International Journal of Advanced Engineering and Management Research

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Electromagnetic Countermeasures Against Autonomous Drone Swarms: High-frequency Field-based Disruption and Control Override Systems

[1]Dr. Shankar Subramanian Iyer, Faculty, Business; Westford University College, Sharjah, UAE. ORCID: 0000-0003-0598-9543,

[2]Dr. Zainab Toyin Jagun; School of Built Environment, Engineering and Computing; Leeds Beckett University, UK

ORCID: 0000-0002-7441-7138, Email: Z.T.

[3]Abdul Jalil Mahama; Independent PhD Researcher; Faculty; Economics; Department; Finance and Credit; National University of Uzbekistan named after Mirzo Ulugbek, ORCID: 0000-0002-8622-1714,

[4]Dr. Fitriyah Razali; Faculty; Built Environment and Surveying; Department: Real Estate Management Universiti Teknologi Malaysia, ORCID: 0000-0002-4067-2245,

[5]Dr Brinitha Raji, Faculty, Global Business Studies, DKP, Dubai, Orcid no: https://orcid.org/0000-0002-8633-0099,

[6]Prof. Rajesh Arora, Senior Faculty, Westford University College, Al Khan, Sharjah, Orcid no: 0000-0002-0736-5315.

[7]Dr Raman Subramanian, Associate Dean, Westford University College, Al Tawuun, Sharjah, UAE,

ORCID No. 0000-0002-7175-3187.

doi.org/10.51505/ijaemr.2025.1507 URL: http://dx.doi.org/10.51505/ijaemr.2025.1507

Received: Oct 23, 2025 Accepted: Oct 29, 2025 Online Published: Nov 07, 2025

Abstract

The proliferation of autonomous drone swarms presents unprecedented security challenges that conventional kinetic countermeasures cannot adequately address. This research investigates the application of high-frequency electromagnetic fields (HF-EMF) operating in the 2.4-5.8 GHz range for disrupting and potentially overriding drone swarm communication and control systems. Through systematic analysis of electromagnetic interference patterns and signal propagation characteristics, The Research Study examines the feasibility of non-kinetic neutralization techniques that can selectively target drone communication protocols while minimizing collateral interference with civilian infrastructure.

This investigation encompasses the theoretical foundations of electromagnetic disruption mechanisms, including RF signal jamming, GPS spoofing, and command link interference. The study analyzes the vulnerability profiles of common drone communication protocols, including Wi-Fi (IEEE 802.11), Bluetooth, and proprietary control links, under various electromagnetic field intensities ranging from 10-100 W/m². The research identifies critical frequency bands

Vol. 10, No. 06; 2025

ISSN: 2456-3676

where drone systems exhibit maximum susceptibility to electromagnetic interference while maintaining operational safety for surrounding electronic systems.

Key findings indicate that targeted electromagnetic fields can effectively disrupt drone swarm coordination by interfering with inter-drone communication protocols, causing formation breakdown and mission failure. The study reveals that swarms operating on distributed consensus algorithms show vulnerability to synchronized electromagnetic pulses, with disruption rates exceeding 85% when exposed to properly calibrated HF-EMF systems. Additionally, the Research Study demonstrates the theoretical possibility of signal override techniques that could redirect individual drones within a swarm, though practical implementation requires precise frequency matching and protocol analysis.

The research contributes to the growing field of counter-drone technologies by providing a comprehensive framework for understanding electromagnetic-based countermeasures. This study presents a systematic analysis of the technical requirements, operational constraints, and effectiveness metrics for HF-EMF systems designed to counter drone swarms. The findings have significant implications for defence applications, critical infrastructure protection, and public safety operations, where unauthorized drone activity poses substantial risks

Keywords: C-UAV systems; drone swarm defence; Electromagnetic countermeasures; RF jamming; signal disruption.

1. Introduction

The rapid advancement and democratization of unmanned aerial vehicle (UAV) technology have fundamentally altered the security landscape across military, civilian, and critical infrastructure domains. Modern drone swarms, characterized by their distributed decision-making capabilities and coordinated autonomous behavior, present a paradigm shift from traditional single-vehicle threats to complex, multi-vector attack scenarios that challenge existing defence frameworks (Shakhatreh et al., 2019); (Sutriadi, Hadicahyono and Drestalita, 2025). These systems leverage sophisticated algorithms for collective intelligence, enabling them to operate with minimal human oversight while maintaining tactical flexibility and mission redundancy (Honig et al., 2018).

Contemporary drone swarms typically employ decentralized control architectures that distribute command and control functions across multiple nodes, making them inherently resistant to single-point failures and traditional interception methods (Tahir et al., 2019). The integration of artificial intelligence and machine learning algorithms has further enhanced their autonomous capabilities, allowing swarms to adapt their behavior in real-time based on environmental conditions and threat responses (Harvey and O'Young, 2019). This technological evolution has created a security gap where conventional air defence systems, designed primarily for larger, more predictable targets, prove inadequate against coordinated micro-UAV attacks (Zhang et al., 2024).

Vol. 10, No. 06; 2025

ISSN: 2456-3676

The economic accessibility of drone technology compounds this security challenge. Commercial off-the-shelf (COTS) components enable the construction of capable drone swarms at relatively low cost, making this technology available to both state and non-state actors with varying levels of technical sophistication (Liaskos et al., 2018); (Berawi, 2022). Recent incidents, including the 2019 attacks on Saudi Aramco facilities and disruptions at major international airports, demonstrate the real-world impact of drone-based threats and the limitations of existing countermeasures (Hubbard and Reed, 2019); (Sabbagh, 2018)

Traditional kinetic countermeasures, including interceptor drones, directed-energy weapons, and projectile systems, face significant operational constraints when deployed against swarm targets. These limitations include engagement time delays, ammunition capacity restrictions, collateral damage risks in populated areas, and cost-effectiveness concerns when confronting large numbers of low-value targets (Michel, 2019). Furthermore, kinetic solutions often prove ineffective against distributed swarms that can absorb losses while maintaining mission capability through redundancy and adaptive behavior (Scharre, 2018).

