Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

Problems and Solutions of Frequency Hopping for Drones :A Review

Taha Ibrahim Ahmed [1*], Husam Noman Mohammed Ali [2]

[1] Al-Furat Al-Awsat Technical University (ATU), Communications Tech. Eng. Dept., Najaf, Iraq
[2] Al-Furat Al-Awsat Technical University (ATU), Communications Tech. Eng. Dept., Najaf, Iraq ,coj.husm@atu.edu.iq
[*]Corresponding author E-mail: taha.ms.etcn35@student.atu.edu.iq

https://doi.org/10.46649/fjiece.v4.1.4a.25.3.2025

Abstract: The paper studies the critical issue of frequency hopping spread spectrum (FHSS) for drone communications, particularly for UAVs in both civilian and military sectors. It reveals the shortcomings of existing FHSS algorithms, which cannot resist jamming, further adaptability, and sensitivity to complex electromagnetic environments where UAVs work. A comprehensive literature review highlighted a decline in different resilience parameters, which demands an adaptive communication strategy with real-time environmental information to support resilient and energy-efficient communications. These challenges are investigated using emerging technologies like machine learning, software-defined radios, and cognitive radio systems. In addition, the paper underlines the necessity of putting well-designed regulations in place to ensure that UAVs are safely integrated within common air spaces. The work also suggests areas where frequency hopping techniques can be improved, especially within swarm drone operations, by proposing adaptive and collaborative communication models. The research is an essential step towards advancing UAV communication technologies and provides fresh information on alleviating interference and jamming threats in the rapidly crowded airspace.

Keywords: *Frequency Hopping; Drone Communication; Adaptive frequency; Bit Error Rate (BER).*

1. INTRODUCTION

During the last few years, drone technology has experienced a fast-growing development capable of revolutionizing telecommunications and flight industries alike. It is becoming such an essential tool for many applications related to any sector, like agriculture, logistics, surveillance, or emergency response. Since drones are used almost everywhere, from civilian to military purposes, hence ensuring security over these communication methods is a must [1]. One such method that has gradually emerged is Frequency-hopping spread spectrum (FHSS) communication—military background. Firstly, the technique was designed for countermeasures regarding jamming: the approach increases a communication system's resistance to different types of obstructions from transmitters ((in particular pairwise signal suppression)). While it all sounds great, there are some inherent drawbacks to the FHSS techniques, mainly when deployed in drone operations. Without compatibility with these legacy systems, it is now vital under current debates around the security, trustworthiness, and compliance providing a base for drone communication — representing growing concern as airspace expands globally [2].

Frequency hopping was developed during World War II to protect military communications. At that time, it was a great advantage to have such security and signal reliability in the struggle for unbreakable communication, where suppression by electromagnetic interference or eavesdropping by enemy interceptors was always on the cards—matured from a theoretical construct into many practical algorithms used in all sorts of applications, drones for example. However, despite some improvements in

communication security brought about by these advances, various limitations have also been exposed. For example, several papers have questioned the practical effectiveness of some frequency hopping algorithms in the face of agile jammers or quickly varying and high-density electromagnetic environments. As drones are increasingly being deployed in urban and rural environments, characterizing the performance bounds of drone communication systems is crucial, given variability likely from interference patterns [3].

This study aims to identify the key challenges of frequency hopping techniques utilized in drone communication systems, notably regarding their sensitivity to interference and jamming. Flying drones in the rapidly changing technological landscape leads to complicated communication environments and specific risks. Until today, the research still lacks a standard evaluation for all types of frequency hopping algorithms and their behaviors under different scenarios. This research provides a unique balance to that gap of current algorithms, presents the strengths and limitations of various algorithms, and proposes solutions to overcome those limitations.

The paper is structured into distinct sections to delve into the challenges and solutions of frequency hopping for drones. It starts with a detailed literature review, consolidating research on frequency hopping, drone communications, and challenges related to interference and jamming. It then analyzes various frequency hopping algorithms, comparing their performance metrics and suitability for drone operations. Case studies are provided to demonstrate real-world applications of frequency hopping, highlighting both successful implementations and vulnerabilities. Lastly, the paper summarizes the research findings and emphasizes the importance of continued exploration in this field.

2. Literature Review

The cutting-edge development that revolutionized logistics, surveillance, agriculture, entertainment, and many more industries owes its power to the rapid drone innovations over the last decade. As drones make their way into the mainstream, ensuring consistent communication and control within the drone has become pertinent. However, such threats and other interference prevent the operator from maintaining a safe and secure communication link [4]. This leads us to another approach called frequency hopping, which changes transmission frequencies rapidly through multiple channels and seems like a strong candidate for attacking these problems. This review falls within the category of drone communications based on frequency hopping, and it compiles a set of solutions from academia to industry. The key significance of studying frequency hopping for drones is that operational reliability, safety, and efficiency can be largely impacted. Now that drones are being used in all shapes and sizes, performing more intricate movements off into every corner of the sky, there is a clear need for sound communication systems. They demonstrate how frequency hopping outweighs conventional solid-state jammers in drone resistance, anti-jamming, and signal unbrokenness, enhancing situational awareness and operational efficiency. Over time, frequency hopping has become increasingly important; especially today, drones are heading towards autonomy, which requires good communication [5]. Primary research has shown the tactical advantages of frequency-hopping spread spectrum (FHSS) systems over standard fixed-frequency systems. These benefits include even better security against signal snooping and privacy improvements. Additionally, improvements in algorithms and modulation types (e.g., adaptive frequency hopping) can tune the communication channels on the fly. Drones can quickly react and respond to shifting environmental barriers and sign fluctuations. Over the years, frequency hopping for drone communication has evolved just as technology has advanced and drone applications have grown more sophisticated. Initially, the emphasis was on essential functions such as avoiding crashes and being resilient to jamming. Initial research on time-synchronized channel hopping (TSCH) laid the groundwork for interference mitigation in wireless networks. This also hinted that decentralized solutions could

