Check for updates

Received: 17 October 2024 | Revised: 21 December 2024 | Accepted: 10 January 2025

IET Smart Grid

DOI: 10.1049/stg2.70000

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

Unmanned aerial vehicles versus smart grids

Alexis Pengfei Zhao[1] | Shuangqi Li[2] | Da Huo[3] | Mohannad Alhazmi[4]

[1]Systems Engineering, Cornell University, Ithaca, New York, USA

[2]Department of Electrical Engineering, The Hong Kong Polytechnic University, Hong Kong, China

[3]Centre for Energy Systems and Strategy, Cranfield University, Bedford, England, UK

[4]Electrical Engineering Department, College of Applied Engineering, King Saud University, Riyadh, Saudi Arabia

Correspondence

Shuangqi Li.
Email: shuangqi.li@polyu.edu.hk

Funding information

King Saud University, Grant/Award Number: RSPD2025R635

Abstract

The increasing threat of unmanned aerial vehicles (UAVs) to smart grid infrastructures poses critical challenges to energy systems security. This study examines smart grid vulnerabilities to UAV-based attacks and proposes a novel optimisation framework to enhance grid resilience. Employing a multi-objective optimisation approach using the Non-dominated Sorting Genetic Algorithm III (NSGA-III) and a game-theoretic Stackelberg model, the research captures the strategic interplay between UAV operators and grid defenders. Key contributions include the development of a multi-objective optimisation framework, integration of adversarial game theory, incorporation of dynamic environmental conditions, and generation of Pareto-optimal solutions for strategic defence planning. This research makes four pivotal contributions: (a) the design of a comprehensive multi-objective optimisation framework tailored for UAV strike optimisation, (b) the integration of game-theoretic principles to model adversarial behaviours, (c) the inclusion of dynamic environmental factors to improve solution robustness, and (d) the application of NSGA-III to generate trade-off solutions, equipping decision-makers with diverse strategies to enhance grid resilience. By addressing an urgent and timely challenge, this work offers practical guidance for fortifying smart grid infrastructures against emerging UAV threats in increasingly complex operational environments.

KEYWORDS

fault diagnosis, optimisation, power system management

1 | INTRODUCTION

The increasing integration of smart grid technology into modern power distribution systems has revolutionised how energy is managed, distributed, and consumed. Smart grids incorporate advanced communication technologies, real-time monitoring, and control systems, providing significant improvements in efficiency, reliability, and sustainability [1, 2]. However, this rapid technological advancement has also introduced new vulnerabilities, particularly concerning the physical and cyber-physical security of critical infrastructure [3]. As the reliance on smart grids grows, so too does the range of potential threats, including unmanned aerial vehicle (UAV) (UAV) strikes, which pose a significant risk to the integrity and functionality of power distribution networks. The threat of UAV-based attacks on smart grid infrastructure has garnered considerable attention in recent years due to the increasing availability, sophistication, and autonomy of these systems [4]. Unmanned aerial vehicles offer a unique set of advantages to potential attackers, including high mobility, relatively low cost, and the ability to execute precise, coordinated strikes on critical infrastructure with minimal human intervention [5]. These characteristics make UAVs a highly effective tool for targeting key components of the power grid, such as substations, transmission lines, and transformers. The ability to strike from the air, bypassing traditional ground-based defences, exacerbates the challenge of protecting the grid from such attacks [6].

In parallel with the increasing use of UAVs for legitimate purposes, their misuse by malicious actors has raised significant concerns among policymakers, grid operators, and security agencies. A well-coordinated UAV strike on a power grid could lead to cascading failures, large-scale blackouts, and substantial

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

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

economic and societal disruption. The vulnerability of the grid to such physical attacks is compounded by the growing interconnectivity between energy, communication, and control systems, making it a prime target for both cyber and physical threats.

The motivation behind this research stems from the urgent need to develop robust defence mechanisms against UAV-based attacks on smart grid infrastructure. Traditional approaches to grid security have predominantly focused on cyber threats, leaving physical vulnerabilities, particularly those posed by UAVs, inadequately addressed. As the sophistication of UAVs continues to evolve, so does their potential to cause widespread damage. This study aims to address this critical gap by introducing an advanced optimisation framework for simulating and optimising UAV strikes against smart grids, with the ultimate goal of enhancing the resilience and security of power systems against such threats. The core research objective of this paper is to model, simulate, and optimise UAV strikes on smart grids using a novel combination of the Non-dominated Sorting Genetic Algorithm III (NSGA-III) algorithm and game-theoretic approaches. By leveraging multi-objective optimisation techniques, this research seeks to provide a deeper understanding of how UAVs can exploit grid vulnerabilities to maximise disruption, while also offering insights into how grid operators can effectively mitigate these risks through strategic defensive measures. The integration of game theory into the optimisation framework allows for a more realistic representation of the adversarial interactions between UAV operators (attackers) and grid defenders, providing a comprehensive approach to defence planning.

This paper specifically focuses on the problem of optimising UAV strikes on smart grids by formulating it as a multi-objective optimisation problem. The three primary objectives are: (a) to maximise the damage inflicted on critical grid components, (b) to minimise the operational costs associated with UAV deployment, and (c) to minimise the risk of UAV detection by surveillance systems. These objectives are inherently conflicting, as maximising damage often requires increased UAV activity, which in turn increases both operational costs and detection risk. To address these conflicting goals, the NSGA-III algorithm is employed to generate a diverse set of Pareto-optimal solutions, offering a range of trade-offs between the objectives. The optimisation framework is built upon a detailed mathematical model that includes both UAV operational parameters and grid vulnerability dynamics. The UAV flight paths are optimised using dynamic environmental data, while the vulnerability of each grid component is modelled as a time-varying function that changes based on the severity of UAV strikes and natural degradation. Game theory is integrated into the model to represent the strategic interaction between UAV operators and grid defenders, with each side attempting to optimise their own objectives while anticipating the actions of their opponent. The key contributions of this paper can be summarised as follows:

(1) This paper presents a novel multi-objective optimisation framework based on the NSGA-III algorithm, which is particularly well-suited for handling high-dimensional, multi-objective problems. The framework optimises UAV strike paths across multiple conflicting objectives, including maximising damage, minimising operational costs, and reducing detection risk.
(2) The paper integrates game-theoretic approaches into the optimisation framework, specifically using a Stackelberg game to model the interaction between UAV operators (attackers) and grid defenders. This novel approach provides a more realistic representation of adversarial interactions, offering valuable insights into how both attackers and defenders can optimise their strategies.
(3) The research introduces a dynamic model of grid vulnerabilities and UAV flight parameters, which evolve over time in response to both UAV strikes and environmental conditions. This dynamic modelling ensures that the optimisation framework is robust and adaptable to real-world scenarios.
(4) By incorporating stochastic environmental factors into the optimisation process, this paper enhances the robustness of the solutions. The framework accounts for uncertainties in weather conditions and sensor accuracy, ensuring that the UAV strike paths remain effective under a wide range of operational conditions.

2 | LITERATURE REVIEW

The growing complexity and interconnectedness of modern smart grids, combined with the increased accessibility and sophistication of UAVs, have highlighted significant vulnerabilities in critical infrastructure. These vulnerabilities necessitate advanced optimisation strategies to mitigate the impact of UAV strikes on smart grids [7]. This review establishes the foundation for the novel contributions of this paper, which integrates these techniques into a comprehensive framework for optimising UAV strikes on smart grids.

The vulnerability of smart grids to both cyber and physical attacks has been widely studied in the literature. Smart grids, characterised by their real-time communication, bi-directional energy flows, and integration of renewable energy sources, have become increasingly susceptible to a variety of attacks due to their highly interconnected nature [8, 9]. Early work in this area primarily focused on cybersecurity threats, particularly those targeting the communication and control systems that regulate energy distribution [10]. Several studies have examined how hackers can exploit vulnerabilities in communication protocols to disrupt grid operations by injecting false data, causing blackouts, or destabilising the system through denial-of-service (DoS) attacks [8]. While these studies provide valuable insights into cyber threats, there is a noticeable gap in the literature addressing physical threats to grid infrastructure, particularly those posed by UAVs. In recent years, UAVs have emerged as a significant physical threat to smart grids, with the potential to bypass traditional ground-based defences and target critical components from the air. The work by Chamola et al. [11] offer a comprehensive review of UAV threats,

25152947, 2025, 1, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/stg2.70000 by Test, Wiley Online Library on [28/02/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

highlighting their capability to carry payloads that can damage transformers, transmission lines, and substations. Despite its limited payload capacity, UAVs can cause substantial disruption by targeting high-impact nodes in the grid, resulting in cascading failures that lead to widespread power outages. This research [11] also emphasises the growing autonomy and availability of UAV technology, which lowers the barrier to entry for malicious actors. However, while this review outlines the broad risks posed by UAVs, it lacks detailed analyses of how these threats can be modelled and optimised for in defensive strategies.

Recent studies have begun to explore the modelling of UAV-based physical attacks on power grids. Zhang and Chandramouli [12] developed a simulation framework for evaluating the impact of single and multiple UAV cyber-physical attacks on energy infrastructure. Their model integrates the behaviour of UAVs with the operational dynamics of the grid, demonstrating the potential severity of well-coordinated attacks. However, their study relies on basic optimisation methods and does not consider more sophisticated algorithms such as NSGA-III, nor does it incorporate the game-theoretic elements necessary to model the strategic interaction between attackers and defenders. This limitation is addressed in the current paper, which extends the literature by using advanced multi-objective optimisation and game-theoretic approaches to explore these threats.

