Bulgarian Academy of Sciences. Space Research and Technology Institute.
Aerospace Research in Bulgaria. 38, 2026, Sofia

DOI: https://doi.org/10.3897/arb.v38.e23

ADAPTIVE ALGORITHMS FOR ENERGY RESOURCE OPTIMIZATION IN ELECTRONIC COUNTERMEASURES TO UAV SWARM ATTACKS

Filip Iliev, Georgi Sotirov

Space Research and Technology Institute – Bulgarian Academy of Sciences
e-mail: fgi@mail.bg; GSotirov@space.bas.bg

Keywords: *Counter-UAV systems, drone swarms, electromagnetic compatibility, adaptive jamming, electronic countermeasures, AI-based security*

Abstract

Coordinated swarm attacks with unmanned aerial vehicles (UAVs) require a reassessment of classical electronic countermeasure (ECM) approaches. Broadband jamming methods are limited by high energy consumption and insufficient spectral selectivity and controllability. These limitations motivate the development of algorithmic models in which counteraction is formulated as an optimisation problem rather than implemented as static emission. This paper presents an approach to countering coordinated drone swarm attacks against high-value assets based on an algorithm for adaptive control of electronic countermeasure (ECM) signals. A real-time decision-making model is proposed to optimise the energy usage of jamming systems by selectively impacting the command and navigation channels of the attacking platforms.

Introduction

The increasing availability and rapid technological evolution of unmanned aerial vehicles (UAVs) are reshaping the modern security paradigm. At present, one of the most significant threats is posed by so-called UAV swarms – groups of drones operating in a coordinated manner to saturate and overwhelm defence systems [4]. It has been established that the use of conventional broadband jamming in urban environments leads to unacceptable levels of electromagnetic pollution, potentially disrupting critical services such as 5G networks, GNSS navigation, and specialised security communications.

In this context, developing algorithms that optimise transmitted power while ensuring electromagnetic compatibility (EMC) becomes a priority research direction in contemporary security and defence technologies.

To address this challenge, the paper proposes an adaptive algorithm for controlling electronic countermeasure (ECM) signals based on EMC principles. Unlike conventional broadband jamming techniques, the proposed model applies dynamic target prioritisation and selective spectral suppression using notch filtering. This approach enables effective disruption of UAV command and navigation links while minimising interference with critical communication infrastructure and legitimate radio networks within the protected area.

1. System Architecture of the Detection and Countermeasure Framework

For this study, a multi-layer counter-UAV architecture is considered, based on the “Antidrone” system concept. The framework is organised into three functionally interconnected layers [6]:

1. *Sensor Layer* – This layer employs multi-sensor data fusion using RF scanners and radar subsystems. Radar sensors provide kinematic parameters such as range, azimuth, and velocity, while RF scanners identify the frequency profile and control protocol characteristics of the detected UAVs.
2. *Processing and Decision Layer* – At this level, incoming sensor data are aggregated and processed, and the decision-making logic is executed. A dynamic threat priority score is computed for each detected target, and an appropriate countermeasure strategy is selected. Instead of activating all transmitters simultaneously, the system calculates the required transmission power and determines the spatial sectors that must be covered, thereby improving energy efficiency and spectral discipline.
3. *Execution Layer* – This layer consists of multiband transmitters with directional antennas and frequency-selective emission capability. Advanced techniques such as beamforming and notch filtering are applied, which are fundamental for maintaining electromagnetic compatibility (EMC) while performing effective electronic countermeasures.

The hierarchical organisation of the architecture, illustrated in Fig. 1, enables clear functional separation between detection, decision, and execution processes. Sensor data from radar and RF subsystems are consolidated within a central decision module, allowing parallel processing and reduced reaction time. This structure supports reliable delivery of software-defined transmission parameters to the antenna subsystems and enables rapid adaptive response under dynamic threat conditions.