Non-kinetic approaches, particularly those based on electromagnetic interference, offer several advantages over conventional countermeasures. Electromagnetic countermeasures can potentially engage multiple targets simultaneously, operate at the speed of light, provide repeatable engagement capability without physical ammunition, and offer scalable response options from temporary disruption to complete system override (Gettinger, 2020). However, the effective implementation of such systems requires precise understanding of target vulnerabilities, careful consideration of electromagnetic spectrum management, and sophisticated signal processing capabilities.

This research addresses the critical knowledge gap in understanding how high-frequency electromagnetic fields can be systematically applied to disrupt and potentially control autonomous drone swarms. The Research Study focuses specifically on the frequency ranges commonly used for drone communication and control (2.4-5.8 GHz), examining both the theoretical foundations and practical considerations for implementing electromagnetic countermeasures in real-world scenarios (Nguyen et al., 2024).

The primary objectives of this investigation are:

(1) to analyze the electromagnetic vulnerability profiles of common drone communication protocols,
(2) to evaluate the effectiveness of targeted RF interference against swarm coordination mechanisms,
(3) to assess the feasibility of signal override techniques for drone control system compromise, and
(4) to examine the operational constraints and safety considerations for deploying HF-EMF countermeasures in civilian environments.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

2. Literature Review and Theoretical Grounding

2.1 Evolution of Drone Swarm Technologies

The concept of coordinated autonomous vehicle operation has evolved significantly from early formation flying demonstrations to sophisticated swarm intelligence implementations. Pioneering work by Reynolds (Reynolds, 1987) on flocking algorithms established the mathematical foundations for distributed coordination, which have been adapted and enhanced for UAV applications. Modern drone swarms implement consensus algorithms that enable collective decision-making without centralized control, creating robust systems capable of maintaining operational effectiveness despite individual unit failures (Olfati-Sabre, Fax and Murray, 2007); (Chen et al., 2024)

Recent advances in swarm robotics have focused on improving scalability, robustness, and mission adaptability. Research by Schranz et al. (2020) demonstrates how bio-inspired algorithms can be applied to create self-organizing drone networks capable of complex coordinated behaviors. These developments have been parallel by improvements in miniaturization, battery technology, and communication systems that enable practical deployment of large-scale drone swarms (Floreano and Wood, 2015; Rodriguez et al., 2025).
The military applications of drone swarms have received considerable attention, with several nations developing swarm-capable systems for reconnaissance, electronic warfare, and precision strike missions. The U.S. Department of Defence's Perdix program and China's demonstrated capabilities in large-scale drone formations illustrate the strategic importance placed on this technology (U.S. Department of Defence, 2017); Gady, 2017). However, the dual-use nature of drone swarm technology means that similar capabilities are increasingly accessible to civilian and potentially hostile actors.

2.2 Current Counter-UAV Technologies

Existing counter-UAV systems can be broadly categorized into kinetic and non-kinetic approaches, each with distinct advantages and limitations. Kinetic systems, including conventional weapons, interceptor drones, and capture nets, offer high reliability against individual targets but face scalability challenges when confronting swarm attacks (D'Innocenzo, Smarra and Di Benedetto, 2016). The cost per engagement often exceeds the value of the target, creating an unfavorable economic exchange ratio (Gettinger and Michel, 2015).

Non-kinetic approaches encompass a range of technologies including RF jammers, GPS spoofers, high-power microwave systems, and cyber warfare techniques. Commercial RF jammers operating in ISM bands (2.4 GHz, 5.8 GHz) have shown effectiveness against individual drones but often lack the sophistication required for selective targeting and swarm engagement (Shin et al., 2012). Military-grade systems offer improved capabilities but are typically restricted from civilian use due to spectrum management concerns (Federal Communications Commission, 2016).

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Recent research has explored the application of machine learning techniques to improve counter-UAV system effectiveness. Work by Shi et al. (2018) demonstrates how pattern recognition algorithms can be used to identify and classify drone threats, enabling more targeted countermeasure deployment. However, the adversarial nature of the counter-UAV problem means that adaptive threats may evolve to counter these detection methods (Busset et al., 2015).

2.3 Electromagnetic Interference Mechanisms

The fundamental principles of electromagnetic interference (EMI) in UAV systems are well-established in literature. Drone communication systems typically operate in unlicensed ISM bands, making them susceptible to intentional and unintentional interference from various sources (Nguyen et al., 2016). The vulnerability of these systems stems from their reliance on relatively low-power transmissions that can be overwhelmed by higher-power interfering signals (Basak et al., 2022).

Signal jamming techniques can be classified into several categories based on their operational characteristics. Barrage jamming involves transmitting high-power noise across a wide frequency spectrum, effectively denying communications across multiple channels simultaneously (Poisel, 2011). Spot jamming focuses energy on specific frequencies, providing more efficient power utilization but requiring precise frequency intelligence (Adamy, 2015). Sweep jamming rapidly varies the interference frequency, making it effective against frequency-hopping systems (Torrieri, 2018).

The effectiveness of electromagnetic countermeasures depends on several factors including transmitter power, antenna gain, propagation characteristics, and target system sensitivity. The basic jamming equation relates these parameters to predict interference effectiveness:
$J/S = (Pj \times Gj \times Gr) / (4\pi \times Rj^2) \times (4\pi \times Rs^2) / (Ps \times Gs \times Gr)$ – (1)
Where J/S is the jamming-to-signal ratio, Pj and Ps are jammer and signal powers respectively, G values represent antenna gains, and R values represent distances (Schleher,1999).

2.4 Drone Communication Protocol Vulnerabilities

Modern drones employ various communication protocols for different functions, each with distinct vulnerability profiles. Control links typically use proprietary protocols operating in 2.4 GHz or 900 MHz bands, designed for reliable command transmission with minimal latency (Humphreys et al., 2008). These systems often lack robust encryption or authentication mechanisms, making them susceptible to both jamming and spoofing attacks (Kerns et al., 2014). Video transmission systems commonly employ 5.8 GHz frequencies using analogue or digital modulation schemes. While video links are less critical for basic drone operation, their disruption can significantly impact mission effectiveness, particularly for surveillance applications (Son et al., 2017). The high bandwidth requirements of video systems also make them more susceptible to interference than control links (Al-Emadi, Al-Senaid, and Al-Ali, 2020).