Unmanned aerial vehicle path planning is a critical component of optimising both the efficiency and effectiveness of UAV-based attacks on infrastructure [13]. Path planning refers to determining the optimal route for a UAV to reach its target while minimising energy consumption, avoiding detection, and maximising the damage inflicted on critical components [14]. A wide range of optimisation techniques has been explored for UAV path planning, from classical approaches, such as dynamic programming and greedy algorithms to more advanced methods, such as genetic algorithms and particle swarm optimisation. Genetic algorithms, which are evolutionary algorithms (EVOs) inspired by natural selection, have been widely used in UAV path planning due to their ability to handle non-linear, multi-objective optimisation problems. Silva Arantes et al. [15] developed a GA-based framework for optimising UAV paths in complex environments, accounting for factors, such as terrain, weather conditions, and fuel consumption. This approach demonstrated the GA's effectiveness in finding near-optimal solutions in high-dimensional search spaces, making it well-suited for UAV operations. However, traditional GAs are limited in their ability to handle high-dimensional, multi-objective problems with many conflicting objectives, such as those encountered in UAV strikes on smart grids.

To address these limitations, more advanced EVOs, such as Non-dominated Sorting Genetic Algorithm II (NSGA-II) and NSGA-III have been developed. NSGA-II, introduced by Deb et al. [16], is a widely used algorithm for multi-objective optimisation that ranks solutions based on Pareto dominance and maintains diversity in the solution set using a crowding distance metric. While NSGA-II has been successfully applied to various UAV path planning problems [17], it struggles with high-dimensional problems where the number of objectives exceeds three. This challenge led to the development of NSGA-III, which extends NSGA-II by introducing reference points to guide the search process in high-dimensional objective spaces. The NSGA-III algorithm, first introduced by Deb and Jain [18], is particularly effective in problems with many conflicting objectives, making it an ideal choice for optimising UAV strikes on smart grids, where objectives such as maximising damage, minimising cost, and reducing detection risk are inherently in conflict. Despite the growing use of NSGA-III in other fields, its application to UAV path planning in the context of infrastructure defence remains underexplored. This paper addresses this gap by employing NSGA-III to optimise the multi-objective problem of UAV strikes on smart grids, offering a novel application of this algorithm to a critical real-world problem.

Following the advancements presented in Table 1, this study further builds on the integration of adversarial dynamics and optimisation to address the critical challenges posed by UAV-based threats to smart grids. The incorporation of environmental factors into the model and the application of NSGA-III mark a significant progression in addressing real-world scenarios. These enhancements provide a robust foundation for developing effective defence strategies tailored to modern grid infrastructures.

3 | MATHEMATICALL MODELLING

The first objective function is designed to maximise the damage inflicted by UAV strikes on critical smart grid components. We model the total damage $\Delta\mathcal{D}$ as a function of the vulnerabilities θ_i of individual components, weighted by the importance w_i of each component in the grid's operation. The damage also depends on the UAV strike effectiveness α_i and the resistance of the component β_i to damage. To incorporate non-linearity and diminishing returns of repeated strikes on the same component, we utilise an exponential decay function, which reduces the effectiveness of strikes after repeated attacks on the same component.

$$\Delta\mathcal{D} = \sum_{i=1}^{n} w_i \cdot \theta_i \cdot \left(1 - \exp\left(-\frac{\alpha_i}{\beta_i}\right)\right) \quad \text{for } i \in \{1, 2, \ldots, n\} \tag{1}$$

This equation captures the trade-off between component vulnerability and UAV effectiveness, providing a framework where damage maximisation is dynamically dependent on the vulnerabilities and the diminishing effect of repeated UAV strikes.

The cost minimisation objective aims to minimise the total operational cost $\mathcal{C}$ incurred by the UAV deployment. This cost is modelled as a function of the distance travelled d_j by UAV j, the fuel consumption rate ϕ_f, maintenance expenses ϕ_m, and personnel costs ϕ_p. The operational cost is weighted by the

25152947, 2025, 1, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/sg2.70000 by Test, Wiley Online Library on [28/02/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

TABLE 1 Comparison of existing research and proposed study.

Aspect	Existing research	Proposed study
Focus of analysis	Primarily on cybersecurity threats targeting communication and control systems [8, 9]. Limited focus on physical threats, such as UAV-based attacks [11].	Addresses UAV-based physical threats to smart grid infrastructures with detailed modelling of UAV capabilities and grid vulnerabilities.
Optimisation techniques	Basic methods such as dynamic programming, greedy algorithms, and genetic algorithms (GA) [15]. Limited application to high-dimensional multi-objective problems.	Employs NSGA-III, specifically designed for high-dimensional, multi-objective optimisation, to handle competing objectives such as damage maximisation, cost minimisation, and detection risk reduction.
Incorporation of game theory	Limited or no integration of adversarial dynamics between attackers and defenders [12].	Integrates a game-theoretic Stackelberg model to simulate strategic interactions, providing realistic insights into adversarial behaviour.
Dynamic environmental factors	Rarely addressed; most studies use static conditions for UAV path planning [13].	Models dynamic environmental conditions, including wind speed, temperature, and visibility, to assess their impact on UAV flight paths and mission success.
Real-world applicability	Focuses on theoretical frameworks with minimal practical implementation or case studies using real-world-inspired data [12].	Provides case studies with synthesised data, reflecting realistic grid configurations and UAV capabilities, enhancing the practical value of the findings.
Key contributions	Highlights UAV risks but lacks advanced optimisation and defence strategies [11].	Develops a comprehensive framework combining NSGA-III optimisation, game theory, and dynamic modelling, offering actionable insights for grid resilience planning.

Abbreviations: NSGA-III, Non-dominated Sorting Genetic Algorithm III; UAV, unmanned aerial vehicle.

relative importance α, β, and γ of these three cost components, respectively.

$$\mathcal{C} = \alpha \cdot \phi_f \cdot \sum_{j=1}^{m} d_j + \beta \cdot \phi_m \cdot \sum_{k=1}^{p} e_k + \gamma \cdot \phi_p \cdot f \quad (2)$$

This equation accounts for various operational costs, ensuring that the optimisation framework balances the resources used during the UAV strikes while considering the need for reducing overall expenses.

The third objective addresses minimising the detection risk $\mathcal{R}$ for the UAVs during their operations. The detection risk depends on the UAV's altitude h, environmental noise ξ, and the sensitivity σ of the surveillance systems. The model uses a scaling factor δ and environmental constant ϵ to balance the environmental impact on UAV detection.

$$\mathcal{R} = \frac{\delta \cdot h^2}{\epsilon + \xi} \cdot \left(1 - \exp\left(-\frac{\theta}{\sigma}\right)\right) \quad (3)$$

This function captures the UAV's risk of being detected by surveillance systems based on altitude and external noise conditions. Lower altitude and higher noise levels reduce detection risks, making it crucial to optimise flight paths accordingly.

The overall multi-objective function $\mathcal{Z}$ is a combination of the three objectives: damage maximisation, cost minimisation, and risk minimisation. The weighted sum approach is used to balance these competing objectives, where λ_1, λ_2, and λ_3 are the relative importance weights for each objective.

$$\mathcal{Z} = \lambda_1 \cdot \Delta\mathcal{D} - \lambda_2 \cdot \mathcal{C} - \lambda_3 \cdot \mathcal{R} \quad (4)$$

This multi-objective formulation ensures that the optimisation problem addresses the necessary trade-offs between maximising damage, minimising costs, and reducing the detection risk.

To address the inherent uncertainty in environmental conditions, we introduce a stochastic component into the optimisation problem. The uncertainty $\mathcal{U}$ in environmental factors such as wind speed, temperature, and visibility is modelled as a random variable ξ, with the UAV's flight path and performance depending on its stochastic variation.

$$\mathcal{U} = \mathbb{E}\left[\frac{1}{1 + \exp(-\xi)} \cdot \left(\frac{\delta \cdot h^2}{\epsilon + \xi}\right)\right] \quad (5)$$

This stochastic term introduces robustness into the model, allowing for uncertainties in real-world conditions and providing a more resilient solution to changes in the environment.

The robust optimisation framework includes a worst-case scenario term $\mathcal{W}$, which ensures that the model accounts for the maximum potential damage that the UAV can inflict under the most unfavourable conditions. This term integrates the highest possible vulnerabilities $\theta_{\max}$ and lowest defence capabilities $\beta_{\min}$ of the grid components.

$$\mathcal{W} = \max_{\theta_{\max}, \beta_{\min}} \sum_{i=1}^{n} w_i \cdot \theta_{\max} \cdot \left(1 - \exp\left(-\frac{\alpha_i}{\beta_{\min}}\right)\right) \quad (6)$$

This robust term ensures that the solution is resilient to worst-case scenarios by preparing for the highest potential damage outcomes.

25152947, 2025, 1, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/stg2.70000 by Test, Wiley Online Library on [28/02/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

The vulnerability score for each grid component $\theta_i(t)$ dynamically evolves over time as a function of past UAV strikes, component degradation, and external environmental conditions. The vulnerability update function includes a time-decaying factor λ and an environmental degradation term η.

$$\theta_i(t) = \theta_i(0) \cdot \exp(-\lambda t) + \eta \cdot \sum_{j=1}^{m} \left(1 - \exp\left(-\frac{\alpha_j}{\beta_j}\right)\right) \quad (7)$$

This dynamic vulnerability function allows for real-time updates of component vulnerabilities based on UAV attacks and external factors, providing a more accurate representation of grid resilience over time.

The game-theoretic formulation of the problem involves a strategic interaction between the UAV operator (attacker) and the grid operator (defender). The attacker seeks to maximise the damage $\Delta\mathcal{D}$, while the defender tries to minimise it by deploying defensive strategies $\mathcal{S}_d$. The payoff functions for both players are described as follows:

$$\mathcal{P}_{\text{attacker}} = \Delta\mathcal{D} - \mathcal{C}_{\text{defense}}, \quad \mathcal{P}_{\text{defender}} = -\Delta\mathcal{D} + \mathcal{C}_{\text{defense}} \quad (8)$$

This game-theoretic model introduces competitive interactions between attacker and defender strategies, optimising UAV strike paths in response to defensive measures.