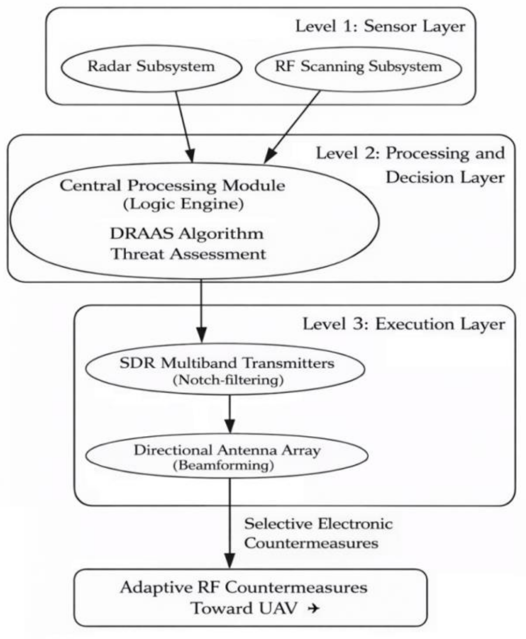

Fig. 1. Hierarchical architecture of the counter-UAV detection and electronic countermeasure system

2. Theoretical Model of the Adaptive Control Algorithm

The study examines the operation of the DRAAS (Dynamic Resource Allocation Anti-Swarm) algorithm, designed to transform a static jamming system into a dynamic, adaptive countermeasure unit. The operational logic is structured as a closed-loop adaptive process consisting of sequential evaluation, selective action, and feedback-based verification.

2.1. Algorithmic Logic and Threat Prioritisation

At the core of the intelligent control mechanism lies a closed-loop decision-support cycle whose primary function is the accurate assessment and prioritisation of detected targets. For each UAV within the swarm, the algorithm computes a dynamic threat coefficient (T_q) based on a weighted combination of key parameters:

(1) $$T_q = w_1 \cdot \frac{V_{app}}{D} + w_2 \cdot S_{int} \ ,$$

approach velocity V_{app}, distance to the protected perimeter D, and received signal intensity S_{int} (serving as an indicator of command-link strength). By applying configurable weighting factors w_1, w_2, the system can automatically prioritise highly dynamic and high-risk targets – for example, assigning greater weight to rapidly approaching objects. As a result, maximum energy resources are directed toward the most critical threats (those with the highest T_q), while lower-risk targets remain under secondary monitoring with reduced countermeasure intensity.

The logical sequence of the algorithm unfolds in three main phases:

1. *Spectral Analysis Phase* – Immediately after detection, the system performs rapid spectrum scanning to identify active legitimate frequencies within the protected area. Based on this scan, protected spectral regions (guard bands) are defined to prevent interference with authorised communications.

2. *Execution Phase* – Using the computed threat coefficient T_q, the algorithm activates selective transmission by combining frequency-domain notch filtering with spatially selective beamforming. Countermeasure energy is therefore concentrated only where and when it is required.

3. *Verification Phase* – RF sensors continuously evaluate the target response in real time (failsafe-state monitoring). Upon confirmation of successful neutralisation or link disruption, transmission resources are automatically reallocated to the next highest-priority target within the swarm [1]. This feedback loop ensures efficient resource reuse and prevents unnecessary prolonged emission.