potentially address the drone protocol space for one [6]. The implications of drone applications extended to high-stakes areas such as military and medical logistics, which led to the demand for jam-resistant drones with stringent security carefully architected. Background research on different jamming techniques disclosed that they could easily disrupt drone signals, and more sophisticated measures were required to improve signal robustness. This provided a layered defense against potential threats as integrating machine learning models for monitoring radio frequency (RF) spectrum usage enabled real-time detection of unauthorized drone activity [7]. There have been recent developments in this regard, e.g., simultaneous wireless information and power transfer (SWIPT) network coding for energy harvesting relay systems demonstrated an advancement in communication efficiency, allowing for reduced requirements in terms of instantaneous channel state information knowledge as well as an energy conservation gain [8]. The shift to greener technology is part of a more significant movement in drone technology research that focuses on drones' operational efficiency and ability to deal with endogenous and exogenous perturbations. Nonetheless, the knowledge gaps of decentralized coordination methods and their deployment in realistic environments have yet to be filled, implying that future studies should tackle these challenges related to drone frequency hopping [8]. Frequency hopping in drone communication systems faces problems concerning interference and the ability to jam. Central coordination is required with traditional time-synchronized channel hopping (TSCH) and can be wasteful in mobile ad hoc networks. DT-SCS (Decentralized Time-Synchronized Channel Swapping) is an effective option; it does not require global control to maintain communication synchronization and provides potential benefits regarding throughput and convergence time in dynamic topologies [9]. This decentralized strategy enables fast adaption and enhanced performances in the regions where a drone may suffer from dynamic interference. Jamming interference is another major threat to drone operations, in particular for vital applications like medical deliveries. These approaches have changed over time, from simple noise attacks to more sophisticated jamming techniques using specific protocols used in communication. This is, therefore, highly relevant when it comes to countering jamming effects [10]. One promising technology that will enable this dynamic change in a sustainably secure fashion is the integration of software-defined radios (SDR) into drones, which allow reading and cryptographically securing at a more responsible time [10]. Many researchers have reported the inherent limitations in traditional frequency hopping systems that make them more vulnerable to jamming, and this issue is widely debated in drone applications. Furthermore, [9] addresses the fault of signal jamming and highlights the need for strong countermeasures, explaining that it is essential to incorporate state-of-the-art attack detection systems that reinforce reliability while enhancing operability. Alternatively, [11] delves into the technical intricacies of radio wave jamming methods and their impact on drone frequency-hopping communications. This study provided essential references for the evolution of jamming methods and counter-jamming processes, which points to the fact that interference needs to be prevented from intelligent adaptive apparatuses such as SDR (software-defined radio). While [9] is more theoretical, focusing on advanced solutions to improve medium access control in drone networks through decentralized time-synchronized channel swapping. It offers improved efficiency and lesser exposure to disruptions by bypassing the constraints set by centralized systems. Considerable work in this area has sought to address these challenges, though gaps remain in empirically evaluating proposed solutions.

Most studies are still in theory, and more innovation and practical experimentation are needed to demonstrate new approaches' effectiveness. As an illustrative example, [11] suggests noncoherent detection mechanisms as a possible guideline in presenting the opportunity for simultaneous information and energy transfer. Still, more investigation is required to actualize it in drone technology. as shown in the discussion. As applied to drone communications, frequency hopping reduces interference and can be more robust against jamming attacks [9]. Conventional jamming has been shifted to targeting the specific protocols from which it emerges a vital role of adaptive technique as frequency hopping in preserving communication integrity [10]. This is further compounded by the decentralized time-synchronized

channel swapping (DT-SCS) protocol, a key advancement in effectively using channel resources with collision avoidance [1]. Theoretically, this provides better control of available bandwidth in ad hoc drone networks. However, related issues emerge regarding the necessity of centralized coordination in traditional hopping protocols, which may result in longer convergence times and less-than-optimal performance in a mobile context [11]. While decentralized strategies similar to DT-SCS attempt to improve things [11], they also point out a deficiency in the literature on scalability and dynamic adaptability, especially under diverse operational circumstances.

By combining these varied conceptual frameworks, a more general picture of frequency hopping problems for drone technology can be achieved and, therefore, pave the way to novel methods. This literature review has outlined numerous issues about frequency hopping in drone communications and potential solutions to these problems. Table 1 relates the results of the manuscripts listed in the literature review.

Table 1. Relates the results of the manuscripts listed in the literature review.

Aspect	Details	Reference
Introduction	Drones have revolutionized multiple industries. Ensuring consistent communication is essential. Threats and interference pose challenges. Frequency hopping is a solution to improve communication safety and reliability.	[4]
Significance	Frequency hopping enhances drones' operational reliability, safety, and efficiency. It is essential as drones become autonomous and perform more intricate movements.	[5]
Tactical Advantages	Frequency-hopping spread spectrum (FHSS) systems provide better security and privacy than fixed-frequency systems. Algorithms and modulation improvements allow dynamic channel tuning.	[6]
High-Stakes Applications	Military and medical logistics demand jam-resistant drones with stringent security measures—integration of machine learning for real-time unauthorized drone activity detection.	[7]
Recent Developments	Simultaneous wireless information and power transfer (SWIPT) for energy efficiency and reduced channel state information requirements. Decentralized coordination methods face knowledge gaps. Need for realistic environment studies.	[8]
Decentralized Coordination	DT-SCS does not require global control and adapts faster to dynamic interference, enhancing performance in mobile ad hoc networks.	[9]
Jamming and Interference	Sophisticated jamming techniques require advanced countermeasures. Integration of software-defined radios (SDR) can enhance secure communication.	[10]
Energy Efficiency	SWIPT paradigm for energy-efficient data transfer in drone networks: improved network efficiency and better handling of interference and threats.	[10]
Limitations and Future Directions	Traditional frequency hopping systems are vulnerable to jamming. Need for state-of-the-art attack detection systems. Further research is required on decentralized strategies, scalability, and dynamic adaptability.	[11]
Summary	Frequency hopping reduces interference and enhances robustness against jamming. DT-SCS provides better bandwidth control in ad hoc drone networks. Noncoherent SWIPT is promising for energy efficiency, but practical implementation needs further validation.	[1], [8], [9], [10], [11]

Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

3. Challenges of Frequency Hopping in Drone Communications

There are significant challenges to using FHSS communication in drone communications, even though FHSS communication has been identified for its utility in increasing security and reducing interference. Thus, Regulatory Compliance is one of the biggest roadblocks, so continued research and developmental interventions must be directed toward addressing these burgeoning challenges.

