PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

ABBES LAGHROUR KHENCHELA UNIVERSITY

Faculty: Science and Technology

Department of Electrical Engineering

Specialization: Telecommunications System

End Of Studies Dissertation

In view of obtaining the Master's degree

Theme

Security and Anti-Jamming Techniques in Drone (UAV) Wireless Communications

Presented by :

Miss. BRIK Nesrine

Thesis committee members:

President : **Dr. GHRIBI Khadidja**

Supervisor : **Prof. CHERGUI Laid**

Co-supervisor: **Dr. BENFARROUDJ Hafiza**

Examiner: **Dr. BOUALI Lazhar**

Academic Year 2025/2026

Résumé

Résumé

Ce mémoire étudie les techniques de protection des communications UAV contre le brouillage et le bruit impulsif. Les UAV utilisent des liaisons radio pour transmettre les commandes de contrôle, la télémétrie et les données de mission. Ces liaisons sont importantes pour la sécurité du vol, mais elles peuvent être perturbées par les interférences, le brouillage volontaire, l'interception, le spoofing et les bruits électromagnétiques. Le travail commence par une étude bibliographique des communications UAV, des technologies utilisées comme Wi-Fi, LTE, 5G et OFDM, ainsi que des principales menaces radio. Ensuite, une étude théorique compare plusieurs méthodes anti-jamming, notamment DSSS, FHSS, les techniques hybrides, le contrôle adaptatif, le beamforming, le codage, la diversité et le filtrage adaptatif CV-VSS-NLMS. Enfin, une étude expérimentale est réalisée pour analyser DSSS, FHSS et CV-VSS-NLMS. Les résultats montrent que le BER diminue lorsque Eb/N0 augmente. À 20 dB, le BER atteint 0,001 pour DSSS et 0,003 pour FHSS. La MSE du filtre CV-VSS-NLMS diminue aussi de 0,25 à 0,005. Ces résultats montrent que les trois techniques sont complémentaires pour améliorer la robustesse d'une communication UAV.

Mots clés : UAV, communication sans fil, anti-jamming, DSSS, FHSS, OFDM, CV-VSS-NLMS, BER, MSE.

Abstract

This thesis studies protection techniques for UAV communications against jamming and impulsive noise. UAVs use radio links to transmit control commands, telemetry and mission data. These links are essential for flight safety, but they can be affected by interference, intentional jamming, interception, spoofing and electromagnetic impulsive noise. The work first presents a bibliographic study of UAV communications, including wireless technologies such as Wi-Fi, LTE, 5G and OFDM, as well as the main radio security threats. Then, a theoretical study compares several anti-jamming methods, including DSSS, FHSS, hybrid techniques, adaptive control, beamforming, coding, diversity and CV-VSS-NLMS adaptive filtering. Finally, an experimental study is carried out to analyze DSSS, FHSS and CV-VSS-NLMS. The results show that BER decreases when Eb/N0 increases. At 20 dB, the BER reaches 0.001 for DSSS and 0.003 for FHSS. The MSE of the CV-VSS-NLMS filter also decreases from 0.25 to 0.005. These results show that the three techniques are complementary and can improve the robustness of UAV communication links.

Keywords: UAV, wireless communication, anti-jamming, DSSS, FHSS, OFDM, CV-VSS-NLMS, BER, MSE.

الملخص

تتناول هذه المذكرة دراسة تقنيات حماية اتصالات الطائرات بدون طيار من التشويش والضوضاء النبضية. تعتمد الطائرات بدون طيار على الروابط اللاسلكية من أجل إرسال أوامر التحكم، القياسات التليمترية، وبيانات المهمة. تعد هذه الروابط مهمة جدا لسلامة الطيران، لكنها قد تتأثر بالتداخلات، والتشويش المتعمد، والتنصت، والخداع، والضوضاء Wi-Fi الكهرومغناطيسية النبضية. بدأ العمل بدراسة ببليوغرافية حول اتصالات الطائرات بدون طيار والتقنيات المستعملة مثل إضافة إلى أهم التهديدات الراديوية. بعد ذلك تم تقديم دراسة نظرية لمجموعة من طرق مقاومة OFDM، و Gو 5 LTE و والتقنيات الهجينة، والتحكم التكيفي، وتشكيل الحزمة، والترميز، والتنويع، والترشيح التكيفي FHSS و DSSS التشويش مثل بينت النتائج أن CV-VSS-NLMS. و FHSS و DSSS وفي الجزء التجريبي تمت دراسة تقنيات CV-VSS-NLMS. و 0.003 بالنسبة لـ DSSS إلى 0.001 بالنسبة لـ BER وصلت قيمة dB عند 20 .Eb/N0 تنخفض عند زيادة BER قيمة من 0.25 إلى 0.005. تبين هذه النتائج أن التقنيات CV-VSS-NLMS الخاصة بالمرشح MSE كما انخفضت قيمة .FHSS الثلاث مكملة لبعضها، ويمكن استعمالها لتحسين موثوقية اتصالات الطائرات بدون طيار.

الكلمات المفتاحية: الطائرات بدون طيار، الاتصال اللاسلكي، مقاومة التشويش CV-VSS-، OFDM، FHSS، DSSS ،

NLMS، BER، MSE.

Acknowledgements

In the name of Allah, the Most Gracious, the Most Merciful. First and foremost, all praise is due to Allah, who granted me strength, patience, guidance, and determination to complete this work.

✦ To My Respected Professors and Teachers ✦

I would like to express my deep appreciation to my supervisor, **Prof. CHERGUI Laid**, for his valuable guidance, continuous support, and helpful advice throughout the preparation of this Master thesis. His remarks and encouragement greatly contributed to the improvement of this work.

My sincere thanks go to **Dr. GHRIBI Khadidja**, President of the thesis committee, for accepting to evaluate this work and for honoring me with her presence.

I am also grateful to **Dr. BOUALI Lazhar**, Examiner of this thesis, for taking the time to read and assess this work, and for his constructive comments and observations.

I would like to extend my thanks to all the teachers who contributed to my academic training during my years of study. Their efforts, knowledge, and guidance have played an important role in my educational journey.

Finally, I would like to thank my family, my friends, and everyone who supported me, directly or indirectly, during the preparation of this thesis. Their encouragement and moral support were very important to me.

Thank you all

Nessrine

Dedication

✦ To Myself ✦

I dedicate this work to myself, in recognition of my patience, perseverance, and determination throughout this academic journey. It has been a path filled with challenges and difficulties, yet I managed to overcome them with willpower and persistence. I am proud of every step I have taken to reach this stage. This achievement is the result of my personal effort and continuous belief in my abilities, and I dedicate it to my limitless ambition and constant desire for growth and success.

✦ To My Beloved Family ✦

I also dedicate this work to my beloved family, especially my parents, to whom words can never fully express my deep gratitude for their unconditional love, great sacrifices, and constant support. You have always been my greatest source of strength and inspiration, and without you, I would not be where I am today.

To my brothers zakou & ayoub , thank you for your love, encouragement, and continuous support. You have stood by me in both difficult and happy moments, and your presence has given me strength and confidence to keep going

✦ To My Dear Friends ✦

Finally, I dedicate this work to my dear friends, who have shared every part of this journey with me and stood by my side during stressful and difficult times, as well as moments of joy and success. Thank you for your true friendship, constant encouragement, and unwavering support. You have made this experience more meaningful and filled it with unforgettable memories (yakine, firouz ,baraa ,karima, rayan ,wiam , nihad ,rouaya, douaa, aya, chaima)

" Success belongs to those who believe in the beauty of their dreams "

List of Figures

List of Tables

List of Acronyms

Acronym	Meaning	Page
3GPP	3rd Generation Partnership Project	7
4G	Fourth Generation	11
5G	Fifth Generation	5
A2A	Air-to-Air	10
A2G	Air-to-Ground	10
ATC	Air Traffic Control	7
BER	Bit Error Rate	15
BPSK	Binary Phase Shift Keying	21
BVLoS	Beyond Visual Line-of-Sight	5
CNPC	Control and Non-Payload Communication	5
CP	Cyclic Prefix	13
CSI	Channel State Information	18
CW	Continuous Wave	16
CV-VSS-NLMS	Complex-Valued Variable Step-Size Normalized Least Mean Square	15
D2D	Device-to-Device	12
DL	Downlink	7
DS/FH-SS	Direct Sequence/Frequency Hopping Spread Spectrum	25
DSSS	Direct Sequence Spread Spectrum	6
Eb/N0	Energy per bit to noise power spectral density ratio	46
EFTP	Electrical Fast Transient Pulses	15
eMBB	enhanced Mobile Broadband	5
FFT	Fast Fourier Transform	13
FHSS	Frequency Hopping Spread Spectrum	6
G2G	Ground-to-Ground	10
GCS	Ground Control Station	5
GNSS	Global Navigation Satellite System	16
GPS	Global Positioning System	19
HVSP	High-Voltage Sinusoidal Pulses	15
IEEE	Institute of Electrical and Electronics Engineers	5
IFFT	Inverse Fast Fourier Transform	13
ISI	Inter-Symbol Interference	55
ITU	International Telecommunication Union	7
LMS	Least Mean Square	38
LoS	Line-of-Sight	5
LTE	Long-Term Evolution	5
MIMO	Multiple-Input Multiple-Output	12
mMTC	massive Machine-Type Communications	12
MSE	Mean Square Error	38
NLMS	Normalized Least Mean Square	15
NOMA	Non-Orthogonal Multiple Access	12
NR	New Radio	5
OFDM	Orthogonal Frequency Division Multiplexing	6
PG	Processing Gain	33
PN	Pseudo-Noise	20
PSK	Phase Shift Keying	13
QAM	Quadrature Amplitude Modulation	13

QPSK	Quadrature Phase Shift Keying	21
RF	Radio Frequency	22
SC-FDE	Single-Carrier Frequency-Domain Equalisation	14
SINR	Signal-to-Interference-plus-Noise Ratio	6
SNR	Signal-to-Noise Ratio	45
SP	Surge Pulses	15
SWaP	Size, Weight and Power	5
UAS	Unmanned Aerial System	6
UAV	Unmanned Aerial Vehicle	5
UAV-OFDM	Unmanned Aerial Vehicle - Orthogonal Frequency Division Multiplexing	6
UL	Uplink	7
URLLC	Ultra-Reliable Low-Latency Communication	5
Wi-Fi	Wireless Fidelity	5

Table of Contents

Chapter 02: Theoretical Study of Existing Anti-Jamming Methods

Chapter 03: Experimental Study of Anti-Jamming Techniques for UAV

General Introduction

Unmanned Aerial Vehicles, or UAVs, now have an important place in several civil, industrial and military fields. They are used for surveillance, precision agriculture, infrastructure inspection, search and rescue, environmental monitoring and delivery. This development makes the communication link essential, because the drone must exchange information with the ground control station, with other drones, or with terrestrial and satellite networks [1], [2].

In a UAV system, communication does not only carry mission data. It also carries flight commands, telemetry and safety information. Command and control communication, called CNPC, requires high reliability and low latency. On the other hand, payload data, such as images, video or sensor measurements, often requires a higher data rate [1]. This difference makes the design of the radio link more difficult, especially when the drone has limitations in size, weight, energy and processing capacity.

Several wireless technologies can be used for UAV communications. Wi-Fi is simple and low-cost, but it remains more suitable for local missions and can be limited by interference and range [3]. LTE networks allow wider connectivity and can support beyond-line-of-sight missions, but they may experience frequent handovers and interference when the drone flies at altitude [4]. 5G networks bring new possibilities through high data rate, low latency and the flexible deployment of relay drones or aerial stations [5]. At the same time, OFDM remains an important physical-layer technique, because it helps to manage frequency-selective channels and multipath propagation [6].

However, the UAV radio channel remains open and vulnerable. Jamming attacks can reduce the signal-to-interference-plus-noise ratio, increase the bit error rate and cause a link loss. Interception attacks can threaten data confidentiality, especially in channels dominated by line- of-sight propagation. Spoofing attacks can inject false navigation or control information and change the drone behavior [7], [12]. In addition to intentional jamming, UAV-OFDM communications can also be affected by impulsive noise of electromagnetic origin, which increases errors at the receiver side [20].

To deal with these problems, several anti-jamming methods have been studied. DSSS spreads the signal using a pseudo-random sequence and provides a useful processing gain against narrowband jamming [26]. FHSS changes the carrier frequency according to a hopping sequence, which makes it possible to avoid disturbed frequencies and to better resist partial-band jamming [31]. Other solutions also exist, such as adaptive power and frequency control, beamforming, coding, diversity and cognitive methods [11], [39]. In UAV-OFDM chains, the CV-VSS-NLMS filter represents a complementary solution, because it acts at the receiver side to reduce impulsive noise with a single-antenna architecture [20], [42].

The general problem of this thesis can therefore be formulated as follows: how can the robustness of a UAV communication link be improved against jamming and impulsive noise, while taking into account the practical constraints related to drones, such as energy, mobility, bandwidth and processing complexity?

The main objective of this work is to study and compare several techniques for protecting UAV communications against radio disturbances. More specifically, it aims to analyse UAV communication needs, present the main radio threats, study existing anti-jamming methods theoretically, and then carry out an experimental study based on DSSS, FHSS and CV-VSS-NLMS. The performances are observed using two main metrics: BER for DSSS and FHSS, and MSE for CV-VSS-NLMS filtering.

This thesis is organized into three chapters. The first chapter presents a bibliographic study on UAV communications, their architectures, the wireless technologies used, OFDM and the main security threats. The second chapter develops a theoretical study of existing anti- jamming methods and compares their advantages and limitations according to criteria such as processing gain, SINR, BER, energy consumption, bandwidth and complexity. The third chapter presents the experimental study, the parameters used, the generated signals, the BER/MSE results and the interpretation of the performances of DSSS, FHSS and CV-VSS-NLMS.

Thus, this work seeks to show that the robustness of UAV communication does not rely on one technique only. A multilayer approach, combining spread spectrum, frequency hopping and adaptive filtering at the receiver, can offer better protection according to the nature of the disturbance and the constraints of the mission.

References

[1] Y. Zeng, Q. Wu, and R. Zhang, "Accessing From the Sky: A Tutorial on UAV Communications for 5G and Beyond," Proceedings of the IEEE, vol. 107, no. 12, pp. 2327-2375, Dec. 2019.

[2] A. L. Imoize, S. M. N. Islam, T. Poongodi, L. K. Ramasamy, and B. V. V. Siva Prasad, Eds., Unmanned Aerial Vehicle Cellular Communications, Springer, 2022.

[3] B. Van den Bergh, A. Chiumento, and S. Pollin, "Ultra-Reliable IEEE 802.11 for UAV Video Streaming: From Network to Application," Springer, 2017.

[4] X. Lin et al., "The Sky Is Not the Limit: LTE for Unmanned Aerial Vehicles," IEEE Communications Magazine, vol. 56, no. 4, pp. 204-210, Apr. 2018.

[5] B. Li, Z. Fei, and Y. Zhang, "UAV Communications for 5G and Beyond: Recent Advances and Future Trends," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2241-2263, 2019.

[6] Y. Li and G. L. Stuber, Eds., Orthogonal Frequency Division Multiplexing for Wireless Communications, Springer, 2006.

[7] G. K. Pandey, D. S. Gurjar, H. H. Nguyen, and S. Yadav, "Security Threats and Mitigation Techniques in UAV Communications: A Comprehensive Survey," IEEE Access, vol. 10, pp. 112858-112897, 2022.

[11] M. A. Aref, S. K. Jayaweera, and E. Yepez, "Survey on cognitive anti-jamming communications," IET Communications, 2020.

[12] O. Ceviz, S. Sen, and P. Sadioglu, "A Survey of Security in UAVs and FANETs: Issues, Threats, Analysis of Attacks, and Solutions," arXiv:2306.14281v4, 2024.

[20] W. Lebbou, L. Chergui, and S. Bouguezel, "Noise-suppression method for UAV-OFDM systems by introducing CV-VSS-NLMS algorithm and single-antenna architecture," TELKOMNIKA, vol. 24, no. 2, pp. 407-419, Apr. 2026.

[26] J. G. Proakis and M. Salehi, Digital Communications, 5th ed., McGraw-Hill, 2008.

[31] D. Roberts, "Spread Spectrum: Basics — Spread Spectrum — Error Correction — Inter-LAN," Stanford University, 2003.