The Stackelberg equilibrium captures the leader-follower dynamics between the attacker and the defender. The UAV operator, acting as the leader, anticipates the defensive actions of the grid operator, optimising their strike strategy accordingly. The Stackelberg equilibrium solution $\mathcal{E}_{\text{Stackelberg}}$ is given by the following:

$$\mathcal{E}_{\text{Stackelberg}} = \arg\max_{\Delta\mathcal{D}} \min_{\mathcal{S}_d} \left(\Delta\mathcal{D} - \mathcal{C}_{\text{defense}}\right) \quad (9)$$

This equilibrium represents the optimal UAV strike strategy that considers both offensive goals and the defender's response, ensuring that the attack is executed in the most effective manner.

Finally, the Pareto front $\mathcal{P}_f$ generated by the NSGA-III algorithm represents the trade-offs between the competing objectives of damage maximisation, cost minimisation, and risk reduction. The Pareto front is a set of non-dominated solutions, where improving one objective would worsen another. The Pareto front is represented as follows:

$$\mathcal{P}_f = \{\mathbf{x} \in \mathbb{R}^n : \nexists \mathbf{y} \in \mathbb{R}^n \quad \text{such that} \quad \mathcal{Z}(\mathbf{y}) \succ \mathcal{Z}(\mathbf{x})\} \quad (10)$$

This equation captures the set of optimal solutions that balance the objectives of the problem, providing decision-makers with a range of optimal trade-offs between competing goals.

The UAV battery life constraint ensures that each UAV's operation is within its energy limits, based on flight time t_j and energy consumption E_j. The total energy consumption depends on the UAV's velocity v_j, distance travelled d_j, and the power consumption rate ρ_j, while factoring in the battery capacity $\mathcal{B}_j$. To account for various mission parameters, we model the battery constraint as follows:

$$t_j \cdot \rho_j \cdot \left(\frac{d_j}{v_j} + \frac{\gamma_j \cdot d_j^2}{v_j^2}\right) \le \mathcal{B}_j, \quad \forall j \in \{1, 2, \ldots, m\} \quad (11)$$

This equation guarantees that the total energy consumed during the mission, factoring in both linear and non-linear energy costs, does not exceed the UAV's available battery capacity. It ensures that UAVs complete their missions without depleting their energy supply.

The payload capacity constraint enforces that the weight of the UAV's carried load w_j does not exceed the maximum payload capacity $\mathcal{W}_{\max}$ for UAV j. The constraint is given by the following:

$$w_j + \sum_{i=1}^{n} \theta_i \cdot \phi_j \cdot \left(1 - \exp\left(-\frac{\alpha_i}{\beta_i}\right)\right) \le \mathcal{W}_{\max}, \quad \forall j \quad (12)$$

This constraint ensures that the UAV's payload, including any damage materials or strike payload, remains within its operational limits, preventing mission failures due to excessive load.

The flight range constraint limits the distance d_j that each UAV can travel based on its fuel capacity and operational range $\mathcal{R}_j$. It is crucial to ensure UAVs can complete their missions and return to their base without running out of power:

$$d_j \cdot \left(1 + \frac{\sigma_j \cdot \rho_j \cdot h_j}{v_j \cdot \mathcal{R}_j}\right) \le \mathcal{R}_j, \quad \forall j \quad (13)$$

This equation accounts for the additional energy consumption due to altitude h_j, velocity v_j, and environmental drag σ_j, ensuring that the UAV stays within its flight range limit.

The communication constraint ensures that UAVs maintain continuous communication within a given range $\mathcal{D}_{\text{comm}}$. The communication between UAVs j and k is restricted by their distance and the strength of their communication link, denoted by γ_{jk}:

$$\sum_{j,k=1}^{m} \left(\frac{\gamma_{jk}}{d_{jk}} \cdot \left(1 - \exp\left(-\frac{d_{jk}}{\mathcal{D}_{\text{comm}}}\right)\right)\right) \ge \eta, \quad \forall j, k \quad (14)$$

This constraint guarantees that all UAVs remain within their communication range, ensuring coordinated operations and reducing the risk of mission failure due to communication breakdown.

The maximum allowable damage constraint ensures that the damage $\Delta\mathcal{D}$ inflicted by UAV strikes on the grid does not exceed the critical damage threshold $\mathcal{D}_{\max}$ that could lead to system-wide collapse:

25152947, 2025, 1, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/stg2.70000 by Test, Wiley Online Library on [28/02/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

$$\Delta\mathcal{D} = \sum_{i=1}^{n} w_i \cdot \theta_i \cdot \left(1 - \exp\left(-\frac{\alpha_i}{\beta_i}\right)\right) \leq \mathcal{D}_{\max} \tag{15}$$

This constraint ensures that while UAVs aim to maximise disruption, the attacks do not cause irreversible damage to the grid, preserving the overall stability of the power distribution system.

The detection risk constraint is modelled to ensure that UAVs minimise the risk of being detected by radar or other surveillance systems. This constraint depends on the UAV's altitude h_j, radar sensitivity ζ_j, and environmental noise ξ_j:

$$\mathcal{R}_j = \frac{\delta_j \cdot h_j^2}{\epsilon_j + \xi_j} \cdot \left(1 - \exp\left(-\frac{\theta_j}{\zeta_j}\right)\right) \leq \mathcal{R}_{\max}, \quad \forall j \tag{16}$$

This equation ensures that UAV operations are conducted within an acceptable detection risk threshold, reducing the probability of interception by security forces.

The flight path optimisation constraint ensures that UAVs follow the most efficient routes to their assigned targets, minimising energy consumption and detection risk. The optimisation problem is expressed as follows:

$$\sum_{j=1}^{m} \left(\min_{\mathcal{P}_j} \sum_{i=1}^{n} \frac{c_{ij}}{v_j} \cdot \left(1 + \frac{\xi_j}{h_j^2}\right)\right) \leq \mathcal{P}_{\text{opt}}, \quad \forall j \tag{17}$$

This constraint ensures that each UAV follows the most optimal path $\mathcal{P}_j$ to its target, minimising both flight time and energy consumption while accounting for environmental conditions and detection risk.

The environmental condition constraint accounts for the impact of wind speed ω_j, temperature T_j, and humidity μ_j on the UAV's performance. The constraint ensures that UAVs can operate effectively under varying environmental conditions:

$$\sum_{j=1}^{m} \left(\frac{v_j^2}{\omega_j + T_j + \mu_j} \cdot \left(1 - \exp\left(-\frac{\theta_j}{\sigma_j}\right)\right)\right) \leq \mathcal{E}_{\max}, \quad \forall j \tag{18}$$

This constraint adjusts UAV performance based on real-time environmental factors, ensuring that missions remain feasible under different weather conditions.

The time constraint ensures that UAV attacks are completed within a given time window $t_{\max}$, accounting for the UAV's velocity v_j and the distance d_j to the target:

$$\sum_{j=1}^{m} \left(\frac{d_j}{v_j} + \frac{\sigma_j \cdot d_j^2}{v_j^2}\right) \leq t_{\max}, \quad \forall j \tag{19}$$

This equation ensures that the UAVs complete their missions within the allocated time frame, factoring in both linear travel times and non-linear effects such as environmental drag and operational delays.

The budget constraint ensures that the total operational costs $\mathcal{C}$ incurred by deploying UAVs remain within the available budget $\mathcal{B}_{\text{total}}$:

$$\mathcal{C} = \sum_{j=1}^{m} \left(\alpha \cdot \phi_f \cdot d_j + \beta \cdot \phi_m \cdot e_j + \gamma \cdot \phi_p \cdot f\right) \leq \mathcal{B}_{\text{total}} \tag{20}$$

This equation ensures that the total cost of the mission, including fuel, maintenance, and personnel costs, remains within the specified budget limits.

The redundancy constraint ensures that key components of the power grid remain operational even after a UAV attack. The constraint guarantees that the grid can tolerate a certain level of damage $\mathcal{D}_r$ without collapsing:

$$\sum_{i=1}^{n} \left(\frac{w_i \cdot \theta_i}{1 + \lambda_i \cdot \Delta\mathcal{D}}\right) \geq \mathcal{D}_r, \tag{21}$$

where $\mathcal{D}_r$ is the redundancy threshold.

This redundancy constraint ensures that critical grid components maintain enough functionality to prevent complete system failure, even in the event of a successful UAV attack.

The security response time constraint ensures that UAV operations are completed before the defensive system is able to respond effectively. The response time t_r of the security system is modelled as a function of the detection delay δ_{detect}, the deployment time δ_{deploy}, and the reaction speed v_{response} of the security forces. Additionally, the distance between the UAV and the defensive system d_{defense} plays a crucial role. The constraint guarantees that the UAV completes its mission t_{mission} before the system reacts:

$$t_{\text{mission}} \leq \delta_{\text{detect}} + \frac{d_{\text{defense}}}{v_{\text{response}}} + \delta_{\text{deploy}}, \quad \forall j \in \{1, 2, \ldots, m\} \tag{22}$$

This constraint ensures that the UAV's operational time does not exceed the total security response time, factoring in the detection, deployment, and reaction speeds of the defensive systems, thus minimising the risk of UAV interception.