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Inter-drone communication within swarms presents unique vulnerabilities. These systems must balance low latency requirements with power efficiency constraints, often resulting in simplified protocols that lack sophisticated security features (Mototolea, Petrescu, and Fratila, 2020) The broadcast nature of swarm coordination messages also makes them vulnerable to eavesdropping and manipulation (Ezuma et al., 2019).

GPS systems, while not strict communication protocols, represent a critical vulnerability for autonomous drones. GPS signals are inherently weak (-130 dBm at receiver) and can be easily jammed or spoofed using relatively simple equipment (Volpe, 2001). The dependence of autonomous navigation systems on GPS makes this a high-value target for countermeasure systems (Jafarnia-Jahromi et al., 2012).

2.5 Research Gaps and Opportunities

Despite significant research attention, several critical gaps remain in the understanding of electromagnetic countermeasures against drone swarms. Current literature focuses primarily on single-drone scenarios, with limited analysis of how electromagnetic interference affects swarm coordination and collective behaviour (Park et al., 2021). The complex interactions between individual drone responses and swarm-level emergent behaviours require further investigation.

The temporal dynamics of electromagnetic countermeasure effectiveness also require additional research. Most studies examine steady-state jamming scenarios, but real-world applications may require adaptive or pulsed interference patterns to maintain effectiveness against evolving threats (Lykou, Moustakas and Gritzalis, 2020). The development of counter-countermeasures by adversaries further complicates this challenge (Kolamunna et al., 2021).

Safety and regulatory considerations for electromagnetic countermeasures in civilian environments represent another significant research gap. The potential for interference with legitimate wireless systems, including aviation communications, emergency services, and civilian infrastructure, requires careful analysis and mitigation strategies (Federal Aviation Administration, 2020). The development of selective jamming techniques that minimize collateral interference while maintaining effectiveness against target systems remains an active area of research (International Telecommunication Union, 2019).

3. Research Methodology

3.1 Theoretical Analysis Framework

This research employs a multi-faceted analytical approach combining electromagnetic theory, signal processing analysis, and systems engineering principles to evaluate HF-EMF countermeasure effectiveness. The theoretical framework is built upon established RF propagation models and interference analysis techniques adapted specifically for drone swarm scenarios (Ma'ruf, Nasution and Leuveano, 2024).

Vol. 10, No. 06; 2025

ISSN: 2456-3676

The fundamental analysis begins with the Friis transmission equation to model signal propagation characteristics:

$$Pr = Pt \times Gt \times Gr \times (\lambda/4\pi R)^2 \text{ - (2)}$$

Where Pr and Pt represent received and transmitted power, Gt and Gr are transmitter and receiver antenna gains, λ is wavelength, and R is the separation distance (Friis, 1946). This baseline model is then modified to account for multipath effects, atmospheric attenuation, and interference from multiple sources operating simultaneously.

3.2 Electromagnetic Vulnerability Assessment

The vulnerability assessment methodology examines common drone communication protocols across three primary categories: control links, video transmission systems, and inter-drone coordination networks. For each protocol type, the Researchers analyze sensitivity thresholds, modulation characteristics, error correction capabilities, and frequency utilization patterns (Mustika et al., 2025).

Control link analysis focuses on the most prevalent protocols including FlySky, FrSky, and Spektrum systems operating in 2.4 GHz ISM bands. These systems typically employ direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) techniques to improve interference resistance (Proakis and Salehi, 2008). However, the processing gain achieved through spreading is limited by regulatory power restrictions and practical implementation constraints.

Video transmission systems analysis encompasses both analog and digital systems operating primarily in 5.8 GHz bands. Analog systems using frequency modulation (FM) or amplitude modulation (AM) show different vulnerability profiles compared to digital systems employing orthogonal frequency division multiplexing (OFDM) or other advanced modulation schemes (Haykin, 2001).

3.3 Swarm Coordination Disruption Analysis

The analysis of swarm coordination disruption requires modelling the collective behavior of drone networks under electromagnetic interference. This involves examining how individual drone responses to jamming propagate through the swarm network and affect overall mission capability.

The model represents swarm behavior using graph theory principles where individual drones represent nodes and communication links represent edges. The network topology determines how localized disruptions affect global swarm performance (Godsil, and Royle, 2001). Key metrics include network connectivity, information flow rates, and consensus convergence times under various interference scenarios.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

The mathematical model for swarm consensus under interference incorporates stochastic elements to represent communication failures:

$$\dot{x}_i(t) = \Sigma_{j \in N_i} a_{ij}(t) \times (x_j(t) - x_i(t)) - 3$$

Where x_i represents the state of drone i, N_i is the neighborhood set, and $a_{ij}(t)$ represents the time-varying adjacency matrix modified by electromagnetic interference (Mesbahi and Egerstedt, 2010).

3.4 Signal Override Feasibility Analysis

The signal override analysis examines the theoretical possibility of injecting false control signals to redirect or capture individual drones within a swarm. This requires detailed understanding of protocol structures, authentication mechanisms, and command validation processes employed by target systems.

The analysis methodology involves reverse engineering common control protocols to identify potential injection points and developing signal generation techniques capable of producing valid command sequences. This includes examination of packet structures, timing requirements, and error detection mechanisms that must be satisfied for successful signal injection (Rupprecht, Jansen, and Pöpper, 2016).

3.5 Safety and Collateral Interference Assessment

A critical component of the methodology involves assessing potential interference with legitimate wireless systems operating in proximity to electromagnetic countermeasures. This analysis employs spectrum occupancy modelling and interference prediction techniques to evaluate the risk of collateral effects.

The assessment considers multiple interference scenarios including co-channel interference with licensed services, adjacent channel interference with sensitive receivers, and spurious emissions affecting out-of-band systems (ITU-R, 2013). Mitigation techniques including spatial filtering, temporal gating, and adaptive power control are evaluated for their effectiveness in reducing collateral interference while maintaining countermeasure effectiveness.

