



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

*Inhibidor semiactivo de sistemas UAS para pequeñas unidades de
infantería*

Grado en Ingeniería Mecánica

ALUMNO: Nicolás García-Amorena Lorente

DIRECTOR: Rubén Nocelo López

CURSO ACADÉMICO: 2025-2026

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

*Inhibidor semiactivo de sistemas UAS para pequeñas unidades de
infantería*

Grado en Ingeniería Mecánica
Intensificación en Tecnología Naval
Cuerpo General

Universida_{de}Vigo

RESUMEN

El presente Trabajo de Fin de Grado aborda el desarrollo y validación de un sistema experimental de detección y neutralización de pequeños sistemas aéreos no tripulados (*UAS*) basado en una arquitectura pasivo-semiactiva. El objetivo del proyecto es explorar la viabilidad de integrar técnicas de inteligencia electrónica y acústica para la protección puntual de unidades desplegadas frente a plataformas de pequeño y medio tamaño.

El sistema propuesto combina tres capacidades principales: detección pasiva mediante análisis acústico, monitorización del espectro electromagnético para la identificación de enlaces de comunicaciones y estimación direccional de la amenaza, y aplicación selectiva de contramedidas de interferencia en radiofrecuencia. Este enfoque permite mantener el silencio electromagnético durante la fase de vigilancia y limitar la emisión activa únicamente al momento en que la amenaza ha sido confirmada.

Para la implementación del sistema se emplea una arquitectura multinodo de bajo coste. Los sensores acústicos están basados en plataformas *Raspberry Pi* equipadas con matrices de micrófonos *MEMS* capaces de capturar audio multicanal y estimar la dirección de llegada de la señal mediante técnicas de *beamforming* y el algoritmo *MUSIC*. En paralelo, nodos de monitorización del espectro emplean receptores radio definida por *software* (*SDR*) *ADALM-Pluto* con antenas direccionales coherentes para la observación de las bandas *ISM* utilizadas habitualmente por *UAS* comerciales.

Los resultados experimentales obtenidos en las instalaciones del *CUD-ENM* demuestran la viabilidad de la arquitectura propuesta: detección acústica pasiva con alcance de hasta 35 metros en exterior mediante la arquitectura híbrida *DSP+ML* y lógico, estimación de dirección de llegada con resolución sectorial de aproximadamente 45° por vía acústica y de $\sim 20^\circ \pm 15^\circ$ por vía radioeléctrica, y degradación efectiva del enlace *FPV* hasta ~ 2 Mbps sobre el *DJI Avata 2* con protocolo *O4/OFDM*, con pérdida completa del enlace de control sobre el *HYT BP S179* con protocolo *FHSS*. La causalidad de la inhibición fue verificada mediante recuperación inmediata del enlace al conmutar desde 2,4 GHz a la banda de 5,8 GHz. El sistema mantiene emisión electromagnética nula durante la fase de vigilancia, preservando el *EMCON* de la unidad protegida.

PALABRAS CLAVE

ELINT, *Counter-UAS*, detección pasiva, arquitectura semiactiva, *EMCON*.

AGRADECIMIENTOS

Quisiera expresar mi agradecimiento a mi familia, a España y a Dios, por todo lo vivido en este camino, las personas conocidas y las decisiones tomadas que han hecho posible llegar hasta aquí. Especialmente me gustaría agradecer a la camareta 102 por el apoyo dado y al profesor don Rubén Nocelo López por su incansable actitud de trabajo.

CONTENIDO

Contenido	4
Índice de Figuras	9
Índice de Tablas.....	11
Lista de Acrónimos	12
1 Introducción y objetivos	15
1.1 Introducción	15
1.2 Objetivo del trabajo.....	17
1.3 Estructura del trabajo	18
2 Estado del arte	19
2.1 Sistemas <i>C-UAS</i> Pasivo-Semiactivos.....	19
2.1.1 Introducción al desafío de los UAS y la evolución de los C-UAS	19
2.1.2 Proliferación de UAS y sus Amenazas (Seguridad, Privacidad, Defensa).....	20
2.1.3 Limitaciones de los sistemas C-UAS activos y la importancia del EMCON.....	20
2.1.4 La Filosofía Pasivo-Activa como Enfoque de Supervivencia	21
2.1.5 Tecnologías de Detección Pasiva de UAS.....	22
2.1.6 Variabilidad del Adversario y la Necesidad de Robustez	24
2.2 Detección Acústica (<i>ACINT</i>)	24
2.2.1 Fundamentos y firmas sonoras	24
2.2.2 Limitaciones y Sensibilidad Ambiental.....	25
2.3 Detección Electroóptica/Infrarroja (<i>EO/IR</i>) Pasiva	25
2.4 Radar Pasivo: Potencial y Desafíos	26
2.4.1 Principios de Funcionamiento	26
2.4.2 Ventajas y Limitaciones Críticas	27
2.5 Fusión Multisensorial y Algoritmos de Decisión	28
2.5.1 Algoritmos de Fusión de Datos y Deep Learning	28
2.6 Lógica de Decisión Escalonada y Criterios de Activación	30
2.7 Estrategias de Interdicción y Mitigación Semiactiva.....	31
2.7.1 Tecnologías de Contramedidas Electrónicas (ECM) Selectivas	31
2.7.2 Inhibición de Radiofrecuencia (RF Jamming).....	32
2.7.3 Interferencia y Engaño de Navegación (GNSS Spoofing/Jamming)	33
2.7.4 Explotación de Vulnerabilidades y Protocolos.....	33
2.7.5 Metodología de Implementación Limitada en Tiempo y Frecuencia.....	35
2.7.6 Dimensiones de la Limitación Operativa	35
2.7.7 Beneficios Estratégicos y Técnicos	36

2.7.8 Gestión Táctica y Eficacia Operacional.....	36
2.7.9 Precisión y Latencia en la Cadena de Control	36
2.7.10 El Dilema del Umbral de Alternancia.....	36
2.7.11 Modos de Neutralización: Recuperación vs. Destrucción	36
2.7.12 Dinámica de Decisión y Latencia Táctica	37
3 Desarrollo del TFG.....	39
3.1 Medios y Disposición empleados	40
3.1.1 Características de los Medios	40
3.2 Arquitectura <i>software</i> y Lógica de operación	42
3.3 Detección Acústica	43
3.3.1 Fundamentos.....	43
3.3.2 Modelado Físico y Espectral de la firma Acústica	44
3.3.3 Fundamentación del Filtrado y Estimación energética.....	45
3.3.4 Umbral Adaptativo y Modelado estadístico del Ruido.....	45
3.3.5 Limitaciones del Medio de Propagación y Desafíos Técnicos	46
3.3.6 Caracterización Espectral de Objetivos	47
3.3.7 Caracterización del Objetivo I: DJI Avata 2.....	48
3.3.8 Caracterización del Objetivo II: HYT BP S179	50
3.4 Detección en el Espectro Electromagnético.....	51
3.4.1 Fundamentos.....	51
3.4.2 Desafíos Críticos y Problemática del Procesado Espacial.....	52
3.4.2.1 Modelado Matemático del Array Lineal Uniforme	53
3.4.2.2 Ambigüedad Espacial y la Condición Crítica de Separación $\lambda/2$	53
3.4.2.3 Formación de haz.....	54
3.4.2.4 Estimación de DOA mediante MUSIC.....	55
3.4.3 Análisis de Limitaciones y Restricciones del Modelo de Estimación	55
3.4.4 Caracterización Experimental en el Espectro RF	56
3.4.5 Caracterización Experimental del Objetivo I: DJI Avata 2	56
3.4.6 Caracterización Experimental del Objetivo II: HYT BP S179.....	58
3.5 Inhibición en Radiofrecuencia	59
3.5.1 Fundamentos de la Inhibición Selectiva	60
3.5.2 Modelado Fisicomatemático de la Interferencia.....	60
3.5.3 Análisis Geométrico-energético de la Interferencia	61
3.5.4 Direccionamiento y formación de haz en transmisión.....	61
3.5.5 Caracterización espectral de la interferencia	62
3.5.6 Limitaciones Físicas y Hardware.....	62

3.5.7 Validación experimental de la respuesta: Emisión de la Interferencia.....	63
4 Resultados y Validación.....	65
4.1 Entorno y condiciones experimentales	65
4.2 Detección Acústica	66
4.2.1 Disposición de los Medios.....	66
4.2.2 Resultados en exteriores	69
4.2.3 Estimación de Dirección de Llegada Acústica	72
4.3 Detección en el Espectro Electromagnético.....	73
4.3.1 Disposición de los Medios.....	73
4.3.2 Resultados.....	74
4.4 Inhibición en Radiofrecuencia	74
4.4.1 Justificación del escenario de prueba: por qué solo exterior	74
4.4.2 Ensayo estático - degradación del enlace FPV	75
4.4.3 Ensayo dinámico - trayectoria hipódromo.....	79
4.4.4 Interferencia generada con técnica de beamforming	81
4.5 Validación	82
4.5.1 Validación del subsistema acústico	82
4.5.2 Validación del subsistema de estimación del DOA.....	83
4.5.3 Validación del subsistema de interferencia RF	83
4.5.4 Evaluación global del sistema	84
5 Conclusiones y líneas futuras	87
5.1 Conclusiones	87
5.1.1 Cumplimento de los objetivos	87
5.1.2 Hallazgos integrados.....	88
5.1.3 Limitaciones	88
5.2 Líneas Futuras	89
5.2.1 Arquitectura distribuida de sensores.....	89
5.2.2 Comunicaciones basadas en tecnologías de largo alcance	89
5.2.3 Portabilidad y reducción SWaP para despliegue operativo	90
6 Bibliografía.....	91
Anexo I: Implicaciones Sociales, Económicas y Ambientales	94
Introducción general al marco de valoración multidimensional	94
Implicaciones sociales, de salud-seguridad	94
Necesidad social de una defensa contra UAS.....	94
Protección de la vida humana y de la integridad personal.....	94

Privacidad y derechos fundamentales.....	95
Seguridad operacional del espacio.....	95
Impacto social indirecto.....	96
Implicaciones económicas	96
Modelo de coste-beneficio basado en componentes COTS	96
Software libre como reducción de OPEX.....	96
Eficiencia energética y autonomía.....	96
Escalabilidad y modularidad como factor de rentabilidad	96
Impacto de la cadena de suministro y en la industria local	97
Implicaciones ambientales	97
Reducción de la huella espectral.....	97
Consumo energético reducido y huella de carbono	97
Gestión del ciclo de vida de los componentes electrónicos.....	97
Impacto de la fabricación y del transporte.....	97
Compatibilidad con energías renovables en el campo.....	98
Anexo II: Reflexiones Éticas y Sociales	99
Implicaciones éticas y sociales	99
El problema del uso dual y la responsabilidad del inventor	99
Reconocimiento de la insuficiencia de las medidas adoptadas	99
Implicaciones para el desarrollo futuro	100
Marco ético propuesto para resolver la tensión	100
Responsabilidad humana, automatización y dilemas de toma de decisiones	100
Riesgo de daño colateral	101
Conclusión	101
Anexo III: Descripción de los programas desarrollados	103
Dependencias y Entorno de Desarrollo.....	104
Python	104
GNU Radio	104
Bloque I - Detección Acústica	104
Detector Acústico Básico - detector_acustico.py	104
Arquitectura	104
Pipeline de Procesado de Señal Digital	105
Umbral adaptativo con Histéresis	105
Parámetros configurables.....	105
Interfaz Gráfica	106
Consola DOA para Array MA-USB8 - Consola_DOA_MAUSB8.py	106

Funcionamiento	106
Interfaz del usuario	106
Detector Avanzado Multibanda con DOA - Detector _Acustico_MERGED.py	106
Mejoras respecto al Detector Básico	106
Estimación de Dirección de Aproximación	107
Parámetros clave del detector avanzado	107
CIC Unificado con Machine Learning - cic_onefile.py	108
Capacidades únicas	108
Pipeline ML	108
Herramienta de Captura y Análisis - Creador de espectogramas.py	108
Funcionalidad	108
Bloque II - Inhibidor <i>RF</i> con GNU Radio	108
Hardware empleado	109
Simulador-v1 (CHIRP + Beamforming básico) - Inhibidor_Semiactivo.grc	109
Cadena de señal	109
Emisor Real PlutoSDR v1 - Inhibidor_Semiactivo_Pluto2TX/2RX.grc	109
Configuración del PlutoSDR	109
EpyBlock DOA.....	110
Emisor v2 con DOA MUSIC- Inhibidor_v2_RX_Beamforming_Pluto.grc	110
Nuevos bloques respecto a v1	110
Principio del algoritmo MUSIC.....	110
Emisor v3 con servo y encontrador de dirección.....	110
Nuevos bloques respecto a v2.....	110
Anexo IV: Uso responsable de IAG	111
Herramientas empleadas	111
Alcance del uso	111
Metodología	111
Listado de prompts utilizados	111

ÍNDICE DE FIGURAS

Figura 1-1 Usos maliciosos de drones.....	15
Figura 1-2 Tiempos de reacción según el tipo de contramedida	17
Figura 1-3 Ciclo operativo del sistema <i>C-UAS</i>	18
Figura 2-1 Métodos de detección de <i>UAS</i>	19
Figura 2-2 Representación gráfica del ciclo sensor - tirador.....	21
Figura 2-3 Diagrama de inhibidor con técnica de “look-through”.....	22
Figura 2-4 Comparación de características de sensores.	28
Figura 2-5 Fusión multisensor para adquisición de blanco	29
Figura 2-6 Clasificación de técnicas de neutralización.	31
Figura 2-7 Clasificación de ciberataques sobre <i>UAS</i>	34
Figura 2-8 Vulnerabilidades de ataque de <i>spoofing GPS</i> sobre <i>UAS</i>	35
Figura 3-1 Taxonomía de la guerra.	39
Figura 3-2 <i>ADALM PlutoSDR</i> de Analog Devices Inc.	40
Figura 3-3 <i>TinySA</i> es un analizador de espectro portátil de código abierto.	41
Figura 3-4 Antena direccional 2,4 GHz TP-LINK TL_ANT2409A.....	41
Figura 3-5 Array de micrófonos <i>MA-USB8</i> utilizado como sensor espacial del sistema.....	41
Figura 3-6 Arquitectura modular del sistema <i>C-UAS</i> semiactivo.	42
Figura 3-7 Fases del desarrollo del detector acústico.....	44
Figura 3-8 Espectrograma del ruido ambiental.	48
Figura 3-9 Ecosistema <i>UAV DJI Avata 2</i>	49
Figura 3-10 Espectrograma acústico <i>DJI Avata 2</i>	49
Figura 3-11 Plataforma <i>UAV HYT BP S179</i> y elementos asociados al sistema.	50
Figura 3-12 Espectrograma acústico del <i>UAS HYT BP S179</i>	50
Figura 3-13 Representación espectral del enlace radioeléctrico del <i>DJI Avata 2</i> en 2,4 GHz.....	57
Figura 3-14 Espectro acumulado del enlace de control del <i>HYT BP S179</i>	58
Figura 3-15 Fases del desarrollo del detector <i>SIGINT</i>	60
Figura 3-16 Espectro y <i>waterfall</i> de la señal de interferente.....	63
Figura 4-1 Vista satelital ENM. Elaboración propia [31].	65
Figura 4-2 Representación esquemática del entorno de ensayo en interiores.	66
Figura 4-3 Sistema de adquisición acústica empleado durante las pruebas experimentales.....	67
Figura 4-4 Configuración del sistema de adquisición acústica en interiores.	67
Figura 4-5 Progresión de la detección acústica en interior mediante Detector_Acústico.....	68
Figura 4-6 Progresión de la detección acústica mediante Detector_Acustico (MERGED).....	69
Figura 4-7 Progresión de la detección acústica mediante cic_onefile.....	69

Figura 4-8 Resultados de detección acústica. Figuras de la Izquierda visión subjetiva, derecha interfaz Detector_Acústico.	70
Figura 4-9 Resultados de detección acústica y adquisición de <i>DOA</i>	70
Figura 4-10 Desarrollo de los estados de alerta de la aplicación “cic_onefile”.	71
Figura 4-11 Progresión de la detección acústica en interior mediante <i>DOA-UAS</i>	72
Figura 4-12 Prueba de campo del sistema de estimación <i>DOA</i> acústico mediante <i>DOA UAS</i>	72
Figura 4-13 Disposición de antenas empleadas durante las pruebas de interferencia en interior. ...	73
Figura 4-14 Dispositivo de interferencia direccional utilizado en las pruebas de campo.	73
Figura 4-15 Resultado experimental de seguimiento in-situ de <i>UAS</i> con "Inhibidor_v2_RX_Beamforming".	74
Figura 4-16 Representación espectral y <i>waterfall</i> de la señal interferente sobre las comunicaciones del <i>Avata 2</i> , izquierda, y el <i>HYT BP S179</i> , derecha.	75
Figura 4-17 Ajustes predeterminados de la unidad transmisora <i>DJI Googles 3</i>	76
Figura 4-18 Interfaz <i>FPV</i> de las <i>DJI Goggles 3</i> , tasa de bits es el número 9 [34].	76
Figura 4-19 Geometría del ensayo de inhibición <i>RF</i>	77
Figura 4-20 Secuencia de degradación del enlace <i>FPV</i> del <i>UAS</i> durante la aplicación de interferencia.	78
Figura 4-21 Vista cenital del ensayo dinámico Elaboración propia.	79
Figura 4-22 Ensayo dinámico de perturbación <i>RF</i> durante un vuelo tipo hipódromo.	80
Figura 4-23 Diagrama de flujo en GNU Radio Companion.	81
Figura 4-24 <i>UAS</i> posado, incapaz de levantar el vuelo debido a telemetría anulada.	82
Figura 4-25 Recuperación de las comunicaciones tras cambio de banda.	84
Figura 0-1 Código QR enlazado con el repositorio de GitHub.	103

ÍNDICE DE TABLAS

Tabla 2-1: Comparativa de tecnologías de detección.....	27
Tabla 3-1: Características del ruido ambiental y de la firma <i>UAS</i>	47
Tabla 3-2: Comparativa entre <i>DJI Avata 2</i> y <i>HYT BP S179</i>	51
Tabla 3-3: Características espectrales del <i>DJI Avata 2</i>	57
Tabla 3-4: Características espectrales del <i>HYT BP S179</i>	59
Tabla 3-5: Comparativa espectral entre <i>DJI AVATA</i> y <i>HYT BP S179</i>	59
Tabla 4-1: Representación de la degradación respecto al tiempo y emisión interferente.	79
Tabla 4-2: Resultados recopilados.....	85

LISTA DE ACRÓNIMOS

Acrónimo Significado

ACCST	Advanced Continuous Channel Shifting Technology
ACINT	Acoustic Intelligence -Inteligencia Acústica
AES-256	Advanced Encryption Standard (clave de 256 bits)
ANN	Artificial Neural Network -Red Neuronal Artificial
ATC	Air Traffic Control -Control de Tráfico Aéreo
AWGN	Additive White Gaussian Noise -Ruido Blanco Gaussiano Aditivo
BDA	Battle Damage Assessment -Evaluación de Daños de Combate
BER	Bit Error Rate -Tasa de Error de Bit
BPF	Band-Pass Filter -Filtro Paso Banda
C2	Command and Control -Mando y Control
CAPEX	Capital Expenditure -Gasto de Capital
CHIRP	Compressed High Intensity Radar Pulse
CIC	Clasificador Integrado Combinado
CNN	Convolutional Neural Network -Red Neuronal Convolutacional
COTS	Commercial Off The Shelf -Componentes Comerciales Estándar
C-UAS	Counter Unmanned Aircraft System -Sistema Contra-UAS
CUD	Centro Universitario de la Defensa
DBN	Deep Belief Network -Red de Creencias Profundas
DJI	Da-Jiang Innovations
DL	Deep Learning -Aprendizaje Profundo
DOA	Direction of Arrival -Dirección de Llegada
DSP	Digital Signal Processing -Procesado Digital de Señal
DSSS	Direct Sequence Spread Spectrum -Espectro Ensanchado por Secuencia Directa
DVB-T	Digital Video Broadcasting – Terrestrial -Televisión Digital Terrestre
ECM	Electronic CounterMeasures -Contramidas Electrónicas
EIRP	Equivalent Isotropically Radiated Power -Potencia Radiada Isotrópica Equivalente
ELINT	Electronic Intelligence -Inteligencia Electrónica
EMCON	Emission Control -Control de Emisión Electromagnética
EMP	Electromagnetic Pulse -Pulso Electromagnético
EO/IR	Electro-Optical / Infrared -Electroóptico / Infrarrojo
ESC	Electronic Stability Control -Control Electrónico de Estabilidad
EVD	Eigenvalue Decomposition -Descomposición en Valores Propios
EW	Electronic Warfare -Guerra Electrónica
FAA	Federal Aviation Administration
FASST	Futaba Advanced Spectrum Spread Technology
FEC	Forward Error Correction -Corrección de Errores hacia Adelante
FHSS	Frequency Hopping Spread Spectrum -Espectro Ensanchado por Salto de Frecuencia
FPGA	Field Programmable Gate Array
FPV	First Person View -Vista en Primera Persona