A. Inherent Vulnerabilities of Frequency Hopping Techniques

The well-known frequency hopping spread spectrum (FHSS) communication techniques initially developed for military purposes to secure and make communication resilient showed fundamental weaknesses that are difficult in the case of drone operations. The main virtue of frequency-hopping is making the transmission on every specific band relatively short, difficult eavesdroppers or jamming. Figure 1 illustrates the basic FHSS process, showing how signals hop across various frequencies. However, while appropriate for static operational environments, the technique loses efficacy in more dynamic ones where high-end adversaries deploy sophisticated jamming tactics and intercept technology that can introduce vulnerabilities. Figure 2 shows how adversary techniques, such as wideband and narrowband jamming, increasingly exploit FHSS vulnerabilities over time [12].

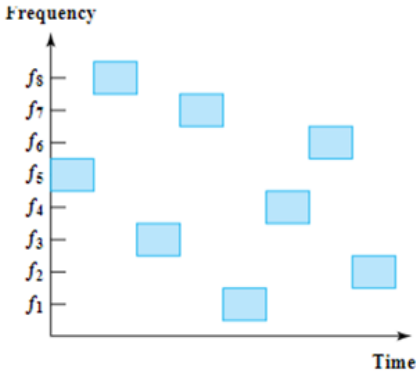

Figure 1. Basic FHSS process

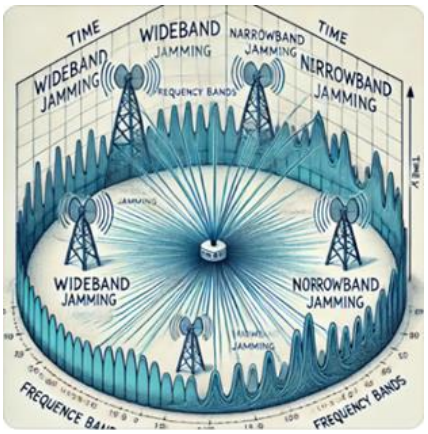

Figure 2. Adversary techniques

Recent studies indicate that the security provided by frequency hopping can be compromised when adversaries utilize a combination of wideband jamming and narrowband jamming, effectively saturating the frequency spectrum and rendering the hopping sequences less effective. Accordingly, the asymmetry in technological capabilities between sophisticated military-grade systems and commercially available drones poses a significant threat to the operational reliability of FHSS techniques [12]. Furthermore, the evolution of drones as versatile tools in civilian and military arenas underscores the necessity to evaluate their communication reliability. Many current frequency hopping algorithms are susceptible to various forms of interference that can significantly impede their performance. Equation 1 quantifies jamming detection probability:

$$P_d = 1 - e^{-\lambda T} \qquad (1)$$

Where λ represents the jamming rate, and T is the observation time.

Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

The potential for significant electromagnetic activity in urban environments can exacerbate these vulnerabilities, leading to severe communication disruptions during critical missions. In addition, the reliance on fixed pseudo-random sequences in older frequency hopping algorithms can create theoretically predictable patterns, permitting attackers to intercept communications if they can discern the hopping sequence. Predictability has inherent weaknesses, and while FHSS tries to preserve an adaptive ability, deploying enough complex algorithms is challenging in practice [13]. Drones' low cost and commercial utility for surveillance or targeting adds dimension to the complex operational environment, allowing adversaries to exploit frequency hopping vulnerabilities with a far lower capital outlay than advanced military systems. This has led to a requirement to re-examine frequency hopping standards and practices to continue operationally relevant in the future while providing a security defense against drone adversaries and becoming aware of perceived weaknesses in drone protocols [14].

This makes the system highly vulnerable to interference and operational conditions, requiring innovative adaptive frequency hopping techniques that can dynamically respond to new interference environments on some frequencies. Figure 3 shows a comparison between traditional and adaptive frequency hopping techniques. These improvements are necessary to guarantee that frequency hopping continues to be an effective communication system, especially in challenging situations [15].

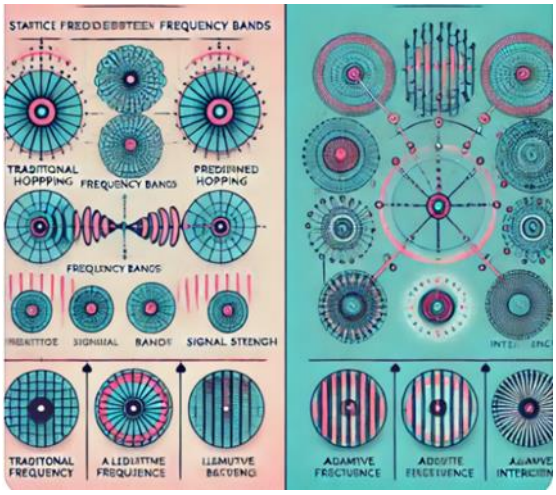

Figure 3. Shows a comparison between traditional and adaptive frequency hopping techniques

Furthermore, new algorithms are needed to minimize those vulnerabilities and adapt frequency hopping techniques based on real-time sensing and data mining under security-conscious operations. Such improvements are necessary to make frequency hopping effective in complex environments [15]. The limitation of frequency hopping as UAV cryptographic techniques is understandable, and it is evident that military and security stakeholders require better training and a more in-depth consideration of how drones are used operationally. Knowledge of this effect is also essential to improve the performance of more secure frequency hopping algorithms and to enhance the technology enabling these operations [16, 17].

B. Interference and Jamming Threats in Diverse Environments

Frequency hopping is one of drones' most common and essential communication mechanisms. Still, it also has to deal with serious challenges from outside, like interference and jamming, primarily as it explores a more diverse world. In busy urban areas, the electrical environment will be even more chaotic, with many wireless signals intersecting at one point. This increased general congestion increases the ambient noise floor, elevating the risk of signal degradation that frequency hopping systems have to overcome. Moreover, in such scenarios, intentional interference (jamming) represents a substantial threat

because an adversary could exploit communication protocol vulnerabilities and block critical support, leading, for example, to unmanned aircraft systems and drones losing control. Since UAVs often engage in sensitive missions such as surveillance or logistics, preventing interference is critical. Investigation of state-of-the-art jamming methods demonstrates that classical multi-channel frequency hopping algorithms may become insufficient, as they might not respond fast enough to attacks aiming at single frequencies or with attacks using knowledge about existing hop patterns [18].