The legal and ethical considerations constraint is designed to ensure that UAV operations comply with international regulations and ethical standards. This constraint is modelled as a set of legal requirements $\mathcal{L}_i$ and ethical bounds $\mathcal{E}_i$, each associated with different aspects of UAV operation, such as maximum altitude $h_{\max}$, prohibited zones $\mathcal{Z}_p$, and limitations on payloads w_j. The constraint is expressed as follows:

$$\sum_{i=1}^{n} \left(\frac{1}{1 + \exp(-\mathcal{L}_i)}\right) \cdot \sum_{j=1}^{m} \left(\frac{h_j}{h_{\max}} + \frac{w_j}{\mathcal{W}_{\max}}\right) \cdot \mathbf{1}_{\mathcal{Z}_p} \leq \mathcal{E}_{\max}, \quad \forall j \tag{23}$$

25152947, 2025, 1, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/sg2.70000 by Test, Wiley Online Library on [28/02/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

This equation ensures that UAV operations remain within the bounds of legal and ethical frameworks, accounting for altitude restrictions, payload limits, and no-fly zones. The function $\mathbf{1}_{\mathcal{Z}_p}$ ensures that UAVs do not enter prohibited zones, ensuring regulatory compliance throughout the mission.

The UAV sensor accuracy constraint is critical for minimising detection risks during operations. Sensor accuracy α_j affects the UAV's ability to detect obstacles and avoid countermeasures. This constraint depends on the quality of the sensors ζ_j, the environmental conditions ξ_j, and the sensor calibration κ_j. The equation ensures that the sensor accuracy remains above a certain threshold $\alpha_{\min}$:

$$\sum_{j=1}^{m}\left(\frac{\zeta_j}{1+\kappa_j\cdot\exp\left(-\xi_j\right)}\cdot\left(1-\frac{\alpha_j}{\alpha_{\min}}\right)\right)\le\mathcal{A}_{\max},\quad\forall j \tag{24}$$

This constraint guarantees that the UAV's sensor system maintains high accuracy under varying environmental conditions, ensuring efficient detection avoidance and safe navigation during missions.

The redundancy of defensive actions constraint ensures that the grid operator can implement multiple defensive strategies to mitigate cascading failures in the event of UAV attacks. The effectiveness of defensive measures $\mathcal{S}_d$ is modelled as a function of the number of defensive actions ρ_i applied to different grid components, weighted by their effectiveness η_i in reducing system vulnerability θ_i. The redundancy constraint ensures that the defensive actions cover enough critical components to prevent failure propagation:

$$\sum_{i=1}^{n}\rho_i\cdot\eta_i\cdot\left(1-\exp\left(-\frac{\theta_i}{\mathcal{S}_d}\right)\right)\ge\mathcal{R}_{\min} \tag{25}$$

This constraint ensures that the grid operator can apply a sufficient number of defensive actions to critical components, effectively mitigating cascading failures and maintaining the resilience of the grid during and after the UAV attack.

4 | METHODOLOGY

In Figure 1, the flowchart visually captures the step-by-step process of the NSGA-III algorithm, with clear distinctions between each stage such as population initialisation, fitness evaluation, and selection for the next generation. The NSGA-III fitness evaluation function is central to the algorithm's ability to assess each solution $\mathbf{x}_i$ in the population across multiple objectives. For UAV strike optimisation, each solution is evaluated based on the damage $\Delta\mathcal{D}$, cost $\mathcal{C}$, and detection risk $\mathcal{R}$. The fitness of solution $\mathbf{x}_i$ is calculated by normalising its objective values and comparing them to reference points $\mathcal{Z}_r$ distributed across the Pareto front:

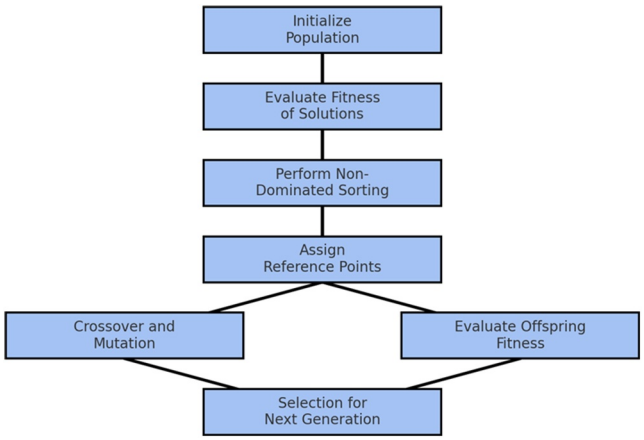

FIGURE 1 Flowchart of NSGA-III algorithm. NSGA-III, Non-dominated Sorting Genetic Algorithm III.

$$\begin{aligned}F(\mathbf{x}_i)=&\sum_{k=1}^{p}\left(\frac{\mathcal{Z}_r^k-f_k(\mathbf{x}_i)}{\max\left(\mathcal{Z}_r^k\right)-\min\left(\mathcal{Z}_r^k\right)}\right)^2\\&+\lambda_k\cdot\left(\Delta\mathcal{D}(\mathbf{x}_i)-\mathcal{C}(\mathbf{x}_i)-\mathcal{R}(\mathbf{x}_i)\right),\\&\forall i\in\{1,2,\ldots,N\}\end{aligned} \tag{26}$$

This equation evaluates the fitness of each solution by considering its proximity to the reference points and balancing the trade-offs between damage, cost, and detection risk. The reference points represent ideal solutions along the Pareto front, while the weighting term λ_k balances the importance of each objective.

The crossover operation combines two parent solutions $\mathbf{x}_p^1$ and $\mathbf{x}_p^2$ to generate new offspring $\mathbf{x}_c$. NSGA-III employs a simulated binary crossover method, where a random variable β_c controls the degree of crossover between the parents. The offspring inherit traits from both parents are as follows:

$$\begin{aligned}&\mathbf{x}_c=\frac{1}{2}\left(\mathbf{x}_p^1+\mathbf{x}_p^2\right)+\beta_c\cdot\left(\mathbf{x}_p^1-\mathbf{x}_p^2\right),\\&\text{where}\quad\beta_c=(2u_c)^{\frac{1}{\eta_c+1}},\quad\text{if}\quad u_c<0.5\end{aligned} \tag{27}$$

The crossover operation ensures diversity in the population by generating offspring that combine genetic material from both parents. The parameter η_c controls the spread of the offspring around the parents, while u_c is a uniform random variable that introduces variability.

The mutation operation introduces random perturbations to the offspring $\mathbf{x}_c$ to explore new regions of the solution space. The mutation rate p_m determines the likelihood of mutation, and the magnitude of the perturbation is governed by a polynomial mutation operator. The mutated solution $\mathbf{x}_m$ is expressed as follows:

25152947, 2025, 1, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/sg2.70000 by Test, Wiley Online Library on [28/02/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

$$\mathbf{x}_m = \mathbf{x}_c + \delta_m \cdot \mathcal{N}(0, \sigma^2),$$
$$\delta_m = \left(1 - \left(\frac{f(\mathbf{x}_c)}{f_{\max}}\right)\right)^{\frac{1}{\eta_m+1}}, \quad (28)$$

σ is a Gaussian noise term.

This mutation equation ensures that the population maintains diversity by perturbing solutions in proportion to their fitness, where σ introduces randomness. The parameter η_m controls the mutation strength, while $\mathcal{N}(0, \sigma^2)$ ensures a Gaussian distribution of the perturbation.

The selection mechanism in NSGA-III is based on Pareto dominance and crowding distance, ensuring that only non-dominated solutions are chosen for the next generation. The selection is performed by comparing the dominance rank R_i and crowding distance D_i of each solution $\mathbf{x}_i$. The probability of selection is given by the following:

$$P(\mathbf{x}_i) = \frac{1}{R_i} + \frac{D_i}{\sum_{j=1}^{N} D_j}, \quad \text{where} \quad R_i = \sum_{j=1}^{N} \mathbf{1}\big(f(\mathbf{x}_j) \prec f(\mathbf{x}_i)\big) \quad (29)$$

This equation prioritises solutions with a lower dominance rank and higher crowding distance, ensuring that the selected solutions are spread uniformly along the Pareto front while maintaining diversity in the population.

The game-theoretic payoff matrix models the strategic interaction between the UAV operator (attacker) and the grid operator (defender). Each player's payoff is a function of their respective strategies $\mathcal{S}_a$ and $\mathcal{S}_d$. The attacker seeks to maximise damage $\Delta\mathcal{D}$, while the defender seeks to minimise it. The payoff matrix is expressed as follows:

$$\mathcal{P} = \begin{pmatrix} \mathcal{P}_{a,d} & \mathcal{P}_{a,\neg d} \\ \mathcal{P}_{\neg a,d} & \mathcal{P}_{\neg a,\neg d} \end{pmatrix} = \begin{pmatrix} \Delta\mathcal{D} - \mathcal{C}_d & \Delta\mathcal{D} - \mathcal{C}_{\neg d} \\ \Delta\mathcal{D}_{\neg a} - \mathcal{C}_d & \Delta\mathcal{D}_{\neg a} - \mathcal{C}_{\neg d} \end{pmatrix} \quad (30)$$

This payoff matrix represents the four possible outcomes, where $\mathcal{P}_{a,d}$ is the payoff when both the attacker and defender play their strategies, while $\mathcal{P}_{\neg a,\neg d}$ represents the scenario where neither takes action. The UAV operator's utility function U_a is derived from the payoff matrix and is maximised based on the damage inflicted and cost of operation:

$$U_a = \max_{\mathcal{S}_a}(\Delta\mathcal{D} - \mathcal{C}) = \sum_{i=1}^{n} w_i \cdot \theta_i \cdot \left(1 - \exp\left(-\frac{\alpha_i}{\beta_i}\right)\right) - \sum_{j=1}^{m} \left(\alpha \cdot \phi_f \cdot d_j + \gamma \cdot \phi_p\right) \quad (31)$$

This utility function ensures that the UAV operator optimises their attack strategy to maximise grid damage while minimising operational costs. The first term accounts for the damage inflicted on grid components, while the second term captures the cost of deployment.