Acrónimo Significado

FSM	Finite State Machine -Máquina de Estados Finita
GCS	Ground Control Station -Estación de Control en Tierra
GLONASS	Globalnaya Navigatsionnaya Sputnikovaya Sistema -Sistema de Navegación Ruso por Satélite
GNSS	Global Navigation Satellite System -Sistema Global de Navegación por Satélite
GPIO	General Purpose Input/Output -Entrada/Salida de Propósito General
GPU	Graphics Processing Unit -Unidad de procesamiento gráfico
GPS	Global Positioning System -Sistema de Posicionamiento Global
GUI	Graphical User Interface -Interfaz Gráfica de Usuario
IAG	Inteligencia Artificial Generativa
ICNIRP	International Commission on Non-Ionizing Radiation Protection
IED	Improvised Explosive Device -Artefacto Explosivo Improvisado
IMU	Inertial Measurement Unit -Unidad de Medida Inercial
IQ	In-phase / Quadrature -Señal en Fase y Cuadratura
ISM	Industrial, Scientific and Medical -Bandas de Frecuencia Industrial, Científica y Médica
ISR	Intelligence, Surveillance and Reconnaissance -Inteligencia, Vigilancia y Reconocimiento
KNN	K-Nearest Neighbors -K Vecinos más Cercanos
LLM	Large Language Model -Modelo de Lenguaje de Gran Escala
LoRa	Long Range -Protocolo de Comunicación de Largo Alcance
LOS	Line of Sight -Línea de Visión Directa
LPD	Low Probability of Detection -Baja Probabilidad de Detección
LPI	Low Probability of Interception -Baja Probabilidad de Intercepción
LSS	Low, Slow, Small -Bajo, Lento, Pequeño
MAE	Mean Absolute Error -Error Absoluto Medio
MEMS	Micro-Electro-Mechanical Systems -Sistemas Microelectromecánicos
MIMO	Multiple Input Multiple Output -Múltiple Entrada Múltiple Salida
ML	Machine Learning -Aprendizaje Automático
MUSIC	Multiple Signal Classification
NPU	Neural Processing Unit -Unidad de procesamiento neuronal
O4	OcuSync 4 -Protocolo de Transmisión Digital de DJI
OFDM	Orthogonal Frequency Division Multiplexing -Multiplexación por División de Frecuencia Ortogonal
OODA	Observe, Orient, Decide, Act -Observar, Orientar, Decidir, Actuar
OPEX	Operational Expenditure -Gasto Operacional
OTAN	Organización del Tratado del Atlántico Norte
PFA	Probability of False Alarm -Probabilidad de Falsa Alarma
PSD	Power Spectral Density -Densidad Espectral de Potencia
PWM	Pulse Width Modulation -Modulación por Ancho de Pulso
QAM	Quadrature Amplitude Modulation -Modulación de Amplitud en Cuadratura
RCS	Radar Cross Section -Sección Transversal Radar
RGPD	Reglamento General de Protección de Datos

Acrónimo Significado

RNN	Recurrent Neural Network -Red Neuronal Recurrente
RPM	Revolutions Per Minute -Revoluciones por Minuto
RPS	Relative Positioning System -Sistema de Posicionamiento Relativo
RTH	Return To Home -Retorno al Punto de Origen
SCF	Spectral Correlation Function -Función de Correlación Espectral
SDR	Software Defined Radio -Radio Definida por Software
SIGINT	Signals Intelligence -Inteligencia de Señales
SINR	Signal to Interference plus Noise Ratio -Relación Señal a Interferencia más Ruido
SNR	Signal to Noise Ratio -Relación Señal a Ruido
SOP	Signals of Opportunity -Señales de Oportunidad
STFT	Short-Time Fourier Transform -Transformada de Fourier de Tiempo Corto
SVM	Support Vector Machine -Máquina de Vectores de Soporte
SWaP	Size, Weight and Power -Tamaño, Peso y Potencia
TCO	Total Cost of Ownership -Coste Total de Propiedad
TDOA	Time Difference of Arrival -Diferencia de Tiempo de Llegada
TFG	Trabajo de Fin de Grado
TLS	Transport Layer Security -Seguridad de la Capa de Transporte
UAS	Unmanned Aircraft System -Sistema Aéreo No Tripulado
UAV	Unmanned Aerial Vehicle -Vehículo Aéreo No Tripulado
UDP	User Datagram Protocol -Protocolo de Datagrama de Usuario
ULA	Uniform Linear Array -Array Lineal Uniforme
USS	UAS Service Supplier -Proveedor de Servicios UAS
UTM	UAS Traffic Management -Gestión del Tráfico de UAS
VGG-16	Visual Geometry Group 16 -Arquitectura de Red Neuronal Profunda
VID	Visual Identification -Identificación Visual
MFCC	Mel-Frequency Cepstral Coefficients -Coeficientes Cepstrales en la Escala Mel

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Introducción

La transformación del campo de batalla contemporáneo está estrechamente vinculada a la proliferación de los sistemas aéreos no tripulados (*UAS*), particularmente aquellos de clase I y micro-*UAS*, caracterizados por su bajo coste, elevada disponibilidad y rápida adaptabilidad [1]. Estas plataformas, basadas mayoritariamente en tecnologías de comunicaciones civiles y componentes comerciales (*COTS*) [2], han demostrado una capacidad significativa para ejecutar misiones de inteligencia, vigilancia y reconocimiento (*ISR*) [3], adquisición y corrección de objetivos para fuegos indirectos [4], evaluación de daños de combate (*BDA*) y ataque directo mediante municiones improvisadas o cargas explosivas ligeras [5], tal y como se ilustra en la Figura 1-1.

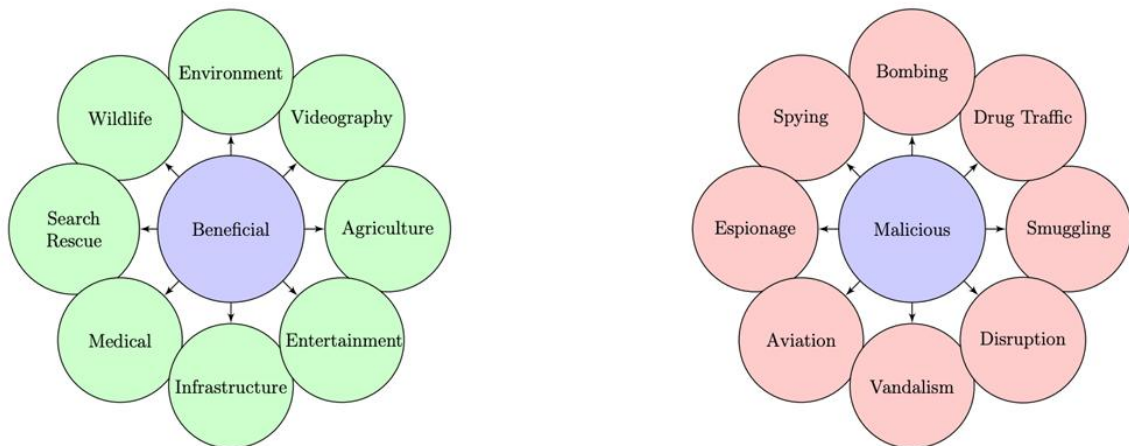


Figura 1-1 Usos maliciosos de drones.

El conflicto en Ucrania ha supuesto un punto de inflexión doctrinal al evidenciar la integración sistemática de *UAS* en todos los escalones tácticos, desde unidades de pequeña entidad hasta operaciones de nivel operacional. Informes de análisis militar coinciden en señalar que la combinación de persistencia aérea, baja firma visual y acústica y enlaces de comunicaciones distribuidos ha reducido drásticamente la profundidad efectiva del despliegue, exponiendo posiciones previamente consideradas seguras y acelerando el ciclo sensor-tirador (*sensor-to-shooter loop*).

Desde el punto de vista de las telecomunicaciones, la mayoría de estos *UAS* emplean enlaces de mando y control (*C2*) en bandas *ISM*, protocolos propietarios o semiestándar, y sistemas de navegación por satélite (*GNSS*) para estabilización y posicionamiento. Esta dependencia del espectro electromagnético ha impulsado el desarrollo y despliegue de capacidades *Counter-UAS* (*C-UAS*) centradas en la detección y negación de dichos enlaces [6].

No obstante, la respuesta predominante ha sido la adopción de sistemas activos, basados en radares de corto alcance, sensores emisores y medios de guerra electrónica (*EW*) capaces de interferir de forma continua o semipermanente los enlaces *C2* y *GNSS*, cuyas limitaciones se desarrollan con mayor detalle en el apartado 2.1.3. Aunque estos sistemas pueden resultar eficaces en términos de neutralización inmediata, su empleo sostenido introduce una vulnerabilidad táctica significativa asociada a la generación de una firma electromagnética elevada y persistente [7].

La experiencia operacional reciente ha demostrado que los emisores de interferencia omnidireccionales, especialmente aquellos operando de forma continua, son fácilmente detectables mediante sensores pasivos adversarios, tales como receptores de alerta electromagnética, estaciones de radiogoniometría o incluso *UAS* dedicados a misiones de *ELINT*. Mediante técnicas de triangulación y multilateración, estas emisiones pueden ser geolocalizadas con suficiente precisión como para permitir su neutralización mediante fuegos indirectos de artillería, municiones guiadas o municiones merodeadoras, comprometiendo la supervivencia del sistema y de la posición que protege.

Desde una perspectiva táctica, este fenómeno entra en conflicto directo con principios fundamentales del despliegue de medios, tales como la gestión de la firma electromagnética (*EMCON*), la dispersión, la movilidad y la negación de inteligencia al adversario. Un sistema *C-UAS* que emite de forma continua se convierte, paradójicamente, en un sensor activo para el enemigo, facilitando la adquisición de objetivos y reduciendo el tiempo de reacción adversario.

En este contexto, las doctrinas más recientes de guerra electrónica y defensa aérea de corto alcance enfatizan la necesidad de arquitecturas de baja probabilidad de interceptación (*LPI*) y baja probabilidad de detección (*LPD*), así como la integración de sensores pasivos capaces de operar sin revelar la posición propia. Estas aproximaciones buscan maximizar la supervivencia del sistema mediante la reducción deliberada de emisiones y la activación selectiva de los actuadores únicamente cuando la amenaza ha sido confirmada.

La motivación fundamental del presente proyecto se enmarca en esta línea doctrinal y técnica: el desarrollo de un sistema semiactivo de inhibición de *UAS*, estructurado en torno a una detección pasiva inicial basada en la observación y análisis del espectro electromagnético y acústico, sin emisión propia, seguida de una fase activa de interferencia limitada en el tiempo, frecuencia y, potencialmente, en el espacio, filosofía cuyo fundamento doctrinal se desarrolla en el apartado 2.1.4. Este enfoque pretende mitigar el riesgo de localización del sistema mediante triangulación, reduciendo la ventana temporal durante la cual el emisor es detectable.

Desde el punto de vista de la ingeniería de telecomunicaciones, este planteamiento introduce retos técnicos de elevada complejidad. La detección pasiva de *UAS* requiere la captación de señales de baja potencia, a menudo inmersas en entornos congestionados, y su posterior procesamiento en tiempo real mediante técnicas de análisis espectral, extracción de características y clasificación de señales. La diferenciación entre emisiones asociadas a *UAS*, interferencias ambientales y tráfico legítimo exige algoritmos robustos y criterios de decisión estrictos para minimizar falsas alarmas.

Adicionalmente, la coordinación entre el subsistema de detección pasiva y el subsistema de inhibición activa debe garantizar latencias reducidas, compatibles con la cinemática del *UAS* y los tiempos de reacción tácticos. La activación del inhibidor debe ser suficientemente eficaz para degradar o negar la funcionalidad del *UAS*, pero al mismo tiempo lo bastante breve y controlada como para limitar la exposición electromagnética del sistema defensor.

El enfoque semiactivo propuesto se concibe, por tanto, no únicamente como una solución técnica aislada, sino como una medida mitigadora del riesgo operacional, alineada con los principios de supervivencia en entornos saturados de sensores y fuegos de precisión. El objetivo final no es solo la neutralización puntual de una amenaza aérea, sino la protección sostenida de posiciones sensibles, evitando que el propio sistema *C-UAS* se convierta en un vector de vulnerabilidad explotable por el adversario.

1.2 Objetivo del trabajo

El presente trabajo tiene como objetivo definir, analizar y diseñar un sistema *C-UAS* de arquitectura pasivo-semiactiva, orientado a la detección y mitigación de amenazas aéreas no tripuladas que representen un riesgo directo para pequeñas unidades de infantería, en particular en escenarios de despliegue expedicionario y de protección de fuerzas (como los propios de la Infantería de Marina).

El alcance del sistema se centra en la neutralización de *UAS* de bajo y medio porte, caracterizados por su dependencia de enlaces de comunicaciones digitales comerciales y perfiles de vuelo tácticos:

- Cuadricópteros y multirrotores ligeros, empleados habitualmente en misiones *ISR*, corrección de fuegos indirectos o ataque mediante cargas ligeras.
- Drones merodeadores de ala fija de tamaño pequeño a medio, caracterizados por perfiles de vuelo a baja o media cota, autonomía limitada y empleo táctico contra objetivos puntuales o concentraciones de personal.

Estos sistemas comparten una serie de características relevantes desde el punto de vista técnico y operativo: dependencia de enlaces de mando y control y/o navegación *GNSS*, empleo de componentes comerciales o semicomerciales, y perfiles de vuelo compatibles con la detección pasiva mediante observación del espectro electromagnético y, de forma complementaria, del dominio acústico (Figura 1-2).

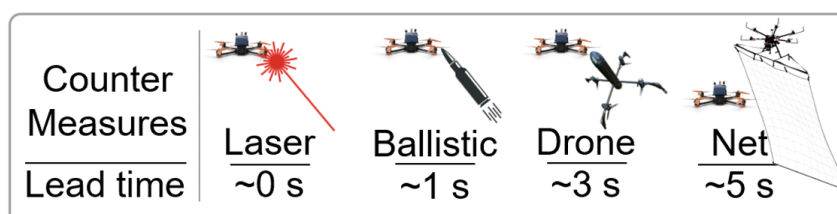


Figura 1-2 Tiempos de reacción según el tipo de contramedida

Desde el punto de vista operativo, el sistema no busca la negación total del espacio aéreo, sino la protección puntual y la reducción de la vulnerabilidad frente a la observación aérea persistente. El proyecto persigue demostrar la viabilidad técnica de una arquitectura que integre:

1. Detección e identificación pasiva de *UAS* mediante el análisis híbrido del espectro electromagnético y el dominio acústico, operando sin emisiones propias para mantener el silencio electrónico, en coherencia con las tecnologías de detección pasiva descritas en el apartado 2.1.5.
2. Localización táctica para la determinación aproximada de la amenaza en tiempos compatibles con la respuesta operativa.
3. Inhibición semiactiva para la activación selectiva y temporalmente limitada de contramedidas electrónicas para degradar la funcionalidad del *UAS* (enlaces *C2* y *GNSS*), priorizando la discreción electromagnética del defensor, tal como se analiza en el apartado 2.7.2.

Con base en la problemática expuesta, el presente trabajo persigue los siguientes objetivos:

1. Analizar las técnicas actuales de detección y neutralización de sistemas aéreos no tripulados en el marco de los sistemas *C-UAS*.
2. Diseñar e implementar un subsistema de detección acústica basado en análisis espectral y detección multibanda.
3. Desarrollar un sistema de estimación de dirección de llegada (*DOA*) utilizando un array de micrófonos *MEMS*.
4. Analizar la detección de señales de control de *UAS* en el espectro electromagnético mediante radio definida por *software*.
5. Explorar la posibilidad de generar interferencia dirigida sobre el enlace de control del *UAS*.
6. Validar experimentalmente el funcionamiento del sistema desarrollado mediante pruebas en entornos controlados.

1.3 Estructura del trabajo

El presente trabajo se estructura en seis capítulos. El Capítulo 1 introduce la problemática operativa que motiva el trabajo, define los objetivos y presenta la estructura general. El Capítulo 2 desarrolla el estado del arte en sistemas *C-UAS* pasivo-semiactivos, abarcando las tecnologías de detección pasiva disponibles acústicas, electroóptica, radar pasivo y *SDR*, los algoritmos de fusión multisensorial y las estrategias de interferencia selectiva, estableciendo el fundamento doctrinal y técnico sobre el que se apoya el diseño propuesto. El Capítulo 3 describe el desarrollo del prototipo experimental, detallando la arquitectura *hardware* y *software* del sistema, el *pipeline* de detección acústica basado en análisis espectral multibanda y umbral adaptativo, la caracterización espectral de los objetivos ensayados, el subsistema de detección y estimación de dirección en el dominio radioeléctrico mediante *SDR*, y el subsistema de inhibición *RF* por barrido *CHIRP* con *beamforming* en transmisión. El Capítulo 4 recoge los resultados experimentales obtenidos en las instalaciones del Centro Universitario de la Defensa en la Escuela Naval Militar, organizados por subsistema acústico, radioeléctrico e inhibición *RF* y evalúa globalmente la arquitectura semiactiva integrada. El Capítulo 5 sintetiza las conclusiones del trabajo, evalúa el grado de cumplimiento de los seis objetivos planteados e identifica tres líneas de investigación futura priorizadas: arquitectura distribuida de sensores, comunicaciones *LoRa* entre nodos y reducción *SWaP* para despliegue operativo. Finalmente, el Capítulo 6 recoge las referencias bibliográficas, y los Anexos I a IV desarrollan las implicaciones sociales, económicas y ambientales, las reflexiones éticas sobre el uso dual de la tecnología, la descripción de los programas desarrollados y el uso responsable de herramientas de inteligencia artificial generativa. La Figura 1-3 resume de forma esquemática el ciclo operativo completo del sistema que se desarrolla a lo largo de los capítulos siguientes.

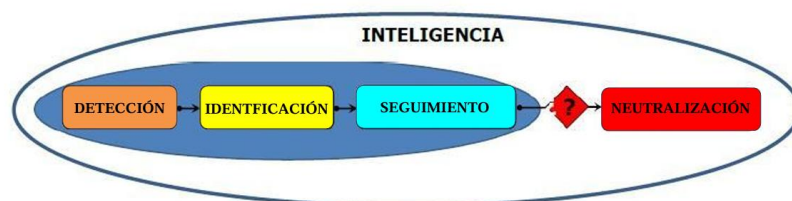


Figura 1-3 Ciclo operativo del sistema *C-UAS*.

2 ESTADO DEL ARTE

2.1 Sistemas C-UAS Pasivo-Semiactivos

2.1.1 Introducción al desafío de los UAS y la evolución de los C-UAS

La proliferación exponencial de los UAS, comúnmente denominados drones, ha impulsado una transformación significativa en múltiples dominios [1]. Su adopción abarca desde aplicaciones comerciales y civiles tales como logística, monitoreo ambiental, agricultura de precisión e inspección de infraestructuras hasta roles críticos en vigilancia, seguridad nacional y respuesta ante emergencias. Este crecimiento, sustentado en la accesibilidad, el bajo coste y la versatilidad de las plataformas, se refleja en las proyecciones de organismos como la *FAA*, que estimaban un incremento de la flota no recreativa en Estados Unidos hasta superar las 835.000 unidades en 2023, aunque estas previsiones seguramente se hayan visto superadas por la realidad operativa en escenarios de conflicto recientes [1, 3 y 4].

Sin embargo, esta rápida expansión conlleva desafíos complejos en materia de seguridad pública y privacidad. La democratización de estas tecnologías exige el desarrollo de soluciones innovadoras capaces de ejecutar con éxito las fases de detección, seguimiento, identificación y mitigación. Cuya taxonomía se recoge en la Figura 2-1.

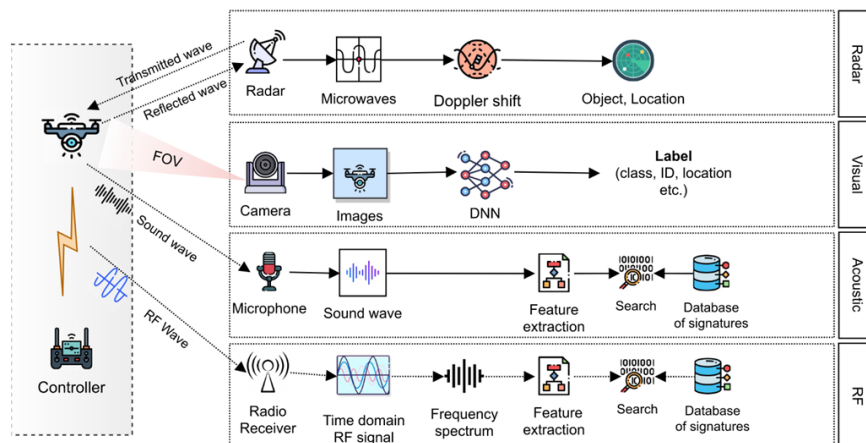


Figura 2-1 Métodos de detección de UAS.