As military and civilian uses of drones frequently overlap, understanding how different environments influence the efficacy of frequency hopping systems becomes crucial. The research indicates that as UAV operations become more intertwined with other critical infrastructures, the potential for interference increases, necessitating the development of more adaptable and resilient communication protocols [19]. Advanced jamming tactics, such as deception techniques, illustrate how UAV operators must consider the vulnerabilities within their communication frameworks. These techniques allow adversaries to mislead UAV systems, complicating recovery or response strategies post-interference

One of the most pressing issues is the rise of machine and deep learning techniques, which have shown significant potential in various drone applications but remain underexplored in counteracting jamming threats. While many studies have been dedicated to evaluating machine learning principles in UAV navigation and autonomous intelligence, a research gap persists regarding their application in jamming mitigation strategies [18]. This gap underscores a need for interdisciplinary approaches that focus on algorithm improvements and consider drone technology's socio-political implications, particularly as these systems proliferate globally. Addressing the dynamic nature of environments where drones operate requires innovative algorithms capable of real-time adaptability.

As emphasized in recent literature, the emergence of high-altitude platforms and the inherent advantages of UAV-enabled communications represent critical opportunities for overcoming interference issues and enhancing the robustness of communication networks [20]. Significantly, the historical context of frequency hopping and its adaptation over decades starkly contrasts with the contemporary developments in communication security within the UAV sector. While frequency hopping was initially a military innovation aimed at securing classified communications, transitioning to civilian applications necessitates reevaluating its foundational algorithms to ensure they cater to varied interference environments. The confluence of civilian and military utilization presents distinct challenges and opportunities that require nuanced understanding and innovative solutions. As the landscape evolves, proactive measures in understanding the implications of jamming and interference must extend beyond technical assessments to include considerations of regulatory frameworks that govern UAV operations, ensuring drones' safe and effective integration into the airspace [20, 21].

C. Performance Limitations of Current Frequency Hopping Algorithms

The theoretical and practical performance of existing frequency hopping schemes for drone communications are severely limited in many aspects and deserve a thorough investigation. Although FHSS can offer better information security and anti-jamming performance, various inherent issues restrict the technique's usefulness. An adaptive and responsive frequency hopping algorithm has to rely on a few direct samples for operation inside a dynamic electromagnetic habitat, which can be the main limitation. Figure 4 compares static hopping sequences with adaptive frequency hopping, highlighting the difference in performance in dynamic environments. On the left, static hopping sequences use fixed frequencies, leading to overlaps and interference, while on the right, AFH dynamically adjusts to avoid interference, improving performance [22].

Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

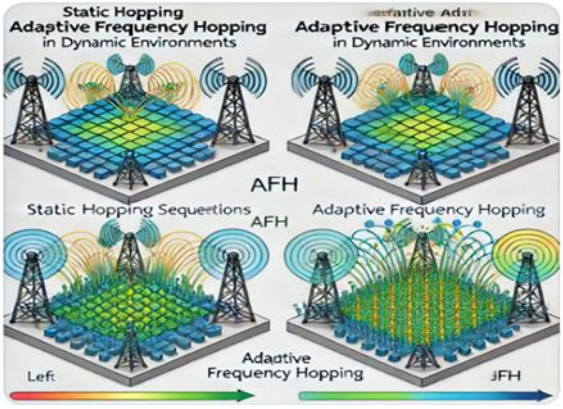

Figure 4. Compares static hopping sequences with adaptive frequency hopping.

However, the FHSS performance can be severely disrupted by competing signals in areas where drones are increasingly used: densely populated urban environments, which can lead to communication failures or delays. Most existing schemes use static hopping sequences that don't consider the interference changes over time, leading to poor adaptability to the dynamic signal environment and suboptimal communication reliability. In addition, the success of frequency hopping depends on highly accurate synchronization between transmitting and receiving devices. Changes in frequency timing would cause latency to increase or connection failure altogether— resulting in a fatal disaster for high-stakes operations like military surveillance and emergency response situations [23]. Equation 2, which represents the Bit Error Rate (BER), demonstrates how this can affect FHSS performance:

$$BER = Q(\frac{E_b}{N_o}) \qquad (2)$$

E_b is the energy per bit, and N_0 is the noise power spectral density.

On top of that, frequency hopping systems may require a lot of computational power to design and deploy, which can become quite a challenge when considering how little the architecture of low-power drones has. Many current algorithms require high computational resources to successfully generate and control hopping sequences. However, the high resource intensity can be an issue; in commercial drones, processing capabilities are often overtaxed, and development primarily emphasizes being light and energy efficient rather than adequate processing power. As a result, such limitations require workarounds that may impact the resiliency of FH but also create new security gaps in communication channels.
Furthermore, because drones fly long distances, signal loss becomes more severe. By design, existing frequency hopping techniques are not well suited to the signal degradation that can occur during long-range transmissions, as this can lead to lower data rates or higher error rates that scale with environmental conditions. At another level, it is difficult to integrate security within schemes based on frequency hopping. While frequency hopping can provide better interception resistance, it does not protect the content of the communication.

As demonstrated in prior studies of communication protocols, including drone technology deployed for intelligent agriculture and innovative city applications, it is crucial to ensure that robustness does not come at the expense of security vulnerabilities [24]. The potential for unintentional and malicious interference remains high, particularly with the proliferation of low-cost drones and the amassing of weak signals in the same frequency bands. Therefore, while frequency hopping does mitigate some risks, it does not comprehensively safeguard against all forms of jamming, especially when facing sophisticated adversaries employing advanced jamming techniques or eavesdropping efforts. Furthermore, the

effectiveness of frequency hopping algorithms has been compromised in scenarios involving mobile devices. Due to hardware limitations or environmental factors such as signal shadows, Malfunctions can introduce unpredictability in wireless communication links. In drone deployment, where mobility is a fundamental characteristic, challenges such as rapid altitude changes and speed variances create complexities in maintaining effective communication protocols. Limited mobility among some drones adversely affects their ability to maintain consistent communication across shifting frequency channels [25].

Current FHSS strategies, unless specifically adapted to reflect these dynamics, often perform terribly on these coverage and event detection failures. Given these constraints, it is necessary to rethink present FH strategies. Recent investigations into alternative communication technologies also support this, and they indicated that a hybrid approach with different communication protocols might better address the issue of more reliable links enabling UAV operations. For example, combining Lora WAN capabilities with frequency hopping could be beneficial in solving bandwidth difficulties and resource efficiency in range and resilience [26]. Solving these myriad problems offers nothing less than a chance to improve frequency hopping algorithms for drones; more broadly, it provides an opportunity to play a key role in discussing tomorrow's secure and safe UAVs in challenging operational environments. The innovation of adaptive, low-complexity frequency hopping algorithms that can adapt to time-varying environments and strong security mechanisms may make drone operations feasible and scalable in civil and military domains, opening up a new era of secure communications for UAVs.