Similarly, the defender's utility function U_d is designed to minimise the damage inflicted on the grid, factoring in the cost of deploying defensive actions $\mathcal{S}_d$:

$$U_d = \min_{\mathcal{S}_d}(\Delta\mathcal{D} + \mathcal{C}_d) = \sum_{i=1}^{n} \rho_i \cdot \eta_i \cdot \left(1 - \exp\left(-\frac{\theta_i}{\mathcal{S}_d}\right)\right) + \sum_{j=1}^{m} \left(\beta \cdot \phi_m \cdot e_j\right) \quad (32)$$

The defender's utility function minimises the overall damage and operational cost of deploying defensive actions, ensuring that the grid's integrity is preserved while controlling costs.

The NSGA-III hypervolume calculation measures the quality of the Pareto front by calculating the volume between the current solutions and the reference points $\mathcal{Z}_r$. The hypervolume HV is computed as follows:

$$HV = \int_{\mathbb{R}^n} \mathbf{1}_{\mathcal{Z}_r}(f(\mathbf{x})) \cdot \prod_{k=1}^{p} \left(\mathcal{Z}_r^k - f_k(\mathbf{x})\right) d\mathbf{x} \quad (33)$$

This hypervolume calculation ensures that the algorithm converges towards a high-quality Pareto front by maximising the volume of non-dominated solutions relative to the reference points.

The leader-follower interaction in the Stackelberg game models the dynamic relationship between the attacker (leader) and the defender (follower). The UAV operator selects the optimal strike strategy $\mathcal{S}_a^*$ based on the anticipated defensive actions $\mathcal{S}_d$. The defender then adjusts their strategy accordingly. The equilibrium is expressed as follows:

$$\mathcal{S}_a^* = \arg\max_{\mathcal{S}_a} U_a, \quad \mathcal{S}_d^* = \arg\min_{\mathcal{S}_d} U_d\big(\mathcal{S}_a^*\big) \quad (34)$$

This leader–follower interaction ensures that the attacker optimises their strategy, anticipating the defender's response, while the defender reacts to the attacker's chosen strategy, resulting in an equilibrium that balances both players' objectives.

The multi-objective function decomposition for UAV path optimisation is aimed at breaking down the path planning problem into multiple smaller objectives such as minimising flight distance, minimising energy consumption, and maximising stealth. Each of these objectives is assigned a weight λ_i

25152947, 2025, 1, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/sg2.70000 by Test, Wiley Online Library on [28/02/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

to balance its contribution to the overall optimisation problem. The function can be decomposed as follows:

$$\mathcal{Z}_{\text{path}} = \sum_{i=1}^{k} \lambda_i \cdot \left(\alpha_i \cdot \frac{d_j}{v_j} + \beta_i \cdot \frac{1}{1+\exp(-h_j)} + \gamma_i \cdot \frac{1}{1+\sigma_j} \right), \quad \forall j \in \{1,2,\ldots,m\} \tag{35}$$

This equation optimises the UAV flight path by minimising the distance d_j, adjusting the altitude h_j for stealth, and accounting for sensor accuracy σ_j. The weights λ_i, α_i, β_i, and γ_i balance the contribution of each sub-objective to the overall path optimisation.

The time-varying vulnerability function captures the dynamic nature of grid component vulnerabilities as they evolve over time due to UAV attacks and environmental factors. The vulnerability $\theta_i(t)$ of component i is modelled as a function of its initial vulnerability $\theta_i(0)$, the number of UAV strikes $s_j(t)$, and the degradation factor λ:

$$\theta_i(t) = \theta_i(0) \cdot \exp(-\lambda t) + \sum_{j=1}^{m} \left(1 - \exp\left(-\frac{s_j(t)}{\beta_j} \right) \right), \quad \forall i \in \{1,2,\ldots,n\} \tag{36}$$

This equation accounts for both the natural decay of vulnerability over time and the increasing impact of repeated UAV strikes. The degradation factor λ controls how fast the vulnerability decreases over time, while the UAV strikes $s_j(t)$ contribute to its dynamic adjustment.

The dynamic adjustment of UAV flight parameters in response to environmental data, such as wind speed ω_j, temperature T_j, and atmospheric pressure P_j, is critical for optimising UAV performance. The flight parameters v_j and h_j are dynamically adjusted based on these factors:

$$v_j(t) = v_j(0) \cdot \exp\left(-\frac{\omega_j}{T_j} \right), \quad h_j(t) = h_j(0) + \frac{\alpha_j}{P_j} \cdot \left(1 - \exp\left(-\frac{T_j}{\omega_j} \right) \right) \tag{37}$$

This equation adjusts the UAV's velocity v_j and altitude h_j based on real-time environmental data. The wind speed ω_j and temperature T_j influence the UAV's speed, while atmospheric pressure P_j modulates the altitude for efficient energy use and stealth.

The cost-benefit analysis for UAV deployment across different grid zones evaluates the trade-off between deployment costs $\mathcal{C}$ and the potential damage $\Delta\mathcal{D}$ inflicted on each grid zone. The cost-benefit ratio $\mathcal{R}_b$ is calculated as follows:

$$\mathcal{R}_b = \sum_{z=1}^{Z} \frac{\Delta\mathcal{D}(z)}{\mathcal{C}(z)} = \sum_{z=1}^{Z} \frac{\sum_{i=1}^{n} w_i \cdot \theta_i \cdot \left(1 - \exp\left(-\frac{\alpha_i}{\beta_i} \right) \right)}{\sum_{j=1}^{m} \left(\alpha \cdot \phi_f \cdot d_j + \gamma \cdot \phi_p \right)}, \quad \forall z \in \{1,2,\ldots,Z\} \tag{38}$$

This equation provides a cost-benefit ratio by comparing the damage inflicted in each zone $\Delta\mathcal{D}(z)$ to the operational costs $\mathcal{C}(z)$, allowing decision-makers to prioritise zones with the highest return on investment for UAV deployment.

The stochastic environmental factor affects UAV flight efficiency and introduces randomness into the optimisation process. The environmental influence $\mathcal{E}_j$ on flight efficiency is modelled as a random variable ξ_j, which follows a Gaussian distribution $\mathcal{N}(0,\sigma^2)$, capturing variations in wind speed, temperature, and humidity:

$$\mathcal{E}_j = \mathbb{E}\left[\frac{1}{1+\exp(-\xi_j)} \cdot \left(\frac{v_j^2}{\omega_j + T_j + \mu_j} \right) \right], \quad \xi_j \sim \mathcal{N}(0,\sigma^2) \tag{39}$$

This equation introduces stochasticity into the UAV's flight performance by considering random variations in environmental conditions. The efficiency $\mathcal{E}_j$ is modulated by factors such as wind speed ω_j, temperature T_j, and humidity μ_j, ensuring robustness in the optimisation process.

The convergence criterion for NSGA-III is based on the generation count G and the improvement in fitness ΔF between generations. The algorithm terminates when the improvement in fitness falls below a predefined threshold ϵ:

$$\Delta F^{(t)} = \left| F^{(t)} - F^{(t-1)} \right| \le \epsilon, \quad G \le G_{\max}, \quad \text{where } F^{(t)} \text{ is the average fitness at generation } t \tag{40}$$

This equation defines the stopping criterion for NSGA-III, ensuring that the algorithm terminates when the change in the average fitness $\Delta F^{(t)}$ between consecutive generations becomes negligible, or when the maximum number of generations $G_{\max}$ is reached.

The multi-target engagement function models the simultaneous targeting of multiple grid components by UAVs. Each

25152947, 2025, 1, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/sg2.70000 by Test, Wiley Online Library on [28/02/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

UAV j is assigned multiple targets $\mathcal{T}_j$, and the engagement strategy is optimised to maximise damage across all targets:

$$\sum_{j=1}^{m}\sum_{k=1}^{|\mathcal{T}_j|}\left(\frac{w_k\cdot\theta_k}{1+\exp\left(-\lambda\cdot d_{jk}\right)}\right)\le\mathcal{T}_{\max},\quad \forall\, k\in\left\{1,2,\ldots,|\mathcal{T}_j|\right\} \tag{41}$$

This equation ensures that each UAV optimises its engagement with multiple targets $\mathcal{T}_j$, balancing the distance d_{jk} and the vulnerability θ_k of each target to maximise overall damage while avoiding overloading any single UAV.

The detection risk model for UAV operations is based on the UAV's speed v_j, altitude h_j, and the sensitivity of the surveillance systems σ_j. The risk of detection $\mathcal{R}_j$ is minimised by adjusting these parameters:

$$\mathcal{R}_j=\frac{\delta_j\cdot h_j^2}{\epsilon_j+\xi_j}\cdot\left(1-\exp\left(-\frac{v_j}{\sigma_j}\right)\right),\quad \forall\, j \tag{42}$$

This equation minimises the detection risk $\mathcal{R}_j$ by dynamically adjusting the UAV's speed v_j, altitude h_j, and the environmental noise ξ_j, ensuring stealth during UAV operations.

The UAV swarm coordination constraint prevents overlap in the attack paths of UAVs, ensuring that no two UAVs target the same grid component simultaneously. The coordination is modelled using a distance-based constraint d_{jk} between UAVs j and k:

$$\sum_{j,k=1}^{m}\left(\frac{1}{d_{jk}}\cdot\mathbf{1}_{\left\{d_{jk}\ge d_{\min}\right\}}\right)\ge\eta,\quad \forall\, j\ne k \tag{43}$$

This constraint ensures that the distance d_{jk} between any two UAVs j and k remains above a minimum threshold $d_{\min}$, preventing path overlap and ensuring efficient swarm coordination.