En este contexto, un sistema C-UAS se define como un conjunto de dispositivos diseñados para deshabilitar, interrumpir o tomar el control de una aeronave no tripulada de forma segura y legal [8]. Estructuralmente, un sistema C-UAS se divide en dos subsistemas principales [9]: el subsistema de detección encargado de la alerta temprana y localización del objetivo; y el subsistema de mitigación

responsable de la neutralización de la amenaza. A pesar de los avances recientes, la madurez operativa de estas soluciones aún presenta limitaciones. Persiste una necesidad crítica de enfoques escalables, modulares y asequibles que permitan contrarrestar de manera efectiva la evolución constante de las amenazas *UAS*. Dentro de esta búsqueda de modularidad y asequibilidad, los sistemas pasivos emergen como una solución clave para minimizar la huella logística y electromagnética del defensor.

2.1.2 Proliferación de UAS y sus Amenazas (Seguridad, Privacidad, Defensa)

La versatilidad de los *UAS*, que abarcan desde pequeños cuadricópteros recreativos hasta plataformas militares avanzadas, permite su empleo en una dualidad de escenarios, tanto beneficiosos como maliciosos. Mientras que su uso civil en búsqueda y rescate, logística médica o monitoreo de infraestructuras es indiscutible, su accesibilidad tecnológica ha permitido que actores estatales y no estatales los exploten con fines nefastos. Las amenazas basadas en *UAS* se clasifican generalmente en tres categorías principales [6, 8]:

- **Seguridad Pública:** Las operaciones inseguras representan un riesgo crítico en entornos civiles, destacando el vuelo en proximidades de aeropuertos, sobre concentraciones de personas o interferencia en servicios de emergencia. La desvinculación física entre piloto y plataforma introduce riesgos operativos, como la pérdida del enlace de mando y control (C2) o la incapacidad de realizar maniobras evasivas ante aeronaves tripuladas. Un hito histórico en esta categoría fue el incidente del aeropuerto de Gatwick (2018), donde el avistamiento de *UAS* forzó la cancelación de 1.000 vuelos, afectando a 140.000 pasajeros y evidenciando la fragilidad de la infraestructura crítica ante estas plataformas.
- **Seguridad Nacional:** Esta categoría engloba el sobrevuelo de instalaciones militares, monumentos nacionales y centrales nucleares. Las capacidades de carga útil de los *UAS* permiten el transporte de contrabando, agentes químicos o cargas explosivas (*IED* aéreos). Asimismo, desde la perspectiva de la Guerra Electrónica, los *UAS* pueden actuar como plataformas de vigilancia y reconocimiento (*ISR*) sigiloso o como vectores para ciberataques, permitiendo la interceptación de señales o el robo de información sensible en perímetros restringidos.
- **Privacidad Individual:** El uso de sensores electroópticos permite la vulneración de la privacidad mediante el acoso o la vigilancia no autorizada de residencias privadas. Esta capacidad de eludir barreras físicas tradicionales subraya la ineficacia de las zonas de exclusión aérea puramente normativas, como la restricción de 30 millas en Washington D.C., si no van acompañadas de sistemas de detección y mitigación técnica.

La *OTAN* proporciona un marco de clasificación basado en peso, altitud y radio de misión. En el contexto de este trabajo, resultan de especial interés las categorías inferiores destacando los mini drones con un peso inferior a 15 kg y micro-drones con una energía máxima inferior a 66 J [10].

2.1.3 Limitaciones de los sistemas C-UAS activos y la importancia del EMCON

La respuesta predominante ante la amenaza de los *UAS* ha sido el despliegue de sistemas activos basados en radares de corto alcance y medios de guerra electrónica (*EW*). Estos dispositivos están diseñados para interferir de forma continua o semipermanente los enlaces de mando y control (C2) y de navegación satelital (*GNSS*) [11]. Sin embargo, esta eficacia en la neutralización inmediata conlleva una vulnerabilidad táctica crítica: la dependencia de la emisión activa.

La principal limitación de los sistemas *C-UAS* activos reside en su inherente necesidad de emitir energía electromagnética para funcionar. Esta emisión continua o frecuente crea una "firma electromagnética" elevada y persistente. En el campo de batalla contemporáneo, caracterizado por una densa "malla" de sensores y enlaces, los emisores de interferencia, especialmente los omnidireccionales, son fácilmente detectables por capacidades adversarias de *ELINT* [12]. Mediante técnicas de triangulación y multilateración, los sensores pasivos enemigos pueden geolocalizar el emisor *C-UAS*

con precisión suficiente para coordinar ataques mediante fuegos indirectos, municiones guiadas o municiones merodeadoras. Esta vulnerabilidad no solo compromete la integridad del propio sistema, sino que revela la ubicación de la unidad táctica a la que pretende proteger, acelerando el ciclo "*sensor-to-shooter*" del enemigo, representado en la Figura 2-2.

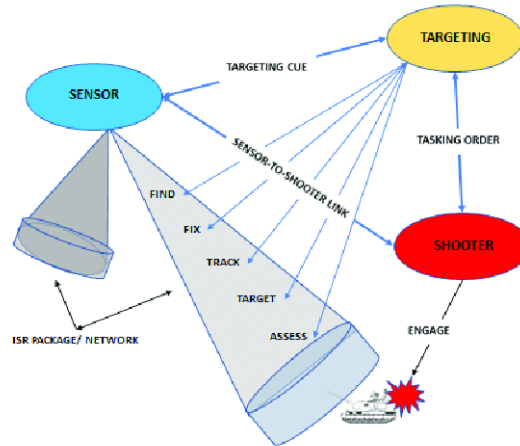


Figura 2-2 Representación gráfica del ciclo sensor - tirador.

Esto no solo compromete la supervivencia del sistema *C-UAS*, sino también la de la unidad o posición que está destinado a proteger. Este fenómeno táctico entra en conflicto directo con principios fundamentales del despliegue de medios militares, tales como:

- **Gestión de la Firma Electromagnética:** La disciplina *EMCON* exige minimizar las emisiones para denegar información al adversario sobre la ubicación y entidad de las fuerzas propias. Un inhibidor continuo es una violación directa de esta disciplina.
- **Dispersión y Movilidad:** Mientras que las unidades ligeras buscan la dispersión para evitar ser objetivos rentables, un emisor activo fijo anula esta ventaja competitiva al fijar una posición estática en el orden de batalla electrónico del enemigo.
- **Negación de Inteligencia al Adversario:** La emisión activa facilita la adquisición de objetivos (*Target Acquisition*) por parte del adversario, permitiéndole mapear el despliegue defensor sin necesidad de sensores visuales, basándose únicamente en el espectro.

En resumen, el hándicap de la defensa activa es su propia señal. Esta realidad subraya la necesidad imperativa de evolucionar hacia sistemas semiactivos, que mantengan el silencio radioeléctrico mediante una detección pasiva y solo activen la respuesta de interferencia de manera selectiva y quirúrgica, maximizando así la supervivencia en entornos de alta letalidad [1, 12].

2.1.4 La Filosofía Pasivo-Activa como Enfoque de Supervivencia

Frente a las limitaciones de los sistemas *C-UAS* puramente activos, las doctrinas modernas de guerra electrónica y defensa aérea de corto alcance enfatizan la necesidad de arquitecturas con *LPI* y *LPD*. La filosofía pasivo-activa se alinea con estas directrices, buscando maximizar la supervivencia del sistema y de la unidad protegida mediante una reducción deliberada de la firma electromagnética y la activación quirúrgica de contramedidas. Esta arquitectura se estructura en torno a dos fases operativas interconectadas:

- **Fase de Detección Pasiva Inicial:** Basada en la observación y análisis del espectro electromagnético y, de forma complementaria, del dominio acústico., arquitectura que en el prototipo se materializa en el apartado 3.2 y en los bloques desarrollados posteriormente. Al no emitir ninguna señal, el sistema es virtualmente invisible para los sensores *ELINT* adversarios. Este enfoque permite monitorizar el entorno en "silencio radioeléctrico", captando emisiones de

baja potencia provenientes de los *UAS* incluso en entornos espectrales congestionados o con alta densidad de ruido (*clutter*).

- **Fase Activa de Interferencia Selectiva:** Solo tras una confirmación fehaciente de la amenaza, basada en criterios de persistencia y clasificación, se activan las contramedidas electrónicas. Esta intervención es limitada en tres dimensiones: en la dimensión temporal ya que la emisión dura el tiempo mínimo necesario para neutralizar el enlace; la dimensión espectral que se enfoca exclusivamente en las frecuencias detectadas (vía *look-through* o análisis previo, tal y como esquematiza la Figura 2-3); y la dimensión espacial potencialmente dirigida para evitar la radiación omnidireccional innecesaria. Esta estrategia reduce drásticamente la ventana de exposición, mitigando el riesgo de que el defensor sea geolocalizado mediante triangulación y minimizando las interferencias colaterales a sistemas legítimos.

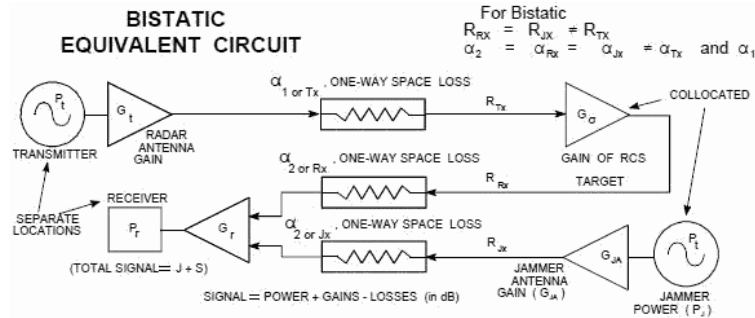


Figura 2-3 Diagrama de inhibidor con técnica de “look-through”.

La implementación de este enfoque introduce retos de cierta complejidad que este trabajo pretende abordar:

- **Sensibilidad y Procesado en Tiempo Real:** La captación de señales de *UAS*, a menudo débiles y con técnicas de salto de frecuencia (*Frequency Hopping*), exige receptores de alta sensibilidad y algoritmos avanzados de extracción de características.
- **Gestión de Falsas Alarmas:** La diferenciación entre señales de drones, interferencias ambientales y tráfico civil (*WiFi*, *Bluetooth*, radioaficionados) requiere criterios de decisión robustos para evitar activaciones accidentales del inhibidor.
- **Coordinación de Baja Latencia:** La transición entre la fase pasiva y la activa debe ser casi instantánea. Una latencia elevada permitiría que el *UAS* completara su misión (ej. envío de coordenadas o suelta de carga) antes de ser neutralizado.
- **Control de la Interferencia:** El inhibidor debe ser lo suficientemente potente para degradar el enlace del *UAS*, pero lo suficientemente controlado para no colapsar las comunicaciones propias de la unidad protegida.

El objetivo final no es solo la neutralización del *UAS*, sino la protección sostenida. Al priorizar la discreción y el análisis sobre la emisión constante, la arquitectura pasivo-semiactiva logra un equilibrio crítico entre capacidad defensiva y supervivencia, evitando que el sistema *C-UAS* se convierta en una vulnerabilidad explotable por el enemigo.

2.1.5 Tecnologías de Detección Pasiva de UAS

La piedra angular de cualquier sistema *C-UAS* pasivo-semiactivo es la capacidad de detectar una amenaza sin comprometer la propia posición. Esto se logra mediante el empleo de sensores que explotan las emisiones o características físicas inherentes a los *UAS*. Al no irradiar energía electromagnética, estos sistemas operan bajo el umbral de detección de los sensores *ELINT* adversarios, cumpliendo con el principio de supervivencia en entornos contenciosos. Las principales modalidades de detección pasiva se dividen según el dominio físico de la señal captada en: detección por radiofrecuencia, detección

acústica, detección electroóptica/infrarroja (*EO/IR*) y detección radar activa y pasiva [6, 8]. Cada una de estas modalidades ofrece ventajas únicas y presenta desafíos específicos en términos de procesamiento de señal y alcance. Esta complementariedad subraya la necesidad de un enfoque multisensorial para minimizar las tasas de falsas alarmas [7, 8] y maximizar la probabilidad de detección ante amenazas que empleen técnicas de silencio radioeléctrico o vuelo autónomo.

La inteligencia electrónica se ha consolidado como una capacidad crítica en los conflictos armados contemporáneos, dada la creciente y ubicua dependencia de los sistemas militares y, de manera prominente, de los *UAS*, al espectro radioeléctrico. Las plataformas modernas, especialmente las de bajo coste y *COTS*, dependen de enlaces de *C2* y sistemas de navegación por satélite para funciones de telemetría, estabilización y pilotaje [10, 13]. Estos enlaces operan mayoritariamente en las bandas *ISM* de 2,4 GHz y 5,8 GHz. La detección *RF* pasiva capitaliza estas emisiones para identificar y rastrear la amenaza sin revelar la posición del defensor, garantizando una discreción operativa vital; su aplicación experimental en este trabajo se presenta en el apartado 3.4.4.

El principio operativo reside en la interceptación y el análisis de las señales electromagnéticas mediante receptores *SDR*. La flexibilidad del *hardware SDR* permite el escaneo de amplios rangos de frecuencia y el procesamiento digital en tiempo real para extraer características únicas de las transmisiones [6, 13]. Las ventajas de la detección *RF* pasiva son sustanciales:

- **Baja Probabilidad de Intercepción/Detección:** Al operar de forma puramente receptiva, el sistema es invisible para los sensores de búsqueda del adversario [12].
- **Eficiencia en el Despliegue:** El uso de *hardware COTS* y *SDR* reduce drásticamente los costes de adquisición y facilita la integración en unidades pequeñas.
- **Capacidad de Clasificación e Identificación:** El análisis de patrones permite discriminar entre diferentes modelos de *UAS* mediante tres técnicas principales [14]:
 - **Patrones Espectrales:** Uso de momentos estadísticos (pendiente, asimetría o *skewness* y curtosis) procesados mediante *ANN*, para el reconocimiento de firmas *RF*.
 - **Análisis de Flujo de Datos:** Identificación basada en la longitud de los *frames* y la distribución de paquetes (huella digital *WiFi/FPV*), permitiendo identificar modelos específicos en menos de 20 segundos.
 - **Firmas Acopladas Movimiento-Señal:** Detección de las variaciones de fase o amplitud inducidas en la señal inalámbrica por las vibraciones físicas del chasis y motores del dron (sistema *Matthan*).

Sin embargo, a pesar de sus ventajas, la detección pasiva enfrenta obstáculos críticos en teatros de operaciones saturados:

- **Congestión Espectral y Clutter:** En las bandas *ISM*, las señales de *UAS* coexisten con redes *WiFi*, Bluetooth e IoT (Internet of things). La dificultad radica en extraer una Relación Señal a Ruido (*SNR*) útil en un entorno con alta densidad de señales y comportamientos dinámicos.
- **Exigencia de Procesamiento Avanzado de Señales:** La simple detección de energía es insuficiente para evitar falsas alarmas. Se requiere un análisis tiempo-frecuencia complejo y el estudio de protocolos de modulación específicos.
- **Geolocalización y Multilateración:** Para una respuesta táctica eficaz, no basta con detectar; es necesario localizar. Esto se logra mediante la Dirección de Llegada (*DOA*) o la multilateración (*TDOA*). Esta última requiere una sincronización temporal extremadamente precisa entre sensores distribuidos y una gestión avanzada de la propagación por trayectos múltiples (*multipath*), especialmente en entornos urbanos o con orografía compleja.

2.1.6 Variabilidad del Adversario y la Necesidad de Robustez

La eficacia de la detección *RF* pasiva se ve desafiada por las tácticas de evasión del adversario, diseñadas para reducir la detectabilidad y la vulnerabilidad de sus plataformas. Estas contramedidas incluyen el uso de técnicas de salto de frecuencia (*FHSS*), la gestión dinámica de la potencia de transmisión, el empleo de enlaces redundantes y la implementación de protocolos propietarios o cifrados.

Tales tácticas reducen la persistencia espectral de las emisiones, obligando a los sistemas *ELINT* a operar con ventanas de observación extremadamente cortas y a correlacionar eventos dispersos en el tiempo para mantener la trazabilidad del objetivo. Dado que los métodos basados en patrones de tráfico dependen críticamente del protocolo de telemetría, su eficacia decae ante protocolos desconocidos o encriptados. Para contrarrestar esta variabilidad, la investigación actual se centra en tres pilares:

- **Reconocimiento Multiprotocolo en Sistemas Embebidos:** Es imperativo desarrollar algoritmos capaces de identificar múltiples estándares de comunicación simultáneamente. Estos deben ser optimizados para su ejecución en dispositivos móviles embebidos (como la *Raspberry Pi*), donde los recursos computacionales son limitados, pero se requiere una alta estabilidad operativa.
- **Evolución del *Hardware SDR*:** A pesar de su flexibilidad, los *SDR* convencionales presentan desafíos en términos de peso, consumo energético y portabilidad. La tendencia se orienta hacia el diseño de dispositivos de análisis *RF* de bajo coste, ligeros y con un rendimiento de procesamiento (*FPGA/DSP*) optimizado para la detección de *UAS*, facilitando su integración en despliegues expedicionarios.
- **Inteligencia Artificial y Deep Learning:** El *DL* representa la solución más prometedora para mejorar la robustez frente a señales complejas. Con la capacidad de procesar volúmenes masivos de datos espectrales por segundo, el *DL* permite alta precisión por ejemplo en la clasificación de drones mediante sus huellas digitales en *RF*, adaptabilidad mediante técnicas de transfer learning para adaptar modelos maduros a nuevos escenarios o amenazas emergentes con un entrenamiento mínimo y eficiencia temporal máxima para la detección y clasificación, lo cual es compatible con los requisitos de baja latencia del sistema [7, 15].

2.2 Detección Acústica (*ACINT*)

La detección acústica, o *ACINT*, es una modalidad pasiva que complementa la detección *RF*. Es particularmente eficaz para neutralizar *UAS* que operan en silencio radioeléctrico o con firmas *RF* evasivas. Esta técnica aprovecha las perturbaciones sonoras distintivas generadas por la rotación de las hélices y el funcionamiento de los motores eléctricos.

2.2.1 Fundamentos y firmas sonoras

El principio operativo se basa en la captación y análisis de las componentes tonales y armónicas del *UAS*, cuya formulación dentro del sistema desarrollado se retoma en el apartado 3.3.2. La frecuencia fundamental f_0 producida por las hélices es un indicador crítico para la identificación y puede modelarse mediante la expresión:

$$f_0 = \frac{N \times RPM}{60} \quad (2 - 1)$$

donde N representa el número de palas por hélice y *RPM* la velocidad de rotación del motor. La intensidad y distribución espectral de esta firma dependen de la precisión mecánica y de los efectos aerodinámicos de la plataforma.

Entre las características de propagación cabe destacar la atenuación de la onda donde la presión sonora decae aproximadamente 6 dB cada vez que se duplica la distancia, la direccionalidad ya que el perfil acústico no es omnidireccional (los niveles de emisión suelen ser hasta 10 dB superiores a 45° respecto a la horizontal en comparación con la vertical directa) y el ancho de banda ya que aunque la energía predomina por debajo de los 2 kHz, ciertas componentes armónicas pueden extenderse hasta los 15 kHz.

Para la localización, se emplean *arrays* de micrófonos que permiten determinar la *DOA* mediante el análisis de las diferencias de fase y tiempo de llegada de la onda sonora a cada sensor [14, 16]. Mediante el análisis de las diferencias de fase en el sonido entre los micrófonos, es posible triangular la posición del *UAS*. La capacidad de reconocer y localizar *UAS* con precisión mediante enfoques acústicos ha avanzado, cumpliendo con los requisitos de precisión en la detección.

El uso de *Machine Learning* y *Deep Learning* ha permitido procesar señales acústicas incluso cuando la *SNR* es negativa (el ruido ambiental supera a la señal del dron). Las Redes Neuronales Convolucionales (*CNN*) son especialmente eficaces al tratar los espectrogramas de audio como imágenes, logrando clasificar modelos de *UAS* y distinguirlos de fuentes de ruido biológico o urbano con alta precisión [17].