[39] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 767-809, 2022.

[42] W. Lebbou, L. Chergui, and S. Bouguezel, "Noise-suppression method for UAV-OFDM systems by introducing CV-VSS-NLMS algorithm and single-antenna architecture," TELKOMNIKA Telecommunication Computing Electronics and Control, vol. 24, no. 2, pp. 407-419, Apr. 2026.

Chapter 01: Bibliographic Study

1.1. Introduction

Unmanned Aerial Vehicles (UAVs) have evolved from predominantly military platforms into versatile systems used in surveillance, precision agriculture, infrastructure inspection, search-and-rescue, environmental monitoring, and package delivery [1]. This expansion has made wireless communication a central element of UAV design, because the aircraft must remain connected to a Ground Control Station (GCS), and, in advanced deployments, to relay UAVs, terrestrial networks, satellite links, and cloud services.

UAV communication must satisfy two categories of requirements. Control and Non-Payload Communication (CNPC) carries command, control, telemetry, and safety information; therefore, it requires high reliability and low latency. Payload communication carries mission data such as images, video streams, and sensor measurements; therefore, it usually requires higher throughput. These needs are constrained by the size, weight, and power (SWaP) limitations of UAV platforms, which turns communication design into a multi-objective engineering problem [1].

Several wireless technologies have been investigated to meet these requirements. IEEE 802.11 (Wi-Fi) offers low-cost and high-throughput connectivity in unlicensed bands, but its reliability can degrade because of interference and limited range. LTE enables beyond visual line-of-sight (BVLoS) connectivity through cellular infrastructure, although aerial users introduce altitude-dependent interference and frequent handovers [4]. The 5G New Radio (NR) ecosystem extends this vision through ultra-reliable low- latency communication (URLLC), enhanced mobile broadband (eMBB), massive connectivity, and UAV-assisted network deployment [5]. In addition to these access technologies, recent work on UAV-OFDM links has highlighted the need for lightweight impulsive-noise suppression methods, especially when electromagnetic pulses degrade the complex-valued OFDM signal at the receiver [20].

At the same time, the open wireless medium exposes UAV links to major security threats. Jamming attacks intentionally reduce the Signal-to-Interference-plus-Noise Ratio (SINR), interception attacks exploit the often dominant Line-of-Sight (LoS) channel to capture confidential data, and spoofing attacks inject false navigation or control information [7], [12]. These threats motivate the study of robust anti-jamming techniques such as Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), adaptive power and frequency control, and beamforming.

This chapter presents the technical background required for the remainder of the work. It first reviews UAV communication systems, their architecture, and the main wireless technologies. It then describes OFDM as a key physical-layer technique used in modern wireless systems. The chapter subsequently analyses security threats in UAV communications and compares major anti-jamming techniques. The final discussion identifies the spread-spectrum principles that justify a more focused theoretical analysis of anti-jamming methods in the following chapter.

1.2. UAV Communication Systems

1.2.1. Overview of UAV Communication Requirements [1]

Wireless communication is an enabling technology for unmanned aerial systems (UAS). UAVs must exchange safety-critical information with remote pilots, nearby aerial vehicles, and air traffic control entities to ensure safe and reliable flight. This category is commonly referred to as CNPC. Depending on the mission, UAVs may also transmit or receive payload data such as high-resolution images, video streams, and sensor measurements to or from operators, end users, or ground gateways.

CNPC and payload communication differ in their performance priorities. CNPC generally requires only a low data rate, typically in the order of tens of kilobits per second, but it imposes strict requirements on reliability and latency. Payload communication, by contrast, often requires much higher throughput, especially for real-time video transmission.

Link direction	Data type	Data rate	Reliability	Latency
DL (Ground station to UAV)	Command and control	60-100 Kbps	<= 10^-3 packet error rate	<= 50 ms
UL (UAV to ground station)	Command and control	60-100 Kbps	<= 10^-3 packet error rate	<= 50 ms
Application data	Payload / mission data	Up to 50 Mbps	Mission-dependent	Similar to terrestrial services

TABLE 1: UAV communication requirements specified by 3GPP [1].

The ITU classifies CNPC functions into three operational categories:

A. Command and control:

Telemetry reporting from the UAV to the ground pilot, telecommand signalling from the ground station to the UAV, and periodic command updates for autonomous missions.

B. Air Traffic Control (ATC) relay:

Communication between air traffic control and the GCS through the UAV to avoid safety conflicts with manned aviation.

C. Sense and avoid support:

Exchange of information that helps the UAV maintain safe separation from other aerial vehicles, terrain, and obstacles.

Payload communication depends strongly on the application. Full high-definition video generally requires several megabits per second, while 4K video can exceed 30 Mbps. Table 2 summarises typical requirements for common UAV applications.

UAV application	Height coverage (m)	Payload latency (ms)	Payload data rate (DL/UL)
Drone delivery	100	500	300 Kbps / 200 Kbps
Drone filming	100	500	300 Kbps / 200 Kbps
Access point	500	500	50 Kbps / 200 Kbps
Surveillance	100	3000	300 Kbps / 200 Kbps
Infrastructure inspection	100	3000	300 Kbps / 200 Kbps
Drone fleet show	200	100	200 Kbps / 200 Kbps
Precision agriculture	300	500	300 Kbps / 200 Kbps
Search and rescue	100	500	300 Kbps / 200 Kbps

TABLE 2: Communication requirements for typical UAV applications [1].

Four categories of wireless solutions are commonly considered for UAV communication: direct links, satellite communication, ad-hoc networking, and cellular networking. Their suitability depends on range, capacity, cost, scalability, and SWaP constraints. Direct links are simple but limited; satellite communication offers global coverage but has high cost, latency, and equipment constraints; ad-hoc networks provide flexibility but require complex routing; and cellular networks provide wide-area connectivity when terrestrial coverage is available.

Technology	**Description**	**Advantages**	**Disadvantages**
Direct link	Direct point-to-point communication with a ground node.	Simple and low cost.	Limited range, limited data rate, vulnerable to interference, and difficult to scale.
Satellite	Communication and Internet access through satellite links.	Global coverage.	Costly, bulky, energy-consuming equipment, high latency, and significant signal attenuation.
Ad-hoc network	Self-organising and infrastructure-free network.	Robust, adaptable, and suitable for high mobility.	Complex routing, intermittent connectivity, cost, and lower spectrum efficiency.
Cellular network	Communication using terrestrial cellular infrastructure.	Wide accessibility, cost effectiveness, good performance, and scalability.	Unavailable in remote areas and may create interference with terrestrial users.

TABLE 3: Comparison of wireless technologies for UAV communication.

1.3. Architecture of UAV Communication Systems [2]

A UAV communication architecture usually includes onboard transceivers, antennas, processing units, navigation sensors, a GCS, and, when required, relay nodes, satellite links, or cloud-based services. The architecture must support reliable Air-to-Ground (A2G), Air-to-Air (A2A), Ground-to-Ground (G2G), and satellite communication paths. It must also combine radio design, antenna placement, network protocols, and management functions so that the UAV can operate safely under mobility, altitude variation, and interference constraints.

Figure 1 illustrates examples of UAV communication modules and antenna- related requirements. These elements affect the available bandwidth, coverage area, payload capacity, cost, and resistance to interference.

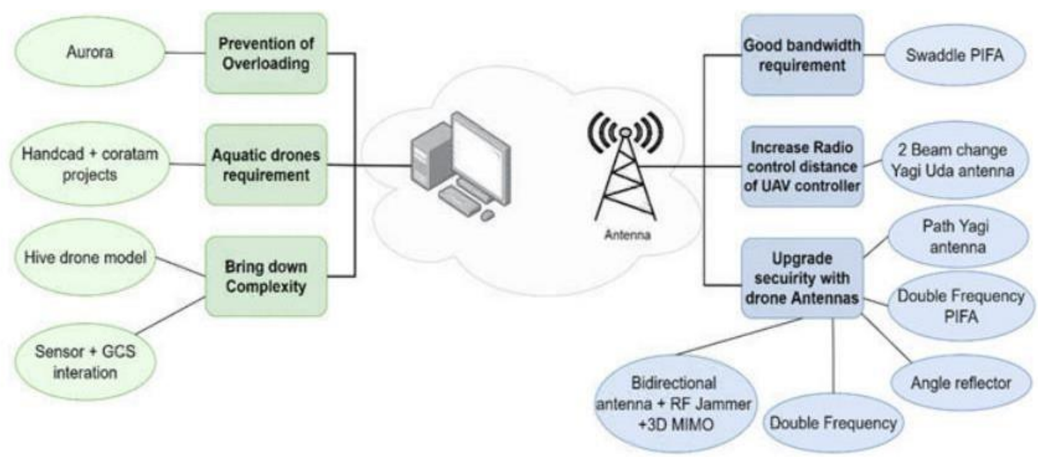

Fig. 1: Drones and antennas holding different communication modules.

1.4. Wireless Technologies Used in UAV Communications

Wireless technologies used in UAV systems must support command and control, telemetry, and payload data transmission. The choice of technology depends on the mission profile, required range, throughput, latency, reliability, and deployment environment.

1.4.1. Wi-Fi (IEEE 802.11) [3]

IEEE 802.11, commonly known as Wi-Fi, is widely used in UAV systems because it is inexpensive, widely available, and capable of high throughput in unlicensed spectrum. Compared with dedicated point-to-point microwave links, Wi-Fi is easier to deploy and does not require large ground station infrastructure.

Wi-Fi is particularly suitable for short-range payload transmission, including video streaming, and it can also support control communication in local missions. However, aerial operation changes the interference conditions. As the UAV altitude increases, the aircraft may receive signals from a larger number of access points because of reduced shadowing. This improves visibility to the network but can also increase co- channel interference and reduce link reliability.

To address these limitations, multi-access-point strategies and application-layer error correction can be used to improve reliability. Nevertheless, Wi-Fi remains most appropriate for local or short-range missions rather than wide-area BVLoS operation.

1.4.2. LTE (4G Long-Term Evolution) [4]

Long-Term Evolution (LTE), commonly known as 4G, is a promising technology for UAV communication because it offers wide-area coverage, secure connectivity, and relatively high data rates. Unlike Wi-Fi, LTE can support BVLoS missions, which are essential for delivery, surveillance, infrastructure inspection, and search-and-rescue applications.

Many small UAVs use Wi-Fi by default, but this is not sufficient for missions that require continuous connectivity over large geographic areas. Cellular networks provide a scalable alternative by using existing infrastructure. This potential motivated 3GPP studies on enhanced LTE support for aerial vehicles.

However, LTE-based UAV communication also introduces challenges. At higher altitudes, UAVs are more likely to establish LoS paths with several base stations, which can increase interference. UAV mobility across cells also creates frequent handovers, potentially affecting latency and reliability. Despite these constraints, field trials have demonstrated that terrestrial LTE networks can provide practical connectivity for small UAVs.

1.4.3. 5G New Radio (5G NR) [5]

5G NR is designed to support highly diverse service requirements, including eMBB, URLLC, and mMTC. These capabilities are relevant to UAV systems because UAVs may require high-throughput payload links, low-latency command and control, and connectivity for large numbers of devices or aerial nodes.

UAVs can also contribute to 5G networks by acting as aerial base stations, relays, or temporary infrastructure in disaster-stricken areas. Their flexible deployment allows rapid restoration or extension of network coverage when terrestrial infrastructure is damaged or unavailable.

Three attributes make UAV-assisted 5G communication attractive. First, UAVs often have a higher probability of LoS links with ground users. Second, they can be dynamically positioned to improve coverage and link quality. Third, swarms of UAVs can form scalable multi-UAV networks to provide ubiquitous connectivity.

The altitude of a UAV creates a trade-off: higher altitude increases the probability of LoS propagation, but it also increases propagation distance and path loss. To improve spectrum and energy efficiency, research on UAV communications increasingly considers massive MIMO, millimetre-wave communication, non-orthogonal multiple access (NOMA), device-to-device (D2D) communication, and cognitive radio.

1.5. Modulation and Multiple Access Techniques

1.5.1. Orthogonal Frequency Division Multiplexing (OFDM) [6]

OFDM is a multi-carrier modulation technique in which data symbols are transmitted over a set of orthogonal sub-carriers. Although the spectra of the sub-carriers overlap, orthogonality allows the receiver to separate them, resulting in high spectral efficiency.

OFDM is particularly useful in channels with delay spread and frequency selectivity, because it converts a frequency-selective channel into multiple approximately flat sub-channels.

The sub-carrier spacing must be selected in relation to the channel coherence bandwidth. When this spacing is properly designed, equalisation becomes simpler, and techniques originally developed for flat fading channels can be applied to each sub- carrier. This explains why OFDM is a core physical-layer technique in modern wireless systems such as Wi-Fi, LTE, and 5G NR.

1.5.2. OFDM Transmitter and Receiver Concept

In a basic OFDM transmitter, a block of N data symbols, usually chosen from a QAM or PSK constellation, is processed by an N-point Inverse Fast Fourier Transform (IFFT). A cyclic prefix (CP) is then inserted by repeating the last samples of the OFDM symbol. The CP reduces inter-symbol interference caused by multipath delay spread, although it introduces a bandwidth and power overhead.

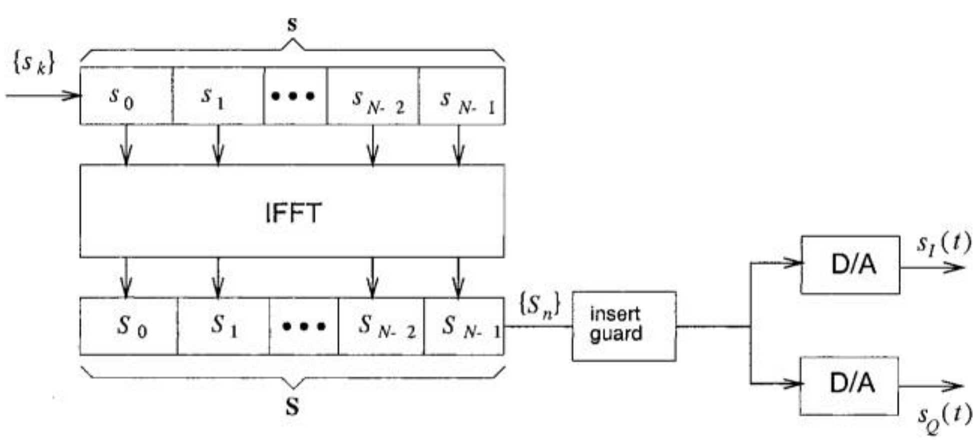

Fig. 2: Block diagram of a basic OFDM transmitter.

At the receiver, the cyclic prefix is removed, and the received samples are transformed back into the frequency domain using the Fast Fourier Transform (FFT). Each sub-carrier can then be equalised using a one-tap frequency-domain equaliser to recover the transmitted symbols.

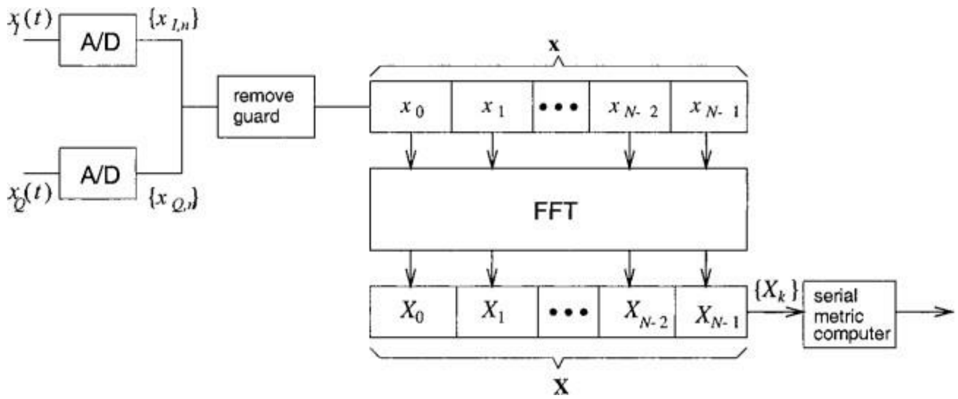

Fig. 3: Block diagram of a basic OFDM receiver.