The NSGA-III termination condition is based on solution diversity. The algorithm terminates when the diversity of the population, measured by the crowding distance D_i, falls below a critical threshold $D_{\min}$:

5 | CASE STUDIES

To demonstrate the effectiveness of the proposed NSGA-III and game-theoretic framework for optimising UAV strikes on smart grids, a detailed case study is conducted using synthesised and assumed data. The smart grid system is modelled as a 123-bus power distribution network, which includes 150 substations, 300 transformers, and 500 transmission lines. Each grid component is assigned a vulnerability score ranging from 0 to 1, with higher values indicating more critical or fragile infrastructure. The UAVs are modelled as commercial-grade drones with varying operational capabilities, including a flight range of 50–80 km, a battery life of 90–120 min, and payload capacities between 3 and 5 kg. The data setup allows for the simulation of both individual and swarm-based UAV attacks, targeting multiple components of the grid under different environmental and operational conditions. The assumed data includes time-series information for power loads, operational parameters from grid substations, and potential attack windows based on real-time weather and grid activity. Environmental conditions such as wind speed (ranging from 5 to 25 km/h), visibility (clear, foggy, or overcast), and temperature (between −5°C and 35°C) are randomly generated for each scenario to evaluate their impact on UAV performance. Additionally, the UAVs' detection risk is modelled based on altitude, flight speed, and noise levels, with varying degrees of counter-surveillance activity by grid operators. Each attack scenario simulates between 5 and 25 UAVs executing coordinated strikes on critical grid components, and the performance of these strikes is evaluated based on the damage inflicted, operational costs, and the risk of detection. The computational environment for running the optimisation experiments is based on a high-performance computing system equipped with an Intel Xeon processor (3.6 GHz) with 32 cores and 128 GB of RAM, running on a Linux-based operating system. The optimisation framework is implemented using Python 3.9, with specialised libraries such as NumPy, SciPy, and PyGAD for the execution of NSGA-III algorithms. Each scenario is run 50 times to account for stochastic variations in environmental data and UAV performance, with average values reported for robustness analysis. The total computational time for each scenario ranges from 3 to 6 h, depending on the complexity of the grid configuration, the number of UAVs involved, and the environmental conditions. This setup ensures that the case study is both computationally feasible and scalable, allowing for realistic and detailed simulations of UAV strikes on smart grids [19–23].

Figure 2 illustrates the critical relationship between UAV flight time and payload capacity, highlighting the trade-off between these two parameters. As depicted in the scatter plot, as the payload capacity of the UAV increases, the available flight time decreases significantly. For instance, when the payload is at its minimum of 0.5 kg, the UAV achieves a flight time of 55 min. However, with a payload of 5 kg, the flight time sharply drops to 20 min. This indicates that as the UAV's load increases by 1 kg, the flight time declines by approximately 6 min on average. The trend line clearly follows a downward trajectory, reinforcing the inverse relationship between payload and operational endurance. The figure's scatter points are supplemented by a smooth blue line, which enhances the understanding of the overall trend across various payload capacities. For example, at a payload of 2 kg, the flight time is observed to be 40 min, marking a steep decline from the initial flight time of 55 min at 0.5 kg. The transition from 2.5 to 5 kg shows a slower decline in flight time, suggesting that UAVs with heavier payloads may have optimised their energy efficiency within this range, as indicated by the slight flattening of the blue line beyond 4 kg. This figure provides valuable insights for UAV operations, especially for missions where payload and

25152947, 2025, 1, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/stg2.70000 by Test, Wiley Online Library on [28/02/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

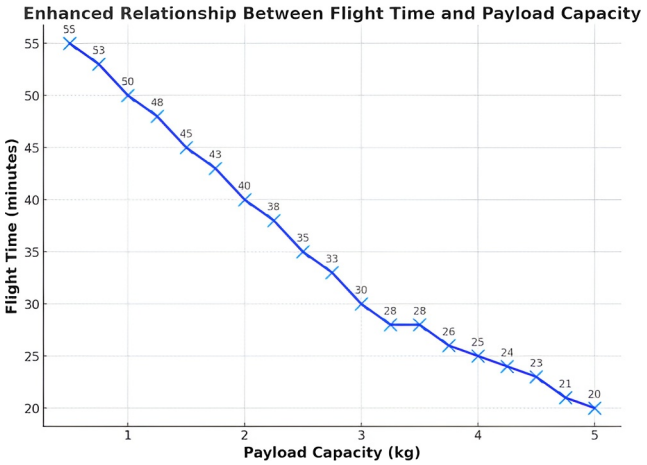

FIGURE 2 Relationship between UAV flight time and payload capacity. UAV, unmanned aerial vehicle.

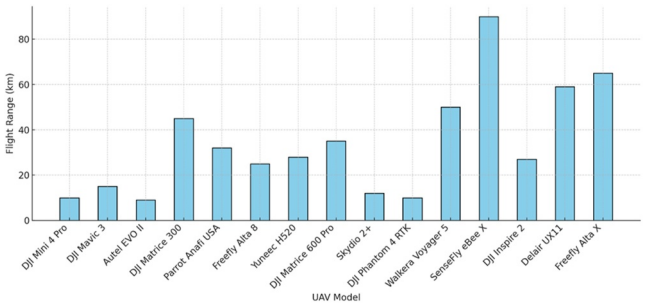

FIGURE 3 Flight range of different UAV models. UAV, unmanned aerial vehicle.

battery life are critical factors. For example, in scenarios where UAVs are used to deliver medical supplies or perform industrial inspections, operators must balance the payload weight with the need for longer operational times. The data points around 3 kg payload, showing a flight time of approximately 28 min, could represent a sweet spot for balancing these trade-offs. Ultimately, understanding this relationship helps in planning UAV missions more effectively, ensuring that flight range, payload, and endurance are optimised for specific operational requirements.

Figure 3 presents the flight range of 15 different UAV models, ranging from consumer-grade to professional and military-grade drones. The UAV models showcased have flight ranges varying from 9 km to as much as 90 km. Among the consumer-grade drones, the Da-Jiang Innovations (DJI) Mini 4 Pro has a relatively lower range of 10 km, while more advanced consumer drones such as the DJI Mavic 3 offer an extended range of 15 km. On the higher end of the professional drone spectrum, the DJI Matrice 300 offers a flight range of 45 km, making it suitable for industrial applications such as inspections and search-and-rescue missions. Similarly, models such as the Freefly Alta X and Delair UX11 showcase higher capabilities with ranges of 65 and 59 km, respectively, suited for surveying and mapping operations. A notable trend in the figure is the dramatic difference in range when comparing consumer drones to higher-end models. While drones such as the Autel II and DJI Phantom 4 Real-Time Kinematic remain in the 9–12 km range, military-grade drones such as the Walkera Voyager 5 and SenseFly eBee X significantly outclass them, boasting ranges of 50 and 90 km, respectively. This range disparity indicates the increasing operational flexibility provided by professional and military drones, which can cover large areas without the need for frequent battery recharges. In particular, the SenseFly eBee X's range of 90 km represents one of the highest operational distances for fixed-wing drones used in large-scale mapping and environmental monitoring. In analysing this figure, it's clear that drone manufacturers focus on extending flight range for specific applications. Consumer-grade drones are designed for shorter missions, generally within line-of-sight regulations, while professional and military UAVs prioritise longer missions and endurance. The Freefly Alta 8 and DJI Matrice 600 Pro, for example, provide robust solutions with flight ranges of 25 and 35 km, ideal for carrying heavier payloads or extended filming sessions in remote areas. Understanding these variations in flight range is critical for operators in choosing the right UAV model based on the mission's distance, complexity, and operational requirements.

In Figure 4, the heatmap demonstrates the effect of environmental factors, specifically wind speed and temperature, on the flight range of UAVs. The x-axis represents wind speeds ranging from 0 mph to 36 mph, while the y-axis represents temperatures spanning from −10°C to 40°C. The colour gradient, shifting from deep blue to light red, visually indicates how the UAV's flight range diminishes under more challenging environmental conditions. Under calm winds (0 mph) and moderate temperatures (around 15°C), UAVs achieve their optimal flight range of approximately 120 min. However, as the wind speed increases or the temperature deviates from the optimal range, the flight time gradually decreases. The heatmap provides an intuitive overview of the diminishing flight efficiency caused by harsh conditions. One critical observation is the substantial impact of wind speed. As wind speeds rise beyond 15 mph, the flight range starts to drop noticeably. At wind speeds of 36 mph, typical for extreme weather, the UAV's range falls to approximately 50–60 min, even under mild temperatures of around 15°C. This reduction occurs because the UAV expends additional energy to stabilise and fight the increased air resistance. Such conditions severely restrict the drone's operational time, making high-wind scenarios risky for long-duration missions. Even moderate wind speeds of 20 mph result in a significant decrease, with flight times reducing to around 80 min under ideal temperatures. Temperature also plays a pivotal role in the UAV's performance, with the extremes of −10°C and 40°C being particularly detrimental. At −10°C, the reduced battery efficiency leads to ranges of around 60–70 min, even with minimal wind. Similarly, at 40°C, the additional strain on motors and battery due to heat results in a similar decline in performance. Notably, at the intersection of high wind speeds (36 mph) and extreme temperatures (40°C), the flight range is reduced to just around 40–50 min,

25152947, 2025, 1, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/sgr2.70000 by Test, Wiley Online Library on [28/02/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

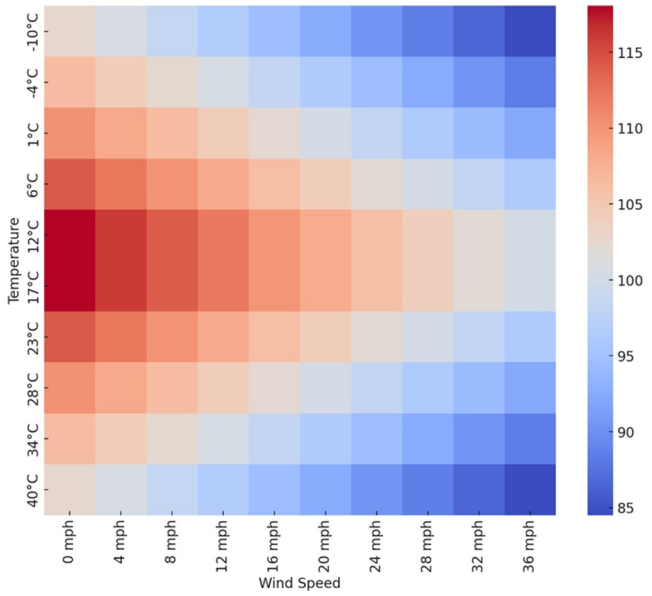

FIGURE 4 Unmanned Aerial Vehicle (UAV) flight range under varying wind speeds and temperature conditions.