2.2.2 Limitaciones y Sensibilidad Ambiental

A pesar de su bajo coste, la modalidad *ACINT* presenta restricciones intrínsecas que deben ser gestionadas en el diseño del sistema [18]:

- **Alcance Reducido de Detección:** Limitado típicamente a un radio de 150 metros debido a la rápida atenuación atmosférica del sonido.
- **Vulnerabilidad al "Clutter" Acústico:** El viento (crítico por encima de 5 m/s), la lluvia y el ruido de tráfico pueden enmascarar las firmas de los *UAS*.
- **Ego-ruido en plataformas móviles:** La integración en vehículos o drones defensores es compleja debido a la necesidad de algoritmos de cancelación de ruido para eliminar las vibraciones de la propia plataforma.
- **Tendencias de Diseño:** La evolución hacia hélices de baja sonoridad y motores más eficientes obliga a desarrollar técnicas de filtrado adaptativo más sofisticadas.
- **Costo Computacional:** Si bien los sensores acústicos son de bajo costo, los algoritmos avanzados de procesamiento de señal y *ML/DL* necesarios para la detección y clasificación precisas requieren una capacidad computacional considerable, especialmente para operar en tiempo real.

A pesar de estas limitaciones, la detección acústica sigue siendo una modalidad relevante en un enfoque multisensorial. En operación real, a menudo se utiliza como un sensor de detección temprana local o como un refuerzo para la fusión de datos, aportando una fuente adicional de información independiente del espectro radioeléctrico. La investigación continúa buscando formas de mejorar la fiabilidad de la detección mediante técnicas de filtrado adaptativo, análisis espectral acústico avanzado y clasificación basada en características tonales y armónicas [18, 19].

2.3 Detección Electroóptica/Infrarroja (EO/IR) Pasiva

La detección *EO/IR* constituye la modalidad de sensor visual del sistema *C-UAS*. Su función principal es captar imágenes o firmas térmicas de la amenaza sin emitir energía, manteniendo la integridad del silencio radioeléctrico. En arquitecturas pasivo-semiactivas, estos sistemas suelen actuar como sensores de confirmación, reduciendo la tasa de falsas alarmas generadas por otros subsistemas. A diferencia de los sensores de *RF* o acústicos, que detectan señales invisibles o audibles, los sistemas *EO/IR* se basan en el procesamiento digital de imágenes para realizar una identificación visual positiva

(*VID*) del objetivo. El Espectro Visible utiliza cámaras convencionales para segmentar el *UAS* del fondo y analizar su morfología. Es la herramienta más potente para distinguir modelos específicos cuando existe línea de visión (*LOS*) y buena iluminación. En el Espectro Infrarrojo (*IR*) las cámaras térmicas detectan el calor residual generado por los motores, las baterías y la fricción de las hélices. Esto permite la operación nocturna y facilita el contraste del dron contra cielos fríos. A pesar de su precisión, la eficacia de la detección visual está condicionada por factores externos críticos:

- **Dependencia Ambiental:** El rendimiento se degrada drásticamente ante fenómenos meteorológicos (niebla, lluvia intensa) o condiciones de baja visibilidad.
- **El Problema de las aves:** Distinguir entre un *micro-UAS* y un ave en vuelo es uno de los mayores retos algorítmicos debido a la similitud en tamaño y patrones de movimiento a larga distancia.
- **Carga Computacional:** La segmentación y clasificación mediante redes neuronales en tiempo real exigen una alta capacidad de procesamiento (*GPU/NPU*), lo que complica su integración en sistemas de bajo consumo (*SWaP*).

La evolución de la visión artificial ha introducido soluciones prometedoras para superar estas barreras:

- **Redes Neuronales Convolucionales (*CNN* y *Faster R-CNN*):** Modelos como *VGG-16* han demostrado un rendimiento excepcional en la detección de objetos pequeños, permitiendo incluso el entrenamiento con imágenes sintéticas para mejorar la robustez.
- **Cámaras de Eventos (*Event Cameras*):** A diferencia de las cámaras tradicionales, estos sensores capturan solo los cambios de brillo por píxel de forma asincrónica. Esto elimina el desenfoque por movimiento (*motion blur*) y permite identificar la frecuencia de rotación de las hélices, permitiendo diferenciar de forma inequívoca un dron de un pájaro.

A pesar de estos avances, el desafío persiste en cómo implementar algoritmos de reconocimiento que sean robustos, ajustables y precisos en múltiples y variables entornos [7, 13]. Se necesita una mayor solidez frente a variaciones rápidas del entorno y la mitigación de la distorsión de la imagen causada por el cambio climático. La movilidad de los *UAS* también plantea un reto, requiriendo que las imágenes se capturen y reconozcan en diferentes niveles de movilidad.

2.4 Radar Pasivo: Potencial y Desafíos

El radar pasivo, a diferencia de los sistemas convencionales, prescinde de un transmisor dedicado. En su lugar, explota las Señales de Oportunidad (*SOP*) ya presentes en el espectro radioeléctrico, como la televisión digital (*DVB-T*), la radio FM, la telefonía móvil o incluso redes Wi-Fi, para detectar y localizar objetivos. Esta característica lo convierte en una herramienta estratégica para arquitecturas *C-UAS* discretas, ya que el sistema defensor permanece en completo silencio electromagnético [8, 20].

2.4.1 Principios de Funcionamiento

El sistema opera analizando las variaciones en las señales *SOP* causadas por el reflejo de estas en un objeto en movimiento. El procesamiento se basa en la comparación de dos canales:

- **Canal de Referencia:** Captura la señal directa desde la fuente (ej. una torre de telefonía).
- **Canal de Vigilancia:** Capta el eco reflejado por el *UAS*.

La extracción de parámetros como la distancia y la velocidad se apoya en el efecto micro-Doppler, generado por los micromovimientos de las hélices y motores. Esta firma es crucial para la clasificación, aunque su visibilidad depende del material del dron (siendo las hélices de fibra de carbono más detectables que las de plástico). Dependiendo de su configuración, se clasifican en:

- **Radar Pasivo de Estación Única:** Analiza una única fuente para detectar la aparición del *UAS*.

- **Radar Pasivo Distribuido (Multiestático):** Utiliza múltiples fuentes o receptores para mejorar la cobertura y la precisión mediante el procesamiento de señales *OFDM* o *DVB-T*.

2.4.2 Ventajas y Limitaciones Críticas

Entre las ventajas del Radar Pasivo cabe citar la indetectabilidad ya que, al no emitir energía, es inmune a los ataques antirradiación y a la detección por sensores *ELINT*, la robustez meteorológica ya que a diferencia de los sistemas *EO/IR*, funciona bajo lluvia, niebla o en oscuridad total y el bajo coste de infraestructura ya que reutiliza emisores existentes, eliminando la necesidad de transmisores costosos y complejos.

Entre los principales desafíos y limitaciones del sistema de radar pasivo cabe mencionar la carga computacional extrema ya que extraer ecos débiles inmersos en el ruido ambiental requiere algoritmos de post-procesamiento masivo y aprendizaje automático para la clasificación, la baja sección radar (*RCS*) ya que los microdrones suelen tener una *RCS* inferior a 1 m^2 , lo que, sumado a sus bajas velocidades de vuelo, dificulta el procesamiento Doppler y la dependencia de terceros ya que la eficacia del sistema está supeditada a la disponibilidad y estabilidad de fuentes externas que el defensor no controla.

La integración de la detección por radar pasivo en un esquema de fusión de datos multisensor puede ayudar a mitigar sus limitaciones de identificación y robustecer la detección general. Por ejemplo, la combinación de radares y sensores de audio, donde el radar detecta objetos en movimiento y un array acústico los clasifica como *UAS*, puede mejorar significativamente el rendimiento.

Tipo	Definición	Ventajas	Contras
Imagen EO/IR	Detección basada en sistemas visuales que utilizan cámaras para capturar y analizar la presencia de drones, cubriendo el espectro visible e infrarrojo.	• Uso de algoritmos de inteligencia artificial y visión por computador. • Disponibilidad de cámaras de alta resolución. • Capacidad de seguimiento en tiempo real.	• Alcance limitado. • Dependencia de las condiciones meteorológicas. • Requiere línea de visión (LoS). • Problemas en condiciones de baja iluminación.
Acústico	Detección auditiva que emplea matrices de micrófonos para identificar los sonidos producidos por drones, cubriendo el espectro entre 20 Hz y 20 kHz [21].	• Detección pasiva. • No requiere línea de visión (LoS). • Bajo consumo energético.	• Sensible al ruido ambiental. • Alcance de detección muy reducido. • Dependencia del nivel de ruido generado por el dron.
Radar	Detección basada en el análisis de la sección radar equivalente (<i>RCS</i>) reflejada o en la firma micro-Doppler, utilizando sistemas radar que operan en rangos de frecuencia desde 3 MHz hasta 300 GHz.	• Gran alcance de detección. • Cobertura de 360°. • Operación en cualquier condición meteorológica.	• Requiere una <i>RCS</i> relativamente grande. • Posible confusión con otros objetos voladores como aves. • Requiere línea de visión. • Alto coste.
Radiofrecuencia	Monitorización del espectro radioeléctrico para identificar señales de comunicación específicas entre el dron y su controlador.	• Detección pasiva. • No requiere línea de visión. • Baja complejidad y fácil implementación. • Actualizaciones sencillas mediante arquitectura modular. • Posibilidad de decodificar señales de comunicación. • Potencial para localizar al piloto.	• Requiere una base de datos extensa de señales <i>RF</i> de drones o radiocontrol. • Posible confusión con otras comunicaciones <i>RF</i>, especialmente en entornos complejos. • Vulnerable a <i>hardware RF</i> modificado ilegalmente que supere las capacidades del receptor.

Tabla 2-1: Comparativa de tecnologías de detección.

2.5 Fusión Multisensorial y Algoritmos de Decisión

La complejidad de las amenazas *UAS*, caracterizada por la heterogeneidad de plataformas, perfiles de vuelo y firmas multimodales, hace que cualquier enfoque monosensor sea insuficiente para garantizar una protección robusta. La Figura 2-4 compara las principales características de los sensores disponibles, justificando la necesidad de combinarlos. La solución más eficaz reside en la fusión multisensorial, una integración sistemática de diversas fuentes de datos que permite generar un "reporte accionable" y una toma de decisiones informada para la activación de contramedidas, enfoque que en el prototipo se describirá en el apartado 3.2 [22, 23].

		Characteristics						
Detection Methods		Range	Position accuracy	Classification	Autonomous targets	Multiple targets	Low visibility conditions	Price
	Human surveillance	**	***	*****	✓	✗	✗	*****
	Passive Electro-optical/infrared	***	*****	*****	✓	✗	✗	*
	Acoustic	*	**	**	✓	✓	✓	***
	Active Radar	*****	*****	***	✓	✓	✓	**

Figura 2-4 Comparación de características de sensores.

El problema de los sistemas basados en un único sensor radica en su vulnerabilidad ante escenarios específicos y su degradación bajo condiciones ambientales variables. La fusión de datos no solo mejora la fiabilidad, sino que permite explotar las ventajas de un sensor para compensar las carencias de otro. En un despliegue táctico, esta sinergia se manifiesta en la validación cruzada ya que un radar o un sensor de *RF* puede realizar una detección temprana de largo alcance, mientras que la confirmación final para activar el Inhibidor Semiactivo proviene de un array acústico o una cámara térmica, minimizando drásticamente la tasa de falsas alarmas; en la conciencia situacional mejorada ya que la combinación de acústica y *RF* permite detectar drones incluso si vuelan en silencio radioeléctrico (gracias a la firma sonora) o si están fuera del alcance acústico (gracias a la *RF*); y en la persistencia temporal ya que el sistema puede mantener el seguimiento de un objetivo aunque este pase temporalmente por una zona de sombra para uno de los sensores (por ejemplo, un dron que vuela tras un edificio, perdiendo la señal visual pero manteniendo la acústica).

Este enfoque multidominio, aunque incrementa la complejidad del procesado y el esfuerzo computacional, es la única vía para cumplir con el ciclo detectar, identificar y actuar con las garantías de seguridad que requieren las unidades de infantería en entornos hostiles [22, 24].

2.5.1 Algoritmos de Fusión de Datos y Deep Learning

La fusión de datos, definida como el proceso de integrar múltiples fuentes de datos para producir información más consistente, precisa y útil, es fundamental para los sistemas *C-UAS*. En el contexto de la detección de *UAS*, los enfoques de fusión de datos se pueden clasificar en tres categorías principales:

- **Fusión de Datos de Múltiples Sensores (del mismo tipo o homogénea):** Se refiere a la combinación de datos de varios sensores del mismo tipo (ej., un array de sensores acústicos o múltiples antenas *RF*). El objetivo es mejorar el rango de detección, la precisión de localización (ej., mediante *TDOA* o *DOA*) y añadir funciones que un solo sensor no podría ofrecer, como la capacidad de determinar la dirección de llegada de una señal *RF* usando múltiples antenas omnidireccionales. Un ejemplo clásico es el array de sensores acústicos distribuidos para localizar *UAS* mediante diferencias de fase en el sonido.
- **Fusión de Datos de Múltiples Tipos de Sensores (heterogéneos):** Combina información de diferentes tipos de sensores (ej., acústicos, ópticos, radares) para mitigar las desventajas de un sensor único en entornos variables y para satisfacer múltiples requisitos de rango. Este enfoque es crucial cuando la mejora en la cantidad de sensores de un solo tipo no puede compensar las

limitaciones inherentes a su naturaleza. Por ejemplo, la combinación de tecnologías de detección de largo y corto alcance, donde los receptores *RF* pasivos detectan señales de telemetría de *UAS*, mientras que los sensores de video y acústicos se utilizan para aumentar la precisión de detección en el campo cercano. La implementación de un array acústico de 120 nodos, cámaras ópticas de alta resolución y radar *MIMO* para detección remota ha demostrado un rendimiento sobresaliente en áreas restringidas, ilustrando el flujo de fusión representado en la Figura 2-5.

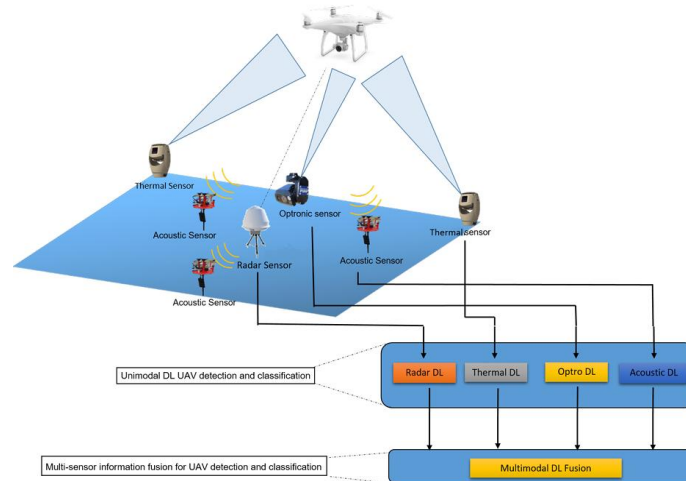


Figura 2-5 Fusión multisensor para adquisición de blanco

- **Fusión de Múltiples Algoritmos de Detección (Multimodal):** Implica la combinación de algoritmos de procesamiento de señales o de *ML* que pueden activarse dinámicamente según el estado de la detección o el escenario. Estos algoritmos pueden ajustar su precisión para satisfacer los requisitos de detección una vez que se detectan señales anómalas. Por ejemplo, en, se utilizaron enfoques no supervisados para extraer características de señales acústicas en diversos escenarios (aves, aviones, tormentas, lluvia, viento y *UAS*), activando máquinas de vectores de Soporte (*SVM*) y k-vecinos más cercanos (*KNN*) para detectar drones aficionados en áreas restringidas. Esta combinación mejora la eficiencia, la precisión y reduce la sobrecarga del sistema, adaptándose a las necesidades del *C-UAS*.

El *DL* ha transformado la fusión de datos al automatizar la ingeniería de características (*feature engineering*), permitiendo al sistema descubrir patrones abstractos en grandes volúmenes de datos heterogéneos. En el contexto *C-UAS*:

- **Automatización de la Ingeniería de Características:** El *DL* automatiza el proceso de ingeniería de características, que tradicionalmente requiere mucho esfuerzo en el machine learning convencional.
- **Procesamiento de Espectrogramas Doppler:** Las *CNN* se utilizan para aprender características distintivas en distribuciones 2D de espectrogramas Doppler con alta precisión de clasificación, lo cual es crucial para identificar *UAS* basándose en el efecto micro-Doppler de sus hélices.
- **Análisis de Funciones de Correlación Espectral (*SCF*):** Las *DBN* se aplican para caracterizar las características contenidas en patrones de *SCF* generados, permitiendo la detección e identificación automática de diferentes tipos de *UAS* de manera efectiva.
- **Modelado Consciente del Movimiento:** Para la predicción de trayectorias de *UAS*, se han desarrollado marcos de aprendizaje multimodal supervisado que integran modelado consciente del movimiento, alineación de proyección de trayectoria y detección basada en Vision-Mamba. Estos sistemas pueden superar a las líneas de base supervisadas de solo imagen y audiovisuales en la predicción de trayectorias a largo plazo, incluso sin etiquetas 3D manuales. Esto es crucial

para permitir tiempos de respuesta adecuados para diversas contramedidas, desde láseres casi instantáneos hasta drones interceptores o redes que requieren varios segundos de anticipación.

- **Transfer Learning:** La capacidad de "transfer learning" permite implementar modelos *DL* maduros y de alto rendimiento en múltiples escenarios con pocos episodios de entrenamiento, lo que mejora la adaptabilidad y eficiencia del sistema *C-UAS*.
- **Datos de Eventos para Detección:** Los sensores de visión dinámicos o "cámaras de eventos", al registrar solo los cambios de brillo a nivel de píxel, son inmunes al desenfoque por movimiento y ofrecen un alto rango dinámico. La integración de estos datos con redes neuronales recurrentes para el aprendizaje profundo (*RNN*) de patrones temporales puede ser altamente efectiva para la detección y clasificación de drones, especialmente en entornos dinámicos y con baja latencia.

A pesar de su potencial, la fusión de datos enfrenta desafíos técnicos de primer orden: la gestión de la inconsistencia entre formatos de datos de distintos fabricantes, la sincronización temporal precisa y el equilibrado de pesos en la lógica de decisión final para evitar que un sensor degradado (ej. una cámara en la niebla) invalide la detección correcta de otro (ej. un sensor acústico).

2.6 Lógica de Decisión Escalonada y Criterios de Activación

La efectividad de un sistema *C-UAS* pasivo-semiactivo reside en su capacidad para discernir entre tráfico legítimo y amenazas reales mediante una lógica de decisión escalonada. Este enfoque jerárquico es imperativo para garantizar que las contramedidas activas se desplieguen de forma quirúrgica, maximizando la supervivencia del defensor y minimizando daños colaterales en el espectro.

El proceso se estructura como una progresión de estados donde el nivel de certeza aumenta en cada etapa. En entornos con alta congestión espectral, la implementación de criterios de persistencia temporal es vital para filtrar detecciones espúreas y evitar respuestas precipitadas.

El sistema de toma de decisiones no opera de forma aislada, sino que debe integrarse con la infraestructura de gestión del espacio aéreo (*ATC*) y los sistemas de gestión de tráfico de *UAS* (*UTM*). Los componentes fundamentales de esta lógica incluyen:

- **Clarificación y Protocolos de Identificación:** Ante una detección, el sistema debe clasificar el *UAS* como cooperativo o no cooperativo mediante un "modelo post-detección":
 - **Bases de Datos de Identidad (ID-DB) y Autorización (AUTH-DB):** Consulta de registros de identidad y misiones autorizadas (quién, cuándo y dónde tiene permiso para volar).
 - **Identificación Remota (Remote ID):** Recepción y validación de la firma digital obligatoria del *UAS* contra las bases de datos de la autoridad aeronáutica.
 - **Máquina de Estados Finitos (FSM):** Modelado del proceso de decisión desde la "Vigilancia" hasta la "Misión Autorizada" o "Amenaza Confirmada". Las transiciones se disparan tras cada verificación técnica.
- **Protocolos de Clarificación:** En casos de irregularidades (ID expirado, violación de zona o falta de telemetría), se activan protocolos específicos de comunicación con el operador o el proveedor de servicios *UAS* (*USS*). Estos protocolos permiten a la autoridad decidir entre tres cursos de acción: tolerar el incidente, ordenar la interrupción de la misión o autorizar la interdicción inmediata.
- **Dinámica de Respuesta y Latencia Táctica:** Un parámetro crítico en la ingeniería del sistema es la latencia acumulada. Para que la respuesta sea eficaz contra la cinemática de un *UAS* ágil, el tiempo transcurrido desde la detección hasta la mitigación debe ser mínimo.

- **Evaluación de Riesgo y Activación Selectiva:** La activación del inhibidor solo ocurre cuando el *UAS* es suficientemente confirmado y su comportamiento (trayectoria hacia zona sensible o vuelo errático) eleva el nivel de riesgo a un umbral crítico. Esta activación es limitada en tiempo y frecuencia, alineándose con los principios de supervivencia y discreción electromagnética que rigen este trabajo.