4. Potential Solutions and Advances in Frequency Hopping Technology

The advances in frequency hopping techniques provide many opportunities to enhance drone communication reliability and security, especially in massive interference and jamming environments. These inherent limitations of frequency hopping— vulnerability to sophisticated jamming methods and the need for rapid adaptation to changing electromagnetic environments— necessitate novel algorithm research and deployment approaches. A possible example is the use of adaptive frequency hopping, which means analyzing the access environment in real-time, where frequencies may be changed and hop patterns as required.

Such methods will substantially increase immunity to interference by allowing drones to avoid congested bands and, better yet, switch frequencies while flying, lowering the risks of a compromising impact.

Additionally, cognitive radio technology extends these capabilities, allowing drones to sense spectrum availability and dynamically set their communication parameters. This will benefit challenging operational environments, such as urban areas or congested airspace carrying multiple electronic equipment densities with mesh radiation zones and services. Moreover, machine learning (ML) developments enable revolutionary functionalities in frequency hopping systems that would predict utilizing historical data to guide an error analysis. As new data are collected from the network, these machine learning algorithms would be able to progressively refine their methods for frequency selection and hop patterns, adapting their ways of communicating over time with emerging situational awareness of the operational context [27].

In addition, new developments in distributed UAV networks mean more significant potential for improving frequency hopping strategies. These networks enable multiple drones to communicate with each other, allowing them to function effectively as a single network that broadcasts interference and environmental conditions in real-time. Drones can communicate faster and more efficiently together instead of individually, so jamming or interference is minimal. Here, swarm intelligence can optimize

frequency hopping algorithms, enabling drones to coordinate their operations spontaneously through collective decision-making and information sharing, improving communication efficiency and redundancy [28].

Drones can also significantly improve this through autonomous high-performance mesh networking with frequency-hopping communication systems. These systems enable lower density and efficient distribution of communication nodes. Moreover, they make the whole network more robust because an individual point of failure precipitates catastrophic collapse in an overall communication network. And on top of that, regulatory compliance is the bare-medal entry for state-of-the-art frequency hopping technologies. Drone operations, in general, have to be aligned with Federal Communications Commission rules and those of other agencies that govern wireless communications. It will take continuous collaboration to develop policy among all parties, public oversight bodies, the military, and industry so that the scales can be leveled on fostering innovation, compliance, and safety. Similarly, concerns about ethics that underpin present-day debates on whether and how to incorporate AI in missions must be availed. A strategic approach that advances technological progress and enshrines ethical values can secure the trust and social license to base more advanced deployable frequency hopping for drones. Measures that promote transparency of the process from the development and deployment of algorithms may also address privacy-related concerns and other unknown side effects [27].

One of the most significant yet-to-be-explored areas is the move towards future communication systems, such as 5G and upcoming 6G technologies that would provide hyper-connectivity and zero latency. It is believed that adapting existing frequency hopping techniques to such advanced network infrastructure could enable an order of magnitude improvement of basic communication capabilities for drones, like real-time data transfer and reliable command and control functionalities. 5G also provides high-frequency bands that can serve many devices at the same time, ensuring the quality of service under different loads and making it more suitable for frequency hopping systems used in drone communications. Also, as artificial intelligence and automation will be welcome within the 6G network, drones could use that to take advantage of improved communication strategies. For example, suppose terahertz communications and intelligent interfaces are used. In that case, frequency hopping methods can significantly benefit by accelerating data transmission rates and increasing the network's resilience to intra-network interferences. Ultimately, frequency hopping technology for drones is treated by adaptive algorithms and collaborative networking technology and developed with other related technologies [29].

A. Adaptive Frequency Hopping Strategies

Adaptive Frequency Hopping strategies help to elaborate the next generation of communication protocols for drones, enabling a solution when strong and unpredictable interferences exist. The frequency hopping spread spectrum (FHSS) has been known for its advantages in enhancing communication reliability and security. The dynamic nature of the modern communication environment also requires adaptive techniques to adapt to changing conditions, such as increasingly common environmental interferences that modify the electromagnetic spectrum. With the help of algorithms capable of learning and adapting to these circumstances in real time, drones can maximize their effectiveness at communicating. The adjustment requirement must become more prominent as the pool of devices increases and occupancy in the unlicensed bands grows denser; a situation worsens when one device can jam another [30].

One potential way to improve frequency hopping efficiency lies in implementing artificial intelligence techniques inside communication protocols. For example, reinforcement learning algorithms allow frequency hopping systems to adjust their hopping schemes using historical data on interference levels, reducing the influence of external disturbances [30]. The method is well suited when the sources of interference come and go, as adaptive frequency hopping systems can adapt their channel usage in

response to environmental changes. Adaptation is essential to maintain the communication link and improve the resilient features of drones since jamming functions can be more elaborate and more challenging to mitigate using static algorithms.

Near-future developments in wireless communication technology (e.g., in-band full-duplex (IBFD) radio systems [12] also encourage newer lengthy adaptive strategies. With these systems, the same frequency is used for transmission and reception simultaneously, preventing interference and increasing throughput. The use of IBFD technology combined with adaptive frequency hopping enables drones to simultaneously connect multiple devices and ensure the clarity of communication, resulting in a considerable improvement in network performance for high-dense scenarios [31].

It has also been shown that adaptive frequency hopping strategies can significantly improve performance, as in the case of Dimmer, which designed a reinforcement learning agent to tune communication parameters under interference conditions [32]. Drones can ascertain the conditions over which they are flown and learn from this to become more reliable in complex environments. In response to various interference, these adaptive protocols provide better communication quality and reduce energy consumption, which is crucial for operating small UAVs as battery life limits are always set. However, experiences from current adaptive strategies (e.g., Hybrid-Vehfog when dealing with situations replete with obstacles) shed light on the need for responsive network designs that cover disconnection periods and allow for effortless information dissemination among vehicles and drones [33]. This system can include fog computing interoperability to multi-hop configuration and is the best example of how adaptive frequency hopping would support better communication in critical operational scenarios.