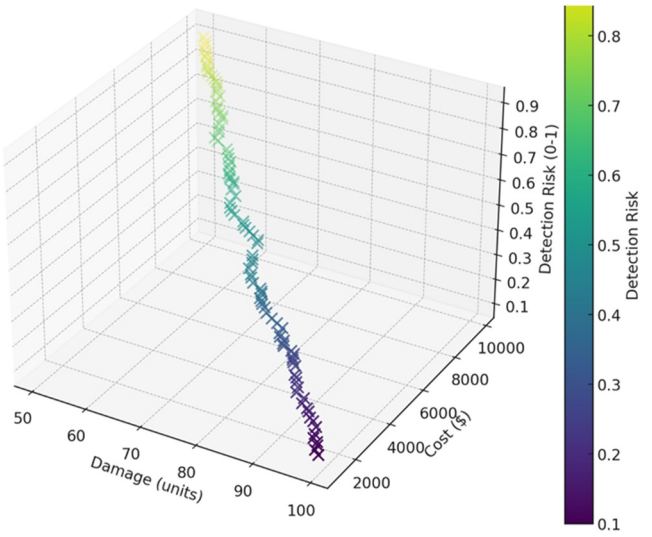

FIGURE 5 Pareto front: Trade-off between damage, cost, and detection risk in UAV strikes on smart grids. UAV, unmanned aerial vehicle.

showing how the combination of both factors can critically limit the UAV's capabilities. This visualisation underscores the need for careful mission planning when UAVs are deployed in challenging environments.

Figure 5 represents the Pareto front for the multi-objective optimisation of UAV strikes on smart grid infrastructure, focussing on three critical variables: damage inflicted on the grid, operational costs, and detection risk. The scatter plot shows how these objectives trade-off against each other in an NSGA-III optimisation framework. As observed, the damage inflicted on the grid, represented on the x-axis, ranges from 50 to 100 units, while the associated costs on the y-axis span from $1,000 to 10{,}000$. Each point on the plot is a non-dominated solution, meaning it balances these conflicting objectives as efficiently as possible. One key insight from the figure is that as damage increases, the cost also increases significantly. For example, achieving damage levels near 100 units incurs operational costs close to $10,000. On the other hand, UAV operations that inflict lower damage, around 50–60 units, can be executed at much lower costs, typically around $1500 to $3000. This trade-off highlights the significant financial resources needed to inflict severe damage on smart grid components, particularly when aiming to maximise the efficiency of UAV strikes. Another notable pattern is the relationship between detection risk and the other two variables. Higher damage levels tend to correlate with lower detection risks, shown by the colour gradient from light yellow (high detection risk) to dark blue (low detection risk). For example, UAV operations inflicting over 90 units of damage tend to have detection risks below 0.3, while lower-damage operations, inflicting around 50–60 units, often face detection risks of 0.7 or higher. This pattern suggests that more expensive and higher-damage strikes are generally more covert, possibly due to the UAVs' ability to avoid detection through more sophisticated strategies. These insights provide valuable information for balancing UAV strike efficiency, costs, and detection risks in real-world scenarios.

Figure 6 displays the convergence behaviour of the NSGA-III algorithm over 400 iterations, demonstrating how the objective value improves over time. The x-axis represents the number of iterations, while the y-axis shows the objective value in arbitrary units. Initially, the objective value decreases rapidly, indicating that the algorithm quickly finds better solutions. In the first 50 iterations, the objective value drops significantly from approximately 19 to around 8. This rapid early improvement is typical of NSGA-III, as it quickly explores the solution space to identify high-quality solutions in the initial generations. After about 100 iterations, the convergence rate slows, and the objective value stabilises. Between iterations 100 and 250, the objective value declines more gradually, from approximately 8 to 4. This phase reflects the algorithm's transition from exploration to exploitation, where the search for optimal solutions becomes more refined. The smaller improvements in this phase suggest that the NSGA-III algorithm is focussing on fine-tuning solutions rather than discovering entirely new ones. This trend indicates that the algorithm is converging towards an optimal set of trade-offs between conflicting objectives, such as minimising operational costs and maximising damage in UAV strikes on smart grids.

The heatmap in Figure 7 illustrates the distribution of damage across a 10×10 grid of components in a simulated smart grid system under UAV strikes. The colour gradient ranges from cool blue (indicating lower damage) to warm red (indicating higher damage), providing a visual representation of how certain grid components experience more severe impacts than others. The grid's central components show significantly higher damage, with values approaching 100, while damage diminishes towards the grid's edges, suggesting that central components are either more critical or more vulnerable to UAV strikes. The pattern of damage is Gaussian-like, where the

25152947, 2025, 1, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/sg2.70000 by Test, Wiley Online Library on [28/02/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

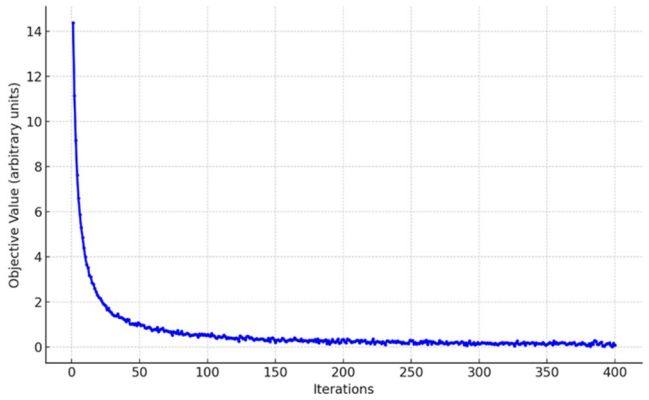

FIGURE 6 Convergence plot of NSGA-III algorithm performance over 400 iterations. NSGA-III, Non-dominated Sorting Genetic Algorithm III.

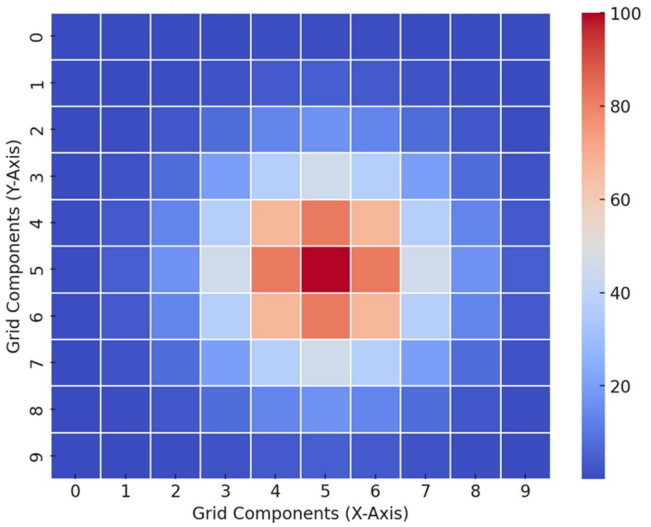

FIGURE 7 Heatmap of damage distribution across the grid.

highest damage is concentrated near the centre, and this gradually decreases as we move outward. This distribution could indicate that the central components represent key infrastructures, such as substations or transformers, which are more heavily targeted due to their critical roles in maintaining grid stability. The heatmap suggests that the components located at the edges of the grid experience less severe impacts, with damage values dropping to as low as 10–20. Such a pattern aligns with the strategic focus of UAV strikes, targeting the most impactful components for maximum disruption.

Figure 8 presents two 3D surface plots that demonstrate the relationship between flight time, payload capacity, and wind speed under two distinct scenarios. The *x*-axis represents the payload capacity in kilograms, ranging from 1 to 10 kg, while the *y*-axis represents wind speed, which varies from 0 to 30 mph. The *z*-axis shows the resulting flight time in minutes. Both plots reveal the expected trend: as payload capacity and wind speed increase, flight time decreases, indicating how these two factors directly affect UAV efficiency. In the first scenario (left plot), which uses a blue colour map, flight time is modelled with a logarithmic curve, reflecting a smooth decline as the payload increases, with wind speed having a more consistent effect across the range. In the second scenario (right plot), which uses a green colour map, the decline in flight time follows a square root pattern, where the relationship between increasing payload and flight time is less pronounced at lower payloads but becomes sharper as the payload grows heavier. For instance, at a payload of 2 kg and wind speed of 10 mph, the flight time is approximately 95 min in the second scenario, compared to around 100 min in the first scenario. This difference becomes more substantial at higher payloads: at 8 kg and the same wind speed, the flight time drops to around 50 min in the second scenario and 60 min in the first. These differences highlight how slight variations in the operational environment or drone configuration can have significant effects on mission endurance. The impact of wind speed is also evident in both plots. At higher wind speeds (e.g., 20–30 mph), flight times drop sharply for heavier payloads. For example, at a payload of 10 kg and a wind speed of 25 mph, flight time falls

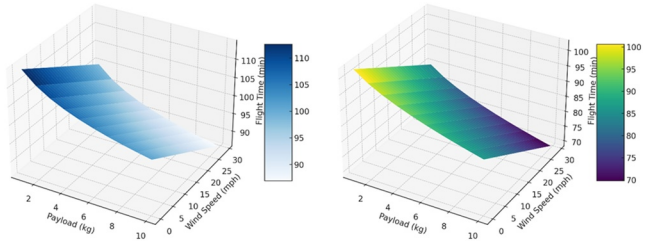

FIGURE 8 3D surface plots of flight time versus wind speed and payload under two scenarios.

below 40 min in both scenarios. This emphasises the importance of accounting for environmental factors in UAV mission planning, as higher wind speeds can drastically reduce operational efficiency. The two plots provide a comprehensive comparison of how different factors interact to influence UAV performance, giving operators insights into the trade-offs between payload, wind conditions, and flight time.