Single-Carrier Frequency-Domain Equalisation (SC-FDE) has a structure and complexity comparable to OFDM. The main difference is that OFDM applies the IFFT at the transmitter and the FFT at the receiver, whereas SC-FDE avoids the transmitter-side transform and performs FFT/IFFT processing mainly at the receiver [6].

1.5.3. Impulsive Noise Suppression in UAV-OFDM Systems [20]

Although OFDM is robust against frequency-selective fading and can mitigate inter-symbol interference through the cyclic prefix, UAV-OFDM links remain vulnerable to impulsive electromagnetic interference. Such interference may be produced by high-voltage sinusoidal pulses, electrical fast transient pulses, surge pulses, switching processes, ignition noise, and nearby electromagnetic sources. When these pulses are frequent or strong, they can raise the error probability of the OFDM receiver and reduce the reliability of payload and control-related transmissions [20].

Earlier OFDM-based UAV noise-suppression approaches relied mainly on blind source separation using a dual-antenna architecture. These methods can separate useful OFDM signals from electromagnetic pulse noise, but they require de-meaning, covariance estimation, whitening, iterative separation, and convergence testing. Therefore, their block-based processing and matrix operations increase computational complexity, which may limit their suitability for real-time SWaP-constrained UAV platforms [20].

A recent contribution by Lebbou, Chergui, and Bouguezel proposed a complex-valued variable step-size normalized least mean square (CV-VSS-NLMS) algorithm combined with a single-antenna receiver architecture for UAV-OFDM systems. The method uses three adaptive noise cancellers associated with three impulsive-noise models, namely high-voltage sinusoidal pulses (HVSP), electrical fast transient pulses (EFTP), and surge pulses (SP). A cost-function module then selects the best de-noised signal according to the average residual energy. This approach is important for this thesis because it complements anti-jamming techniques with adaptive receiver-side noise suppression, while reducing the number of matrix operations and improving BER performance under impulsive interference [20].

1.6. Security Threats in UAV Communications [7]

UAV communication links are exposed to both cyber and physical threats. Depending on the technology used, risks may differ across cellular, satellite, and Wi-Fi links. UAVs controlled through Wi-Fi or operating in multi-tier networks can be particularly vulnerable because attackers may target both the communication link and the stored data.

Physical access to a damaged or captured UAV may allow attackers to retrieve data through interfaces such as USB, JTAG, or embedded debugging ports. More advanced attacks may involve embedded system decryption, side-channel analysis, or fault injection. Therefore, communication security must be complemented by encryption, secure key management, and hardware protection mechanisms.

At the communication layer, three threats are especially important for UAV systems: jamming, interception, and spoofing. These threats directly affect availability, confidentiality, integrity, and navigation reliability.

Besides deliberate cyber or radio attacks, UAV-OFDM communication may also be affected by non-intentional or environmental impulsive electromagnetic noise. This type of disturbance differs from strategic jamming because it is not necessarily generated by an intelligent adversary; however, its physical-layer effect is similar in practice, since it degrades the useful signal and increases BER. For this reason, receiver-side impulsive-noise suppression is a relevant complementary protection mechanism for UAV communication reliability [20].

1.7. Jamming Attacks

Jamming attacks occur when an adversary deliberately transmits interference in order to prevent a receiver from extracting the legitimate signal. Such attacks may target UAV control links, payload links, inter-UAV links, or navigation signals. Because UAV communication often relies on open wireless channels and LoS propagation, it is particularly exposed to intentional interference [7], [8].

1.7.1. Types of Jamming

Jammers are malicious wireless nodes or devices designed to generate intentional interference. Their effectiveness depends on their transmitted power, location, bandwidth, duty cycle, and knowledge of the target waveform. The most common categories are summarised below.

D. Continuous Wave (CW) jamming:

A narrow tone is transmitted on or near a GNSS or communication carrier frequency, reducing the receiver ability to correlate or demodulate the legitimate signal [9].

E. Broadband noise jamming:

Noise is transmitted over a wide frequency range, raising the noise floor and potentially affecting multiple GNSS constellations or communication channels [9].

F. Barrage or swept jamming:

Energy is spread across a large portion of the target spectrum, often with a high duty cycle. This approach is simple but consumes more power [10].

G. Partial-band jamming:

Only a fraction of the frequency band is jammed. It can be efficient against some single-carrier systems, but strong coding may reduce its effectiveness against OFDM signals [10].

H. Reactive or follow-on jamming:

The jammer senses the channel and starts transmitting only when legitimate activity is detected. This makes it more energy-efficient and more difficult to detect than continuous jamming [11].

I. Cognitive or smart jamming:

The jammer uses sensing and learning capabilities to identify transmission patterns and adapt its strategy while minimising power, bandwidth, and duty-cycle consumption [11].

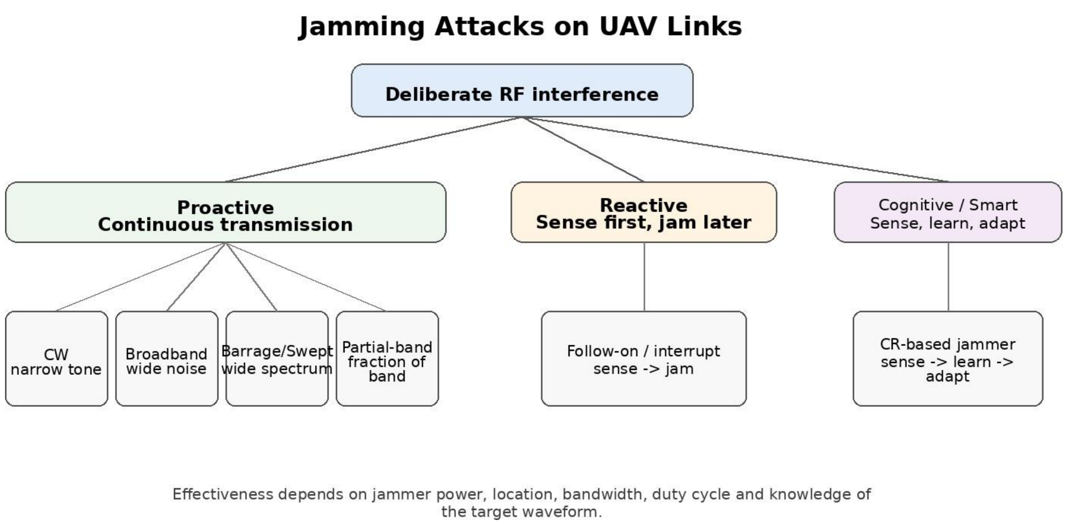

Fig. 4: Simplified taxonomy of jamming attacks on UAV links.

1.7.2. Impact on UAV Communications

The main impact of jamming is the degradation of SINR, which increases bit error rate, reduces data rate, and may interrupt the communication link. In the case of CNPC links, this can compromise flight safety by delaying or blocking control commands. In payload links, it can degrade video quality, sensor data delivery, and mission awareness.

Jamming can also affect inter-UAV communication in swarm networks. Internal or external interference may reduce coordination reliability, increase latency, and weaken collaborative mission execution. In navigation systems, GNSS jamming can prevent the UAV from obtaining reliable positioning information, which may force fallback navigation modes or mission abortion.

1.8. Interception Attacks

Interception attacks, also called eavesdropping attacks, occur when an unauthorised party captures UAV communication. Passive eavesdropping only listens to the communication without disrupting it, while active eavesdropping may combine interception with jamming, message modification, or injection of false data.

The LoS-dominant nature of UAV channels can increase interception risk. A receiver positioned within the propagation path may obtain a strong copy of the transmitted signal. If the attacker gains Channel State Information (CSI) or benefits from favourable propagation conditions, the confidentiality of the UAV link becomes more difficult to preserve [12].

Full-duplex and cooperative half-duplex eavesdropping scenarios create additional risks. In full-duplex attacks, an adversary may jam the legitimate receiver while simultaneously intercepting the confidential signal. In cooperative half-duplex attacks, different adversarial nodes may divide these tasks to imitate full-duplex behaviour. Both cases can force the UAV to increase transmission power, which may unintentionally strengthen the eavesdropper signal.

1.9. Spoofing Attacks

Spoofing attacks introduce falsified information into the UAV system. Passive spoofing captures and observes data without directly modifying system behaviour, whereas active spoofing injects or modifies information to influence the UAV trajectory or control decisions. GPS spoofing is the most common example: a malicious transmitter sends fake positioning signals to mislead the UAV navigation system.

Because sensors may not always distinguish genuine data from falsified data, spoofing can cause the UAV to deviate from its planned route, behave unpredictably, lose communication with the remote controller, or fly toward an unintended location where it can be damaged or captured. Experimental studies have shown that commercial drones can be vulnerable to GPS spoofing under certain conditions [12].

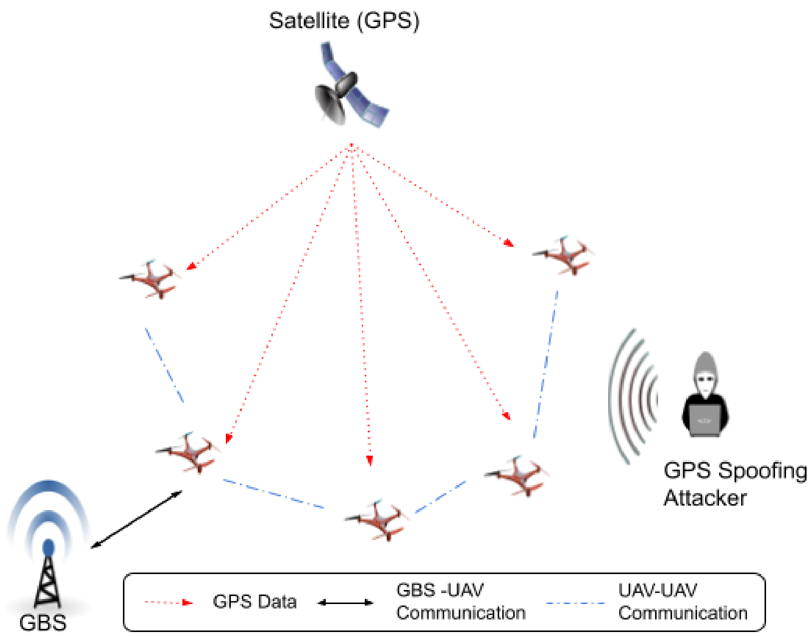

Fig. 5: Example of a GPS spoofing attack.

1.10. Anti-Jamming Techniques for UAV Communications

1.10.1. Introduction to Anti-Jamming Techniques [13]

UAV communications face increasingly complex interference conditions, especially in dynamic and adversarial environments. Anti-jamming techniques aim to maintain reliable communication by reducing the impact of intentional interference on control, telemetry, payload, and navigation links.

Classical anti-jamming methods include spread-spectrum techniques such as DSSS and FHSS, interference suppression, adaptive frequency selection, power control, and spatial filtering through beamforming. These methods differ in complexity, bandwidth cost, hardware requirements, and suitability for small UAVs. In practice, no single method is optimal for all scenarios, which motivates a comparative analysis before selecting the technique for this work.

1.10.2. Frequency Hopping Spread Spectrum (FHSS)

FHSS spreads a narrowband information signal by rapidly changing the carrier frequency according to a pseudo-random hopping sequence known by the legitimate transmitter and receiver. The signal remains on each frequency for a short dwell time before moving to another frequency. This makes it difficult for an attacker to predict the next carrier frequency unless the hopping sequence is known.

FHSS is effective against narrowband and partial-band jamming because the jammer must either predict the hopping pattern or jam a large portion of the band. Its main limitation is that a sufficiently powerful broadband jammer can still affect the system. Synchronisation between transmitter and receiver is also critical, especially in mobile UAV channels with Doppler shifts and fast link variations [15].

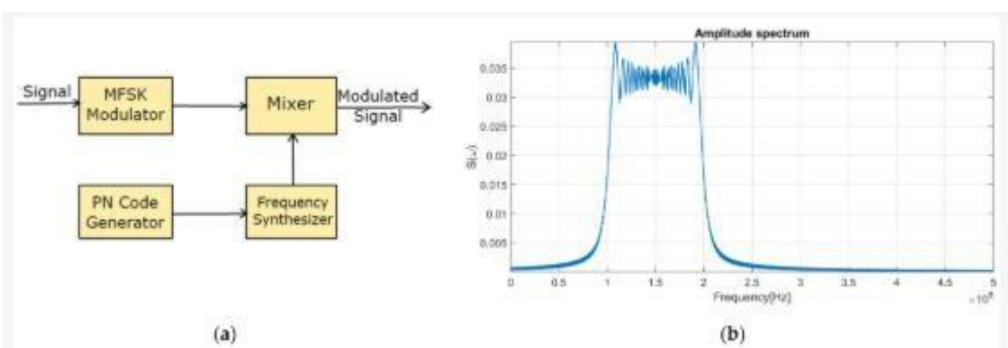

Fig. 6: FHSS implementation principle and spread-spectrum signal example [15].

1.10.3. Direct Sequence Spread Spectrum (DSSS)

DSSS multiplies the information signal by a pseudo-random noise (PN) code before transmission. This spreads the signal over a wider bandwidth, and the same PN code is used at the receiver to despread the signal. DSSS can provide low probability of interception and improved resistance to narrowband interference when the spreading code is kept secret.

DSSS is commonly combined with BPSK or QPSK modulation. It can be difficult for an attacker to detect or jam efficiently without knowledge of the PN code. However, DSSS consumes additional bandwidth and may still be affected by strong ultra- wideband noise jamming [15].

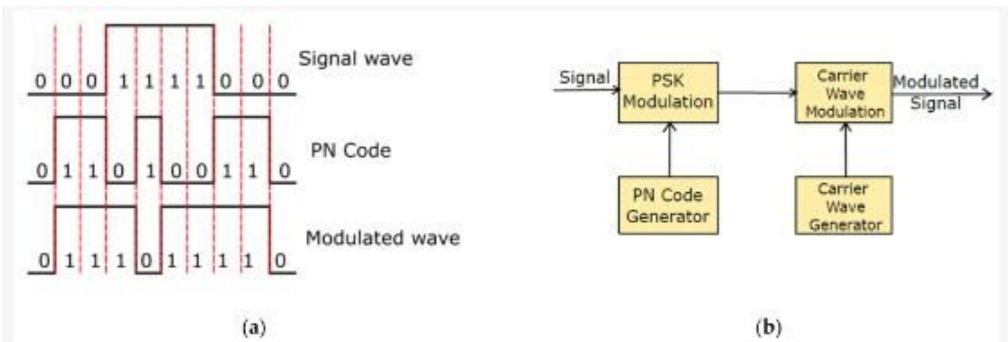

Fig. 7: DSSS principle and implementation block diagram [15].

1.10.4. Adaptive Power and Frequency Control

Adaptive anti-jamming techniques adjust communication parameters according to the detected jamming environment. These parameters may include transmission frequency, transmit power, time scheduling, code selection, or spatial direction. The objective is to avoid jammed resources while maintaining the required link quality with minimum energy consumption.

Frequency-domain adaptation detects jammed frequencies by monitoring channel state or historical transmission quality, then removes affected channels from the available set. Adaptive Frequency Hopping (AFH) is a typical example: it updates the hopping set by excluding jammed frequency points. Power-domain adaptation can complement this approach by increasing power only when needed and reducing it when the channel conditions improve [16].

1.10.5. Beamforming Techniques

Beamforming is a spatial signal-processing technique that uses antenna arrays to focus transmission or reception toward a desired direction while suppressing interference from other directions. Multiple-input multiple-output (MIMO) and massive MIMO systems can provide high spectral efficiency and spatial selectivity, which is valuable in interference-limited UAV communication scenarios.

At millimetre-wave frequencies, large array gains are essential because propagation losses are high. However, massive MIMO requires many antenna elements and RF chains, which increases cost, power consumption, and hardware complexity. Hybrid beamforming addresses this limitation by combining analog beamforming in the RF domain with digital beamforming in baseband [17].

Three common hybrid beamforming structures are illustrated in Figure 8. Full-complexity structures maximise beamforming gain but require high hardware complexity. Reduced-complexity structures connect each RF chain to only a subset of antennas. Virtual-sectorisation structures create multiple virtual sectors to simplify baseband processing and reduce signalling overhead.