La integración de estas capacidades de decisión en un sistema unificado capaz de detectar y mitigar *UAS* es esencial para su integración segura en el sistema de espacio aéreo.

2.7 Estrategias de Interdicción y Mitigación Semiactiva

Una vez consolidada la fase de detección y clasificación mediante el análisis de fuentes pasivas, el sistema *C-UAS* debe transicionar hacia una respuesta ejecutiva capaz de neutralizar la amenaza con la máxima eficacia y el mínimo impacto colateral. Esta sección detalla el marco operativo de las Contramedidas Electrónicas (*ECM*) y la explotación de vulnerabilidades, fundamentándose en una filosofía de intervención semiactiva. A diferencia de los sistemas de inhibición convencionales, este enfoque prioriza la selectividad temporal y frecuencial bajo criterios de *EMCON*, gestionando el compromiso técnico entre la potencia de interdicción y la supervivencia del propio sistema defensor. A continuación, se analizan las modalidades de interferencia de *RF* y *GNSS*, los protocolos de inyección de fallos y la lógica de decisión que rige la transición entre la recuperación controlada del *UAS* y su inhabilitación definitiva.

2.7.1 Tecnologías de Contramedidas Electrónicas (*ECM*) Selectivas

Una vez que la amenaza ha sido detectada y clasificada mediante la lógica de decisión, el sistema activa el subsistema de mitigación. La clave de un diseño semiactivo es la selectividad: la capacidad de intervenir únicamente sobre el enlace de la amenaza, minimizando el consumo energético y la firma electromagnética del defensor. Este enfoque garantiza un bajo coste por enfrentamiento y reduce drásticamente el impacto colateral en el espectro. Las modalidades de contramedidas electrónicas (*ECM*) se dividen en tres categorías principales según el vector de ataque (véase Figura 2-6):

Type	Optical	Acoustic	Radio	Radar
Sensor	• EO/IR CAM	• Acoustic/Ultrasonic Sensors	• Spectrometer • Frequency Scanner	• SAR, Scanning Radar (X-band, C-band)
Method	• Taking picture and auto-recognition 	• Recognition engine /propeller noise 	• Control signal scan and recognition 	• Radar scan 
cases	• Silent Strike (Boeing) • Counter-UAV System (Airbus)	• Drone Tracker (Dedrone, US)	• Drone Tracker (Dedrone, US) • Falcon Shield (SELEX-ES, Italy) • AUDS (Blighter, UK)	• ATHENA(LM, US) • HEL Effector (Rheinmetall, DE) • Drone Dome (Rafael, Israel)
Pros.	• Well detection and identification in LOS	• Well detect and identify in NLOS	• Long range detection and tracking/controls	• Long range detection and tracking/controls
Cons	• Short scan range • Non-operation in fog and rainy condition	• Required noise characteristic DB • Easy to jamming	• Weakness for secured signal • Unavailable to detect scheduled navigation system	• High cost • Impossible to classify

Figura 2-6 Clasificación de técnicas de neutralización.

2.7.2 Inhibición de Radiofrecuencia (RF Jamming)

El *jamming* de radiofrecuencia (RF) consiste en la emisión de señales de ruido intencionadas para interferir, degradar o negar la funcionalidad de los enlaces de comunicación y navegación del receptor del UAS o de la estación de control terrestre [25]. Los UAS dependen críticamente de enlaces de mando y control (C2) para recibir órdenes de su piloto remoto y de sistemas de navegación por satélite (GNSS, como el GPS) para su posicionamiento y estabilización. Al interferir estas señales, se puede interrumpir el control del operador, desorientar al UAS, forzarlo a regresar al punto de origen (*Return to Home*), aterrizar en una zona segura o incluso provocar su caída.

Los radios definidos por *software* (SDR) juegan un papel fundamental en la implementación del *jamming*, permitiendo interceptar las señales del control remoto del UAS, reconocer su protocolo de comunicación y generar comandos para controlar el UAS o emitir señales de interferencia específicas [26]. Un sistema de drones autónomos puede utilizar un SDR para alternar entre transmisiones de *jamming* y funcionalidades de barrido de espectro para lograr la interrupción del GPS deseada y la auto localización del dron perseguidor. La versatilidad de los dispositivos SDR permite implementar diversas técnicas de inhibición según el objetivo [8, 15]:

- **Jamming de Enlace C2:** Corta la comunicación de mando y control, forzando al UAS a ejecutar protocolos de emergencia (aterrizaje preventivo o retorno al RTH).
- **Jamming de Telemetría/Vídeo:** Degrada el flujo de datos e imágenes hacia el operador, cegando la capacidad de pilotaje FPV o ISR. Por ejemplo. Emitiendo una señal de tipo CHIRP lineal que barre una banda de frecuencia más amplia (por ejemplo, la banda ISM de 2,4 GHz) para interrumpir comunicaciones en múltiples canales.
- **Jamming Consciente del Protocolo (Protocol-Aware):** Es la técnica más eficiente, ya que imita o interfiere la estructura específica de protocolos como FASST o ACCST (*Advanced Continuous Channel Shifting Technolog*), logrando la neutralización con una fracción de la potencia requerida por el *jamming* de barrido.

El uso de ECM presenta beneficios estratégicos frente a métodos cinéticos (redes o proyectiles) tales como:

- **Neutralización Amigable y de Daño Cero:** Permite desalojar al intruso sin destrucción física, ideal para entornos civiles o zonas sensibles.
- **Escalabilidad:** Los sistemas basados en SDR pueden mantenerse operativos durante periodos prolongados y adaptarse a nuevas frecuencias mediante cambios en el *software*.
- **Cooperación Multidrón:** Existe la posibilidad de coordinar una red de drones defensores para concentrar la potencia de inhibición de forma colaborativa.

A pesar de su eficacia, la implementación de un inhibidor introduce ciertos retos técnicos o desafíos dentro de la arquitectura del sistema tales como:

- **Gestión del EMCOM y Energía:** El *jamming* convencional es omnidireccional y consume recursos críticos. Tu diseño debe priorizar el *Jamming* Reactivo, que solo radia energía tras la confirmación de la amenaza por el subsistema pasivo.
- **Auto-interferencia (Ego-jamming):** Un desafío crítico es que la interferencia destinada al intruso puede degradar el propio GPS del sistema defensor. Para mitigar esto, se desarrollan sistemas de Posicionamiento Relativo (RPS) basados en sensores inerciales (IMU) y visión artificial, permitiendo que el defensor navegue incluso bajo sus propios ataques de *jamming*.
- **Latencia del Efecto:** El dron hostil requiere un tiempo de exposición al ruido antes de que su lógica de control falle. Esto subraya la importancia de una detección temprana.

- **Impacto en el Agente Perseguidor:** En los experimentos de *jamming* basados en *SDR*, se ha observado que la reducción del número de satélites debido a la interferencia también afecta al propio agente perseguidor si este utiliza receptores *GPS* con antenas omnidireccionales. Esto crea una disyuntiva entre el rendimiento del *jamming* y la precisión del posicionamiento del agente perseguidor, destacando la necesidad de sistemas de posicionamiento relativo para el dron defensor. Para mitigar el impacto en el propio dron perseguidor, se desarrollan sistemas autónomos con capacidades de *jamming* y posicionamiento relativo. Estos sistemas utilizan un *SDR* para alternar entre el *jamming* y el barrido de espectro para la auto-localización. En experimentos de campo, se ha demostrado que el *jamming* de un dron *DJI Mavic* (que utiliza solo *GPS*) puede hacer que su trayectoria se desvíe significativamente de la trayectoria real, especialmente con mayor potencia de transmisión. El documento muestra cómo el *GPS* de un dron es afectado por el *jamming* en diversas distancias y altitudes. A medida que la potencia de transmisión aumenta, se logra un mayor rendimiento de *jamming*, reduciendo el número de satélites disponibles para el dron infractor. El sistema propuesto en integra detección y seguimiento basado en visión, información de *SOP* y unidades de medición inercial (*IMU*) para posicionamiento relativo, y un método de *jamming* para secuestrar drones. Este sistema puede cambiar eficientemente entre un módulo de navegación (utilizando una trayectoria relativa) y un módulo de *jamming* para interrumpir las acciones del dron intruso y permitir que el agente perseguidor navegue incluso si sus datos *GPS* no están disponibles o no son fiables. El documento ilustra cómo el número de satélites disponibles para el *UAS* atacante disminuye a medida que aumentan los ataques de *jamming*, lo que impide que el *UAS* atacante recupere su precisión de localización. Los experimentos han mostrado que el sistema *RPS-JS* (*Relative Positioning System-Jamming System*) logra un posicionamiento relativo preciso incluso durante ataques de *jamming* prolongados, con un error absoluto medio (*MAE*) significativamente menor en comparación con el *GPS* en escenarios de *jamming* [27].

2.7.3 Interferencia y Engaño de Navegación (*GNSS Spoofing/Jamming*)

Afecta a la capacidad del *UAS* para conocer su posición global mediante satélites (*GPS*, *GLONASS*, *Galileo*). Podemos clasificar la interferencia como:

- ***GNSS Jamming*:** Bloquea la recepción de señales satelitales, provocando que el *UAS* pierda su estabilidad posicional o su capacidad de navegación autónoma por *waypoints* [28, 29].
- ***GNSS Spoofing*:** Técnica más avanzada que consiste en emitir señales falsas pero coherentes que "engañan" al receptor del *UAS*, haciéndole creer que está en una ubicación distinta. Esto permite desviar al dron de su ruta o forzar su descenso en una zona segura controlada por el defensor. Es decir, el *UAS*, al procesar estas señales falsas, calcula una posición, velocidad o tiempo erróneos, lo que puede tener varias consecuencias:
 - **Desvío de Trayectoria:** El *UAS* puede ser guiado fuera de su curso previsto o desviado hacia un área controlada por el defensor.
 - **Aterrizaje Forzado:** Se puede inducir al *UAS* a realizar un aterrizaje en una ubicación específica o segura.
 - **Secuestro de Navegación:** En casos avanzados, el *spoofing* puede permitir al atacante tomar el control de la navegación del dron, dirigiéndolo a voluntad.

2.7.4 Explotación de Vulnerabilidades y Protocolos

Los *UAS* son sistemas complejos que dependen de múltiples tecnologías y enlaces, lo que los hace susceptibles a diversas vulnerabilidades explotables. Las tres áreas principales de vulnerabilidad son el *GPS*, los sensores de control y el protocolo de comunicación. A diferencia del *jamming* convencional (capa física), estas técnicas actúan sobre la capa de enlace y aplicación. Las áreas críticas de explotación se dividen en tres dominios:

- **Manipulación de Sensores y Fusión de Datos:** Los *UAS* utilizan algoritmos de fusión de sensores (frecuentemente basados en Filtros de Kalman) para estimar su estado y posición. La inyección de datos falsos (*False Data Injection*) permite desestabilizar la aeronave:
 - **Ataques al Barómetro:** La inyección de lecturas erróneas a través de filtros de paso bajo de primer orden puede degradar la precisión de la altitud, forzando al dron a colisionar o a elevarse fuera de control.
 - **Inyección en la IMU/GPS:** Modificar las funciones de cálculo de las mediciones permite engañar al autopiloto sobre su orientación o posición real, invalidando la respuesta del sistema de control de vuelo.
- **Vulnerabilidades en Protocolos de Comunicación:** Los protocolos como *MAVLink*, *WiFi* o enlaces celulares presentan vulnerabilidades que permiten ataques de precisión sin necesidad de saturar el espectro. La clasificación de estas técnicas se recoge en la Figura 2-7:
 - **Ataques *Man-in-the-Middle* (MitM):** Interceptación y modificación de comandos de control entre la *GCS* y el *UAS*, permitiendo la inyección de comandos maliciosos como el apagado de motores o cambio de misión.
 - **Secuestro de Enlace (*Skyjacking*):** Explotación de fallos en el cifrado o autenticación para tomar el control total del piloto automático.

Attack	Type	Threat Target	Level
Dispatch System Attack	Active	Confidentiality, Integrity, Availability, Privacy	High – Requires installation of malware or trojans designed for the UAV.
ADS-B Attack	Active	Confidentiality, Integrity, Privacy	Medium – Used commercially but requires knowledge of ADS-B transmission protocols.
TCAS Induced Collision	Active	Integrity, Availability	High – Requires another attack (malware or misguidance) to enable collision to occur.
TCAS Attack	Active	Availability	High – Attacker must be familiar with the equipment (transmit TCAS messages) and protocols.
Eavesdropping	Passive	Confidentiality, Privacy	Low – Can be done using receiver such as SDR. Easier if communication channels are not encrypted.
Man-in-the-Middle Attack	Passive	Confidentiality, Integrity, Availability, Privacy	High – Attacker must insert a device between UAV and ground stations.
Jamming	Active	Availability	Low-Med – Can be done by transmitting high powered signals at set frequencies. More difficult if sophisticated methods are used.
Wi-Fi Attack	Active	Confidentiality, Availability, Privacy	Med – Requires knowledge of the Wi-Fi protocol and a transmitter.
Exploitation of Recorded Video	Active	Confidentiality, Integrity, Privacy	High – Requires the attacker to install malware on the UAV and relay false videos to the kernel.
Denial of Service	Active	Availability	Med – Attacker can spam UAVs with useless packets. Requires a transmitter and other hardware.
GPS Spoofing	Active	Integrity, Availability	Low-Med – Attacker must transmit GPS signals. Such devices are available in commercial markets.

Figura 2-7 Clasificación de ciberataques sobre *UAS*.

- **Protocol-Aware Spoofing:** El uso de *SDR* permite reconocer el protocolo, descifrar paquetes en tiempo real y modificar la configuración de vuelo para forzar un retorno al punto de origen controlado por el defensor.

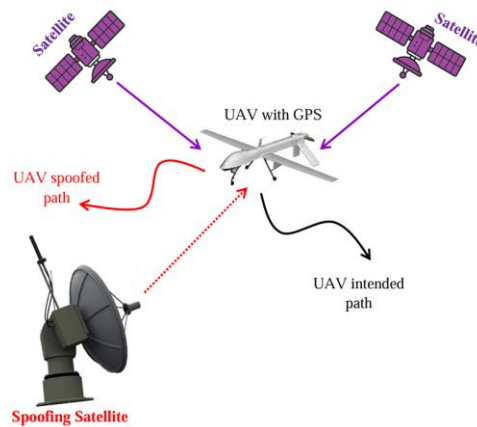


Figura 2-8 Vulnerabilidades de ataque de *spoofing GPS* sobre *UAS*.

- **Ataques de Denegación de Servicio (DoS):** La evolución de los drones ha llevado a que tengan sus propios sistemas operativos, lo que brinda a los defensores una oportunidad de explotar las vulnerabilidades. La integración de sistemas operativos embebidos en estos drones modernos amplía la superficie de ataque:
 - **Explotación del OS:** Al igual que en un sistema informático tradicional, las vulnerabilidades en el *kernel* o servicios del dron pueden ser explotadas para obtener privilegios de administración.
 - **DoS de Sensores:** Ataques probabilísticos que saturan un subconjunto de sensores específicos, forzando al sistema a entrar en modos de fallo o inhabilitando su capacidad de navegación autónoma.

La explotación de estas vulnerabilidades representa una solución de baja huella y bajo daño colateral. Al requerir una potencia de emisión mínima y actuar de forma quirúrgica sobre la lógica del *UAS*, se alinea perfectamente con la filosofía pasivo-semiactiva, maximizando la supervivencia del sistema defensor y minimizando la interferencia en servicios legítimos cercanos.

2.7.5 Metodología de Implementación Limitada en Tiempo y Frecuencia

La fase de respuesta en una arquitectura *C-UAS* pasivo-semiactiva se rige por una restricción deliberada de las emisiones. A diferencia de los sistemas activos convencionales, que operan de forma persistente, este enfoque emplea ráfagas de interferencia quirúrgicas. Esta estrategia es una respuesta directa a la necesidad de supervivencia en el campo de batalla moderno, donde cualquier emisión continua es geolocalizada y batida en cuestión de segundos.

2.7.6 Dimensiones de la Limitación Operativa

El diseño del sistema busca optimizar el uso del espectro mediante dos vectores de control:

- **Control Temporal (Duty Cycle):** Las contramedidas (*jamming* o *spoofing*) solo se activan tras la confirmación de la amenaza por los sensores pasivos. Al reducir la "ventana de exposición" al mínimo necesario para neutralizar el enlace, el sistema cumple con las directrices de *EMCON*, negando al adversario la oportunidad de realizar una triangulación precisa de la posición del defensor.
- **Selectividad Espectral (Band-Specific):** En lugar de una emisión omnidireccional de banda ancha (*barrage jamming*), el sistema enfoca la energía únicamente en las sub-bandas de

frecuencia detectadas (ej. canales específicos en 2,4 GHz). Esto maximiza la Densidad Espectral de Potencia sobre el objetivo y minimiza la probabilidad de causar interferencias a sistemas legítimos o aliados.

2.7.7 Beneficios Estratégicos y Técnicos

El diseño busca optimizar los beneficios estratégicos y técnicos basados en:

- **Reducción del Costo por Enfrentamiento:** Al ser una contramedida dirigida, se requiere una fracción de la potencia de un sistema activo tradicional, permitiendo el uso de *hardware* más ligero y eficiente (bajo *SWaP*) como el propuesto en este trabajo basado en *SDR* y *Raspberry Pi*.
- **Minimización del Daño Colateral:** Esencial para operar en entornos urbanos o espacios aéreos civiles congestionados, donde el bloqueo total de las bandas *ISM* (*WiFi*, *Bluetooth*) sería inaceptable por sus repercusiones económicas y de seguridad.
- **Gestión de la Autolocalización:** Al no saturar el espectro de forma continua, el sistema permite que sus propios sensores pasivos sigan monitorizando el entorno en los intervalos de silencio (*look-through capability*), manteniendo la conciencia situacional durante el combate electrónico.

2.7.8 Gestión Táctica y Eficacia Operacional

La implementación de una respuesta limitada en tiempo y frecuencia introduce desafíos críticos que el sistema debe resolver para ser tácticamente viable. La efectividad de esta estrategia no depende solo de la potencia de emisión, sino de la precisión y la sincronización del ciclo de interdicción.

2.7.9 Precisión y Latencia en la Cadena de Control

La eficacia de una activación limitada está supeditada a una detección y localización extremadamente precisas [1]. Cualquier error en la estimación de la trayectoria del *UAS* resulta en una contramedida ineficaz o en una exposición electromagnética prolongada e innecesaria del defensor [1].

- **Algoritmos en Tiempo Real:** Los motores de decisión deben procesar la fusión multisensorial y determinar el instante óptimo de activación con una latencia mínima.
- **Impacto de la Clarificación:** Se estima que el tiempo dedicado a verificar la identidad de la amenaza puede representar la mayor parte del retraso total del sistema, lo que exige procesos de validación altamente optimizados para no perder la ventana de oportunidad contra *UAS* ágiles.

2.7.10 El Dilema del Umbral de Alternancia

En escenarios donde el sistema defensor (o un dron perseguidor) utiliza receptores *GPS*, sus propias emisiones de *jamming* pueden degradar su capacidad de autolocalización. La solución técnica reside en un mecanismo de alternancia basado en un umbral de tiempo o error (T_d):

- **Prioridad de Localización:** Un T_d elevada pausa el *jamming* con más frecuencia para permitir que el Sistema de Posicionamiento Relativo (*RPS*) corrija errores, garantizando que el defensor no pierda su propia ruta [17].
- **Prioridad de Interdicción:** Un T_d bajo minimiza las pausas, maximizando la presión sobre el *UAS* hostil a riesgo de degradar la navegación propia.

2.7.11 Modos de Neutralización: Recuperación vs. Destrucción

Dependiendo del contexto operativo y de la tecnología empleada, el sistema puede buscar dos objetivos distintos:

- **Captura y Recuperación:** Mediante técnicas de Hacking (explotación de protocolos) o *jamming* C2 dirigido, es posible forzar al *UAS* a aterrizar de forma intacta para su posterior análisis forense. Este método es robusto y minimiza riesgos en zonas civiles.
- **Inhabilitación y Caída:** Utilizando métodos más agresivos como el *jamming* de *GNSS*, la inyección de fallos en sensores o el *EMP* direccional, se busca colapsar los circuitos de control o los algoritmos de estabilización para provocar la caída inmediata de la aeronave.

2.7.12 Dinámica de Decisión y Latencia Táctica

La eficacia de la activación limitada depende de una detección y localización extremadamente precisas. Los errores en la estimación de la trayectoria podrían resultar en una activación ineficaz o en una exposición electromagnética innecesaria.