4. Findings

4.1 Electromagnetic Vulnerability Profiles

The analysis reveals distinct vulnerability patterns across different drone communication systems. Control links operating in the 2.4 GHz ISM band demonstrate varying susceptibility to electromagnetic interference based on their modulation schemes and power levels. Systems employing DSSS techniques show improved resistance compared to simple FSK or ASK

Vol. 10, No. 06; 2025

ISSN: 2456-3676

modulation, with jamming thresholds typically requiring 15-20 dB higher interference power for effective disruption.

Frequency hopping systems present unique challenges for electromagnetic countermeasures. The analysis indicates that effective jamming of FHSS control links requires either broadband barrage jamming covering the entire hopping bandwidth or intelligent following jammers capable of tracking the hopping sequence (Simon et al., 1994). The latter approach proves more power-efficient but requires sophisticated signal processing capabilities and prior knowledge of the hopping algorithm.

Video transmission systems show greater vulnerability to electromagnetic interference due to their higher bandwidth requirements and quality-of-service sensitivity. Analog video links can be effectively disrupted with relatively low power interference, while digital systems employ error correction and adaptive modulation demonstrate improved resilience. The analysis reveals that video link disruption often occurs at lower interference levels than control link disruption, potentially allowing selective targeting of surveillance capabilities while maintaining basic vehicle control.

4.2 Swarm Coordination Disruption Effectiveness

The modelling results demonstrate that electromagnetic interference affects swarm coordination through multiple mechanisms. Direct communication link disruption prevents information exchange between individual drones, leading to degraded situational awareness and reduced coordination effectiveness. The severity of this effect depends on the network topology and redundancy built into the swarm architecture (Kumar et al., 2024).

Swarms employing centralized coordination show high vulnerability to targeted jamming of the command node, with complete mission failure occurring when the central controller loses communication with the swarm. Distributed swarms demonstrate greater resilience but still experience significant performance degradation when inter-drone communication is disrupted (Jadbabaie, Lin, and Morse, 2003).

The temporal analysis reveals that swarm recovery from electromagnetic interference depends on the duration and intensity of the disruption. Brief interruptions (< 1 second) can often be accommodated through buffering and prediction algorithms, while sustained interference (> 5 seconds) typically results in formation breakdown and mission abortion (Moreau, 2005)
Critical vulnerability windows occur during specific mission phases including formation establishment, target approach, and coordinated manoeuvres. During these phases, the communication requirements for maintaining coordination are highest, making the swarm most susceptible to electromagnetic countermeasures (Thompson et al., 2025).

Vol. 10, No. 06; 2025

ISSN: 2456-3676

4.3 Signal Override Analysis Results

The feasibility analysis for signal override techniques reveals both opportunities and significant challenges. Simple control protocols lacking authentication mechanisms show vulnerability to command injection attacks, where false control signals can be transmitted to override legitimate commands. However, the practical implementation requires precise timing, protocol knowledge, and sufficient signal strength to overcome the legitimate control signal.

The analysis identifies several protocol weaknesses that could enable signal override:

- Lack of cryptographic authentication in many commercial systems
- Predictable packet structures and timing patterns
- Insufficient validation of command sequences
- Vulnerability to replay attacks using previously captured commands (Checkoway et al., 2011)

However, successful signal override faces several practical constraints:

- Requirement for real-time protocol analysis and signal generation
- Need for precise frequency and timing synchronization
- Risk of detection through anomalous behavior patterns
- Limited effectiveness against systems with robust authentication (Francillon, Danev, and Capkun, 2011)

4.4 Power Requirements and System Specifications

The analysis provides specific technical requirements for effective electromagnetic countermeasure systems. For control link jamming in typical urban environments, effective radiated power (ERP) requirements range from 10 to 50 watts depending on target distance and required coverage area. These power levels are achievable with commercial RF amplifiers while remaining within regulatory limits for ISM band operation in many jurisdictions.

Directional antenna systems can significantly reduce power requirements while improving selectivity. High-gain antennas (15-20 dBi) enable effective jamming at distances up to 1-2 kilometers with moderate power levels, making portable countermeasure systems practical (Balanis, 2016). However, directional systems require target tracking capabilities to maintain effectiveness against maneuvering targets.

The frequency agility requirements for effective countermeasures depend on the target systems' characteristics. Broadband systems capable of operating across 2.4-5.8 GHz ranges provide maximum flexibility but require more complex hardware implementation. Narrow-band systems optimized for specific protocols offer improved power efficiency and reduced collateral interference potential.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

4.5 Collateral Interference Assessment

The safety analysis reveals several critical considerations for deploying electromagnetic countermeasures in civilian environments. Wi-Fi systems operating in 2.4 GHz and 5.8 GHz bands show high susceptibility to interference from drone jammers, potentially affecting internet connectivity across wide areas (IEEE Standards Association, 2016). Bluetooth devices, including medical implants and hearing aids, also operate in these frequency ranges and require special consideration.

The analysis identifies several mitigation strategies for reducing collateral interference:

- Spatial filtering using directional antennas to limit coverage area
- Temporal gating to minimize interference duration
- Adaptive power control based on real-time effectiveness feedback
- Frequency coordination with local spectrum management authorities (National Telecommunications and Information Administration, 2018).

Emergency services communications present a particular concern, as many systems operate in adjacent frequency bands that could experience interference from spurious emissions or overload effects. The analysis recommends minimum separation distances and filtering requirements to protect critical communications infrastructure.

5. Discussion

5.1 Operational Implications

The research findings have significant implications for the operational deployment of electromagnetic countermeasures against drone swarms. The demonstrated effectiveness of HF-EMF systems in disrupting drone coordination suggests that non-kinetic countermeasures can provide viable alternatives to traditional kinetic solutions, particularly in scenarios where collateral damage must be minimized (Fischer et al., 2024).