Implementing these adaptive strategies in drone communication networks will lead to extensive utilization in domains like logistics, surveillance, and emergency response. So, by maximizing the benefits of adaptive frequency hopping technology, stakeholders can further not only an essential element for safety and security in drone operations but also overall aerial integration for drones into increasingly crowded airspace. The interoperability between adaptive frequency hopping methods and next-generation wireless must be considered in future investigations to promote reliable communications systems suitable for future UAV use. Such exploration is essential since the recent revolution in the aerial robotics ecosystem necessitates the development of sophisticated communication methods that can be adapted to evolving operational requirements and technological trends. In all cases, implementing these adaptive frequency hopping strategies should either set or reset the baseline for drone communication standards.

B. Integration of Advanced Signal Processing Techniques

Advanced signal processing in frequency-hopping communication systems for drones is a key solution to improving the resilience and reliability of UAV operations. Although frequent hopping spread spectrum (FHSS) communication has shown its merit in suppressing the possibility of being intercepted and jammed, with drones being deployed over complex electromagnetic environments even for crowded situations, the conventional FHSS methods urgently require optimization using state-of-the-art signal processing strategies. This refinement process includes sophisticated algorithms that can alter frequency hopping patterns on the fly depending on an ongoing analysis of the operational environment [34, 35].
One of the key features of FHSS is the ability to quickly switch frequencies based on environmental conditions. The hopping sequence can be represented mathematically as:

$$f_h(t) = f_0 + \Delta f . H(t) \quad (3)$$

Where:

- $f_h(t)$Is the frequency at time *t*.
- f_0Is the base frequency.

- Δf Is the step size between hops.
- $H(t)$ He hopping sequence can be adaptive based on signal conditions or interference.

Using the features of adaptive filtering, machine learning, and radio cognitive attributes, drones can select frequencies less susceptible to interferences and jamming based on environmental factors and historical data. This lets UAVs make better use of the spectrum and, in doing so, allows other entities to work on their tasks without interference. For example, SIGINT systems have the Frequency Spectrum Monitoring & Tracking feature that helps avoid frequencies currently used by any other entity, greatly sub-optimized communication channels, and situational awareness while conducting their roles. It could also be used as a feature that requires a communication channel with a low error rate at the receivers facilitated by frequency hopping and known advanced signal processing [36, 37].

In dynamic environments, where the characteristics of the environment (like terrain, weather, and urban structures) can cause multipath fading and signal degradation, equalization and diversity combining processing techniques are essential to guarantee data accuracy. Doing so helps counteract the signal distortion effects of urban multipath while mitigating undesirable propagation simultaneously. UAVs can also achieve increased reliability of FHSS communications by leveraging spatial diversity using multiple antennas, known as MIMO (for numerous input and output) configurations. The potential impact of these technologies intertwining will pave the way to an era of communication that will strive to keep data throughput and connection robustness under high interference. As UAV systems become more integrated with advanced processing techniques, cybersecurity has a significant role other than improving frequency hopping algorithms [38, 39].

As drones increasingly employ sophisticated signal processing methods, they become more attractive targets for cyber threats. The use of offensive and defensive cyber techniques may be necessary to protect against vulnerabilities exploited by adversaries, especially those utilizing commercial off-the-shelf (COTS) components—an area well highlighted in studies, which indicate the susceptibility of COTS UAV systems to sophisticated attacks on their communication links [40]. Additionally, as seen in the capabilities of advanced aerial systems equipped with novel technologies, employing a holistic and layered approach to cybersecurity can significantly bolster the operational integrity of UAVs [42]. Integrating cyber resistance frameworks directly into the signal processing architecture enables UAVs to execute timely countermeasures while minimizing disruption to mission-critical tasks.

Moreover, advanced signal processing will contribute to streamlining drone operation dynamics and improve their performance through efficient operation in cooperating scenarios. Swarm technology, which allows multiple drones to carry out coordinated operations, relies on solid communication systems that can recover quickly and keep the connection during interruptions. More sophisticated processing techniques allow the UAVs to share data more rapidly and effectively with each other, often in real-time, making them significantly more capable when working as part of a team in scenarios such as disaster response or military operations.

Drones using cognitive radio networks allow them to individually adapt their own frequency hopping patterns based on the group's holistic operating circumstances of all nearby drones, ensuring minimum secure communication quality is reached while maximizing standard frequency use. This calls for migrating legacy centralized communication strategies to more decentralized approaches that enable the UAVs enough agility to perform appropriately in dynamic environments.

Integrating advanced signal processing techniques into the frequency hopping communication framework for drones is not just a matter of enhancing security and reliability—it represents a necessary evolution in the resilience of UAV operations against interference and jamming threats.

C. Case Studies on Successful Implementations of Enhanced Frequency Hopping

Analysis of frequency-hopping techniques in the context of military and advanced commercial markets has revealed several case studies that show FH systems are likely to prove successful for drone operations in the future. Using case studies through various organizations provides a compelling picture of how these methods have been used to address identified communication vulnerabilities and improve operational efficiencies. Secure and reliable communication is indispensable. For example, frequency hopping algorithms have become more widespread in military operations where uncrewed aerial vehicles (UAVs) are operated. One of the most prominent examples was the U.S. Navy's development and deployment of a frequency hopping system to avoid potential jamming threats posed by enemies.
These systems have integrated adaptive algorithms that can actively change hopping patterns based on situational context, enabling communication integrity even in the most heavily contested environments. This has ultimately allowed for real-time tactical adjustments during missions. These implementations have shown substantial performance improvements, making drone communications less likely to be intercepted and not as vulnerable to attackers, increasing the number of successful missions [41]. Commercially, better frequency hopping has also made drone deliveries safer and more efficient. Some companies have used EFH to ensure drones can safely communicate with control systems even when other communications might operate within the congested airspace above cities. An example of this can be found in a primary logistics provider that has installed frequency-hopping technology on its delivery drones to allow them to work within metropolitan areas, as urban clutter makes things problematic for the utilization of older styles of communication. In this frequency, a wider range of hops enables a lower probability of signal collision in other places. It guarantees that the control data sent is robust, reliable, and safe. Success in this area has broader implications beyond communication reliability, as regulatory bodies mandate licensed secure radio links for drone operations over populated areas [4].