6 | CONCLUSION

This paper presents a comprehensive framework for optimising UAV-based attacks on smart grid infrastructures, focusing on damage maximisation, cost minimisation, and detection risk reduction. The proposed methodology combines the NSGA-III multi-objective optimisation algorithm with game-theoretic principles, providing a robust tool for grid defenders and attackers to anticipate each other's strategies in a dynamic environment. The results demonstrate that UAVs can exploit smart grid vulnerabilities efficiently, with trade-offs between the three key objectives. Through our case studies, we observed that UAV strikes on critical grid components, such as substations and transformers can inflict damage ranging from 50 to 100 units, depending on the UAV's operational efficiency and environmental conditions. For example,

25152947, 2025, 1, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/sg2.70000 by Test, Wiley Online Library on [28/02/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

high-damage scenarios, where damage levels approached 100 units, were associated with increased operational costs of up to $10,000 per mission. However, more conservative strikes, inflicting around 50–60 units of damage, could be executed at lower costs, typically between $1500 and $3000. This provides a clear trade-off between the financial resources required for high-damage operations and the more cost-effective, lower-damage strategies. In addition, the NSGA-III algorithm successfully generated a set of Pareto-optimal solutions, balancing damage, cost, and detection risk. The Pareto front showed that UAV strikes with lower detection risks (below 0.3) were typically associated with higher operational costs and higher damage, whereas UAV operations with detection risks exceeding 0.7 were more cost-efficient but inflicted less damage, averaging around 55 units. This insight highlights the challenge of maintaining stealth while maximising damage, especially in well-defended grid environments.

Furthermore, the integration of dynamic environmental conditions into the optimisation model, including wind speeds and temperatures, proved critical in assessing UAV performance. The flight time of UAVs, for example, could be reduced by up to 50% when wind speeds exceeded 20 mph, with flight times dropping from 90 min to as low as 45 min under heavier payloads (5 kg). These environmental factors must be carefully considered in UAV mission planning, as they significantly impact both the operational endurance and success rates of UAV strikes. Overall, this research contributes significantly to the understanding of UAV threats to smart grid systems by introducing a robust optimisation framework that balances multiple conflicting objectives. The application of the NSGA-III algorithm, combined with game-theoretic insights, provides a novel and practical approach for grid operators to strengthen defences against emerging UAV threats. Future work may focus on integrating real-world grid data and expanding the framework to address more complex grid topologies and attack scenarios.

AUTHOR CONTRIBUTIONS

Alexis Pengfei Zhao contributed to the conceptualisation of the research framework and methodology, the development of the mathematical models and optimisation techniques, and the draughting and revising of the manuscript, including the preparation of figures and tables. Zhao also supervised the overall research process and validated the results.

Shuangqi Li, as the corresponding author, was responsible for communication with the journal and took the lead in data analysis and interpretation. Li oversaw the simulation design and case study implementation and provided the final review and approval of the manuscript for submission.

Da Huo contributed to the literature review and identification of research gaps, supported data preparation and experimental setup, and provided feedback on the manuscript, assisting with revisions.

Mohannad Alhazmi assisted in the conceptualisation, particularly in the cyber-resilience aspect, provided critical insights into the application of methodologies, and reviewed and edited the manuscript for technical accuracy and clarity.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the support provided by the Researchers Supporting Project (Project number: RSPD2025R635), King Saud University, Riyadh, Saudi Arabia.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ORCID

Alexis Pengfei Zhao https://orcid.org/0000-0001-8751-9750

REFERENCES

1. Kumar, B.V., Farhan, M.A.A.: Optimal simultaneous allocation of electric vehicle charging stations and capacitors in radial distribution network considering reliability. J. Mod. Power Syst. Clean Energy, 1–12 (2024). https://doi.org/10.35833/MPCE.2023.000674
2. Li, S., et al.: Online battery-protective vehicle to grid behavior management. Energy 243, 123083 (2022/03/15/ 2022). https://doi.org/10.1016/j.energy.2021.123083
3. Zhao, P., et al.: A social computing method for energy safety. J. Saf. Sci. Resilience 5(1), 64–82 (2024/01/12/ 2024). https://doi.org/10.1016/j.jnlssr.2023.12.001
4. Puchalski, R., Giernacki, W.: UAV fault detection methods, state-of-the-art. Drones 6(11), 330 (2022). https://doi.org/10.3390/drones6110330
5. Wu, J., et al.: Path planning for solar-powered UAV in urban environment. Neurocomputing 275, 2055–2065 (2018/01/31/ 2018). https://doi.org/10.1016/j.neucom.2017.10.037
6. Ly, B., Ly, R.: Cybersecurity in unmanned aerial vehicles (UAVs). J. Cyber Secur. Technol. 5(2), 120–137 (2021). https://doi.org/10.1080/23742917.2020.1846307
7. He, D., et al.: An effective countermeasure against UAV swarm attack. IEEE Network 35(1), 380–385 (2020). https://doi.org/10.1109/mnet.011.2000380
8. Gamage, D., et al.: Distributed consensus controlled multi-battery-energy-storage-system under denial-of-service attacks. J. Energy Storage 86, 111180 (2024/05/01/ 2024). https://doi.org/10.1016/j.est.2024.111180
9. Du, D., et al.: Distributed security state estimation-based carbon emissions and economic cost analysis for cyber–physical power systems under hybrid attacks. Appl. Energy 353, 122001 (2024/01/01/ 2024). https://doi.org/10.1016/j.apenergy.2023.122001
10. Alasali, F., et al.: Smart grid resilience for grid-connected PV and protection systems under cyber threats. Smart Cities 7(1), 51–77doi (2023). https://doi.org/10.3390/smartcities7010003
11. Chamola, V., et al.: A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques. Ad Hoc Netw. 111, 102324 (2021). https://doi.org/10.1016/j.adhoc.2020.102324
12. Zhang, X., Chandramouli, K.: Critical infrastructure security against drone attacks using visual analytics. In: Tzovaras, D., et al. (eds.) Computer Vision Systems, pp. 713–722. Springer International Publishing, Cham (2019)
13. Aggarwal, S., Kumar, N.: Path planning techniques for unmanned aerial vehicles: a review, solutions, and challenges. Comput. Commun. 149, 270–299 (2020). https://doi.org/10.1016/j.comcom.2019.10.014
14. Yang, L., et al.: A literature review of UAV 3D path planning. In: Proceeding of the 11th World Congress on Intelligent Control and Automation, pp. 2376–2381. IEEE (2014)
15. Silva Arantes, J.d., et al.: Heuristic and genetic algorithm approaches for UAV path planning under critical situation. Int. J. Artif. Intell. Tool. 26(01), 1760008 (2017). https://doi.org/10.1142/s0218213017600089

25152947, 2025, 1, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/sg2.70000 by Test, Wiley Online Library on [28/02/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

16. Deb, K., et al.: A fast and elitist multiobjective genetic algorithm: NSGA-II. IEEE Trans. Evol. Comput. 6(2), 182–197 (2002). https://doi.org/10.1109/4235.996017
17. Singh, M.K., et al.: Multi-objective NSGA-II optimization framework for UAV path planning in an UAV-assisted WSN. J. Supercomput. 79(1), 832–866 (2023/01/01 2023). https://doi.org/10.1007/s11227-022-04701-2
18. Deb, K., Jain, H.: An evolutionary many-objective optimization algorithm using reference-point-based nondominated sorting approach, part I: solving problems with box constraints. IEEE Trans. Evol. Comput. 18(4), 577–601 (2013). https://doi.org/10.1109/tevc.2013.2281535
19. Zhou, B., et al.: Multi-objective optimal operation of coastal hydro-electrical energy system with seawater reverse osmosis desalination based on constrained NSGA-III. Energy Convers. Manag. 207, 112533 (2020). https://doi.org/10.1016/j.enconman.2020.112533
20. Ai, Y., et al.: The optimization of reactive power for distribution network with PV generation based on NSGA-III. CPSS Trans. Power Electron. Appl. 6(3), 193–200 (2021). https://doi.org/10.24295/CPSSTPEA.2021.00017
21. Trotta, D., et al.: Optimal tuning for robust control of a small fixed-wing UAV. In: AIAA Scitech 2021 Forum. AIAA SciTech Forum: American Institute of Aeronautics and Astronautics (2021)
22. Zhao, A.P., et al.: Electric vehicle charging planning: a complex systems perspective. IEEE Trans. Smart Grid, 1-1 (2024). https://doi.org/10.1109/TSG.2024.3446859
23. Tsao, K.-Y., Girdler, T., Vassilakis, V.G.: A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. Ad Hoc Netw. 133, 102894 (2022). https://doi.org/10.1016/j.adhoc.2022.102894

How to cite this article: Pengfei Zhao, A., et al.: Unmanned aerial vehicles versus smart grids. IET Smart Grid. e70000 (2025). https://doi.org/10.1049/stg2.70000

25152947, 2025, 1, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/stg2.70000 by Test, Wiley Online Library on [28/02/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

https://dspace.org/

Unmanned aerial vehicles versus smart grids

Pengfei Zhao, Alexis; Li, Shuangqi; Huo, Da; Alhazmi, Mohannad

2025-01
Institution of Engineering and Technology (IET)
https://doi.org/10.1049/stg2.70000
Pengfei Zhao A, Li S, Huo D, Alhazmi M. (2025) Unmanned aerial vehicles versus smart grids. IET Smart Grid, Volume 8, Issue 1, January/December 2025, Article number e70000

Downloaded from a DSpace repository. https://dspace.org/