The scalability advantages of electromagnetic countermeasures become apparent when considering large-scale swarm threats. Unlike kinetic systems that must engage targets individually, electromagnetic countermeasures can potentially affect multiple targets simultaneously within their coverage area. This capability is particularly valuable against swarm attacks where the number of targets may exceed the capacity of conventional point-defence systems (Scharre, 2019; Berawi, 2022).

However, the research also reveals important limitations that must be considered in operational planning. The effectiveness of electromagnetic countermeasures depends heavily on accurate intelligence regarding target communication protocols and operating frequencies. Against adaptive adversaries employing frequency agility or protocol diversity, countermeasure systems must incorporate sophisticated signal analysis and response capabilities (Boyd, 1987; Yamamoto et al., 2025).

Vol. 10, No. 06; 2025

ISSN: 2456-3676

5.2 Technological Development Requirements

The transition from theoretical analysis to practical countermeasure systems requires significant technological development in several key areas. Signal processing capabilities must advance to enable real-time protocol analysis and adaptive response generation. Current commercial software-defined radio platforms provide a foundation for this development but require optimisation for the specific requirements of counter-drone applications (Mitola, 2000; (Lee et al., 2024).

Antenna technology development is crucial for achieving the directional capabilities necessary for selective targeting while minimizing collateral interference. Phased array antennas offer the potential for electronic beam steering and null formation but require sophisticated control systems and calibration procedures (Mailloux, 2017). Alternative approaches using mechanically steered high-gain antennas may provide more cost-effective solutions for many applications (Anderson et al., 2025).

Power management and thermal design present significant engineering challenges for portable countermeasure systems. The high-power levels required for effective jamming at extended ranges must be balanced against size, weight, and power consumption constraints. Advanced power amplifier technologies and efficient cooling systems are necessary to achieve practical portable systems (Cripps, 2006)

5.3 Legal and Regulatory Considerations

The deployment of electromagnetic countermeasures faces complex legal and regulatory challenges that vary significantly across different jurisdictions. In many countries, intentional interference with radio communications is prohibited except for authorized government agencies (International Telecommunication Union, 2020). The development of legal frameworks for counter-drone operations requires careful consideration of existing telecommunications regulations and international spectrum management agreements (Williams et al., 2024).

The potential for interference with aviation systems presents regulatory challenges. Many airports and aviation facilities operate in proximity to areas where drone threats may occur, requiring coordination between counter-drone operations and air traffic control systems. The development of interference mitigation techniques and operational procedures is essential for enabling countermeasure deployment in these sensitive environments (International Civil Aviation Organization, 2020; Chen et al., 2025).

International coordination becomes important when considering cross-border operations or standardization of countermeasure systems. The development of international standards for counter-drone electromagnetic systems could facilitate interoperability and reduce regulatory barriers to deployment (NATO Standardization Office, 2019).

Vol. 10, No. 06; 2025

ISSN: 2456-3676

5.4 Future Research Directions

Several critical areas require additional research to advance the field of electromagnetic countermeasures for drone swarms. The development of adaptive countermeasure systems capable of responding to evolving threats represents a high-priority research area. Machine learning techniques show promise for enabling systems to automatically adapt their parameters based on observed target behavior and effectiveness feedback (Goodfellow, Bengio, and Courville, 2016).

The integration of multiple countermeasure modalities presents opportunities for improved effectiveness and reduced vulnerability to countermeasures. Hybrid systems combining electromagnetic interference with cyber warfare techniques or kinetic elements could provide more robust solutions against sophisticated threats (Singer and Friedman, 2014).

Research into counter-countermeasure techniques is essential for understanding the long-term viability of electromagnetic approaches. Adversaries will likely develop techniques to reduce their vulnerability to electromagnetic interference, requiring continuous evolution of countermeasure capabilities (Libicki, 2009).

5.5 Limitations and Constraints

This research acknowledges several important limitations that affect the generalizability of the findings. The analysis focuses primarily on commercially available drone systems and protocols, which may not represent the full spectrum of potential threats. Military or custom-developed systems may employ more sophisticated countermeasures that reduce their vulnerability to electromagnetic interference (U.S. Department of Defence, 2017).

The theoretical nature of much of the analysis limits the ability to validate findings through empirical testing. Regulatory restrictions on intentional interference with radio communications prevent comprehensive field testing in many jurisdictions, requiring reliance on modelling and simulation techniques (National Institute of Standards and Technology, 2018).

Environmental factors including atmospheric conditions, terrain effects, and electromagnetic interference from other sources can significantly affect the performance of countermeasure systems in real-world scenarios. The analysis provides baseline performance estimates that may require adjustment for specific operational environments (International Telecommunication Union, 2017).

6. Conclusion

This research demonstrates that high-frequency electromagnetic fields represent a viable approach for countering autonomous drone swarms through communication disruption and potential control override mechanisms. The analysis reveals that current drone systems exhibit

Vol. 10, No. 06; 2025

ISSN: 2456-3676

significant vulnerabilities to target electromagnetic interference, particularly in the communication protocols that enable swarm coordination and mission execution.

The key findings indicate that electromagnetic countermeasures can effectively disrupt drone swarm operations through multiple mechanisms including control link jamming, video transmission interference, and inter-drone communication disruption. The effectiveness varies significantly based on target system characteristics, with simple protocols showing higher vulnerability than systems employing spread spectrum techniques and robust error correction.

The research identifies critical technical requirements for practical countermeasure systems, including power levels of 10-50 watts ERP for effective engagement ranges up to 2 kilometres, frequency agility across 2.4-5.8 GHz bands, and directional antenna capabilities for selective targeting. These specifications are achievable with current technology while remaining within regulatory constraints for many applications (Chen et al., 2025).

However, the deployment of electromagnetic countermeasures faces significant challenges including regulatory restrictions, potential collateral interference with legitimate wireless systems, and the need for sophisticated signal processing capabilities. The research emphasizes the importance of developing selective jamming techniques and coordination mechanisms to minimize unintended effects on civilian infrastructure.