On the other hand, frequency hopping is essential for advanced drone systems, which use a spectrum for constant communication between UAVs and ground stations, such as in military surveillance. Many drones working together in the same place, i.e., deploying them in a swarm, required complex architecture, mainly to avoid any one unit from interfering with another, even at such close distances demanded intelligent communications mechanisms. By coordinating the frequency hopping of all drones, research shows that communication loss and jamming can be significantly reduced, allowing effective data sharing and flight control cooperation across a large drone fleet comprising several different models. This level of coordination is essential in operational scenarios requiring timing and precision, such as reconnaissance missions [43].

Another successful instance can be drawn from research on using software-defined radios (SDRs) in drone communications. This innovative technology allows for dynamic frequency hopping capabilities, enabling drones to adapt to changing electromagnetic environments. Various experimental studies demonstrate that SDR-equipped drones employing enhanced frequency hopping have shown remarkable resilience against jamming attempts. The versatility of SDRs positions them as a strong candidate for future drone communication architecture, providing opportunities for enhanced electromagnetic spectrum sensing and employment during critical operations [44].

Moreover, these developments inherently address the issue of scalability, meaning that communication methods can grow as UAV technologies develop without the need to be replaced and rebuilt. Thus, the evidence from the successful practice of improving the frequency hopping communication technology in drone operations proves the potential of innovative strategic communication methods. It turns out that frequency hopping strengthens the drone communication network to the greatest extent, and the opportunities it opens up are progressive and change the approach to the whole area. Drones can operate and organize their interactions with the rest of the devices in the airspace environment

more safely and effectively. Removing the ineffective boundaries for new opportunities creates a unique communication and airspace environment for the expanded scope of drone operations.

5. Conclusion

The study explores the challenges of frequency hopping in drone communications, focusing on the unique challenges uncrewed aerial vehicles (UAVs) face in civilian and military applications. The research highlights the vulnerabilities of current FHSS algorithms, such as susceptibility to jamming, limitations of current algorithms, and the complex electromagnetic landscapes in which drones commonly operate. These issues are critical for advancing drone communications systems, ensuring they can perform securely and efficiently in increasingly congested airspaces.

The analysis of existing literature highlights the need for adaptive strategies that leverage real-time environmental data to optimize communication. Current solutions lack the adaptability to respond to dynamic conditions, exposing drone operations to disruption. This narrative directs attention towards the imperative need for further innovation, urging researchers and industry stakeholders to contribute to more robust and resilient communication frameworks.

The results also reveal critical flaws in frequency hopping communication and suggest ways to prevent such vulnerabilities from being exploited. The study on adaptive algorithms, the integration of machine learning, and the need for software-defined radio systems underlines the demand for a new design paradigm for FHSS in UAVs. These methods are expected to make communication systems more agile and efficient while providing better protection against interference and jamming attacks.

These implications go beyond specific technical changes, as they argue for a regulatory regime in which drones can be used safely in collaboration with other airspace users, representing the crucial balancing act between innovation and safety required to integrate UAV technologies under operational conditions effectively.

The review also highlights several gaps in the current body of research that warrant further exploration. Future studies should investigate the performance of adaptive frequency hopping algorithms in real-world scenarios, integrate real-time data analytics and cognitive radio technologies, and explore collaborative communication frameworks among multiple drones. Swarm technology exemplifies the potential for enhanced operational capabilities, and studying how frequency hopping can be optimized for these scenarios could yield significant insights.

In conclusion, this research has thoroughly examined the problems and solutions related to frequency hopping in drone communications, each component intricately interlinked within the broader landscape of UAV operations. Critically analyzing the vulnerabilities of current frequency hopping systems and proposing innovative solutions contribute meaningful insights to the ongoing discourse surrounding drone communication technologies.

REFERENCES

1. Quamar, M. M., Al-Ramadan, B., Khan, K., Shafiullah, M., & El Ferik, S. (2023). Advancements and applications of drone-integrated geographic information system technology—A review. Remote Sensing, 15(20), 5039.

2. Lei, Z., Yang, P., & Zheng, L. (2018). Detection and frequency estimation of frequency hopping spread spectrum signals based on channelized modulated wideband converters. Electronics, 7(9), 170.
3. Ristić, V. B., Todorović, B. M., & Stojanović, N. M. (2022). Frequency hopping spread spectrum: History, principles, and applications. Vojnotehnički glasnik/Military Technical Courier, 70(4), 856-876.
4. Daud, S. M. S. M., Yusof, M. Y. P. M., Heo, C. C., Khoo, L. S., Singh, M. K. C., Mahmood, M. S., & Nawawi, H. (2022). Applications of drone in disaster management: A scoping review. Science & Justice, 62(1), 30-42.
5. Tripathi, A. K., Potnis, A. A., & Pushpad, A. (2016). A REVIEW ON FREQUENCY HOPPING SPREAD SPECTRUM-BASED ANTI-JAMMING IMPROVEMENT WITH ENCRYPTED SPREADING CODES.
6. Sharma, A., Vanjani, P., Paliwal, N., Basnayaka, C. M. W., Jayakody, D. N. K., Wang, H. C., & Muthuc, P. (2020). Communication and networking technologies for UAVs: A survey. Journal of Network and Computer Applications, 168, 102739.
7. Smart, G., Deligiannis, N., Surace, R., Loscri, V., Fortino, G., & Andreopoulos, Y. (2015). Decentralized time-synchronized channel swapping for ad hoc wireless networks. IEEE Transactions on Vehicular Technology, 65(10), 8538-8553.
8. Conley, K. (2019). Involuntary Signal-Based Grounding of Civilian Unmanned Aerial Systems (UAS) in Civilian Airspace.
9. Kulp, P., & Mei, N. (2020, October). A framework for sensing radio frequency spectrum attacks on medical delivery drones. In 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 408-413). IEEE.
10. Scheller, W. D. (2017). Detecting drones using machine learning (Master's thesis, Iowa State University).
11. Grigoryan, H., Kirakosyan, L., & Sargsyan, S. S. (2024). A method of protocol-aware multi-tone sweep jamming. Труды института системного программирования РАН, 36(3), 273-282.
12. Tripathi, A. K., Potnis, A. A., & Pushpad, A. (2016). A REVIEW ON FREQUENCY HOPPING SPREAD SPECTRUM-BASED ANTI-JAMMING IMPROVEMENT WITH ENCRYPTED SPREADING CODES.
13. Zhi, L., Jianhua, Z., Hao, C., Xu, G., & Jian, L. (2019). Parameter estimation of frequency hopping signals based on analog information converter. IET Communications, 13(13), 1886-1892.
14. Thiessen, C. M., Van Bossuyt, D. L., & Hale, B. (2023). Reducing Asymmetry in Countering Unmanned Aerial Systems. Naval Engineers Journal, 135(1), 83-93.
15. Fu, W., Hu, Z., & Li, D. (2020). A sorting algorithm for multiple frequency-hopping signals in complex electromagnetic environments. Circuits, Systems, and Signal Processing, 39, 245-267.
16. Steyn, C. (2022). Towards a critical review of cybersecurity risks in anti-poaching systems in South Africa.
17. Nichols, R. K., Mumm, H. C., Lonstein, W. D., Ryan, J. J., Carter, C., & Hood, J. P. (2020). Counter unmanned aircraft systems technologies and operations. New Prairie Press.
18. Šimon, O., & Götthans, T. (2022). A survey on using deep learning techniques for UAV jamming and deception. Electronics, 11(19), 3025.
19. Nichols, R. K., Mumm, H. C., Lonstein, W. D., Ryan, J. J., & Carter, C. (2018). Unmanned Aircraft Systems (UAS) in the Cyber Domain: Protecting USA's Advanced Air Assets.
20. Dai, M., Huang, N., Wu, Y., Gao, J., & Su, Z. (2022). Unmanned-aerial-vehicle-assisted wireless networks: Advancements, challenges, and solutions. IEEE Internet of Things Journal, 10(5), 4117-4147.