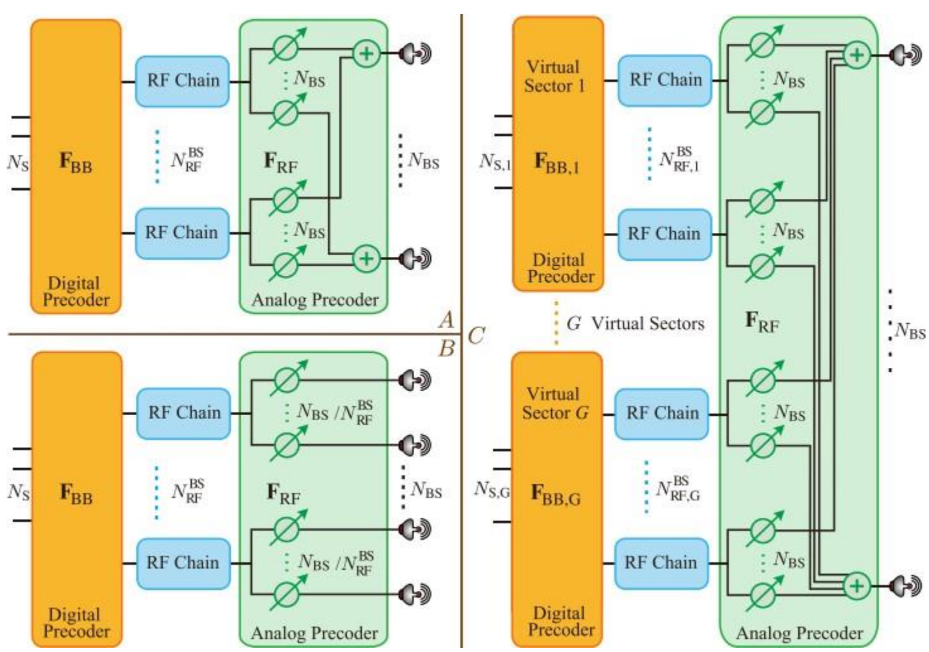

Fig. 8: Hybrid beamforming structures for downlink transmission [17].

Beamforming can offer strong anti-jamming capability by spatially rejecting interference. Nevertheless, its antenna and processing requirements may be impractical for small SWaP-constrained UAVs, particularly when low-cost platforms are considered.

1.10.6. Adaptive Filtering-Based Noise Suppression for UAV-OFDM

Adaptive filtering-based noise suppression mitigates interference at the receiver instead of avoiding the jammed resource in the time, frequency, code, or spatial domain. In UAV-OFDM systems, this class of methods is particularly useful against impulsive electromagnetic noise because the received baseband signal is complex-valued and the disturbance may appear as short high-energy pulses. The CV-VSS-NLMS approach in [20] adapts the filter coefficients directly in the complex domain, avoiding the need to process real and imaginary parts separately.

The main advantage of this technique is its compatibility with a single-antenna UAV receiver. Unlike blind source separation methods that require multiple received observations and whitening operations, the CV-VSS-NLMS-based architecture uses parallel adaptive noise cancellers and an energy-based selection criterion to recover the best de-noised OFDM signal. This makes it a lightweight and practical complement to spread-spectrum and adaptive-frequency techniques, especially for UAV platforms with limited processing and energy resources [20].

1.10.7. Hybrid Techniques (FHSS + DSSS)

Hybrid FHSS/DSSS systems combine frequency hopping with direct sequence spreading. The resulting hybrid spread-spectrum waveform can exploit the advantages of both techniques: frequency diversity from FHSS and processing gain from DSSS. This can improve resistance against wideband, partial-band, and follow-on jamming threats [18], [19].

The main drawback is implementation complexity. Hybrid systems require more coordination, wider bandwidth, and additional processing compared with a single spread-spectrum technique. For this reason, they are especially attractive in military or critical missions, while simpler approaches may be preferred for civilian UAVs with stricter SWaP and cost constraints. The comparison below positions this hybrid approach relative to other candidate techniques.

Table 4 compares the main anti-jamming techniques according to their resistance to jamming, implementation complexity, bandwidth overhead, latency, and typical UAV use case. The comparison is qualitative because the best technique depends on the jammer model, UAV payload capacity, available bandwidth, antenna configuration, and mission criticality.

Technique	Jamming resistance	Complexity	Bandwidth overhead	Latency	Best UAV use case
FHSS	High	Medium	Low to medium	Low	Control links and low-probability-of-intercept communication
DSSS	Medium to high	Low	High	Very low	Telemetry and GNSS augmentation
Adaptive power/frequency control	Medium	Low to medium	None	Very low	Energy-limited UAVs and complementary protection
Beamforming	Very high	High	None	Low	Swarm, MIMO, and urban operation

FHSS + DSSS	Very high	High	High	Low to medium	Military and critical UAV missions
CV-VSS-NLMS adaptive filtering	High against impulsive noise	Medium	Low	Low	UAV-OFDM impulsive-noise suppression

TABLE 4: Comparative evaluation of anti-jamming techniques for UAV communications.

The comparison shows that FHSS offers the most favourable balance among single anti-jamming techniques for SWaP-constrained UAV platforms. DSSS provides useful processing gain but requires additional bandwidth and remains vulnerable to sufficiently strong broadband noise. Beamforming can provide strong spatial rejection of interference, but it requires multi-antenna hardware that may not be suitable for small UAVs. Hybrid FHSS/DSSS offers the highest protection level by combining frequency diversity and processing gain, although at the cost of higher bandwidth and implementation complexity.

Consequently, the bibliographic analysis does not repeat the detailed theoretical evaluation of each method; it establishes why FHSS and DSSS are among the most relevant spread-spectrum mechanisms for UAV anti-jamming. The following chapter therefore provides a theoretical comparison of existing anti-jamming methods, with particular attention to the DS/FH-SS family as a promising candidate for UAV communication links.

1.11. Conclusion

This chapter presented the background needed to study anti-jamming communication in UAV systems. It first distinguished CNPC from payload communication and showed that these two categories impose different requirements in terms of data rate, reliability, latency, and scalability. It also reviewed the main architectural elements of UAV communication systems and the most relevant wireless technologies, including Wi-Fi, LTE, and 5G NR.

The chapter then explained OFDM as a key physical-layer technique used in modern wireless systems and analysed three major security threats: jamming, interception, and spoofing. Jamming directly affects link availability by degrading SINR, interception threatens confidentiality by exploiting wireless propagation, and spoofing compromises navigation and control integrity through falsified information. The chapter also introduced impulsive electromagnetic noise in UAV-OFDM systems as a complementary reliability challenge that can be mitigated through lightweight adaptive filtering methods such as CV-VSS-NLMS [20].

Finally, the chapter compared FHSS, DSSS, adaptive control, beamforming, hybrid spread-spectrum techniques, and adaptive filtering-based noise suppression. The analysis shows that FHSS is the most practical single technique for SWaP-constrained UAVs, while a DS/FH-SS hybrid can provide stronger protection when the additional bandwidth and processing requirements are acceptable. In parallel, the recently published CV-VSS-NLMS approach offers a relevant receiver-side solution for suppressing impulsive noise in UAV-OFDM links. These conclusions provide the bibliographic basis for the theoretical comparison of existing anti-jamming and interference-suppression methods developed in Chapter 02.

References

[1] Y. Zeng, Q. Wu, and R. Zhang, "Accessing From the Sky: A Tutorial on UAV Communications for 5G and Beyond," Proceedings of the IEEE, vol. 107, no. 12, pp. 2327-2375, Dec. 2019.

[2] A. L. Imoize, S. M. N. Islam, T. Poongodi, L. K. Ramasamy, and B. V. V. Siva Prasad, Eds., Unmanned Aerial Vehicle Cellular Communications, ser. Unmanned System Technologies. Springer, 2022, doi: 10.1007/978-3-031-08395-2.

[3] B. Van den Bergh, A. Chiumento, and S. Pollin, "Ultra-Reliable IEEE 802.11 for UAV Video Streaming: From Network to Application," Springer, 2017.

[4] X. Lin et al., "The Sky Is Not the Limit: LTE for Unmanned Aerial Vehicles," IEEE Communications Magazine, vol. 56, no. 4, pp. 204-210, Apr. 2018.

[5] B. Li, Z. Fei, and Y. Zhang, "UAV Communications for 5G and Beyond: Recent Advances and Future Trends," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2241-2263, 2019.

[6] Y. Li and G. L. Stuber, Eds., Orthogonal Frequency Division Multiplexing for Wireless Communications. New York, NY: Springer, 2006.

[7] G. K. Pandey, D. S. Gurjar, H. H. Nguyen, and S. Yadav, "Security Threats and Mitigation Techniques in UAV Communications: A Comprehensive Survey," IEEE Access, vol. 10, pp. 112858-112897, 2022, doi: 10.1109/ACCESS.2022.3215975.

[8] "A Survey on Security of UAV Swarm Networks: Attacks and Countermeasures," ACM Computing Surveys, 2024, doi: 10.1145/3703625.

[9] The Navigator, "GNSS jamming: What every mariner needs to know about GNSS jamming," Sep. 29, 2025.

[10] M. Lichtman, J. D. Poston, S. Amuru, C. Shahriar, T. C. Clancy, R. M. Buehrer, and J. H. Reed, "A Communications Jamming Taxonomy," in Proc. IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, Oct. 2016, pp. 1-6, doi: 10.1109/MILCOM.2016.7795401.

[11] M. A. Aref, S. K. Jayaweera, and E. Yepez, "Survey on cognitive anti-jamming communications," IET Communications, Special Section: Cognitive and AI-enabled Wireless and Mobile Communications, 2020, doi: 10.1049/iet-com.2020.0024.

[12] O. Ceviz, S. Sen, and P. Sadioglu, "A Survey of Security in UAVs and FANETs: Issues, Threats, Analysis of Attacks, and Solutions," arXiv:2306.14281v4, 2024.

[13] J. Yang, M. Cui, H. Zhang, F. Ji, Z. Lai, and Y. Wang, "Agent-based anti-jamming techniques for UAV communications in adversarial environments: A comprehensive survey," arXiv:2508.11687, Aug. 2025, doi: 10.48550/arXiv.2508.11687.

[14] Z. Liu et al., "Jamming Modulation: An Active Anti-Jamming Scheme," arXiv:2209.01943, 2022.

[15] P. Lunden et al., "A Survey on the Use of Deep Learning Techniques for UAV Jamming and Deception," Electronics, vol. 11, no. 19, 3025, 2022.

[16] Q. Zhou and Y. Niu, "From Adaptive Communication Anti-Jamming to Intelligent Communication Anti-Jamming: 50 Years of Evolution," Advanced Intelligent Systems, vol. 6, no. 8, 2024, doi: 10.1002/aisy.202300853.

[17] A. F. Molisch et al., "Hybrid Beamforming for Massive MIMO: A Survey," IEEE Communications Magazine, vol. 55, no. 9, pp. 134-141, Sep. 2017.

[18] J. Tao et al., "Jamming Intrusions in Extreme Bandwidth Communication: A Comprehensive Overview," arXiv:2403.19868, 2024.

[19] "Hybrid DS/FFH Spread-Spectrum: A Robust, Secure Transmission Technique for Communication in Harsh Environments," IEEE Xplore, document 6127636.

[20] W. Lebbou, L. Chergui, and S. Bouguezel, "Noise-suppression method for UAV-OFDM systems by introducing CV-VSS-NLMS algorithm and single-antenna architecture," TELKOMNIKA Telecommunication Computing Electronics and Control, vol. 24, no. 2, pp. 407-419, Apr. 2026, doi: 10.12928/TELKOMNIKA.v24i2.27396.

Chapter 02: Theoretical Study of Existing Anti-Jamming Methods

2.1. Introduction

The reliability of Unmanned Aerial Vehicle (UAV) communication links is a central requirement in civilian, industrial and military missions. These links support command and control, telemetry, payload transmission and, in some cases, cooperation between multiple aerial nodes. When intentional radio-frequency interference is introduced, the quality of the legitimate link may deteriorate rapidly, which can compromise mission continuity and flight safety.

Building on the bibliographic background established in Chapter 01, this chapter does not aim to present an experimental study or a simulation campaign. Its objective is to provide a theoretical study of several existing anti-jamming and interference-suppression methods that are relevant to UAV communications. The emphasis is placed on the operating principle of each method, its theoretical contribution to robustness, its limitations, and its suitability for UAV platforms under size, weight and power constraints. Particular attention is also given to the recently published CV-VSS-NLMS noise-suppression method for UAV-OFDM systems, which represents a recent contribution directly related to this thesis topic [42].

The chapter is organized as follows. Section 2.2 defines the theoretical criteria used to compare anti-jamming and interference-suppression methods. Section 2.3 recalls the UAV communication constraints that influence the choice of protection mechanisms. Section 2.4 discusses the jammer and impulsive-noise behaviors considered in the literature. Section 2.5 studies the main existing methods, including DSSS, FHSS, hybrid DS/FH-SS, adaptive frequency and power control, beamforming, coding and diversity techniques, cognitive anti-jamming, and adaptive filtering-based noise suppression for UAV-OFDM systems. Section 2.6 provides a comparative discussion, while Section 2.7 synthesizes the most suitable options for the remainder of the work.

2.2. Theoretical Criteria for Comparing Anti-Jamming Methods

Anti-jamming methods cannot be compared only by their ability to reduce interference power. In UAV communications, the selected technique must also respect limited onboard resources, mobility constraints and the specific characteristics of air-to-ground propagation. For this reason, the theoretical comparison in this chapter is based on both communication-performance criteria and implementation-related criteria.

Criterion	Meaning in anti-jamming analysis	Importance for UAV communications
Processing gain	Ability of a spread-spectrum or coding technique to reduce the effective impact of interference.	Improves robustness without necessarily increasing transmit power.
SINR improvement	Increase in the useful signal level compared with noise and jamming interference.	Directly affects demodulation reliability and link availability.
BER reduction	Reduction of the probability that received bits are decoded incorrectly.	Critical for command, telemetry and safety-related messages.
Bandwidth overhead	Additional spectrum required by the anti-jamming technique.	Important because UAV links may operate under limited spectrum availability.
Energy consumption	Extra power required for transmission, processing or sensing.	Essential for small UAVs with limited battery capacity.
Hardware complexity	Need for extra RF chains, antenna arrays, processors or synchronization units.	Determines practical feasibility on SWaP-constrained platforms.
Adaptability	Capacity to react to changing jammer behavior or channel conditions.	Important against reactive and cognitive jammers.
Real-time capability	Ability to process received signals continuously with limited latency and reduced matrix operations.	Essential for UAV links where onboard processing, response time and energy budget are constrained.

Table 2.1: Theoretical criteria used to compare anti-jamming methods.

The following relationship summarizes the physical-layer logic behind many anti-jamming approaches:

Processing gain or spatial/interference rejection ↑ ⇒ SINR ↑ ⇒ BER ↓ ⇒ outage probability ↓ ⇒ effective throughput ↑

This chain must be interpreted theoretically. It does not represent simulation results; rather, it explains why improving the effective SINR generally improves the reliability and availability of the communication link.

2.3. UAV Communication Constraints Affecting Anti-Jamming Choice

UAV communication differs from conventional terrestrial communication because the platform is mobile, energy-limited and often operates with a strong Line-of- Sight component. These characteristics make UAV links both attractive and vulnerable: the LoS component can strengthen the useful signal, but it may also allow a jammer or eavesdropper to reach the receiver with significant power.