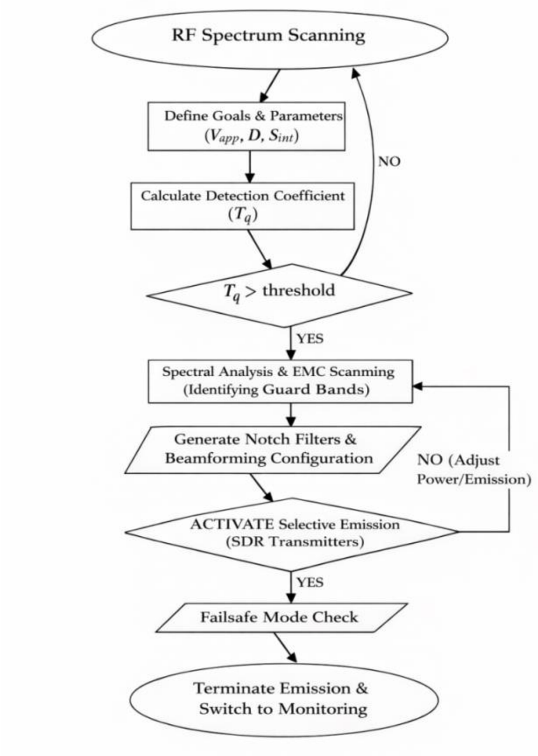

Fig. 2. Adaptive decision-making cycle of the DRAAS algorithm

The graphical representation of the algorithm in Fig. 2 illustrates the dynamic real-time threat-processing cycle. The system operates in a continuous monitoring mode and transitions to an active emission phase only when the critical threshold of the threat coefficient T_q is exceeded. A key element of the algorithmic logic is the introduction of an intermediate spectral analysis stage that precedes signal transmission. This verification step ensures that countermeasures are not initiated before protective guard bands for authorised communications have been properly defined. Such a closed-loop feedback mechanism enables precise adjustment of the countermeasure effect until complete target neutralisation is achieved, while minimising the risk of software conflicts and unnecessary energy allocation within the system.

2.2. Frequency-Selective Isolation Algorithm (EMC-Notch Method)

The primary challenge in countering UAV threats is not merely signal suppression itself, but the prevention of electromagnetic degradation affecting legitimate communication systems operating within the same spectrum – including Wi-Fi networks, Bluetooth devices, cellular infrastructure, and specialised operational radio services.

To achieve full electromagnetic compatibility (EMC), the proposed approach applies a form of "surgical" jamming. Instead of emitting conventional wideband noise across the entire band, the algorithm adaptively synthesises spectral notches around authorised signals. This enables dynamic spectral isolation, allowing security and operational communications to remain functional while UAV command-and-control links are selectively disrupted through digitally synthesised interference generated in real time [2].

The process is implemented in four principal stages:

1. *Spectral Monitoring and Identification* – The RF scanner performs continuous real-time spectrum monitoring. It reports active legitimate frequencies within the protected area (for example, a local Wi-Fi channel centre frequency). These signals are classified as protected spectrum users.

2. *Dynamic Notch Filter Computation* – The algorithm calculates protective guard bands with adaptive bandwidth around each identified legitimate signal. The guard band width Δf is selected to ensure sufficient isolation margins and to eliminate the risk of harmful interference [7].

3. *Adaptive Spectrum Shaping* – The transmitter generates controlled broadband interference across the target band (for example, within the 2.4 GHz range), while digitally carving out spectral notches at the frequencies reserved for legitimate communications. This produces a shaped emission spectrum that preserves authorised channels while suppressing hostile control links.

4. *Dynamic Spectrum Tracking* – The system performs high-speed continuous monitoring to detect frequency-hopping behaviour and other rapid spectral changes. When such shifts are detected, the notch filters are repositioned in near real time, ensuring that protected spectral windows continuously follow legitimate signals regardless of their frequency agility.

The effect of the proposed algorithm on the radio-frequency spectrum is illustrated in Fig. 3.