- **Algoritmos de Decisión:** Deben procesar la información multisensorial en tiempo real para determinar el momento y la duración óptimos de la interdicción.
- **Tiempo de Clarificación:** Estudios de simulación demuestran que este proceso es el que más contribuye al retraso total del sistema; por tanto, la latencia debe minimizarse para ser efectiva contra *UAS* ágiles.

3 DESARROLLO DEL TFG

El desarrollo del sistema se ha abordado desde una perspectiva de ingeniería de sistemas, estructurando la solución en una arquitectura modular orientada a la detección, localización y neutralización de sistemas aéreos no tripulados en entornos tácticos. Esta aproximación permite desacoplar funcionalmente los distintos procesos involucrados, facilitando tanto la evolución del sistema como su adaptación a distintos escenarios operativos. El contexto doctrinal que enmarca esta arquitectura queda recogido en la Figura 3-1.

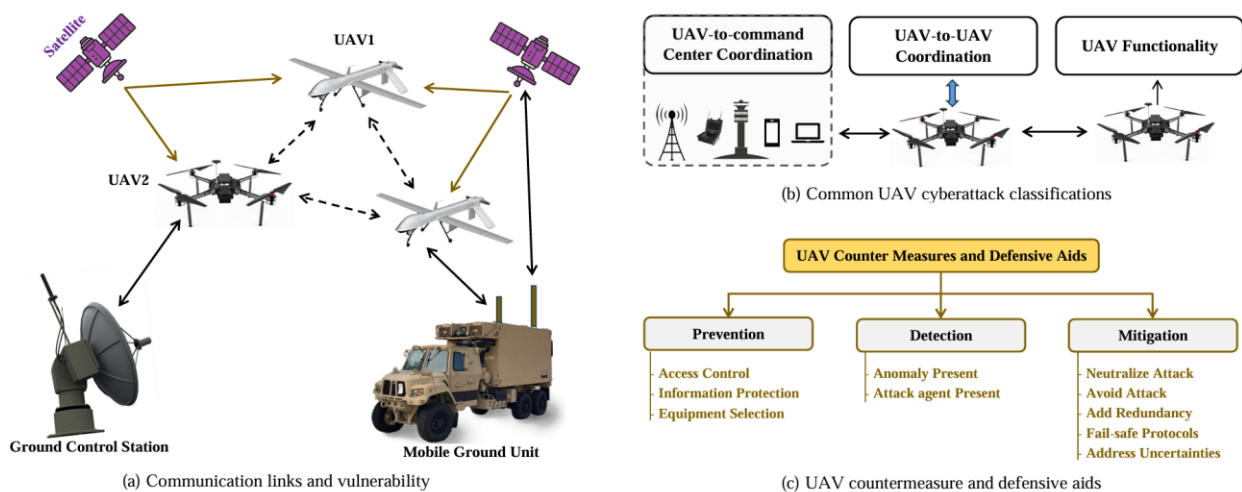


Figura 3-1 Taxonomía de la guerra.

La arquitectura propuesta se organiza en tres subsistemas principales: adquisición de señal, procesamiento y análisis, y actuación sobre la amenaza. El subsistema de adquisición integra sensores acústicos basados en matrices de micrófonos *MEMS* y receptores de radiofrecuencia, permitiendo la captación simultánea de información en el dominio acústico y electromagnético. Esta dualidad responde a la necesidad de aumentar la probabilidad de detección mediante la combinación de firmas físicas complementarias.

El subsistema de procesamiento constituye el núcleo del sistema, encargándose de la extracción de características relevantes a partir de las señales captadas. En el caso acústico, se emplean técnicas de análisis espectral basadas en transformadas de Fourier para la generación de espectrogramas y la estimación de la energía en bandas de frecuencia características asociadas al funcionamiento de rotores de *UAS*. Sobre estas magnitudes se implementa un mecanismo de umbral adaptativo, diseñado para

ajustar dinámicamente la sensibilidad del sistema en función del nivel de ruido ambiental, evitando tanto falsas alarmas como pérdidas de detección.

De forma complementaria, se implementa un módulo de estimación de dirección de llegada (*DOA*) basado en técnicas de *beamforming* y algoritmos de estimación espacial como *MUSIC*. Este módulo permite transformar la información multicanal del array de micrófonos en una estimación angular del origen de la señal, proporcionando una capacidad de localización direccional aproximada de la amenaza.

En paralelo, el subsistema de radiofrecuencia realiza la monitorización del espectro electromagnético en las bandas de operación habituales de los *UAS* comerciales, permitiendo identificar la presencia de enlaces de control y transmisión de vídeo. Esta información se integra con la detección acústica para reforzar la fiabilidad del sistema y reducir la ambigüedad en entornos complejos.

Finalmente, el subsistema de actuación se basa en el uso de radio definida por *software* para la generación de señales de interferencia dirigidas hacia la fuente emisora. La activación de este subsistema se realiza de forma condicionada a la detección previa de la amenaza, configurando una arquitectura semiactiva que minimiza la emisión innecesaria y reduce la exposición electromagnética del sistema.

El conjunto de estos subsistemas define un flujo de operación secuencial en el que la detección pasiva inicial permite activar mecanismo de localización y, posteriormente, de neutralización, configurando un sistema *C-UAS* integrado de bajo coste con capacidad de adaptación a diferentes entornos operativos.

3.1 Medios y Disposición empleados

3.1.1 Características de los Medios

El sistema experimental desarrollado en este trabajo se apoya en cuatro elementos *hardware* principales: el transceptor *SDR ADALM-Pluto*, el receptor de radiofrecuencia *TinySA*, las antenas direccionales TP-Link TL-ANT2409A y el array de micrófonos *MA-USB8*.

El *ADALM-Pluto* (*PlutoSDR*) es un transceptor de radio definida por *software* desarrollado por Analog Devices, basado en el chip AD9363, que integra tanto cadena de recepción como de transmisión en un único dispositivo compacto. Opera en un rango de frecuencias comprendido entre 325 MHz y 3,8 GHz, con un ancho de banda instantáneo de hasta 20 MHz, lo que lo hace idóneo para el trabajo en las bandas *ISM* de 2,4 GHz y 5,8 GHz empleadas por los *UAS* comerciales. Su interfaz *USB* permite la integración directa con entornos de desarrollo como GNU Radio, posibilitando la síntesis y recepción de señales en tiempo real desde una plataforma de bajo coste y reducidas dimensiones. En este proyecto, el *ADALM-Pluto* desempeña un papel dual: actúa como receptor en los bloques de detección *RF* y radiogoniometría, y como transmisor en el bloque de inhibición, generando las señales de barrido *CHIRP* que constituyen la contramedida electromagnética.

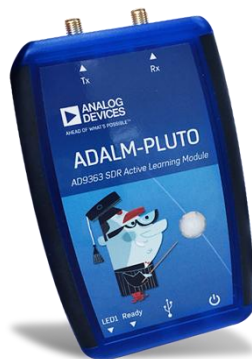


Figura 3-2 *ADALM PlutoSDR* de Analog Devices Inc.

El *TinySA* es un analizador de espectro portátil de bajo coste utilizado para caracterización y verificación, basado en el chip RTL2832U con sintonizador R820T2, cubre un rango de frecuencias de

aproximadamente 24 MHz a 1,7 GHz. Aunque su rango no alcanza la banda de 2,4 GHz de forma nativa, su utilidad en el sistema reside en la monitorización de bandas auxiliares y en tareas de verificación espectral de baja exigencia computacional. Su reducido consumo energético y perfil de tamaño lo hacen compatible con el requisito de bajo *SWaP* que rige el diseño del sistema.



Figura 3-3 *TinySA* es un analizador de espectro portátil de código abierto.

Las antenas TP-Link TL-ANT2409A son antenas de panel direccional diseñadas para operar en la banda de 2,4 GHz, con una ganancia nominal de 9 dBi y un ángulo de radiación de aproximadamente 30° en el plano horizontal. Esta directividad moderada permite orientar tanto la recepción como la transmisión hacia un sector angular concreto, lo que resulta fundamental para la implementación del *beamforming* y para la reducción de la firma electromagnética lateral durante la fase de inhibición. Su diseño de montaje fijo facilita la integración en arreglos lineales de dos elementos, condición necesaria para la estimación *DOA* mediante el algoritmo *MUSIC* descrita en el bloque *RF*.



Figura 3-4 Antena direccional 2,4 GHz TP-LINK TL_ANT2409A.

El *MA-USB8* es un sistema de captura acústica multicanal diseñado para aplicaciones de localización sonora, *beamforming* y análisis espacial de audio. Se trata de una tarjeta circular que integra ocho micrófonos *MEMS* digitales distribuidos radialmente, junto con un procesador dedicado que realiza el preprocesado del sonido antes de enviarlo al ordenador a través de una interfaz *USB*. En el contexto del presente proyecto, este dispositivo constituye el sensor utilizado para estimar la *DOA* de la señal acústica generada por un *UAS*.



Figura 3-5 Array de micrófonos *MA-USB8* utilizado como sensor espacial del sistema.

3.2 Arquitectura *software* y Lógica de operación

El sistema desarrollado sigue una arquitectura modular basada en tres subsistemas principales: detección acústica, detección en el espectro electromagnético y neutralización mediante interferencia dirigida. La información procedente de los sensores acústicos y radioeléctricos se procesa de forma independiente, permitiendo la identificación de posibles amenazas *UAS* antes de la activación de cualquier contramedida activa. Esta filosofía responde al concepto de sistema *C-UAS* semiactivo, en el que la emisión de interferencia únicamente se produce tras la confirmación previa de la amenaza mediante sensores pasivos.

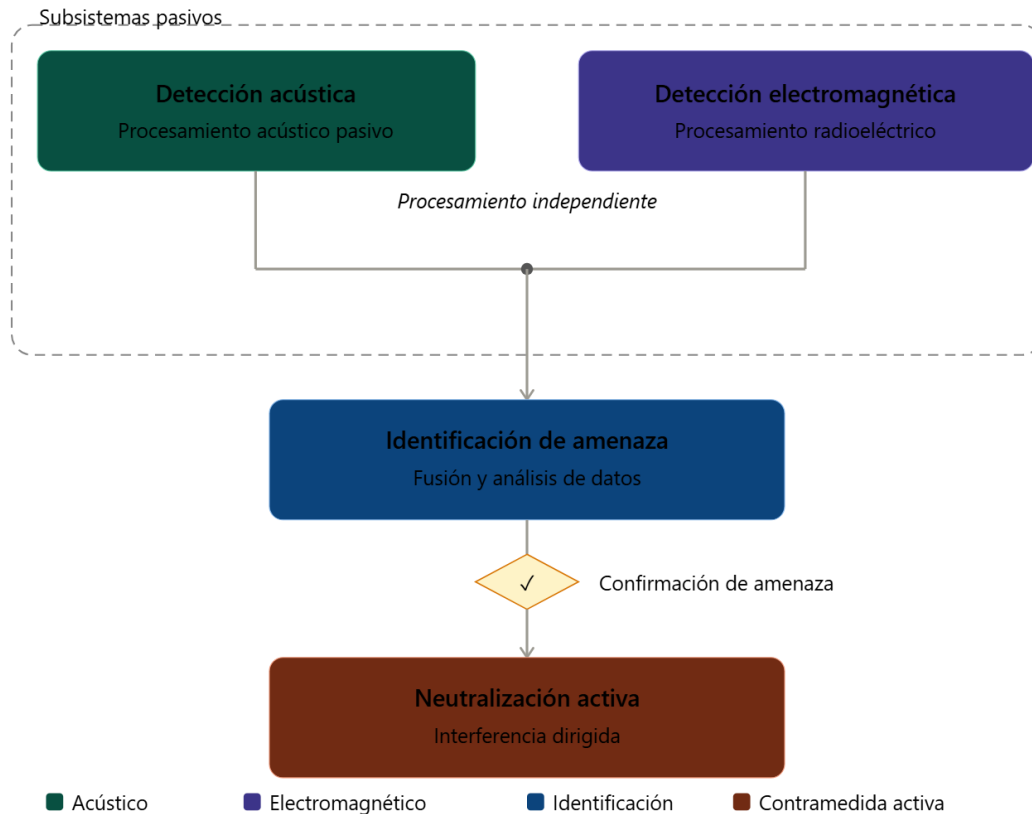


Figura 3-6 Arquitectura modular del sistema *C-UAS* semiactivo.

El desarrollo *software* del subsistema acústico comprende cinco módulos Python diferenciados, cuya evolución refleja el propio avance del prototipo. El módulo `detector_acustico.py` constituye la versión inicial, centrada en una única banda de detección (3.000-6.000 Hz) con umbral adaptativo simple. A partir de él se desarrolló `Detector_Acustico_MERGED.py`, el núcleo definitivo del sistema, que integra en un único ejecutable de 2.046 líneas la detección multi-banda, la estimación *DOA* mediante el array *MA-USB8* y la interfaz gráfica completa. En paralelo, `Consola_DOA_MAUSB8.py` implementa una consola independiente de visualización espacial con salida *UDP*, útil para integración con otros sistemas. El módulo `cic_onefile.py` representa la versión más avanzada, al incorporar un clasificador de aprendizaje automático basado en el espectrograma de Mel con entrenamiento incremental. Por último, `Creador_de_espectrogramas.py` es una utilidad auxiliar de captura y generación de espectrogramas diseñada para la construcción del *dataset* de entrenamiento.

El subsistema de radiofrecuencia se implementa mediante GNU Radio Companion en tres versiones progresivas: inhibidor básico con barrido *CHIRP*, versión con *beamforming* en recepción para dos antenas, y versión con servo para radiogoniometría activa, cada una disponible tanto en variante *simulada* como en variante de *hardware* real sobre *PlutoSDR*.

El desglose del funcionamiento de cada programa se encontrará en el Anexo III: Descripción de los programas desarrollados, y los programas creados para las pruebas de concepto se situarán en el directorio de *GitHub* [30].

3.3 Detección Acústica

3.3.1 Fundamentos

El primer bloque del sistema se fundamenta en la detección pasiva mediante análisis de la firma acústica generada por drones multirrotor. Tales drones generan un perfil espectral único debido al régimen de giro de los motores (*RPM*) y la interacción aerodinámica de las hélices. Estas firmas se caracterizan por una frecuencia fundamental y una serie de armónicos que sobresalen del ruido de fondo, generalmente en el espectro audible medio.

Para transformar la captura de audio en un reporte accionable, se ha implementado la siguiente cadena de procesamiento digital de señal en tiempo real:

- **Filtrado Digital:** Se aplica un filtro Butterworth de quinto orden en la banda de interés. La elección de este filtro responde a su respuesta en frecuencia plana en la banda de paso (*maximally flat*), lo que asegura que la energía de las hélices no se vea distorsionada antes del análisis.
- **Análisis Espectral:** Sobre la señal filtrada, el sistema calcula la densidad espectral de potencia y genera un espectrograma dinámico. Esto permite no solo detectar picos de energía, sino observar la persistencia de la firma en el tiempo, diferenciando un dron de un ruido impulsivo transitorio.
- **Cálculo de Energía:** Se cuantifica la energía en dB y se monitoriza la relación señal-ruido (*SNR*) para validar la robustez de la detección.

Uno de los mayores retos de la detección acústica es el ruido ambiental variable que hace de la lógica de detección una dificultad. Para solventarlo, se han integrado algoritmos de control avanzados:

- **Umbral Adaptativo:** El sistema recalibra automáticamente el nivel de referencia bajo condiciones de estabilidad. Si el ruido de fondo sube (ej. viento o tráfico), el umbral se ajusta para evitar falsas alarmas.
- **Persistencia N-de-M:** Para evitar disparos accidentales, el sistema requiere que la detección sea positiva en *N* de los últimos *M frames* analizados.
- **Histéresis y Bloqueo de Recalibración:** Una vez detectada una amenaza, se inhibe la recalibración automática. Esto evita que el sistema se acostumbre al sonido del dron y lo acabe integrando como ruido de fondo, lo que causaría una desactivación prematura de la alarma.

Este bloque constituye el sensor primario del sistema y actúa como un sensor disparador (*trigger*). No emite una simple señal binaria; entrega métricas cuantitativas que sirven de entrada para el bloque de radiofrecuencia. Solo cuando el sensor acústico confirma la presencia de una firma compatible, el sistema despierta al transceptor *PlutoSDR* para iniciar la fase de confirmación electromagnética [1, 7].

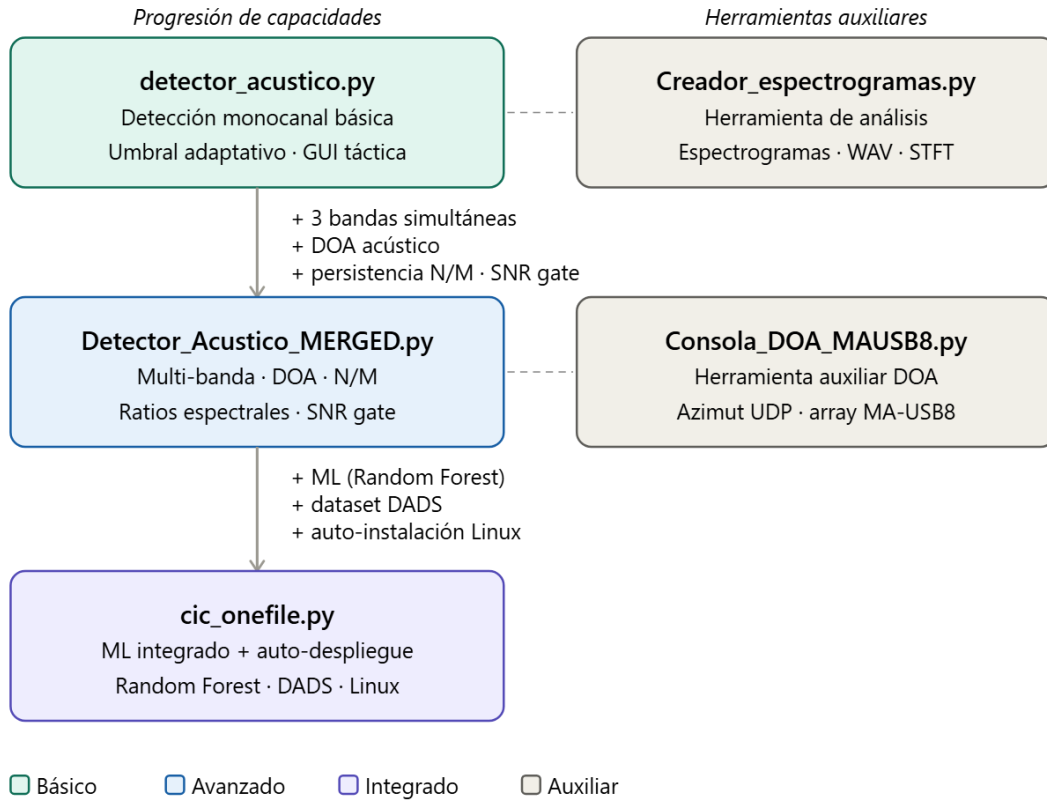


Figura 3-7 Fases del desarrollo del detector acústico.

3.3.2 Modelado Físico y Espectral de la firma Acústica

Desde el punto de vista físico, el ruido generado por un dron multirrotor no es aleatorio, sino que puede modelarse como la superposición de componentes periódicas asociadas al régimen de giro de las hélices (ruido tonal) y componentes aerodinámicas de banda ancha (ruido de banda ancha) debidas a la turbulencia e interacción entre el flujo del rotor y la estructura.

Si consideramos una hélice girando a una velocidad angular ω (rad/s) con B palas, la frecuencia fundamental asociada al paso de pala o BPF viene dada por:

$$f_0 = \frac{B\omega}{2\pi} \quad (3 - 1)$$

Esta frecuencia fundamental genera una estructura armónica aproximadamente múltiplo-entera, donde la energía se distribuye en armónicos de orden k :

$$f_k = kf_0, \quad k = 1, 2, 3, \dots \quad (3 - 2)$$

En una plataforma multirrotor, la combinación de varios motores introduce ligeras desincronizaciones y modulaciones de amplitud que producen un ensanchamiento espectral alrededor de cada armónico. Por tanto, la señal acústica total $S(t)$ capturada por el sensor puede aproximarse mediante el siguiente modelo:

$$S(t) = \sum_{m=1}^M \sum_{k=1}^K A_{m,k} \cdot \cos(2\pi k f_{0,m} t + \phi_{m,k}) + n(t) \quad (3 - 3)$$

donde M es el número de rotores de la aeronave, $A_{m,k}$ es la amplitud del armónico k para el motor m , $f_{0,m}$ es la frecuencia fundamental del motor m y $n(t)$ representa el ruido ambiental o ruido gaussiano de fondo.

Este modelo físico explica por qué la energía acústica no se distribuye de forma uniforme en el espectro audible, sino que presenta concentraciones claras en bandas medias, generalmente entre 1 kHz y 8 kHz para drones comerciales de pequeño tamaño (clase I/II).