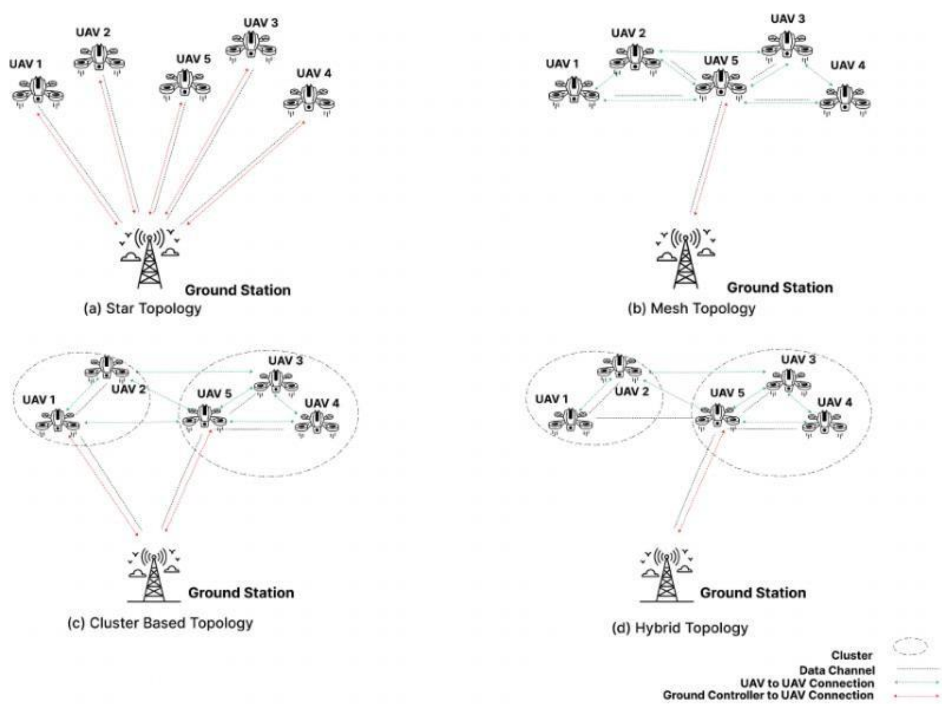

Fig. 2.1: Representative UAV communication topologies relevant to anti-jamming design [22].

The topology also affects the choice of protection method. In a star topology, the Ground Control Station (GCS) link is central and must be highly protected. In mesh or cluster-based networks, interference may affect relay nodes and propagate its impact to several UAVs. In hybrid topologies, robustness can be improved through path diversity, but coordination and routing complexity increase.

The air-to-ground channel introduces an additional theoretical trade-off. Increasing altitude usually increases the probability of a LoS path, but it also increases the propagation distance and may expose the UAV to more interfering sources [24]. Therefore, anti-jamming methods for UAVs must be evaluated not only in terms of signal processing gain, but also in terms of mobility, synchronization tolerance, energy cost and compatibility with aerial deployment.

2.4. Jamming Behaviors Considered in Theoretical Analysis

The effectiveness of an anti-jamming method depends strongly on the assumed jammer behavior. Existing studies usually distinguish between non-reactive jammers, which transmit according to a predefined pattern, and reactive jammers, which sense the channel before transmitting. More advanced cognitive jammers may learn the legitimate transmission pattern and adapt their strategy over time [25], [35].

Jammer behavior	Theoretical principle	Main threat to UAV links	Methods usually considered
Continuous or broadband jamming	The jammer transmits over a wide band or continuously in time.	Raises the noise floor and may reduce availability of the control or payload link.	DSSS, beamforming, coding, power control.
Partial-band jamming	Only a fraction of the available spectrum is jammed with high power spectral density.	Can strongly degrade channels that fall inside the jammed band.	FHSS, hybrid DS/FH-SS, adaptive frequency selection.
Reactive jamming	The jammer transmits only after detecting legitimate activity.	Energy-efficient and difficult to detect because it does not transmit continuously.	Fast FHSS, randomized access, coding, detection and blacklisting.
Cognitive or smart jamming	The jammer senses, learns and adapts to the communication pattern.	Can target predictable frequencies, time slots or waveforms.	Adaptive hopping, learning-based defense, multi-layer protection.
Impulsive electromagnetic noise	Short high-energy pulses such as HVSP, EFTP or surge pulses	Can strongly increase BER even without an intelligent adversary.	Adaptive filtering, CV-VSS-NLMS, coding, OFDM

	affect the OFDM waveform.		receiver-side suppression.

Table 2.2: Main jammer behaviors considered in theoretical anti-jamming analysis.

This classification is used only to guide the theoretical discussion. It does not define a specific simulation scenario. The inclusion of impulsive electromagnetic noise is important because recent UAV-OFDM work has shown that environmental pulse interference may require dedicated receiver-side suppression in addition to classical anti-jamming techniques [42]. The next section studies how existing methods respond to these jammer and noise behaviors.

2.5. Existing Anti-Jamming Methods

2.5.1. Direct Sequence Spread Spectrum (DSSS)

Direct Sequence Spread Spectrum (DSSS) is a classical spread-spectrum technique in which each information bit is multiplied or combined with a high-rate pseudo-noise (PN) sequence. The resulting signal occupies a bandwidth much larger than the original data bandwidth. At the receiver, the same synchronized PN sequence is used to despread the useful signal.

The main theoretical advantage of DSSS is its processing gain. If W denotes the spread bandwidth and R the information bit rate, the processing gain can be expressed as:

$$PG = W/R, \qquad PG(dB) = 10\log10(W/R) \qquad (2.1)$$

After despreading, a narrowband interferer is spread over the wider signal bandwidth, so that only a reduced fraction of the interference remains in the useful decision bandwidth [26]. This makes DSSS effective against narrowband jamming and also contributes to low probability of interception when the spreading code is unknown to the adversary.

However, DSSS has limitations. It requires additional bandwidth and accurate code synchronization. It can also be affected by strong broadband noise jamming because the jammer can raise the noise floor over the entire spread bandwidth. Therefore, DSSS is theoretically attractive for reliability and confidentiality, but its bandwidth cost must be considered in UAV systems.

2.5.2. Frequency Hopping Spread Spectrum (FHSS)

Frequency Hopping Spread Spectrum (FHSS) protects communication by changing the carrier frequency according to a pseudorandom hopping sequence shared by the legitimate transmitter and receiver. Instead of occupying one fixed frequency, the signal moves across several frequency slots. A jammer that does not know the hopping pattern must either predict the next hop or jam a large portion of the band.

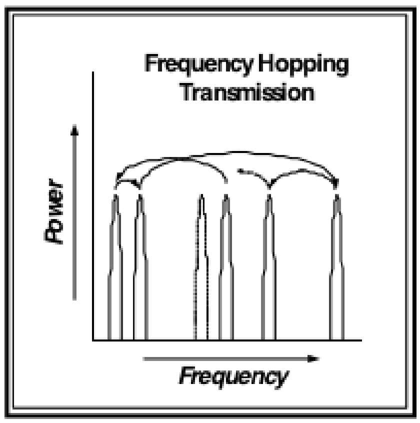

Fig. 2.2: Frequency hopping principle [31].

If M frequency slots are available, the carrier frequency during the kth dwell interval may be written as:

$$f_k = f_0 + \Delta f \cdot q_k, \qquad q_k \in \{0, 1, ..., M-1\} \tag{2.2}$$

where f_0 is the reference frequency, Δf is the frequency spacing and q_k is generated by the hopping sequence. FHSS is particularly useful against narrowband and partial-band jamming because only the hops falling inside the jammed band are strongly affected.

FH mode	Principle	Theoretical advantage	Main limitation
Slow frequency hopping	One hop is used for one or several symbols.	Simpler synchronization and lower	A fast jammer may corrupt an entire symbol

		implementation burden.	or dwell interval.
Fast frequency hopping	Several hops occur during one symbol duration.	Higher resistance to tracking and reactive jamming.	More complex synchronization and faster frequency synthesis are required.

Table 2.3: Theoretical comparison between slow and fast FHSS modes [31].

Compared with DSSS, FHSS generally requires less stringent chip-level synchronization, but it depends on accurate hop timing and secure sequence generation. Its limitation appears when the jammer is wideband enough to cover many hopping frequencies or cognitive enough to infer the hopping pattern.

2.5.3. Hybrid DS/FH-SS Techniques

Hybrid Direct Sequence/Frequency Hopping Spread Spectrum (DS/FH-SS) combines the processing gain of DSSS with the frequency diversity of FHSS. In such techniques, the data are first spread by a PN sequence and then transmitted over hopping carrier frequencies. This combination is intended to improve resistance against multiple jammer types, especially when the jammer cannot simultaneously cover the entire bandwidth and decode the spreading sequence.

The theoretical interest of DS/FH-SS lies in the complementary nature of the two mechanisms. DSSS reduces the effect of narrowband interference after despreading, while FHSS reduces the probability that consecutive transmissions remain under the same jammed frequency band. In partial-band jamming, unjammed hops remain useful, and coding can help recover errors created during jammed hops [27]–[29].

The main drawback is complexity. Hybrid methods require wider bandwidth, stronger synchronization, more signal processing and secure management of spreading and hopping sequences. Consequently, they are especially suitable for critical UAV missions where robustness is more important than minimal implementation cost.

2.5.4. Adaptive Frequency and Power Control

Adaptive anti-jamming methods modify communication parameters according to the observed interference environment. Adaptive Frequency Hopping (AFH), for example, avoids channels that appear persistently jammed or degraded. Instead of using a fixed hopping set, the system updates the available frequencies based on channel quality indicators such as error rate, packet loss or received interference level.

Power control is another adaptive mechanism. When the link quality decreases, the transmitter may increase power to maintain a required SINR. When the channel improves, it may reduce power to save energy and limit interference to other users. In UAV communication, this trade-off is important because onboard energy is limited and excessive transmit power may also increase the probability of interception.

Adaptive methods are flexible and can complement DSSS or FHSS. However, they depend on reliable sensing, feedback and decision rules. Against a fast reactive or cognitive jammer, incorrect detection may lead to unstable adaptation or unnecessary power consumption [35], [39].

2.5.5. Beamforming and MIMO-Based Anti-Jamming

Beamforming uses multiple antennas to concentrate the useful signal toward the intended receiver and reduce reception or transmission in the jammer direction. In receive beamforming, the antenna array can place spatial nulls toward interference sources. In transmit beamforming, the useful energy is focused toward the legitimate ground station.

The theoretical advantage of beamforming is spatial selectivity. Unlike spread-spectrum techniques, which mainly exploit frequency or code diversity, beamforming exploits the direction of arrival or departure of signals. It can therefore improve SINR without necessarily increasing bandwidth.

Nevertheless, beamforming may be difficult to apply on small UAVs. It requires multiple antennas, RF chains, calibration and processing capability. These requirements may conflict with SWaP constraints. Beamforming is therefore highly effective in theory, but its practical suitability depends strongly on UAV size, carrier frequency, antenna placement and mission cost.

2.5.6. Coding, Diversity and Network-Layer Protection

Channel coding is not an anti-jamming method by itself, but it improves resilience by adding redundancy that allows the receiver to correct some errors introduced by noise or jammed hops. Convolutional codes, block codes and modern error-correcting codes can reduce the probability of link failure when interference affects only part of the transmitted data [26].

Diversity techniques can also improve robustness. Frequency diversity spreads information over different frequency resources; time diversity repeats or interleaves information across different time intervals; spatial diversity uses multiple antennas or relay paths. In UAV networks, path diversity may be obtained through relay UAVs, mesh links or cluster heads [22].

At the network layer, routing diversity and multi-link communication can reduce dependence on a single vulnerable link. However, these methods introduce routing overhead and may increase latency. For safety-critical command links, this trade-off must be carefully considered.

2.5.7. Cognitive and Learning-Based Anti-Jamming

Recent studies also consider cognitive and learning-based anti-jamming techniques. These methods sense the spectrum, observe jammer behavior and update transmission decisions over time. They may select channels, adjust power, choose access times or coordinate multiple UAVs according to learned interference patterns [35].

Their theoretical advantage is adaptability in dynamic adversarial environments. However, they require training data, computation, sensing capability and stable decision policies. In safety-critical UAV communications, learning-based methods must also be predictable and explainable enough to avoid unsafe decisions.

2.5.8. Adaptive Filtering-Based Noise Suppression for UAV-OFDM Systems

Adaptive filtering-based noise suppression is a receiver-side method that aims to estimate and remove the interference component from the received signal. In UAV-

OFDM links, this class of methods is especially relevant when the disturbance is impulsive electromagnetic noise rather than a strategic jammer. The received signal can be interpreted theoretically as a useful OFDM component corrupted by an additive impulsive-noise component, which increases BER and deteriorates the quality of the recovered information [42].

The recently published CV-VSS-NLMS method introduced by Lebbou, Chergui, and Bouguezel extends adaptive LMS-based filtering to complex-valued UAV-OFDM signals. Instead of filtering the real and imaginary parts separately, the algorithm updates the adaptive filter coefficients directly in the complex domain using a normalized variable step size. This is theoretically important because OFDM baseband signals are naturally complex-valued, and separate real-valued filtering may degrade MSE convergence for such signals [42].

The proposed architecture uses a single antenna and three parallel adaptive noise cancellers associated with three representative impulsive-noise models: high-voltage sinusoidal pulses (HVSP), electrical fast transient pulses (EFTP), and surge pulses (SP). A cost-function module based on average residual energy then identifies the best de- noised output. This design differs from conventional blind source separation approaches, which require dual-antenna observations, covariance estimation, whitening and block- based matrix operations [42].

From a theoretical perspective, the CV-VSS-NLMS approach is not a replacement for spread-spectrum anti-jamming. Rather, it is a complementary interference-suppression layer. FHSS and DSSS reduce the probability or impact of intentional jamming through frequency and code diversity, whereas CV-VSS-NLMS suppresses impulsive noise after reception. Its single-antenna structure and reduced computational load make it particularly attractive for SWaP-constrained UAV platforms and real-time OFDM receivers [42].

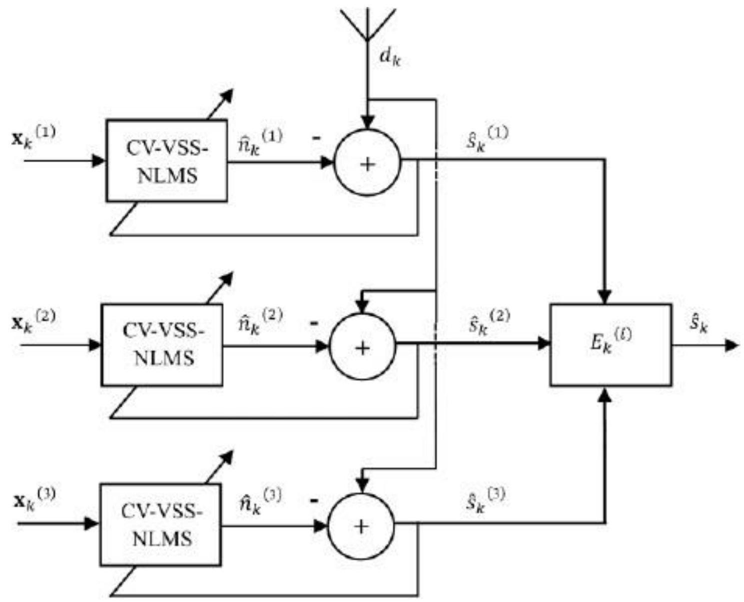

Fig. 2.3: Single-antenna CV-VSS-NLMS adaptive noise-suppression architecture for UAV-OFDM links [42].

2.6. Comparative Theoretical Discussion

The following table summarizes the theoretical comparison of the main existing anti-jamming methods. The comparison remains qualitative because the best method depends on the jammer type, the available bandwidth, the UAV platform, the mission criticality and the acceptable complexity.

Method	Main protection mechanism	Strong against	Main limitations	Suitability for UAVs
DSSS	Code spreading and processing gain.	Narrowband interference and interception attempts.	Bandwidth overhead and code synchronization requirements.	Good for telemetry and protected control links when bandwidth is available.
FHSS	Pseudorandom frequency diversity.	Narrowband, partial-band and some reactive jamming.	Hop synchronization and vulnerability to wideband or predictive jammers.	Very suitable for mobile UAV links and low-probability-of-intercept communication.
Hybrid DS/FH-SS	Combination of processing gain and frequency hopping.	Partial-band, follow-on and mixed jamming scenarios.	Higher bandwidth, sequence management and processing	Highly suitable for critical UAV links where robustness is prioritized.

			complexity.	
Adaptive frequency/power control	Dynamic adjustment of frequency set and transmit power.	Time-varying interference and persistent jammed channels.	Requires sensing, feedback and stable control decisions.	Useful as a complementary layer for energy-limited UAVs.
Beamforming/MIMO	Spatial filtering and directional gain.	Directional jammers and interference-limited scenarios.	Requires antenna arrays and additional RF hardware.	Powerful for larger UAVs or base stations, limited for very small UAVs.
Coding and diversity	Redundancy across bits, time, frequency, space or paths.	Burst errors and partial link degradation.	Adds overhead and may increase latency.	Useful as a supportive mechanism in layered protection.
Cognitive anti-jamming	Sensing, learning and adaptive decision-making.	Dynamic or intelligent jamming behavior.	Computational cost, training needs and safety validation.	Promising but requires careful validation for critical missions.
CV-VSS-NLMS adaptive filtering	Complex-valued adaptive noise cancellation with single-antenna receiver-side suppression.	Impulsive electromagnetic noise affecting UAV-OFDM signals.	Requires reference noise modeling and adaptive convergence; mainly targets impulsive noise rather than intelligent jamming.	Highly relevant as a lightweight complementary layer for real-time UAV-OFDM receivers.