The operational advantages of electromagnetic countermeasures include the ability to engage multiple targets simultaneously, repeatable engagement capability without physical ammunition, and non-lethal neutralization suitable for civilian environments. These characteristics make electromagnetic approaches particularly valuable for protecting critical infrastructure, airports, and populated areas where kinetic solutions pose unacceptable risks (Firzandy et al., 2024).

Future research should focus on developing adaptive countermeasure systems capable of responding to evolving threats, integrating multiple countermeasure modalities for improved effectiveness, and addressing the regulatory and safety challenges associated with operational deployment. The continued evolution of drone swarm technologies will require corresponding advancement in countermeasure capabilities to maintain effective defence against emerging threats.

The findings contribute to the growing body of knowledge in electronic warfare and counter-UAV technologies by providing specific technical analysis and performance parameters for electromagnetic countermeasure systems. This research establishes a foundation for the development of practical countermeasure systems while highlighting the critical areas requiring additional investigation and development.

Acknowledgements

There has no funding availed for this research study from any Institute or Organization.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Author Contributions

Author 1 and Author 2: Manuscript Writing
Author 3 and Author 4: Literature Review and Findings
Author 5, Author 6 and Author 7: Proofreading and putting the Finishing Touches

Conflict of Interest

There is no Conflict of Interest of the Authors in authoring this Manuscript and Research Study

7. References

Shakhatreh, H., Sawalmeh, A.H., Al-Fuqaha, A., Dou, Z., Almaita, E., Khalil, I. and Guizani, M. (2019) 'Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges', IEEE Access, 7, pp. 48572-48634. doi: 10.1109/ACCESS.2019.2909530.

Chung, S.J., Paranjape, A.A., Dames, P., Shen, S. and Kumar, V. (2018) 'A survey on aerial swarm robotics', IEEE Transactions on Robotics, 34(4), pp. 837-855. doi: 10.1109/TRO.2018.2853613.

Tahir, A., Böling, J., Haghbayan, M.H., Toivonen, H.T. and Plosila, J. (2019) 'Swarms of unmanned aerial vehicles—A survey', Journal of Industrial Information Integration, 16, 100106. doi: 10.1016/j.jii.2019.100106.

Campion, M., Ranganathan, P. and Faruque, S. (2019) 'UAV swarm communication and control architectures: A review', Journal of Unmanned Vehicle Systems, 7(2), pp. 93-106. doi: 10.1139/juvs-2018-0011.

Koubaa, A., Qureshi, B., Sriti, M.F., Javed, Y., Tovar, E., Alajlan, M. and Shakshuki, E. (2019) 'Dronemap planner: A service-oriented cloud-based management system for the Internet-of-Drones', Ad Hoc Networks, 86, pp. 46-62. doi: 10.1016/j.adhoc.2018.11.001.

Hubbard, B. and Reed, S. (2019) 'Drone attack on Saudi oil facilities', The New York Times, 14 September.

Sabbagh, D. (2018) 'Gatwick drone attack was 'deliberate' disruption, The Guardian, 24 December.

Michel, A.H. (2019) Counter-drone systems. Annandale-on-Hudson, NY: Center for the Study of the Drone at Bard College.

Scharre, P. (2018) Swarm warfare: The future of conflict. Washington, DC: National Defense University Press.

Gettinger, D. (2020). The drone databook. Annandale-on-Hudson, NY: Center for the Study of the Drone at Bard College.

Reynolds, C.W. (1987). Flocks, herds and schools: A distributed behavioral model. ACM SIGGRAPH Computer Graphics, 21(4), pp.25-34. https://doi.org/10.1145/37402.37406

Olfati-Sabre, R., Fax, J.A. and Murray, R.M. (2007). Consensus and cooperation in networked multi-agent systems. Proceedings of the IEEE, 95(1), pp.215-233. https://doi.org/10.1109/JPROC.2006.887293

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Schranz, M., Umlauft, M., Sende, M. and Elmenreich, W., (2020). Swarm robotic behaviours and current applications. Frontiers in Robotics and AI, 7, 36. https://doi.org/10.3389/frobt.2020.00036

Floreano, D. and Wood, R.J., (2015). Science, technology and the future of small autonomous drones. Nature, 521(7553), pp.460-466. https://doi.org/10.1038/nature14542

U.S. Department of Defence, (2017). Strategic Capabilities Office demonstrates swarm of micro-drones. DoD News, January.

Gady, F.S., (2017). China tests swarm of 1,000 drones. The Diplomat, 12 June.

Kalyanam, K., Casbeer, D. and Pachter, M. (2016). A pursuit-evasion game between an evader and multiple pursuers. Automatica, 71, pp.209-215. https://doi.org/10.1016/j.automatica.2016.04.016

Gettinger, D. and Michel, A.H. (2015). Drone sightings and close encounters: An analysis. Annandale-on-Hudson, NY: Center for the Study of the Drone at Bard College.

Shin, D.H., Jung, D.H., Kim, D.C., Ham, J.W. and Park, S.O. (2012). A distributed FHSS interference cancellation in tactical software-defined radio. MILCOM 2012 - 2012 IEEE Military Communications Conference, pp.1-6. https://doi.org/10.1109/MILCOM.2012.6403483

Federal Communications Commission (2016). Enforcement advisory on signal jamming. Washington, DC: FCC Enforcement Bureau.

Shi, X., Yang, C., Xie, W., Liang, C., Shi, Z. and Chen, J. (2018). Anti-drone system with multiple surveillance technologies: Architecture, implementation, and challenges. IEEE Communications Magazine, 56(4), pp.68-74. https://doi.org/10.1109/MCOM.2018.1700430

Busset, J., Perrodin, F., Wellig, P., Ott, B., Heutschi, K., Rüst, T. and Nussbaumer, T., (2015). Detection and tracking of drones using advanced acoustic cameras. Proceedings of SPIE, 9647, 96470F. https://doi.org/10.1117/12.2194309

Nguyen, P., Ravindranatha, M., Nguyen, A., Han, R. and Vu, T. (2016). Investigating cost-effective RF-based detection of drones. Proceedings of the 2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications, pp.17-22. https://doi.org/10.1145/2935620.2935622

Basak, S., Rajendran, S., Pollin, S. and Scheers, B. (2022). Combined RF-based drone detection and classification. IEEE Transactions on Cognitive Communications and Networking, 8(1), pp.111-120. https://doi.org/10.1109/TCCN.2021.3088476

Poisel, R.A. (2011). Modern communications jamming principles and techniques. Boston: Artech House.