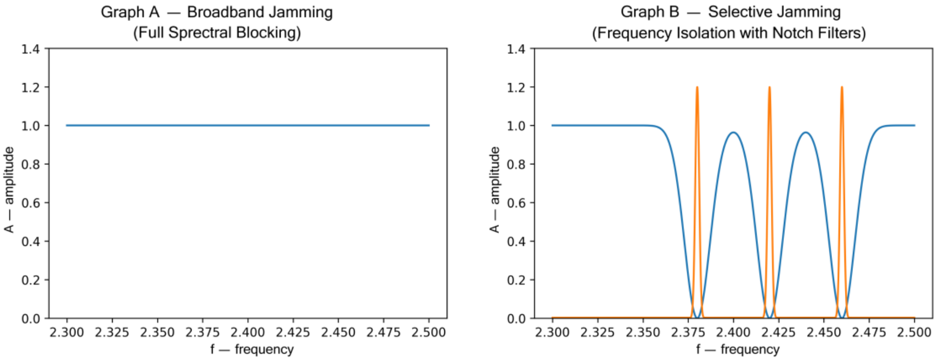

Fig. 3. Comparative spectral diagrams of radio-frequency impact

The visual comparison of the energy spectrum in Fig. 3 demonstrates the practical realisation of the frequency-isolation concept. Under conventional broadband jamming (Graph A), full suppression across the operating band is observed. In contrast, the adaptive model (Graph B) clearly reveals software-synthesised notch filters within the emission spectrum. These precisely defined spectral notches allow legitimate signals within the protected area to preserve their integrity and amplitude, even under active electronic countermeasure conditions. The presented diagrams confirm the algorithm's ability to concentrate energy resources exclusively on UAV command-and-control links while maintaining reliable protective guard bands for critical infrastructure communications.

3. Comparative Analysis of Operational Effectiveness and Energy Characteristics

The effectiveness of the proposed adaptive model is evaluated through comparison with conventional broadband electronic countermeasure techniques. The comparative assessment focuses on electromagnetic compatibility, spectral purity, energy efficiency, operational resilience under swarm attack conditions, and response autonomy. The results of the theoretical and architectural analysis are summarised in Table 1.

Table 1. Comparative Analysis of Key Performance Indicators

Performance Indicator	Broadband Jamming	Adaptive DRAAS Model	Contribution
Electromagnetic Compatibility (EMC)	Low – full disruption of Wi-Fi, cellular, and operational radio services is likely.	High – notch filtering enables isolation of legitimate signals.	Preservation of more than 85% of protected network capacity.
Spectral Purity	Low – generates wideband electromagnetic noise across the operating range.	High – selective spectral suppression using software-defined radio techniques.	Minimisation of frequency collisions in dense electromagnetic environments.
Energy Efficiency	Constant maximum power consumption (P_{max}), with increased thermal stress and reduced hardware longevity.	Dynamic power control based on the computed threat coefficient T_q .	Estimated energy savings of approximately 40–50% during sustained operation.
Resilience Under Swarm Attack Conditions	Risk of overload due to lack of target prioritisation.	Automatic resource focusing on high-priority or leader nodes within the swarm.	Improved neutralisation capability against multiple simultaneous targets.
Response Autonomy	Manual operator configuration of frequency ranges and emission parameters.	Cognitive adaptation to real-time spectral conditions with self-adjusting logic.	Reduction of response time to the millisecond scale.

The comparison indicates that the proposed algorithm achieves a practical balance between countermeasure effectiveness and infrastructure preservation. Reduced energy consumption directly improves hardware reliability and supports longer autonomous operating cycles, which is critical for continuous protection scenarios.

4. Prospects for Artificial Intelligence Integration for Autonomous Cognitive Control

In the context of rapidly evolving autonomous UAV technologies, the future development of countermeasure systems is closely linked to the integration of cognitive modules based on artificial intelligence (AI) and machine learning (ML). The incorporation of such methods enables a transition from operator-defined response scenarios toward fully autonomous, real-time adaptive protection. Three principal development directions can be identified.

- **Autonomous Signal Signature Recognition (RF Fingerprinting)**

Instead of relying solely on static libraries of known frequency profiles and protocols, AI-based models enable deep signal decomposition and feature extraction. By applying neural network architectures, the system can identify previously unknown or modified control protocols based on micro-anomalies and fine-grained spectral features. This capability supports detection of zero-day or obfuscated command links that may not be recognised by conventional RF scanning techniques [8].

- **Predictive Energy Resource Management**

Predictive analytics models enable forward-looking allocation of countermeasure energy resources during swarm attack scenarios. An AI module can estimate likely trajectories and behavioural patterns of UAV groups and pre-position directional countermeasure beams accordingly. Through predictive beam steering and timing optimisation, countermeasure energy can be concentrated within a narrow spatial sector milliseconds before a target enters a critical zone. This approach reduces total emission time and prevents unnecessary load on high-power amplifier stages.