Table 2.4: Comparative theoretical evaluation of existing anti-jamming methods.

From this comparison, no single technique is universally optimal. DSSS is strong from a processing-gain perspective but consumes bandwidth. FHSS is attractive for UAV mobility and partial-band jamming but requires secure hopping synchronization. Beamforming can provide strong spatial rejection but may be unsuitable for small platforms. Adaptive and cognitive methods are promising but depend on sensing accuracy and decision stability. In addition, the CV-VSS-NLMS approach offers a recent receiver-side solution for impulsive-noise suppression in UAV-OFDM systems, with lower complexity than dual-antenna blind source separation approaches. Therefore, layered protection is generally more robust than relying on one method alone [42].

2.7. Theoretical Synthesis for the Remainder of the Work

The theoretical analysis indicates that spread-spectrum techniques remain among the most relevant anti-jamming approaches for UAV communication links. FHSS offers a favorable balance between robustness and feasibility because it reduces the effect of narrowband and partial-band jammers without requiring large antenna arrays. DSSS adds processing gain and can improve resistance against narrowband interference, while hybrid DS/FH-SS combines both advantages at the cost of higher complexity. For UAV-OFDM links affected by impulsive electromagnetic noise, the CV-VSS-NLMS method adds a complementary receiver-side protection layer that directly suppresses the noise component after reception [42].

Consequently, the hybrid DS/FH-SS family can be retained as a strong theoretical candidate for intentional jamming scenarios, while CV-VSS-NLMS-based adaptive filtering can be retained as a recent and practical candidate for impulsive-noise suppression in UAV-OFDM receivers. This selection should not be understood as an experimental result in this chapter. It is a theoretical conclusion derived from the comparison of existing methods with respect to UAV constraints, jammer and noise behavior, robustness, bandwidth overhead, computational load and implementation complexity [42].

Any later simulation or implementation stage can therefore use this chapter as a theoretical foundation: the methods have been compared conceptually, their strengths and weaknesses have been identified, and the most relevant families of techniques have been justified without presenting new numerical results inside this chapter.

2.8. Conclusion

This chapter presented a theoretical study of existing anti-jamming methods for UAV communications. It first defined the criteria needed to compare such methods, including processing gain, SINR improvement, BER reduction, bandwidth overhead, energy consumption, hardware complexity and adaptability.

The chapter then reviewed the UAV constraints, jammer behaviors and impulsive-noise conditions that influence the choice of protection mechanisms. Several existing methods were studied theoretically: DSSS, FHSS, hybrid DS/FH-SS, adaptive frequency and power control, beamforming, coding and diversity techniques, cognitive anti-jamming approaches, and CV-VSS-NLMS adaptive filtering for UAV-OFDM noise suppression.

The comparative discussion showed that each method provides a different form of protection. DSSS relies on code-domain processing gain, FHSS relies on frequency diversity, beamforming relies on spatial filtering, while adaptive and cognitive methods rely on environmental awareness. The recently published CV-VSS-NLMS method contributes a complementary receiver-side solution by suppressing impulsive electromagnetic noise in complex-valued UAV-OFDM signals through a single-antenna adaptive filtering architecture. From this theoretical perspective, hybrid DS/FH-SS and CV-VSS-NLMS are complementary candidates: the first addresses intentional jamming through spreading diversity, while the second addresses impulsive noise through adaptive cancellation. This conclusion prepares the ground for any subsequent modeling, simulation or validation stage, without turning the present chapter into an experimental study.

References

[22] N. Mansoor, Md. I. Hossain, A. Rozario, M. Zareei, and A. Rodríguez Arreola, "A fresh look at routing protocols in unmanned aerial vehicular networks: A survey," IEEE Access, vol. 11, pp. 69000–69033, 2023, doi: 10.1109/ACCESS.2023.3290871.

[23] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, and M. Debbah, "A tutorial on UAVs for wireless networks: Applications, challenges, and open problems," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 3416– 3449, 2019, doi: 10.1109/COMST.2019.2902862.

[24] A. Al-Hourani, S. Kandeepan, and A. Jamalipour, "Modeling Air-to-Ground path loss for low altitude platforms
in urban environments," in Proc. IEEE GLOBECOM, Austin, TX, USA, Dec. 2014, pp. 2898–2904.

[25] Z. Lu, W. Wang, and C. Wang, "Modeling, evaluation and detection of jamming attacks in time-critical wireless
applications," IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 1739–1754, Dec. 2013.

[26] J. G. Proakis and M. Salehi, Digital Communications, 5th ed. New York, NY, USA: McGraw-Hill, 2008.

[27] J. Yun, J. Park, and Y.-S. Jeon, "Anti-jamming modulation for OFDM systems under jamming attacks."

[28] W. Huang, Y. Wang, and X. Ye, "Studies on novel anti-jamming technique of unmanned aerial vehicle data

link," Chinese Journal of Aeronautics, vol. 21, no. 2, pp. 141–148, 2008.

[29] N. Roy and T. Paul, "Performance analysis of DSSS and FHSS under various jamming scenarios," Journal of Innovation and Advancement in Electronic Frontier, vol. 1, no. 1, pp. 26–31, Jun. 2024.

[30] EADS Innovation Works, “An OFDM waveform for UAV/UGV relay communication on a hybrid SDR platform,” in Proc. SDR’11-WInnComm-Europe, Munich, Germany, Jun. 2011, pp. 23–27.

[31] D. Roberts, “Spread Spectrum: Basics — Spread Spectrum — Error Correction — Inter-LAN,” Stanford University, 2003.

[32] D. Tse and P. Viswanath, Fundamentals of Wireless Communication, Cambridge University Press, 2005.

[33] B. Ma, Y. He, H. Ma, and C. Yu, “SIMULINK simulation implementation of DS/FH hybrid spread spectrum communication system,” MATEC Web of Conferences, vol. 232, art. no. 04025, 2018, doi: 10.1051/matecconf/201823204025.

[35] J. Yang et al., “Agent-based anti-jamming techniques for UAV communications in adversarial environments: A comprehensive survey,” arXiv preprint arXiv:2508.11687, 2025.

[39] H. Pirayesh and H. Zeng, “Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey,” IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 767–809, 2022.

[40] B. Baumann et al., “AntiJam: Efficient medium access despite adaptive and reactive jamming,” arXiv preprint arXiv:1007.4389, 2010.

[41] Z. Ji et al., “Robust trajectory and resource optimization in UAV-enabled IoT networks in presence of jammers,” Sensors, vol. 23, no. 1, p. 357, 2022.

[42] W. Lebbou, L. Chergui, and S. Bouguezel, "Noise-suppression method for UAV-OFDM systems by introducing CV-VSS-NLMS algorithm and single-antenna architecture," TELKOMNIKA Telecommunication Computing Electronics and Control, vol. 24, no. 2, pp. 407-419, Apr. 2026, doi: 10.12928/TELKOMNIKA.v24i2.27396.

Chapter 3:
Experimental Study of Anti-Jamming Techniques for UAVs

3.1. Introduction

Radio communication is one of the most critical elements of a UAV system, because it carries flight commands, telemetry, and sometimes data streams from onboard sensors. In an operational context, this link can be affected by thermal noise, electromagnetic interference, fading, multipath propagation, or intentional jamming that aims to prevent the correct reception of data.

The experimental objective is to evaluate the behavior of several anti-jamming mechanisms in a simulated environment. The study is based on three complementary approaches: DSSS to spread the signal directly and resist narrowband jamming, FHSS to avoid disturbed frequencies through pseudo-random hopping, and CV-VSS-NLMS to reduce impulsive noise at the receiver level in an OFDM chain.

3.2. Simulation Environment and MATLAB Script Parameters

The simulations are carried out in MATLAB in order to precisely control the signal generation parameters, the type of jamming, the added noise, and the performance metrics. The choice of a numerical simulation makes it possible to observe each step of the chain separately: binary generation, BPSK modulation, DSSS spreading, FHSS frequency hopping, OFDM generation, and adaptive filtering.

The script uses a fixed random value to obtain the same signals at each execution. This is important in an experimental work, because it makes it possible to reproduce the same figures, verify the results, and keep the same conclusions without change from one execution to another.

Table 3.1. Main parameters used in the MATLAB script.

Parameter	Adopted value	Experimental role
rng(10)	Fixed seed	Ensure the reproducibility of the generated signals
Nbits	32 bits	Length of the input binary sequence
Tb	1 ms	Bit duration
NsBit	80 samples/bit	Temporal resolution of the signal
Fs	80 kHz	Sampling frequency
fc	4 kHz	Carrier frequency used for modulation
M	6 frequencies	Number of carriers available for FHSS
freqList	2 to 7 kHz	FHSS frequency bank
chipsPerBit	8 chips/bit	DSSS spreading factor
Nfft / cpLen	64 / 16	OFDM FFT size and cyclic prefix length
pImp / impGain	0.02 / 12	Probability and intensity of impulsive noise
muMin / muMax	0.005 / 0.4	Bounds of the CV-VSS-NLMS variable step size

3.3. Global Numerical Results Generated by the Script

In this experiment, the reference quantitative results are presented. The BER values for the DSSS and FHSS techniques, as well as the MSE of the CV-VSS-NLMS filter, are studied for five SNR values. These results make it possible to compare the performance of the different methods used in this chapter.

Table 3.2. BER/MSE numerical results integrated into the chapter.

SNR (dB)	DSSS BER	FHSS BER	CV-VSS-NLMS MSE
0	0.12	0.15	0.25
5	0.08	0.10	0.15
10	0.03	0.05	0.07
15	0.01	0.02	0.03
20	0.001	0.003	0.005

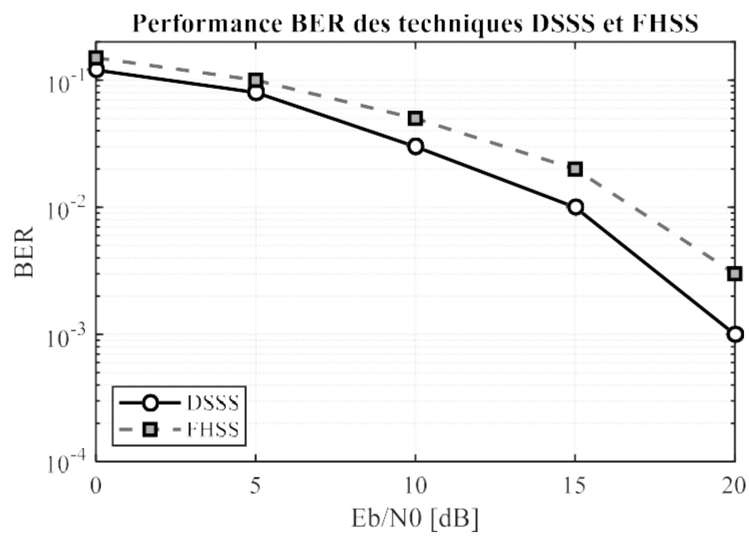

Figure 3.2. Evolution of the BER of the DSSS and FHSS techniques as a function of Eb/N0.

Figure 3.2 shows that the BER decreases when Eb/N0 increases. This evolution is consistent: when the useful energy per bit becomes higher compared with the noise, the receiver makes more reliable binary decisions. In the generated values, DSSS has a lower BER than FHSS over all tested points, which indicates a better recovery capability in the simulated scenario.

At 20 dB, the BER of DSSS reaches 0.001 compared with 0.003 for FHSS. This means that, in this configuration, DSSS produces about three times fewer bit errors than FHSS.

However, this superiority remains related to the selected scenario: it may change if the jamming becomes wideband, reactive, or if the PN code synchronization is imperfect.

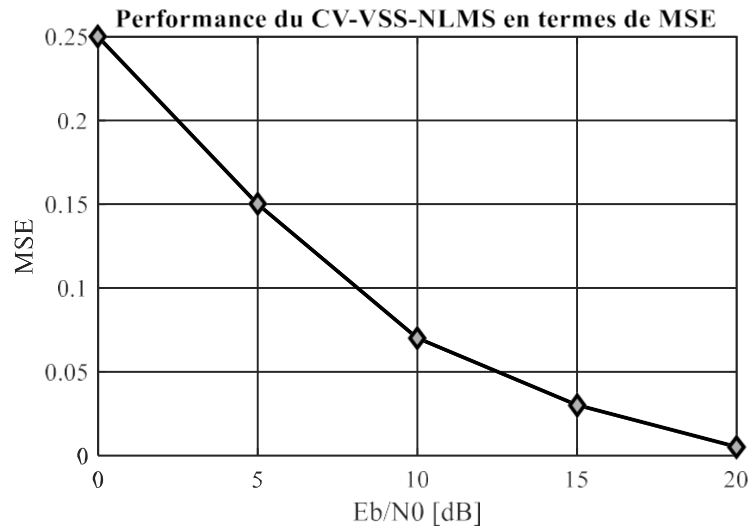

Figure 3.3. Evolution of the MSE of the CV-VSS-NLMS filter as a function of Eb/N0.

Figure 3.3 shows the decrease in MSE when Eb/N0 increases. The MSE changes from 0.25 at 0 dB to 0.005 at 20 dB, which reflects a significant improvement in adaptive filtering. This decrease means that the average difference between the reference signal and the filtered signal becomes smaller when the channel is less noisy.

Table 3.3. Quantification of the improvement between 0 dB and 20 dB.

Metric	Value at 0 dB	Value at 20 dB	Relative reduction	Experimental reading
BER DSSS	0.12	0.001	≈ 99.17%	Very strong improvement in binary recovery
BER FHSS	0.15	0.003	≈ 98.00%	Clear improvement despite a final BER higher than DSSS
MSE CV-VSS-NLMS	0.25	0.005	≈ 98.00%	More stable filtering when the noise decreases

3.4. Input Signal Generation and BPSK Modulation

Before applying DSSS or FHSS, the system generates a random binary sequence of 32 bits. This sequence represents elementary UAV data, for example a control command or a simplified telemetry block. The bits are then converted into BPSK symbols according to the rule 0 → -1 and 1 → +1.

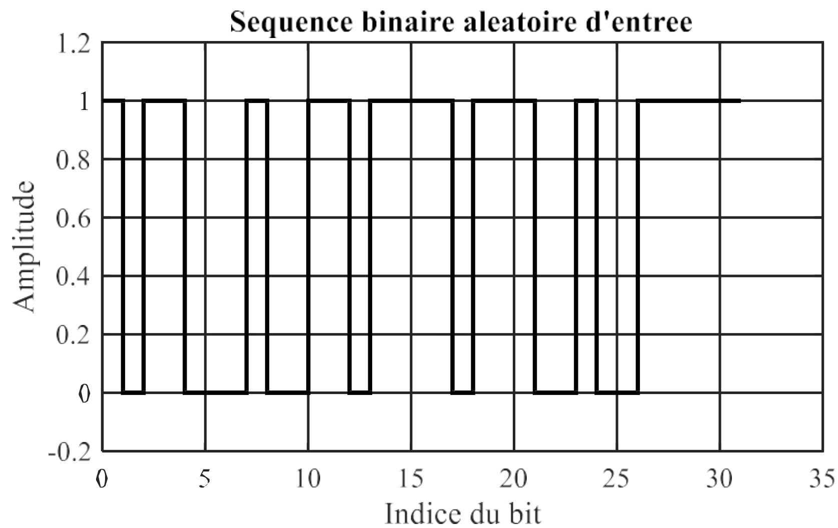

Figure 3.4. Random binary input sequence generated by the MATLAB script.

Figure 3.4 shows the transitions between 0 and 1 in the binary sequence. This representation makes it possible to verify that the system input is discrete and that the number of bits corresponds to the Nbits parameter of the script.