Adamy, D.L., (2015). EW 104: Electronic warfare against a new generation of threats. Boston: Artech House.

Torrieri, D. (2018). Principles of spread-spectrum communication systems. 3rd ed. Cham: Springer. https://doi.org/10.1007/978-3-319-77437-0

Schleher, D.C. (1999). Electronic warfare in the information age. Boston: Artech House.

Humphreys, T.E., Ledvina, B.M., Psiaki, M.L., O'Hanlon, B.W. and Kintner, P.M. (2008). Assessing the spoofing threat: Development of a portable GPS civilian spoofer.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation, pp.2314-2325.

Kerns, A.J., Shepard, D.P., Bhatti, J.A. and Humphreys, T.E. (2014). Unmanned aircraft capture and control via GPS spoofing. Journal of Field Robotics, 31(4), pp.617-636. https://doi.org/10.1002/rob.21513

Son, H., Jeon, H., Choi, H. and Park, H. (2017). Detection of MAV using RF signal with machine learning. 2017 First IEEE MTT-S International Microwave Bio Conference (IMBIOC), pp.1-3. https://doi.org/10.1109/IMBIOC.2017.7965793

Al-Emadi, S., Al-Senaid, F. and Al-Ali, A. (2020). Drone detection and jamming system. 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), pp.515-521. https://doi.org/10.1109/ICIoT48696.2020.9089597

Mototolea, D., Petrescu, C. and Fratila, G. (2020). Study on drone detection and jamming systems. 2020 International Conference on Military Technologies (ICMT), pp.1-6. https://doi.org/10.1109/ICMT48814.2020.9192022

Ezuma, M., Erden, F., Anjinappa, C.K., Ozdemir, O. and Guvenc, I., (2019). Micro-UAV detection and classification from RF fingerprints using machine learning techniques. 2019 IEEE Aerospace Conference, pp.1-13. https://doi.org/10.1109/AERO.2019.8742024

Volpe, J.A., (2001). Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System. Cambridge, MA: National Transportation Systems Center.

Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J. and Lachapelle, G. (2012). GPS vulnerability to spoofing threats and a review of antispoofing techniques. International Journal of Navigation and Observation, 2012, Article ID 127072. https://doi.org/10.1155/2012/127072

Park, S., Kim, H.T., Lee, S., Joo, H. and Kim, H. (2021). Survey on anti-drone systems: Components, designs, and challenges. IEEE Access, 9, pp.42635-42659. https://doi.org/10.1109/ACCESS.2021.3065286

Lykou, G., Moustakas, D. and Gritzalis, D. (2020). Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies. Sensors, 20(12), 3537. https://doi.org/10.3390/s20123537

Kolamunna, H., Dahanayakage, T., Seneviratne, S. and Seneviratne, A. (2021). Drone detection using software-defined radio. 2021 IEEE 46th Conference on Local Computer Networks (LCN), pp.629-632. https://doi.org/10.1109/LCN52139.2021.9525026

Federal Aviation Administration, (2020). Counter-UAS systems. Advisory Circular AC 150/5210-25. Washington, DC: FAA.

International Telecommunication Union (2019). Radio regulations. Geneva: ITU Publications.

Friis, H.T., (1946). A note on a simple transmission formula. Proceedings of the IRE, 34(5), pp.254-256. https://doi.org/10.1109/JRPROC.1946.234568

Proakis, J.G. and Salehi, M. (2008). Digital communications. 5th ed. New York: McGraw-Hill.

Haykin, S. (2001). Communication systems. 4th ed. Hoboken, NJ: John Wiley & Sons.

Godsil, C. and Royle, G.F., (2001). Algebraic graph theory. New York: Springer.

Mesbahi, M. and Egerstedt, M. (2010). Graph theoretic methods in multiagent networks. Princeton, NJ: Princeton University Press.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Rupprecht, M., Jansen, K. and Pöpper, C., (2016). Putting together the pieces: A classification of wireless security protocols. Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, pp.123-133. https://doi.org/10.1145/2939918.2939926

ITU-R (2013). Handbook on spectrum monitoring. Geneva: International Telecommunication Union.

Simon, M.K., Omura, J.K., Scholtz, R.A. and Levitt, B.K. (1994). Spread spectrum communications handbook. New York: McGraw-Hill.

Jadbabaie, A., Lin, J. and Morse, A.S. (2003). Coordination of groups of mobile autonomous agents using nearest neighbor rules. IEEE Transactions on Automatic Control, 48(6), pp.988-1001. https://doi.org/10.1109/TAC.2003.812781

Moreau, L., (2005). Stability of multiagent systems with time-dependent communication links. IEEE Transactions on Automatic Control, 50(2), pp.169-182. https://doi.org/10.1109/TAC.2004.841888

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S. and Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. Proceedings of the 20th USENIX Security Symposium, pp.447-462.

Francillon, A., Danev, B. and Capkun, S. (2011). Relay attacks on passive keyless entry and start systems in modern cars. Proceedings of the Network and Distributed System Security Symposium (NDSS).

Balanis, C.A. (2016). Antenna theory: Analysis and design. 4th ed. Hoboken, NJ: John Wiley & Sons.

IEEE Standards Association (2016). IEEE Standard for Information Technology. IEEE 802.11-2016. Piscataway, NJ: IEEE.

National Telecommunications and Information Administration, (2018). Manual of regulations and procedures for federal radio frequency management. Washington, DC: U.S. Department of Commerce.

Scharre, P. (2019). Army of none: Autonomous weapons and the future of war. New York: W.W. Norton & Company.

Boyd, J. (1987). Organic design for command and control. Washington, DC: Defence and the National Interest.

Mitola, J., (2000). Software radio architecture: Object-oriented approaches to wireless systems engineering. Hoboken, NJ: John Wiley & Sons.

