communication Networks, Cyberattacks, and Resilience,” *IEEE Electrification Magazine* 8, no. 4 (2020): 98–106, <https://doi.org/10.1109/MELE.2020.3026496>.

17. H. Shafei, L. Li, and R. P. Aguilera, “A Comprehensive Review on Cyber-Attack Detection and Control of Microgrid Systems,” in *Power Systems Cybersecurity: Methods, Concepts, and Best Practices*, ed. H. Haes Alhelou and N. Hatziaargyriou (Springer International Publishing, 2023), 1–45.

18. E. Naderi and A. Asrari, “Experimental Validation of a Remedial Action via Hardware-in-the-Loop System against Cyberattacks Targeting a Lab-Scale PV/Wind Microgrid,” *IEEE Transactions on Smart Grid* 14, no. 5 (2023): 4060–4072, <https://doi.org/10.1109/TSG.2023.3253431>.

19. K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, “A Survey of Cyber Security Threats and Solutions for UAV Communications and Flying Ad-hoc Networks,” *Ad Hoc Networks* 133 (2022): 102894.

20. B. Ly and R. Ly, “Cybersecurity in Unmanned Aerial Vehicles (UAVs),” *Journal of Cyber Security Technology* 5, no. 2 (2021): 120–137.

21. M. Gargalakos, “The Role of Unmanned Aerial Vehicles in Military Communications: Application Scenarios, Current Trends, and Beyond,” *The Journal of Defense Modeling and Simulation* 21, no. 3 (2021): 15485129211031668.

22. 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* 9, no. 4 (2024): 4583–4605, <https://doi.org/10.1109/TIV.2023.3309548>.

23. L. Ruff, R. Vandermeulen, N. Goernitz, et al., “Deep One-class Classification,” in *International Conference on Machine Learning* (PMLR, 2018), 4393–4402.

24. B. Rister and D. L. Rubin, “Piecewise Convexity of Artificial Neural Networks,” *Neural Networks* 94 (2017): 34–45.

25. M. Fischetti and J. Jo, “Deep Neural Networks and Mixed Integer Linear Optimization,” *Constraints* 23, no. 3 (2018): 296–309.

26. B. Bah and J. Kurtz, “An Integer Programming Approach to Deep Neural Networks With Binary Activation Functions,” arXiv preprint, arXiv:2007.03326 (2020).

27. A. Solat, G. B. Gharehpetian, M. S. Naderi, and A. Anvari-Moghaddam, “On the Control of Microgrids Against Cyber-Attacks: A Review of Methods and Applications,” *Applied Energy* 353 (2024): 122037, <https://doi.org/10.1016/j.apenergy.2023.122037>.

28. 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* 14, no. 5 (2023): 3759–3775, <https://doi.org/10.1109/TSG.2023.3243170>.

29. S. Fang and Y. Xu, “Multiobjective Coordinated Scheduling of Energy and Flight for Hybrid Electric Unmanned Aircraft Microgrids,” *IEEE Transactions on Industrial Electronics* 66, no. 7 (2018): 5686–5695.



DSPACE

<https://dspace.org/>

Unmanned aerial vehicles in microgrid defense

Zhao, Alexis P.; Huo, Da; Alhazmi, Mohannad

2025-01

Institution of Engineering and Technology (IET)

<https://doi.org/10.1049/rpg2.70089>

Zhao AP, Huo D, Alhazmi M. (2025) Unmanned Aerial Vehicles in Microgrid Defense. IET Renewable Power Generation, Volume 19, January/December 2025, Article number e70089