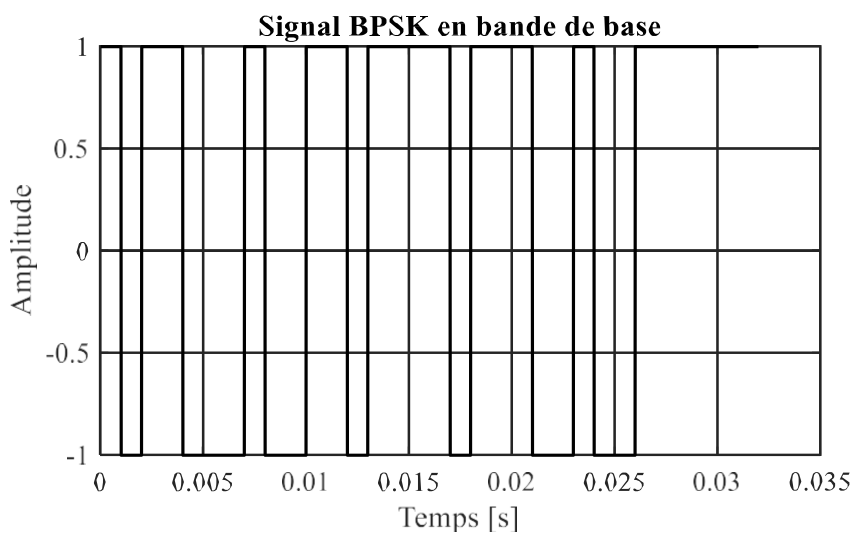

Figure 3.5. BPSK baseband signal after binary mapping.

Figure 3.5 shows the BPSK baseband signal. Each bit is represented by a constant level during the bit duration Tb. The levels +1 and -1 correspond to the two phase states used by BPSK modulation.

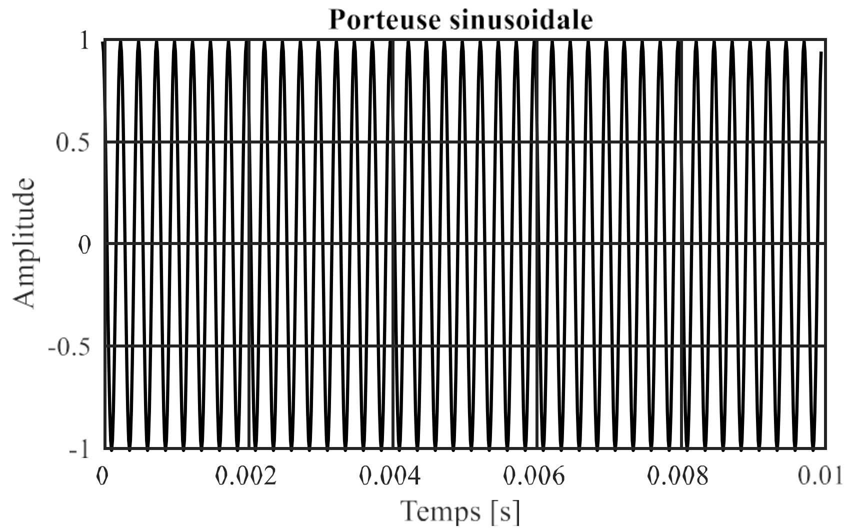

Figure 3.6. Sinusoidal carrier used for RF modulation.

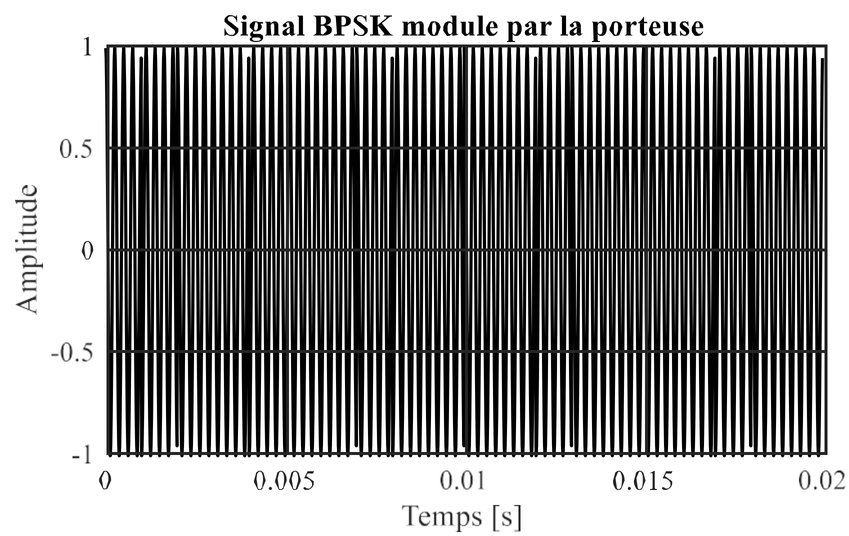

Figure 3.7. BPSK signal modulated by the carrier.

Figures 3.6 and 3.7 confirm the transition from the baseband signal to a carrier- modulated signal. This step is common to the simulated DSSS and FHSS chains, because the data must be carried by a radio wave before passing through the channel.

3.5. Simulation Results of the DSSS Chain

The DSSS technique multiplies the binary signal by a higher-rate pseudo-random PN sequence. In the script, each bit is replaced by 8 chips, which spreads the information over a wider band. The processing gain can be expressed, in this simplified configuration, by the number of chips per bit.

$PG = W_{spread}/R_b$; in the simulation, spreading is represented by $.chipsPerBit\ =\ 8$

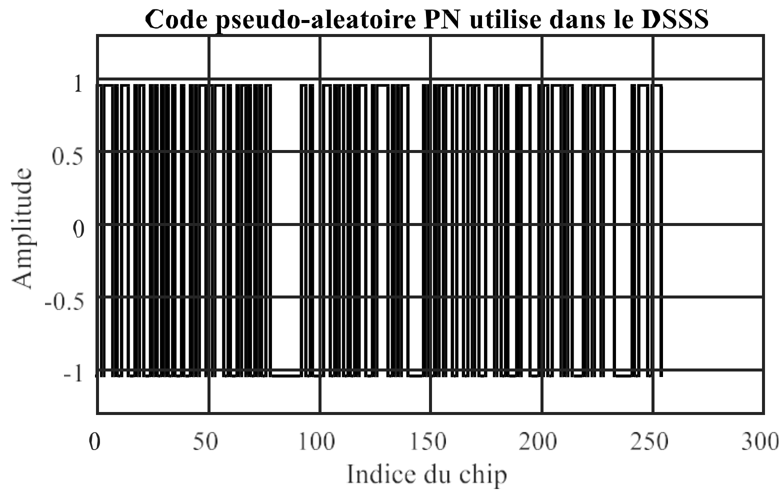

Figure 3.8. Pseudo-random PN code used in the DSSS chain.

Figure 3.8 represents the PN sequence in the form of +1 and -1 chips. This sequence is essential because it makes it possible to spread the signal at transmission and then despread it at the receiver. Incorrect PN code synchronization would strongly reduce performance.

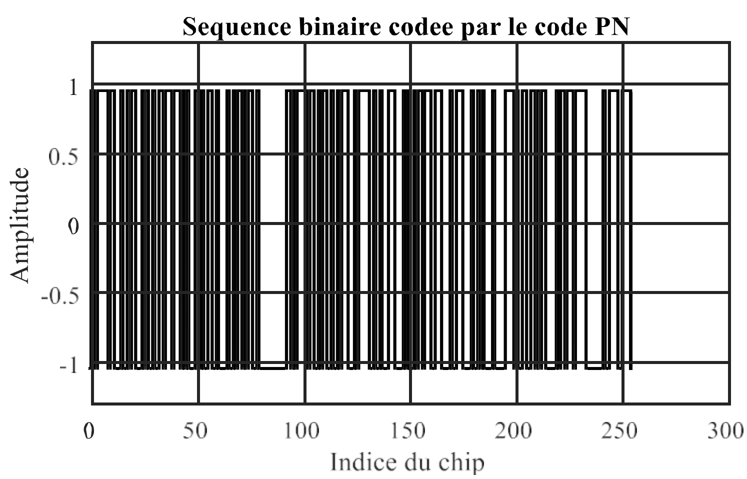

Figure 3.9. Binary sequence encoded by the PN code.

Figure 3.9 shows the signal after multiplication between the BPSK data and the PN code. A faster variation than in the initial binary sequence can be observed, which corresponds to spectral spreading. This dispersion makes the signal less vulnerable to jamming concentrated on a narrow band.

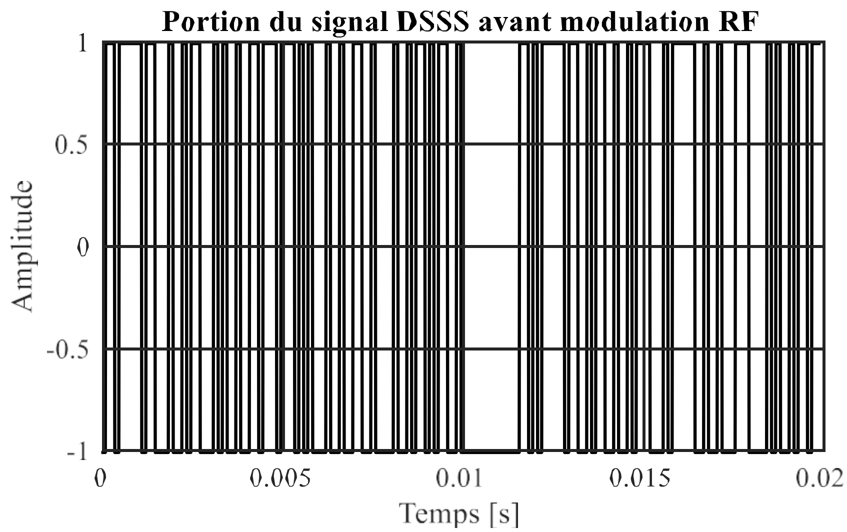

Figure 3.10. Portion of the DSSS signal before RF modulation.

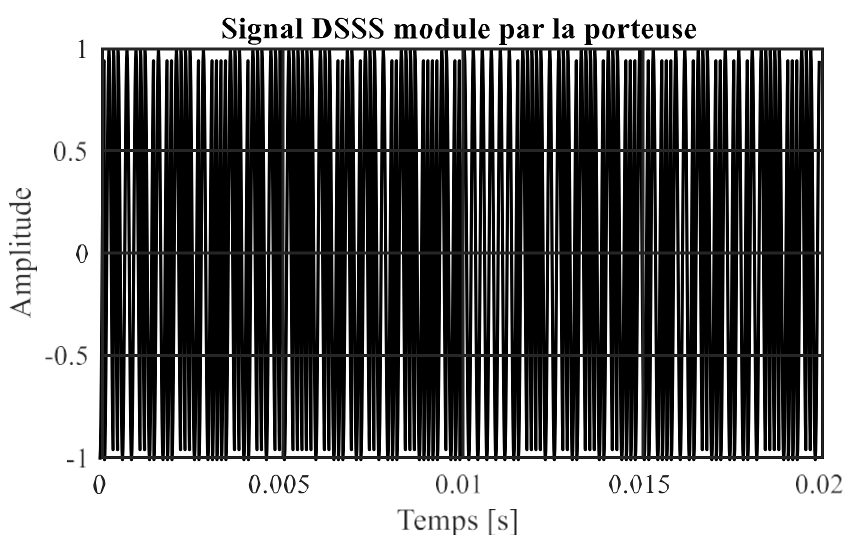

Figure 3.11. DSSS signal multiplied by the carrier.

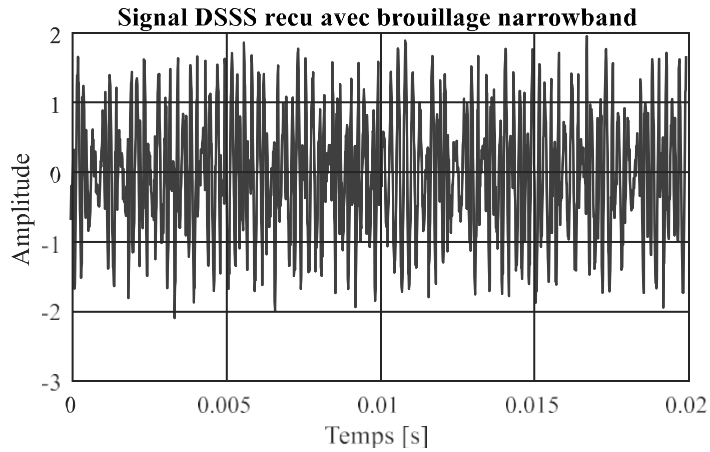

Figure 3.12. DSSS signal received with narrowband jamming and noise.

Figure 3.12 shows the effect of a narrowband jammer added to the DSSS signal. Even if the time-domain signal appears strongly disturbed, the DSSS principle makes it possible, after despreading, to reduce the relative impact of narrowband jamming. This observation explains why the DSSS BER obtained in Figure 3.2 remains lower than the FHSS BER in the simulated scenario.

3.6. Simulation Results of the FHSS Chain

The FHSS technique is based on the pseudo-random change of the carrier frequency. The transmitter and the receiver share the same hopping sequence in order to remain synchronized. In the script, six frequencies are available: 2 kHz, 3 kHz, 4 kHz, 5 kHz, 6 kHz, and 7 kHz.

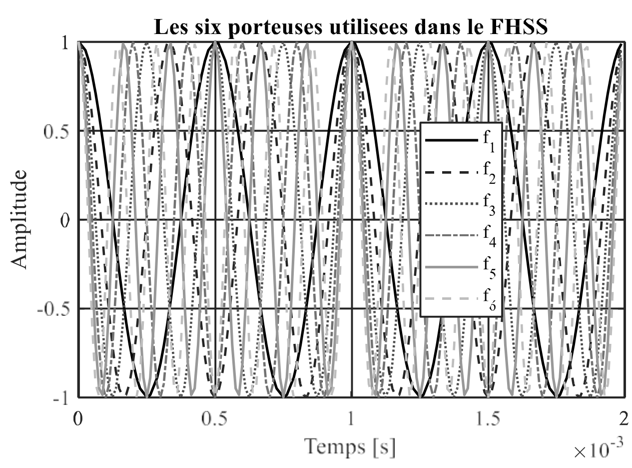

Figure 3.13. The six carriers used in the FHSS chain.

Figure 3.13 shows the frequency bank used by FHSS. Frequency diversity allows the system to avoid staying for a long time on a disturbed frequency. This property is particularly useful against partial or localized jamming.

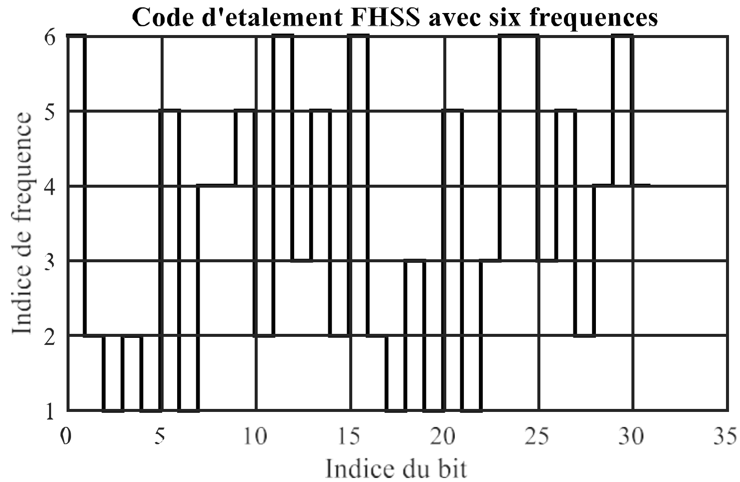

Figure 3.14. FHSS spreading code with six frequencies.

Figure 3.14 indicates the frequency index used for each bit. The pseudo-random choice of frequencies makes the signal less predictable for an unsynchronized jammer. However, if a reactive jammer quickly detects the hops, the advantage of FHSS may decrease.