- **Self-Adaptive Electromagnetic Compatibility Control (Self-Healing EMC)**

One of the most significant advantages of AI integration is the ability to construct and continuously update dynamic spectral maps of the protected environment. The system can autonomously identify and classify legitimate communication signals – including next-generation wireless and broadband services – and maintain real-time protected-frequency whitelists. This reduces operator dependency and minimises configuration errors in notch filter placement. As a result, stable electromagnetic compatibility can be maintained even in rapidly changing and congested spectral conditions [5].

Conclusion

The results of the study demonstrate a substantial improvement in counter-UAV protection effectiveness under high-density aerial threat scenarios. The proposed algorithm replaces static broadband jamming with a dynamic, resource-optimised model of selective electronic countermeasures, directly addressing the key practical constraint in modern systems – the trade-off between required transmission power and electromagnetic compatibility [3].

The developed DRAAS algorithm introduces a formalised framework for threat prioritisation, frequency-selective spectral isolation, and a closed-loop verification process with real-time feedback. The combined application of these mechanisms leads to measurable gains in energy efficiency, reduced spectral interference, and increased resilience against large-scale swarm attacks. The integration of optimisation-driven control logic, EMC-oriented spectral shaping, and adaptive transmission management forms a unified architectural basis for algorithmically controlled electronic countermeasure systems.

Future extension through AI-based modules for signal signature recognition, predictive resource allocation, and autonomous EMC adaptation outlines a transition toward cognitive counter-UAV platforms with a high degree of operational autonomy. This positions the proposed approach as a sustainable technological foundation for next-generation intelligent electronic protection systems based on balanced active intervention and controlled spectral impact.

References

1. Adamy, D. L. *EW 105: Space Electronic Warfare*. Norwood, Artech House, 2024.
2. Bhattacharya, S., S. Sahu. Cognitive Radio Countermeasures: AI-Driven Signal Interference Mitigation. *Journal of Electronic Defense*, 2025.
3. European Union Aviation Safety Agency. *Regulatory Framework for Counter-UAS Operations in Urban Environments*. Cologne, EASA Publications, 2025/2026.
4. IEEE. Special Issue on Drone Swarm Counter-Measures: Deep Learning Approaches. *IEEE Xplore Digital Library*, 2025.
5. ITU. *Report on Electromagnetic Compatibility (EMC) in the Era of 6G and Autonomous Systems*. Geneva, ITU Publications, 2026.
6. Sotirov, G., R. Dimitrov, E. Hubenov. Investigation of the Effectiveness of a Multi-Sensor Drone Detection and Countermeasure System Based on the Results of a Flight Experiment. *SES'24 – Space, Ecology, Safety*, Sofia, 2024, 95–103.
7. Wang, L., et al. Adaptive Beamforming for Counter-UAV Systems: A Real-Time Optimization Approach. *Sensors Journal*, 2026.
8. Zhu, Y., G. Martinez. Neural Networks for Autonomous Jamming Strategy Synthesis. *International Journal of Cyber and Electronic Warfare,* 2025.

АЛГОРИТМИ ЗА АДАПТИВНО УПРАВЛЕНИЕ НА ЕНЕРГИЙНИЯ РЕСУРС ПРИ РАДИОЕЛЕКТРОННО ПРОТИВОДЕЙСТВИЕ НА ГРУПОВИ АТАКИ ОТ БЛА

Ф. Илиев, Г. Сотиров

Резюме

Координираните атаки с рояци БЛА налагат преосмисляне на класическите подходи за радиоелектронно противодействие. Основните ограничения на широколентовите методи за заглушаване се изразяват не само във високата енергийна консумация, но и в липсата на спектрална селективност и контролируемост на въздействието. Това налага разработването на алгоритмични модели, при които противодействието се реализира като оптимизационен процес, а не като статично излъчване. В статията се изследва проблемът с нарастващата заплаха от координирани атаки с дронове (рояци) срещу обекти с висока степен на значимост. Фокусът е върху разработването на алгоритъм за адаптивно управление на сигналите за радиоелектронно противодействие. Предлага се модел за вземане на решения в реално време, който оптимизира енергийния ресурс на системите за заглушаване чрез селективно въздействие върху каналите за управление и навигация на атакуващите платформи.