La estrategia de filtrado Butterworth de quinto orden descrita anteriormente no es, por tanto, arbitraria; responde a la necesidad de maximizar la relación señal-ruido (SNR) en la región donde la densidad espectral asociada al paso de pala es dominante, eliminando ruidos de baja frecuencia (motores de combustión, tráfico) y ruidos de alta frecuencia ajenos a la amenaza.

3.3.3 Fundamentación del Filtrado y Estimación energética

La implementación del filtrado digital es un paso crítico para garantizar que la variable de decisión sea representativa de la amenaza. El uso de un filtro Butterworth de quinto orden ($n=5$) responde a su característica de respuesta en frecuencia monótonamente decreciente en la banda de paso y una respuesta de fase relativamente suave en comparación con otros filtros de mayor selectividad como los Chebyshev o Elípticos. En el dominio de la frecuencia, la magnitud de la respuesta de un filtro Butterworth de orden n viene dada por la expresión:

$$|H(\omega)|^2 = \frac{1}{1 + \left(\frac{\omega}{\omega_c}\right)^{2n}} \quad (3 - 4)$$

donde ω_c es la frecuencia de corte del filtro y n es el orden del filtro (en este caso, $n=5$). Utilizar un orden superior a 5 aumentaría el retardo de grupo (*group delay*) y la carga computacional en la *Raspberry Pi*, sin aportar una mejora sustancial en la discriminación de la firma de un *UAS*.

Esta respuesta permite atenuar eficazmente las componentes fuera de banda (ruido de baja frecuencia y ruido térmico de alta frecuencia) sin introducir ondulaciones (*ripple*) que podrían distorsionar la estimación de la densidad espectral de potencia y, por ende, la estimación energética.

Una vez que la señal ha sido acondicionada y filtrada, la energía instantánea de la señal $x_{filt}[n]$ se estima mediante la integración de la potencia en una ventana temporal definida:

$$E_{dB} = 10 \cdot \log_{10} \left(\frac{1}{N} \sum_{i=1}^N x_{filt}^2[i] \right) \quad (3 - 5)$$

Esta medida proporciona un valor en decibelios (dB) proporcional a la potencia media en la ventana analizada. Esta magnitud constituye la variable primaria de decisión del bloque acústico: un incremento sostenido de E_{dB} por encima del umbral de ruido de fondo caracterizado dispara la transición de estado en la *FSM* hacia la fase de validación en radiofrecuencia.

3.3.4 Umbral Adaptativo y Modelado estadístico del Ruido

La robustez del sistema de detección acústica reside en su capacidad para discernir entre la firma del *UAS* y el ruido ambiental. El ruido de fondo en exteriores no es constante; por ello, un umbral fijo resultaría ineficaz, generando falsas alarmas ante variaciones climáticas o tráfico lejano.

El ruido ambiental se modela, en primera aproximación, como un proceso aleatorio estacionario de media cero y varianza σ_n^2 . Dado que la energía estimada E_{dB} se basa en la suma de los cuadrados de las muestras de la señal filtrada, esta magnitud sigue teóricamente una distribución chi-cuadrado (χ^2) escalada. Ante variaciones de σ_n^2 , el sistema debe recalcular el nivel de referencia para mantener una sensibilidad óptima.

El umbral de decisión γ se adapta dinámicamente en función de la energía media observada durante los periodos de silencio (véase en Tabla 3-1), siguiendo la expresión:

$$\gamma = \mu_E + k \cdot \sigma_E \quad (3 - 6)$$

donde μ_E es la media estimada de la energía del fondo acústico, σ_E es la desviación estándar de la energía del fondo y k es un factor de sensibilidad que actúa como multiplicador de confianza. Este factor k suele configurarse entre 3 y 6. Según la regla empírica (distribución normal), un $k=3$ cubriría el 99.7% de las variaciones del ruido, por lo que cualquier señal que lo supere tiene una alta probabilidad de ser una fuente externa (el dron).

Este enfoque implementa un detector tipo Neyman-Pearson simplificado. Al ajustar el valor de k , el sistema controla la probabilidad de falsa alarma (P_{FA}); un valor de k elevado reduce las falsas alarmas a costa de exigir una relación señal-ruido (SNR) más alta para la detección.

Para evitar que impulsos transitorios (golpes, ráfagas de viento, portazos) disparen la alerta, se ha incorporado un criterio de persistencia temporal N-de-M. Este mecanismo actúa como un filtro lógico temporal donde se analizan M ventanas temporales consecutivas y la detección solo se considera válida si la energía supera el umbral γ en, al menos, N de esas ventanas.

Este proceso reduce drásticamente la probabilidad de disparos espurios, asegurando que la activación del bloque de radiofrecuencia (fase posterior) solo ocurra ante la presencia de una fuente acústica coherente y persistente en el tiempo, característica propia del vuelo de un multirrotor.

3.3.5 Limitaciones del Medio de Propagación y Desafíos Técnicos

El desarrollo del bloque acústico ha permitido identificar limitaciones intrínsecas al medio físico que condicionan la fiabilidad de la detección. A diferencia del dominio de radiofrecuencia (RF), donde la onda electromagnética presenta una estabilidad relativa en campo lejano, la propagación de ondas de presión sonora está sujeta a variables ambientales críticas:

Atenuación y Pérdida de Propagación: En condiciones de campo libre, la presión sonora disminuye inversamente con la distancia, lo que implica que la intensidad acústica decae proporcionalmente a $\frac{1}{r^2}$ en campo libre. Esta atenuación geométrica, sumada a la absorción atmosférica (que aumenta con la frecuencia y la humedad), limita el rango de detección efectiva del sensor primario a distancias cortas o medias, donde la firma del dron aún conserva una SNR positiva.

- **No Estacionariedad y Ruido Ambiental:** El entorno operativo vulnera frecuentemente el supuesto de estacionariedad del ruido. Los desafíos principales incluyen ruido impulsivo donde eventos transitorios (vehículos, viento racheado o conversaciones) generan picos de energía que podrían ser confundidos con un UAS si no existiera el filtrado N-de-M y la lógica de persistencia; efecto del viento donde el flujo de aire sobre la membrana del micrófono genera turbulencias de baja frecuencia (es decir, si no se aplicara el filtrado Butterworth en banda media (1-8 kHz), estas componentes podrían saturar el sistema y falsear la estimación de la energía σ_e^2); entornos urbanos donde la presencia de reflexiones y reverberación puede generar interferencias constructivas o destructivas que modifican la estructura armónica de la firma capturada.
- **Enmascaramiento Espectral:** En escenarios de alta congestión sonora, la señal de un dron lejano puede quedar sumergida bajo el ruido ambiental cuya energía total sea comparable o superior en banda. Esto imposibilita la detección mediante umbrales energéticos simples y justifica la transición hacia RF como método de confirmación definitiva.

En conclusión, el bloque acústico actúa como un centinela de bajo consumo diseñado para explotar la física de la firma rotor-hélice. Sus limitaciones no derivan de la implementación *software*, sino de la naturaleza estocástica del ruido ambiental y las leyes de la acústica ondulatoria.

3.3.6 Caracterización Espectral de Objetivos

El módulo de detección constituye el primer nivel jerárquico de la arquitectura. Su función es identificar la presencia de *UAS* mediante el análisis discriminatorio de su firma acústica frente al ruido de fondo. Para la validación del sistema, se han seleccionado dos plataformas con perfiles aerodinámicos y acústicos sensiblemente distintos:

- **DJI Avata 2:** Un dron tipo *Cinewhoop*. Su diseño incluye protectores de hélice (ductos) que confinan el flujo de aire, lo que genera una firma acústica de alta frecuencia y una estructura armónica muy definida debido al régimen de giro elevado de sus motores de pequeño diámetro. Los protectores de hélice de este dron pueden actuar como pequeñas cajas de resonancia, lo que a menudo desplaza la energía hacia armónicos superiores, haciendo que el sonido sea más "agudo" y fácil de filtrar frente al tráfico (ruido grave).
- **HYT BP S179:** Un *UAS* genérico de bajo coste. Representa la amenaza recreativa estándar, con hélices de mayor superficie y una firma acústica más grave (frecuencias fundamentales más bajas) y menos estable que la de una plataforma estabilizada profesional.

La distinción entre una amenaza real y el entorno se basa en la morfología del espectrograma obtenido en tiempo real. Como se observa en la Figura 3-8, el ruido de fondo se caracteriza por una distribución energética difusa y estocástica (*broadband*). No existen líneas de frecuencia persistentes, lo que indica la ausencia de componentes periódicas. A diferencia del ruido ambiente, los espectrogramas de los drones analizados revelarán trazas horizontales nítidas. Estas líneas corresponderán a la Frecuencia de Paso de Pala (*BPF*) y sus armónicos sucesivos. La persistencia temporal de estas líneas, incluso ante variaciones de amplitud, es el indicador inequívoco que utiliza el algoritmo para disparar la alerta hacia el bloque de radiofrecuencia.

Característica	Ruido Ambiental	Firma <i>UAS</i> (<i>Avata 2</i> / <i>HYT BP</i>)
Distribución	Difusa / Banda ancha	Tonal / Armónica
Estructura	Aleatoria	Líneas horizontales persistentes
Periodicidad	Nula	Alta (asociada a <i>RPM</i>)
Componentes	Transitorios espurios	Fundamental + Armónicos ($f_k = k \cdot f_0$)

Tabla 3-1: Características del ruido ambiental y de la firma *UAS*.

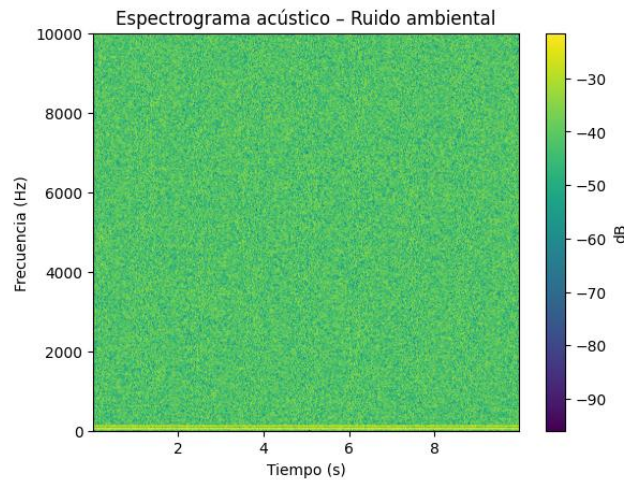


Figura 3-8 Espectrograma del ruido ambiental.

Cabe resaltar que mientras el ruido ambiental es *broadband* (banda ancha), el sonido emitido por el dron es *narrowband* (banda estrecha) en múltiples frecuencias. De ahí que el filtro Butterworth esté diseñado precisamente para dejar pasar esas bandas estrechas donde reside la información del dron.

El espectrograma correspondiente al ruido ambiental muestra una distribución energética difusa a lo largo de todo el rango de frecuencias analizado, sin presencia de componentes tonales ni estructuras armónicas persistentes. A diferencia de los espectrogramas asociados a los drones analizados en los apartados 3.2.3.1 y 3.2.3.2, donde aparecen líneas horizontales correspondientes a la frecuencia de paso de pala y sus armónicos, el ruido ambiental presenta un comportamiento *broadband* característico de fuentes acústicas no periódicas. Esta diferencia estructural constituye uno de los criterios fundamentales que permite distinguir acústicamente la presencia de un *UAV* mediante técnicas de análisis espectral.

3.3.7 Caracterización del Objetivo I: DJI Avata 2

El *DJI Avata 2* es un sistema aéreo no tripulado de pequeño tamaño diseñado para vuelo *FPV* y captura de vídeo inmersiva. Pertenece a la categoría de *UAV* multirrotor de clase ligera, con configuración cuadricóptero y hélices carenadas (*cinewhoop*) que mejoran la estabilidad y reducen el riesgo de impacto en entornos cerrados.

La aeronave utiliza un sistema de propulsión basado en motores *brushless* de alta eficiencia y hélices de cinco palas carenadas. El carenado actúa como una guía de onda acústica que tiende a enfatizar las componentes tonales de alta frecuencia, generando un sonido más agudo y direccional que facilita su detección en la banda de interés (1-8 kHz) definida en el diseño de los filtros Butterworth del sistema.

En términos operativos, este tipo de *UAV* se clasifica dentro de los drones ligeros de corto alcance (*LSS*), ampliamente utilizados en aplicaciones civiles como grabación audiovisual, inspección o recreación, pero que también representan un objetivo típico para sistemas *C-UAS* debido a su pequeño tamaño, baja firma radar y facilidad de adquisición, tal como muestra la Figura 3-9 con su ecosistema de vuelo completo.



Figura 3-9 Ecosistema *UAV DJI Avata 2*

Utilizando la herramienta Creador de Espectrogramas basada en Python, se ha procesado la señal capturada en condiciones de vuelo estacionario (*hovering*).

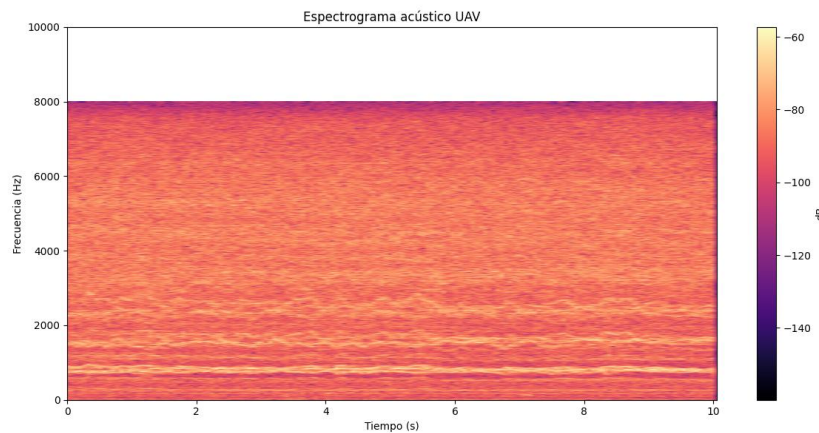


Figura 3-10 Espectrograma acústico *DJI Avata 2*.

Los resultados obtenidos en la Figura 3-10 permiten extraer las siguientes conclusiones técnicas:

- **Frecuencia Fundamental (f_0):** Se identifica con claridad la *BPF* en el rango de 350-400 Hz. Esto concuerda con el régimen de rotación necesario para mantener el sustento de una plataforma de aproximadamente 377g.
- **Estructura Armónica:** Se observa una sucesión de armónicos persistentes que se extienden hasta los 6 kHz. La densidad espectral de potencia (*PSD*) es máxima en la banda de 400 Hz a 1,5 kHz, región donde el detector energético presenta su mayor ganancia.
- **Estabilidad de la Firma:** La morfología de las trazas horizontales en el espectrograma confirma un régimen de revoluciones constante. Esta estabilidad es la que permite al algoritmo de persistencia N-de-M validar la detección, diferenciando al *UAS* de ruidos impulsivos ambientales que carecen de esta continuidad armónica.

Al tener más palas que un dron estándar (que suele tener 2 o 3), la frecuencia fundamental f_0 es más alta para un mismo número de *RPM*, lo que empuja la firma hacia la zona de mejor audición del micrófono y mejor filtrado del sistema.

La detección exitosa de la firma del *Avata 2* a través de sus armónicos superiores (3 kHz - 5 kHz) demuestra que el sistema es capaz de operar incluso si la frecuencia fundamental queda enmascarada por ruidos de baja frecuencia (tráfico o viento), gracias al filtrado selectivo de 5º orden. Esta detección

acústica positiva es la que genera el *trigger* para activar el escaneo de radiofrecuencia en la banda de 2,4 GHz, donde el sistema buscará el protocolo de transmisión *O4* de *DJI*.

3.3.8 Caracterización del Objetivo II: *HYT BP S179*

El *HYT BP S179* representa la amenaza de tipo dron recreativo de bajo coste. A diferencia de plataformas profesionales, su construcción ligera y la ausencia de carenado en las hélices generan una firma acústica con mayor contenido de ruido aerodinámico de banda ancha, como puede apreciarse en la Figura 3-11, pero con una estructura armónica extremadamente marcada debido a la menor estabilidad de sus controladores de velocidad (*ESC*) comparados con sistemas de alta gama.



Figura 3-11 Plataforma UAV HYT BP S179 y elementos asociados al sistema.

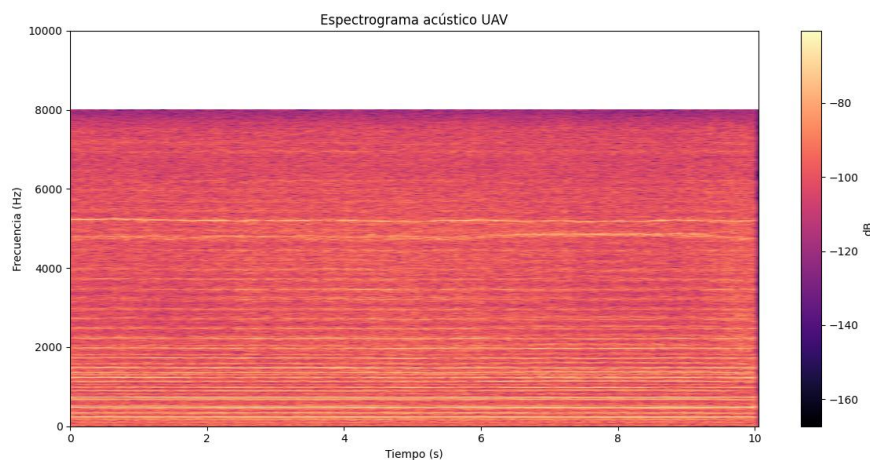


Figura 3-12 Espectrograma acústico del UAS HYT BP S179.

A partir del procesamiento de los datos experimentales y la generación del espectrograma en la Figura 3-12, se extraen los siguientes parámetros técnicos:

- **Frecuencia Fundamental (f_0):** Se localiza en el rango de 200-300 Hz. Al ser una hélice de mayor diámetro y paso que la del *Avata 2*, requiere un régimen de giro (*RPM*) menor para generar el empuje necesario, lo que desplaza la *BPF* hacia el extremo inferior del espectro.
- **Estructura Armónica:** Presenta una estructura de peine muy definida. Los armónicos superiores son detectables hasta los 5 kHz, con una concentración energética crítica entre 2 kHz y 4 kHz. Esta firma es ideal para el sistema de detección propuesto, ya que cae directamente en la banda de paso del filtro Butterworth diseñado.

- **Ruido de Banda Ancha:** Se observa una base de ruido turbulento que se extiende hasta los 6 kHz. Este fenómeno es característico de las hélices sin carenado, donde el desprendimiento de vórtices en las puntas de las palas no está confinado.

La estabilidad de las líneas horizontales durante el intervalo de 10 segundos confirma que, a pesar de ser un dron económico, mantiene una coherencia espectral suficiente para que los algoritmos de umbral adaptativo y persistencia N-de-M operen con una probabilidad de detección (P_D) elevada. En resumen, destacar que el HYT BP es "más ruidoso" en la banda de 2-4 kHz que el *Avata*. Esto significa que, aunque el *Avata* sea un dron más avanzado, el HYT BP es más fácil de detectar acústicamente a mayor distancia por el sistema.

Con la caracterización de ambos objetivos, se valida que el sistema de detección pasiva es capaz de identificar *UAS* con perfiles físicos opuestos. La detección de las componentes tonales del *HYT BP S179* entre 2 y 4 kHz confirma la idoneidad de la arquitectura multisensor: una vez que el bloque acústico "bloquea" estas frecuencias, el sistema tiene la confianza estadística necesaria para activar el bloque de *RF* y proceder a la localización con el *PlutoSDR*,

Parámetro	<i>DJI Avata 2</i>	<i>HYT BP S179</i>
Fundamental (f_0)	350 - 400 Hz (Más aguda)	200 - 300 Hz (Más grave)
Rango Armónico	Hasta 6 kHz	Hasta 5 kHz
Banda de Máxima Energía	400 Hz - 1,5 kHz	2 kHz - 4 kHz
Perfil Aerodinámico	Flujo carenado / Ductos	Hélice abierta / Turbulencia

Tabla 3-2: Comparativa entre *DJI Avata 2* y *HYT BP S179*.

3.4 Detección en el Espectro Electromagnético

3.4.1 Fundamentos

El segundo bloque del sistema aborda el dominio electromagnético, centrado en el análisis de emisiones en la banda *ISM* de 2,4 GHz, comúnmente utilizada para enlaces de control y transmisión de vídeo en *UAS* comerciales. A diferencia del bloque acústico, que opera de forma puramente pasiva en el dominio audible, el bloque *RF* combina recepción, generación controlada de señal y técnicas de direccionamiento espacial.