21. Concha Salor, L., & Monzon Baeza, V. (2023, October). Harnessing the Potential of Emerging Technologies to Break down Barriers in Tactical Communications. In Telecom (Vol. 4, No. 4, pp. 709-731). MDPI.
22. Ye, J., Zou, J., Gao, J., Zhang, G., Kong, M., Pei, Z., & Cui, K. (2021). A new frequency hopping signal detection of civil UAV based on improved k-means clustering algorithm. IEEE Access, 9, 53190-53204.
23. Zhao, J., Gao, F., Ding, G., Zhang, T., Jia, W., & Nallanathan, A. (2018). Integrating communications and control for UAV systems: Opportunities and challenges. IEEE Access, 6, 67519-67527.
24. Citoni, B., Fioranelli, F., Imran, M. A., & Abbasi, Q. H. (2019). Internet of Things and LoRaWAN-enabled future smart farming. IEEE Internet of Things Magazine, 2(4), 14-19.
25. Snyder, M. E. (2014). Foundations of coverage algorithms in autonomic mobile sensor networks. Missouri University of Science and Technology.
26. Conley, K. (2019). Involuntary Signal-Based Grounding of Civilian Unmanned Aerial Systems (UAS) in Civilian Airspace.
27. Poirot, V. (2022). Collaborative, Intelligent, and Adaptive Systems for the Low-Power Internet of Things. Chalmers Tekniska Hogskola (Sweden).
28. Zhu, J., Wang, A., Wu, W., Zhao, Z., Xu, Y., Lei, R., & Yue, K. (2023). Deep-learning-based recovery of frequency-hopping sequences for anti-jamming applications. Electronics, 12(3), 496.
29. Yajie, K., Yan, L., & Yijin, Z. (2022). Intelligent fast frequency hopping algorithm for UAV swarm anti-Jamming based on Bayesian Q-learning. Aerospace Control, 40(2), 73-78.
30. Akyildiz, I. F., Kak, A., & Nie, S. (2020). 6G and beyond: The future of wireless communications systems. IEEE Access, 8, 133995-134030.
31. Pärlin, K. (2023). Multifunction Radios and Interference Suppression for Enhanced Reliability and
32. Poirot, V., & Landsiedel, O. (2021, July). Dimmer: self-adaptive network-wide flooding with reinforcement learning. In 2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS) (pp. 293-303). IEEE.
33. Paranjothi, A., Tanik, U., Wang, Y., & Khan, M. S. (2019). Hybrid-Vehfog: a robust approach for reliable dissemination of critical messages in connected vehicles. Transactions on Emerging Telecommunications Technologies, 30(6), e3595.
34. Hashesh, A. O., Hashima, S., Zaki, R. M., Fouda, M. M., Hatano, K., & Eldien, A. S. T. (2022). AI-enabled UAV communications: Challenges and future directions. IEEE Access, 10, 92048-92066.
35. Gupta, L., Jain, R., & Vaszkun, G. (2015). Survey of essential issues in UAV communication networks. IEEE communications surveys & tutorials, 18(2), 1123-1152.
36. Zeng, Y., Zhang, R., & Lim, T. J. (2016). Wireless communications with uncrewed aerial vehicles: Opportunities and challenges. IEEE Communications Magazine, 54(5), 36-42.
37. Campion, M., Ranganathan, P., & Faruque, S. (2018). UAV swarm communication and control architectures: a review. Journal of Unmanned Vehicle Systems, 7(2), 93-106.
38. Jiang, W., Han, B., Habibi, M. A., & Schotten, H. D. (2021). The road towards 6G: A comprehensive survey. IEEE Open Journal of the Communications Society, 2, 334-366.
39. Lee, C. H., Thiessen, C., Van Bossuyt, D. L., & Hale, B. (2022). Using a cyber-attack approach, a systems analysis of energy usage and effectiveness of a counter-unmanned aerial system. Drones, 6(8), 198.
40. Hanif, A., Ahmed, S., Al-Naffouri, T. Y., & Alouin, M. S. (2023). Exploring the Synergy: A Review of Dual-Functional Radar Communication Systems. arXiv preprint arXiv:2401.00469.

41. Golphin III, A. N., & Offord, B. D. (2021). Counter-Unmanned Aerial Systems (C-UAS) Interoperability in the Global Geopolitical Environment (Doctoral dissertation, Naval Postgraduate School).
42. Kardaras, P. G. (2022). Design, Modeling, and Analysis of Satcoms for UAV operations.
43. DRONÓW, I. W. Z. INTERDISCIPLINARY CHALLENGES OF ANTI-DRONE EFFORTS.
44. Liles, K. H. (2021). ELECTROMAGNETIC SENSING WITH LOW-COST SOFTWARE DEFINED RADIO (Doctoral dissertation, Monterey, CA; Naval Postgraduate School).