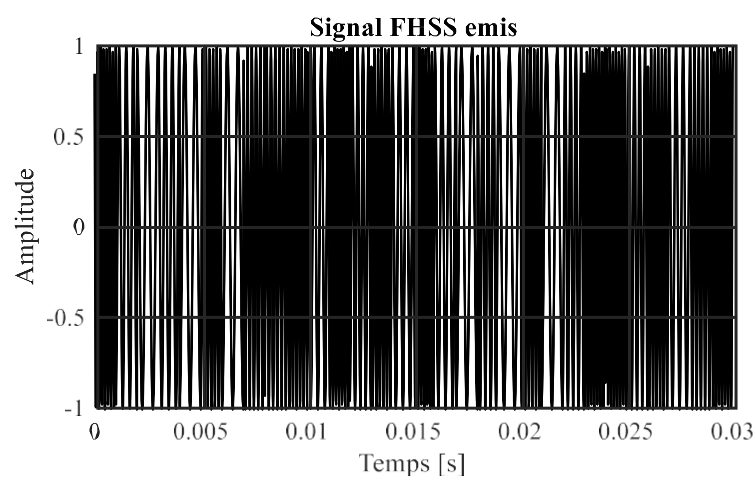

Figure 3.15. Transmitted FHSS signal.

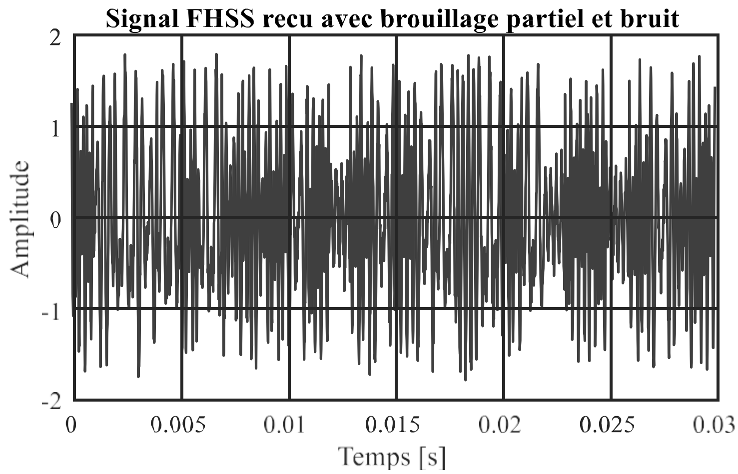

Figure 3.16. FHSS signal received with partial jamming and noise.

Figure 3.16 illustrates the received signal after adding a partial jammer and Gaussian noise. FHSS does not eliminate jamming, but it reduces its impact duration by regularly changing frequency. This logic explains the decrease in BER when Eb/N0 increases, even if the BER remains higher than that of DSSS in the selected scenario.

3.7. OFDM Simulation Results with CV-VSS-NLMS Filtering

The OFDM chain is used to study the effect of impulsive noise and the interest of the CV-VSS-NLMS adaptive filter. The script generates QPSK symbols, applies a 64-point IFFT, adds a cyclic prefix of 16 samples, and then injects Gaussian noise and parasitic impulses.

Table 3.4. Parameters of the OFDM block and the CV-VSS-NLMS filter.

Block	Parameter	Value	Interpretation
OFDM	Nfft	64	Number of subcarriers used
OFDM	cpLen	16	Cyclic prefix to limit ISI
OFDM	NsymOFDM	20	Number of simulated OFDM symbols
Impulsive noise	pImp	0.02	Probability of impulse occurrence
Impulsive noise	impGain	12	Relative intensity of impulses
CV-VSS-NLMS	Lfilter	8	Length of the adaptive filter
CV-VSS-NLMS	muMin / muMax	0.005 / 0.4	Bounds of the variable step size

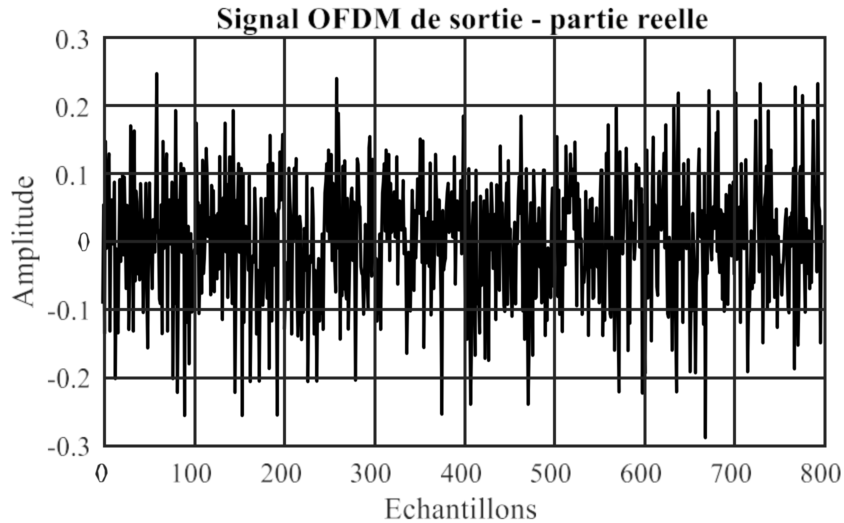

Figure 3.17. OFDM output signal before impulsive noise.

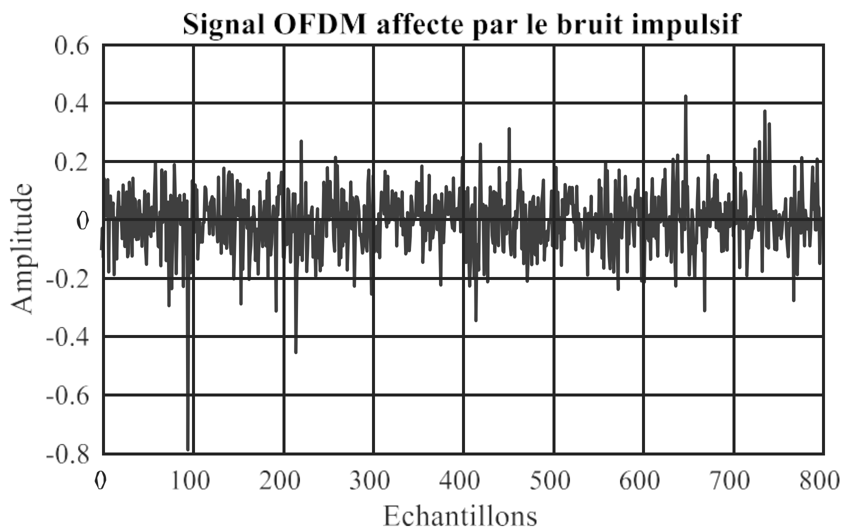

Figure 3.18. OFDM signal corrupted by parasitic impulses.

Figure 3.18 highlights sudden variations due to impulsive noise. This type of disturbance is dangerous for UAV communications, because it can cause strong punctual errors even when the average noise seems limited.

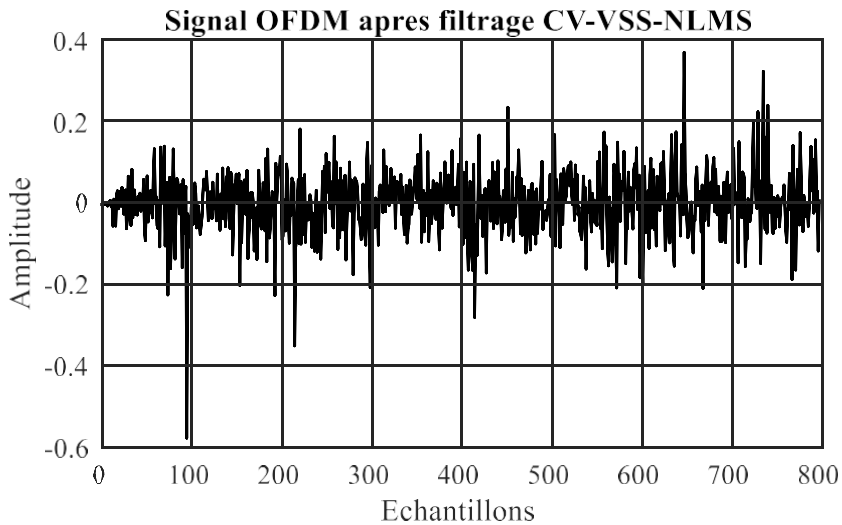

Figure 3.19. OFDM signal after CV-VSS-NLMS filtering.

Figure 3.19 shows the signal after adaptive filtering. The role of CV-VSS-NLMS is to adjust its adaptation step according to the instantaneous error in order to reduce impulsive disturbances without using a multi-antenna architecture. This approach is therefore interesting for a UAV, where mass, consumption, and hardware complexity must remain limited.

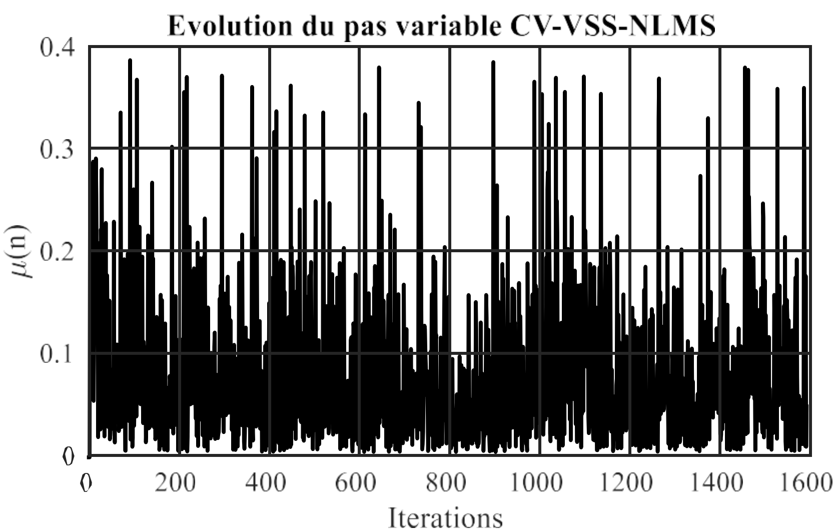

Figure 3.20. Evolution of the variable step size μ(n) of the CV-VSS-NLMS filter.

Figure 3.20 shows the internal behavior of the filter. When the error is large, the adaptation step increases in order to correct the signal more quickly. When the error decreases, the step stabilizes at a lower value, which limits oscillations and improves filtering stability.

3.8. Comparative Synthesis of the Adopted Results

The results generated by the script confirm the complementarity of the three approaches. DSSS acts mainly through direct signal spreading, FHSS acts through frequency mobility, while CV-VSS-NLMS acts at the receiver level to reduce impulsive disturbances. These techniques therefore do not respond to exactly the same type of threat.

Table 3.5. Critical comparison of the techniques based on the integrated results.

Technique	Observed result	Strength	Main limitation	Recommended UAV use
DSSS	BER = 0.001 at 20 dB	Effective against narrowband jamming	Uses more bandwidth	Critical commands and telemetry
FHSS	BER = 0.003 at 20 dB	Avoids disturbed frequencies	Depends on hopping synchronization	Partial or frequency jamming
CV-VSS-NLMS	MSE = 0.005 at 20 dB	Reduces impulsive noise at receiver	Adaptive step tuning	OFDM with impulsive noise

A robust strategy for UAVs should not be limited to a single technique. A multilayer architecture can combine a spreading or frequency-hopping mechanism at the transmission level with adaptive filtering at the reception level. Thus, DSSS or FHSS can reduce exposure to jamming, while CV-VSS-NLMS can correct the remaining disturbances in the received signal.

3.9. Critical Analysis and Experimental Limitations

The obtained figures make it possible to present the chapter results more clearly. They show the behavior of the DSSS, FHSS, and CV-VSS-NLMS techniques in different transmission cases.

In this experiment, the transmission channel is studied in a simple way in order to facilitate the analysis of the results. The main effects of jamming and noise are considered to observe the response of the techniques used.

Synchronization between the transmitter and the receiver is taken into account in the operation of the DSSS and FHSS systems. This synchronization makes it possible to correctly recover the transmitted signal.

For DSSS, narrowband jamming is used in order to study the ability of this technique to resist a disturbance concentrated on a narrow band. For FHSS, partial jamming is applied in order to observe the effect of frequency changing on transmission quality.

The CV-VSS-NLMS filter is used with a noisy OFDM signal. Its role is to reduce the effect of impulsive noise and improve the shape of the received signal. The MSE results show the improvement obtained after filtering.

The filter parameters, such as the filter length and the variable step size, directly influence its convergence. A good choice of these parameters makes it possible to obtain better noise reduction and a more stable response.

Thus, the presented results show that each technique provides a different improvement. DSSS improves resistance to narrowband jamming, FHSS reduces the effect of partial jamming, and CV-VSS-NLMS improves the quality of the OFDM signal in the presence of impulsive noise.

3.10. Conclusion

In this chapter, the conducted experiments make it possible to study the behavior of the DSSS, FHSS, and CV-VSS-NLMS techniques in UAV communication. The analysis shows that, when the value of Eb/N0 increases, the bit error rate decreases for DSSS and FHSS. In the studied case, the DSSS technique gives better performance than FHSS. The CV-VSS-NLMS filter also makes it possible to reduce the MSE, which shows its important role in reducing impulsive noise in an OFDM chain.

Thus, DSSS can be considered an effective technique against narrowband jamming. FHSS is more suitable for partial jamming or frequency-related disturbances. The CV-VSS- NLMS filter represents a complementary solution at the receiver level, because it improves the quality of the received signal.

General Conclusion

This thesis focused on the study of robust communication techniques for UAVs against radio disturbances, especially intentional jamming and impulsive noise. The general objective was to understand the constraints of UAV links, to study existing anti- jamming methods, and to verify, through an experimental study, the behaviour of three complementary approaches: DSSS, FHSS and CV-VSS-NLMS.

The first chapter presented the general context of UAV communications. It showed that drones need reliable links for command, telemetry and payload data transmission. Technologies such as Wi-Fi, LTE, 5G and OFDM offer several possibilities, but they remain exposed to the effects of mobility, line-of-sight propagation, interference and constraints of size, weight, energy and computation. This chapter also showed that jamming, interception and spoofing attacks can directly affect the availability, confidentiality and integrity of communication.

The second chapter presented a theoretical study of the main

anti-jamming methods. DSSS, FHSS, DS/FH-SS, adaptive control, beamforming, coding, diversity, cognitive approaches and adaptive filtering were compared according to several criteria. This analysis showed that no method is perfect in all cases. DSSS provides an interesting processing gain against narrowband jamming, but it consumes more bandwidth. FHSS is suitable for partial-band jamming thanks to frequency hopping, but it depends on hop synchronization. More advanced methods can improve robustness, but they often add complexity.

The third chapter made it possible to move from theoretical analysis to an experimental study. The experiments were organized around three parts: DSSS, FHSS and OFDM with CV-VSS-NLMS filtering. The BER results show that increasing Eb/N0 improves the reliability of transmission for DSSS and FHSS. In the studied scenario, the BER of DSSS decreases from 0.12 at 0 dB to 0.001 at 20 dB, while the BER of FHSS decreases from 0.15 to 0.003. These values show an important reduction in binary errors when the channel quality increases.

The CV-VSS-NLMS filter also showed its interest for an OFDM chain affected by impulsive noise. The MSE decreases from 0.25 at 0 dB to 0.005 at 20 dB. This decrease shows that adaptive filtering reduces the difference between the filtered signal and the reference signal. Thus, CV-VSS-NLMS can be used as a correction layer at the receiver side, in addition to spreading or frequency-hopping techniques used at the transmission side.

In general, the results confirm the complementarity of the studied techniques. DSSS is effective against disturbances concentrated on a narrow band. FHSS is useful when jamming affects only some frequencies. CV-VSS-NLMS improves the quality of the OFDM signal in the presence of impulsive noise. Therefore, the most suitable solution for reliable UAV communication is to combine several mechanisms according to the nature of the threat and the constraints of the mission.

This work also presents some perspectives. It would be interesting to extend the study to more realistic channels, such as Rayleigh or Rician channels, to add the Doppler effect, to vary the drone speed, to test reactive or intelligent jammers, and to compare CV-VSS-NLMS with other adaptive filters such as LMS, classical NLMS or RLS. Another important perspective is to measure the execution time, energy consumption and processor load on a real embedded platform.

In conclusion, this thesis shows that the protection of UAV communications must be considered as a global strategy. Anti-jamming techniques do not replace other security mechanisms, but they strengthen the reliability of the radio link. The association of DSSS, FHSS and CV-VSS-NLMS represents a coherent approach to improve the resistance of UAV communications against jamming and impulsive noise.