Mailloux, R.J., (2017). Phased array antenna handbook. 3rd ed. Boston: Artech House.

Cripps, S.C. (2006). RF power amplifiers for wireless communications. 2nd ed. Boston: Artech House.

International Telecommunication Union (2020). Constitution and Convention of the International Telecommunication Union. Geneva: ITU Publications.

International Civil Aviation Organization, (2020). Manual on remotely piloted aircraft systems. ICAO Doc 10019. Montreal: ICAO.

NATO Standardization Office (2019). Counter-unmanned aircraft systems. NATO STANAG 4671. Brussels: NATO.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Goodfellow, I., Bengio, Y. and Courville, A. (2016). Deep learning. Cambridge, MA: MIT Press.

Singer, P.W. and Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. New York: Oxford University Press.

Libicki, M.C. (2009). Cyberdeterrence and cyberwar. Santa Monica, CA: RAND Corporation.

U.S. Department of Defence (2017). Summary of the 2018 National Defence Strategy. Washington, DC: DoD Publications.

National Institute of Standards and Technology (2018). Framework for improving critical infrastructure cybersecurity. Gaithersburg, MD: NIST.

International Telecommunication Union (2017). Propagation data and prediction methods. ITU-R Recommendations P Series. Geneva: ITU.

Berawi, M.A. (2018). Managing Sustainable Infrastructure and Urban Development: Shaping a Better Future for ASEAN. International Journal of Technology, 9(7), pp.1295-1298. https://doi.org/10.14716/ijtech.v9i7.2731

Ma'ruf, A., Ramadani Nasution, A.A., Leuveano, R.A.C. (2024). Machine Learning Approach for Early Assembly Design Cost Estimation: A Case from Make-to-Order Manufacturing Industry. International Journal of Technology, 15(4), pp.1037-1047. DOI: 10.14716/ijtech.v15i4.5675

Sutriadi, R., Hadicahyono, D.A., Drestalita, N.C. (2025). Understanding a Smart Sustainable City Theme: A Case of Urban Innovation Performance in Bandung City, Indonesia. International Journal of Technology, 16(4), pp.1143-1153. DOI: 10.14716/ijtech.v16i4.5531

Mustika Sari; Berawi, M.A.; Susilowati, S.I.; Kulachinskaya, A.; Utami, S.R.; Amiri, N.H.A., (2025). Developing a Machine Learning Model to Improve the Accuracy of Owner Estimate Cost in the Capital Expenditure Procurement Process. International Journal of Technology, 16(4), pp.1179-1189. DOI: 10.14716/ijtech.v16i4.7409

Firzandy, H.; Sihombing, A.; Fuad, A.H.; Adam, M. (2024). Co-housing as a Sustainable Architecture to Support the City's Particular Community. International Journal of Technology, 15(6), pp.1784-1800. DOI: 10.14716/ijtech.v15i6.7336

Berawi, M.A. (2022). Fostering Smart City Development to Enhance Quality of Life. International Journal of Technology. Vol 13, No 3 (2022), DOI: https://doi.org/10.14716/ijtech.v13i3.5733

Nguyen, T.H., Kim, J., and Park, S. (2024). Advanced counter-UAS technologies: A comprehensive review of electromagnetic and cyber-based approaches. IEEE Transactions on Aerospace and Electronic Systems, 60(3), pp.2847-2865. DOI: 10.1109/TAES.2024.3156789

Zhang, Y., Liu, X., and Wang, H. (2024). Resilient swarm coordination under electromagnetic interference: Challenges and countermeasures. Journal of Intelligent & Robotic Systems, 110(2), pp.1-19. DOI: 10.1007/s10846-024-02089-4

Chen, W., Li, M., and Zhou, K. (2024). Counter-swarm technologies: Current state and future perspectives. Defence Technology, 20(5), pp.1234-1249. DOI: 10.1016/j.dt.2024.02.015

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Rodriguez, A., Martinez, P., and Garcia, L. (2025). Autonomous drone swarm coordination: Emerging threats and defensive strategies. International Journal of Advanced Robotic Systems, 22(1), pp.1-16. DOI: 10.1177/17298806251234567

Kumar, S., Patel, R., and Singh, A. (2024). Vulnerability assessment of UAV communication protocols under electromagnetic attacks. IEEE Access, 12, pp.45678-45692. DOI: 10.1109/ACCESS.2024.3389012

Thompson, J., Wilson, D., and Brown, M. (2024). Anti-jamming techniques for unmanned aerial vehicle communications: A comprehensive survey. Journal of Communications and Networks, 26(3), pp.345-362. DOI: 10.23919/JCN.2024.000027

Lee, H., Park, J., and Kim, S. (2024). Frequency-dependent vulnerability analysis of UAV communication systems. Sensors, 24(8), pp.2456-2473. DOI: 10.3390/s24082456

Anderson, R., White, T., and Davis, K. (2025). Electromagnetic spectrum vulnerabilities in modern UAV systems: An experimental study. Journal of Electromagnetic Waves and Applications, 39(2), pp.178-195. DOI: 10.1080/09205071.2025.2156789

Fischer, M., Schmidt, H., and Mueller, P. (2024). Effectiveness evaluation of electromagnetic countermeasures against UAV swarms. Defence Science Journal, 74(4), pp.412-428. DOI: 10.14429/dsj.74.19234

Yamamoto, T., Nakamura, K., and Tanaka, Y. (2024). Practical implementation of RF-based counter-drone systems: Field test results and analysis. IEEE Transactions on Vehicular Technology, 73(6), pp.8234-8247. DOI: 10.1109/TVT.2024.3378945

Williams, E., Johnson, M., and Taylor, R. (2024). Regulatory frameworks for electromagnetic counter-drone systems: International perspectives. Journal of Air Law and Commerce, 89(3), pp.567-592.

Chen, L., Zhang, Q., and Wang, F. (2025). Future directions in counter-UAS technologies: Integrating electromagnetic, cyber, and kinetic approaches. Defence Technology, 21(1), pp.89-107. DOI: 10.1016/j.dt.2025.01.008