El desarrollo experimental realizado en GNU Radio evidencia una evolución progresiva desde una arquitectura básica de generación de señal hasta un sistema capaz de estimar dirección de llegada (*DOA*) mediante técnicas de subespacios como el algoritmo *MUSIC* [4]. Inicialmente, se implementó un generador de *CHIRP* con barrido de 20 MHz centrado en 2,41 GHz, transmitido mediante *PlutoSDR* y distribuido en dos ramas con control de fase relativo. Este esquema permitió estudiar el comportamiento de un *ULA* de dos elementos separados aproximadamente $\lambda/2$, condición que minimiza lóbulos secundarios y evita ambigüedades espaciales en el rango angular principal.

El control de fase entre ambas ramas se implementó mediante ajuste paramétrico en GNU Radio, permitiendo aplicar un desfase proporcional a la expresión clásica del *beam steering*:

$$\Delta\phi = \frac{2\pi d}{\lambda} \sin(\theta) \quad (3 - 7)$$

donde d es la separación entre antenas y θ el ángulo de apuntamiento deseado. Este control paramétrico en GNU Radio permite orientar el máximo de radiación (o el nulo de recepción) hacia la posición estimada del *UAS*, optimizando la relación señal-ruido y la selectividad de la contramedida.

Posteriormente, la arquitectura evolucionó hacia un esquema de recepción coherente con dos canales sincronizados del *PlutoSDR*, habilitando la aplicación de un estimador *DOA* basado en *MUSIC*. Este algoritmo explota la descomposición en auto valores de la matriz de correlación espacial para separar subespacios de señal y ruido, permitiendo estimar el ángulo de llegada con mayor resolución que los métodos clásicos de máxima potencia. La implementación requirió garantizar coherencia entre canales, control preciso de sample-rate y definición explícita de la separación física entre antenas.

Como alternativa complementaria, se podría experimentar un enfoque mecánico basado en antena direccional montada sobre servo, realizando barridos angulares controlados y determinando la dirección mediante máxima potencia recibida. Aunque esta solución presenta menor resolución y mayor latencia, reduce la complejidad electrónica y elimina la necesidad de coherencia multicanal, constituyendo una opción viable para configuraciones de bajo coste.

En conjunto, el bloque *RF* transforma el sistema en una plataforma de radiogoniometría digital capaz de confirmar emisiones, estimar dirección y proporcionar parámetros espaciales necesarios para una eventual actuación dirigida.

3.4.2 Desafíos Críticos y Problemática del Procesado Espacial

La transición desde la detección escalar (energía) hacia la detección vectorial (dirección) introduce una serie de limitaciones prácticas que emanan de principios fundamentales del electromagnetismo y la teoría de estimación estadística. El desarrollo experimental con el *PlutoSDR* ha permitido categorizar estos desafíos en tres ejes principales:

- **Ambigüedad espacial y aliasing:** en el diseño del array lineal ULA, la separación entre antenas d es el parámetro crítico. Si $d > \lambda/2$, el sistema introduce lóbulos de ambigüedad (*grating lobes*). Matemáticamente, el vector de dirección de la señal deja de ser unívoco, provocando que el algoritmo *MUSIC* o el *beamforming* identifiquen "falsas direcciones" de llegada. Dado que la banda *ISM* de 2,4 GHz tiene una longitud de onda de ≈ 12.5 cm, cualquier error milimétrico en el montaje físico de las antenas TP-Link TL-ANT2409A repercute directamente en la precisión angular.
- **Coherencia de fase y sincronismo hardware:** Para que un algoritmo de subespacios como *MUSIC* funcione, es imperativo que los canales de recepción sean coherentes. Esto implica usar un oscilador local único donde ambos canales deben compartir la misma referencia de frecuencia. Aunque el chip AD9363 del *PlutoSDR* lo permite, existen derivas térmicas y desfases internos (*phase noise*) que deberían ser calibrados por *software*. Por otro lado, la latencia de muestreo donde cualquier *jitter* o desfase temporal en la captura de las muestras *IQ* entre ambas entradas se traduce en un error de fase $\Delta\phi$, lo que el sistema interpreta erróneamente como un cambio en la dirección de llegada θ .
- **Multitrayectoria y entornos no anecoicos:** En escenarios reales, la señal del *UAS* no llega por un único camino. Las reflexiones en el suelo, edificios o vegetación generan un fenómeno de multitrayectoria (*multipath*) donde las señales reflejadas están altamente correlacionadas con la señal directa, lo que provoca que la matriz de correlación espacial pierda rango. En estas condiciones, el algoritmo *MUSIC* puede fallar al intentar separar el subespacio de señal del de ruido, fusionando varios frentes de onda en un único pico ancho o errático.

- **Limitaciones del SDR de bajo coste (Rango Dinámico):** El *PlutoSDR*, al ser un dispositivo de 12 bits, presenta un rango dinámico limitado. En presencia de interferencias fuertes en la banda *ISM* (como *routers WiFi* cercanos), el receptor puede saturarse o elevar el suelo de ruido, enmascarando la débil señal de telemetría del dron y degradando la resolución del espectro espacial.

3.4.2.1 Modelado Matemático del Array Lineal Uniforme

Para que el sistema pueda estimar la dirección de la amenaza, es necesario modelar la geometría del frente de onda incidente. Se considera un arreglo lineal uniforme de M elementos (en este prototipo, $M=2$) separados una distancia física d . Para una onda plana monocromática (asumiendo que el dron está en campo lejano) incidente desde un ángulo θ respecto a la normal del array, el desfase espacial entre elementos consecutivos viene dado por:

$$\Delta\phi = k \cdot d \cdot \sin(\theta) \quad (3 - 8)$$

donde $k = \frac{2\pi}{\lambda}$ es el número de onda. Este desfase es la base de la información espacial que el sistema debe extraer de las muestras *IQ* capturadas. La señal recibida en el elemento m -ésimo del array puede modelarse en el dominio de la frecuencia compleja como:

$$x_m(t) = s(t) \cdot e^{-j(m-1)kdsin(\theta)} + n_m(t) \quad (3 - 9)$$

Para el conjunto de antenas, la expresión se simplifica en forma vectorial:

$$\mathbf{x}(t) = \mathbf{a}(\theta) \cdot s(t) + \mathbf{n}(t) \quad (3 - 10)$$

donde el vector de dirección (steering vector) $\mathbf{a}(\theta)$ define la respuesta del array para una dirección específica:

$$\mathbf{a}(\theta) = \begin{bmatrix} 1 \\ e^{-jkdsin(\theta)} \\ \vdots \\ e^{-j(M-1)kdsin(\theta)} \end{bmatrix} \quad (3 - 11)$$

donde se supone una onda plana (fuente en campo lejano), señal en banda estrecha (el ancho de banda de la señal del dron (ej. 20 MHz) es mucho menor que la frecuencia portadora (2,4 GHz) permitiendo tratar el retardo temporal entre antenas como un simple desfase de fase) y coherencia entre canales.

Aquí surge el primer desafío teórico-práctico: el modelo ideal supone una coherencia perfecta. Sin embargo, en el *PlutoSDR*, aunque ambos canales comparten el mismo oscilador local, factores como el *drift* térmico, las diferencias en la longitud de los cables SMA y los retardos internos de los ADCs introducen un término de error adicional $\Delta\phi_{error}$:

$$\mathbf{a}'(\theta) = \mathbf{a}(\theta)e^{-j\Delta\phi_{error}} \quad (3 - 12)$$

Este error rompe la correspondencia exacta entre el modelo matemático y la realidad física. Si $\Delta\phi_{error}$ no se compensa mediante una calibración previa (inyectando una señal de referencia conocida), el algoritmo de localización (*MUSIC* o *beamforming*) podría reportar un ángulo de llegada θ sesgado, invalidando la precisión de la interdicción selectiva.

3.4.2.2 Ambigüedad Espacial y la Condición Crítica de Separación $\lambda/2$

Uno de los desafíos técnicos más críticos en la implementación de la radiogoniometría digital es la aparición de lóbulos de ambigüedad (*grating lobes*). Este fenómeno ocurre cuando la separación entre

los elementos del arreglo no cumple con el criterio de muestreo espacial de Nyquist. Para que el sistema de detección *RF* pueda asociar un único ángulo de incidencia θ a un desfase observado $\Delta\phi$, la separación entre antenas d debe satisfacer la condición:

$$d \leq \frac{\lambda}{2} \quad (3 - 13)$$

Si esta condición se vulnera (es decir, si $d > \frac{\lambda}{2}$) el término del desfase espacial $e^{-jk d \sin(\theta)}$ se vuelve periódico dentro del rango visible de $[-90^\circ, 90^\circ]$, generando múltiples soluciones válidas para el mismo desfase observado y provocando que el sistema identifique "drones fantasma" en direcciones erróneas. Cuando la separación excede el límite crítico, el algoritmo de estimación (ya sea *MUSIC* o *beamforming*) encuentra picos de máxima verosimilitud en ángulos indistinguibles:

$$k d \sin(\theta_1) = k d \sin(\theta_2) + 2\pi n, \quad n = 1, 2, 3, \dots \quad (3 - 14)$$

lo que conduce a ángulos espurios indistinguibles. Este error es análogo al *aliasing* en el procesamiento digital de señales temporales, pero aplicado al dominio del espacio. En el entorno de 2,4 GHz, donde la longitud de onda $\lambda \approx 12.5$ cm, la separación crítica es de aproximadamente 6.25 cm. La elección geométrica del arreglo de antenas TP-Link en este proyecto no es arbitraria, sino una respuesta a esta restricción matemática. Al fijar la distancia $d \approx 6$ cm, se garantiza la unicidad de la solución ya que cada desfase $\Delta\phi$ capturado por el *PlutoSDR* corresponde a una única dirección real del *UAS* y la optimización del haz ya que se maximiza la resolución angular sin introducir lóbulos secundarios que degraden la selectividad de la futura interdicción.

3.4.2.3 Formación de haz

El *beamforming* clásico (o conformado de haz) es la técnica geo-espacial que permite orientar la sensibilidad del array de antenas sin necesidad de movimiento mecánico. Se fundamenta en la aplicación de un vector de pesos complejos w a las señales capturadas o transmitidas por cada elemento del array:

$$y(t) = w^H x(t) \quad (3 - 15)$$

donde W^H indica la transpuesta conjugada (hermitiana) del vector de pesos. Para maximizar la ganancia en una dirección de interés θ_0 , el vector de pesos debe sintonizarse con el vector de dirección (*steering vector*) correspondiente:

$$w = a(\theta_0) \quad (3 - 16)$$

entonces el sistema maximiza la ganancia en la dirección θ_0 , ya que:

$$w^H a(\theta) = \sum_{m=0}^{M-1} e^{j m k d (\sin(\theta) - \sin(\theta_0))} \quad (3 - 17)$$

Cuando el vector de pesos coincide exactamente con el frente de onda incidente ($\theta = \theta_0$), el sistema alcanza su máxima eficiencia. En el caso de nuestro prototipo con $M=2$ elementos, esto se traduce en una ganancia teórica de 3 dB adicionales sobre la señal recibida, además de la propia ganancia de las antenas direccionales TP-Link.

La respuesta angular del sistema, o factor de array, para una dirección de apuntamiento θ_0 viene dada por la expresión:

$$AF(\theta) = \frac{\sin\left(\frac{M}{2}kd(\sin\theta - \sin\theta_0)\right)}{\sin\left(\frac{1}{2}kd(\sin\theta - \sin\theta_0)\right)} \quad (3 - 18)$$

Esta expresión evidencia la dependencia no lineal entre la ganancia y el ángulo de incidencia. La pendiente de esta función en las proximidades del lóbulo principal explica la sensibilidad extrema a pequeños errores de fase: un ligero desajuste en θ_0 (debido a errores de calibración en el *PlutoSDR* o desplazamientos físicos del array) puede desplazar el máximo de radiación fuera de la posición real del UAS, invalidando la efectividad de la contramedida.

3.4.2.4 Estimación de DOA mediante MUSIC

Para superar las limitaciones de resolución del *beamforming* clásico, el sistema implementa un enfoque de alta resolución basado en subespacios. El algoritmo *MUSIC* explota la estructura geométrica de los datos multicanal para proporcionar una estimación de la Dirección de Llegada (DOA) extremadamente precisa. El primer paso consiste en estimar la matriz de correlación espacial R_{xx} a partir de las muestras *IQ* recibidas en los dos canales del *PlutoSDR*. Esta matriz captura la dependencia estadística entre las antenas:

$$R_{xx} = E[\mathbf{x}(t)\mathbf{x}^H(t)] \quad (3 - 19)$$

Sustituyendo el modelo de señal desarrollado anteriormente ($\mathbf{x}(t) = \mathbf{a}(\theta) \cdot s(t) + \mathbf{n}(t)$), y asumiendo que el ruido no está correlacionado con la señal, la matriz se descompone como:

$$R_x = \sigma_s^2 \mathbf{a}(\theta)\mathbf{a}^H(\theta) + \sigma_n^2 \mathbf{I} \quad (3 - 20)$$

donde σ_s^2 es la potencia de la señal del UAS y σ_n^2 la potencia del ruido térmico.

Mediante una descomposición en autovalores (*EVD*) de R_{xx} , el sistema separa el espacio de observación en dos conjuntos ortogonales: subespacio de señal, asociado al autovalor dominante (el de mayor magnitud); y subespacio de ruido E_n , formado por los autovectores correspondientes a los autovalores menores. El fundamento matemático de *MUSIC* reside en la propiedad de ortogonalidad: el vector de dirección real de la señal a (θ_{real}) debe ser perpendicular al subespacio de ruido:

$$\mathbf{a}^H(\theta_{real})E_n = 0 \quad (3 - 21)$$

Dado que en condiciones reales (ruido, errores de fase, muestras limitadas) el producto anterior nunca es exactamente cero, se define una función de búsqueda denominada pseudoespectro $PMUSIC(\theta)$. Esta función se evalúa para todos los ángulos posibles $\theta \in [-90^\circ, 90^\circ]$.

$$P_{MUSIC}(\theta) = \frac{1}{\mathbf{a}^H(\theta)E_n E_n^H \mathbf{a}(\theta)} \quad (3 - 22)$$

Cuando el ángulo de búsqueda θ coincide con la dirección real del dron, el denominador tiende a cero, provocando un pico agudo de resonancia en el pseudoespectro. La posición de este pico constituye la estimación final de la dirección de la amenaza, que el sistema utilizará para orientar la respuesta electrónica.

3.4.3 Análisis de Limitaciones y Restricciones del Modelo de Estimación

El desarrollo del bloque de radiofrecuencia ha evidenciado que las limitaciones encontradas no responden a fallos de implementación, sino a restricciones inherentes al propio modelo de estimación

espacial y a la física de la propagación. La dependencia exponencial compleja del vector de dirección $a(\theta)$ convierte la precisión mecánica en un requisito matemático. Pequeñas desviaciones milimétricas en la separación d entre las antenas TP-Link alteran el término del desfase espacial y cualquier error en d desplaza el máximo del pseudoespectro *MUSIC*, provocando un error sistemático en la localización del *UAS* que no puede ser corregido mediante *software* si la geometría física es inestable.

El modelo de subespacios asume una onda plana única (campo lejano). Sin embargo, en entornos reales, las reflexiones (multitrayectoria) introducen componentes incidentes que correlacionan la señal directa con las reflejadas, degradan la descomposición en autovalores de la matriz R_{xx} y generan picos espurios o ensanchamiento del haz, dificultando la distinción entre el dron real y su rebote en un obstáculo.

El modelo supone que el vector de dirección es constante en frecuencia. Dado que las señales de vídeo de drones como el *DJI Avata 2* pueden ocupar hasta 20 MHz (un 0.8% de la portadora de 2,4 GHz), el sistema roza el límite de la hipótesis de banda estrecha. Si el ancho de banda aumentara, el desfase dejaría de ser único para toda la señal, exigiendo técnicas *wideband* de una complejidad computacional mucho mayor.

La calidad de la estimación es directamente proporcional a la Relación Señal-Ruido (*SNR*). Con una *SNR* baja, la distinción entre el autovalor de la señal y los del ruido se desvanece, provocando inestabilidad angular. Finalmente, la coherencia de fase entre los canales del *PlutoSDR* es la condición estructural más crítica: cualquier desfase fijo no calibrado ($\Delta\phi_{error}$) actúa como una perturbación matricial que desplaza sistemáticamente la estimación, haciendo que el sistema "vea" el dron en una posición donde no está

En conjunto, estas limitaciones ponen de manifiesto que la radiogoniometría digital con *SDR* de bajo coste depende críticamente de la coherencia física, la validez de los supuestos teóricos y la calidad estadística de la señal. Este análisis cierra el desarrollo conceptual del bloque *RF* y justifica la necesidad de los experimentos de validación que se detallan a continuación.

3.4.4 Caracterización Experimental en el Espectro RF

La detección de objetivos mediante radiofrecuencia (*RF*) requiere una plataforma de *hardware* capaz de procesar señales de banda ancha con alta fidelidad. Para validar los algoritmos de localización (*MUSIC/beamforming*), se han empleado los mismos *UAV* del bloque acústico (*DJI Avata 2* e *HYT BP S179*), cuyas emisiones en la banda *ISM* de 2,4 GHz presentan firmas electromagnéticas diferenciadas.

Se ha utilizado el transceptor *ADALM-Pluto* integrado con una estación de procesamiento basada en GNU Radio. Este dispositivo permite monitorizar el espectro radioeléctrico en tiempo real, proporcionando dos herramientas de análisis fundamentales. Para recibir se ha utilizado el *TinySA*.

3.4.5 Caracterización Experimental del Objetivo I: DJI Avata 2

El *DJI Avata 2* emplea el sistema de transmisión digital *O4*, el cual optimiza el uso del espectro mediante técnicas de ensanchamiento por secuencia directa (*DSSS*) y salto de frecuencia (*FHSS*). El análisis mediante el analizador de señales *TinySA* permite caracterizar este enlace para diseñar una contramedida específica.

La monitorización en la banda *ISM* de 2,4 GHz revela una firma electromagnética de alta complejidad. A diferencia de otros drones recreativos, el *Avata 2* presenta:

- **Densidad Espectral de Potencia (*PSD*):** Se observa una ocupación de canal de banda ancha (típicamente entre 20 MHz y 40 MHz). La potencia se distribuye de forma casi uniforme en la banda ocupada, lo que indica un uso eficiente del canal para el transporte de vídeo 4K y telemetría crítica.
- **Análisis Temporal (*Waterfall*):** Como se aprecia en la Figura 3-13, la representación en cascada muestra una traza vertical continua y densa. Esta persistencia temporal confirma que el enlace no es

esporádico (como un sensor *IoT*), sino un flujo constante de datos necesario para el pilotaje *FPV* en tiempo real.

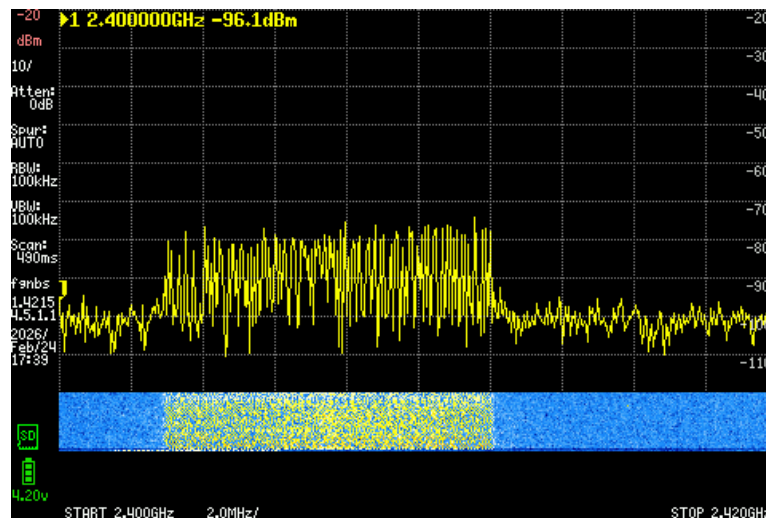


Figura 3-13 Representación espectral del enlace radioeléctrico del *DJI Avata 2* en 2,4 GHz.

El análisis espectral realizado dicta la arquitectura del bloque de actuación. Debido a la naturaleza de la señal detectada, se extraen las siguientes directrices de diseño para la contramedida:

- **Ineficacia del *jamming* Puntual:** Una señal de interferencia de banda estrecha sería fácilmente ignorada por los algoritmos de corrección de errores (*FEC*) del protocolo *DJI*.
- **Estrategia de Barrido (*CHIRP*):** Para degradar el enlace de forma efectiva, el sistema debe generar una señal que recorra rápidamente el ancho de banda ocupado. Esta técnica de barrido rápido asegura que la densidad temporal de la interferencia sea suficiente para corromper los paquetes de sincronización del dron.
- **Ruido de Banda Ancha:** Alternativamente, la inyección de ruido blanco gaussiano aditivo (*AWGN*) sobre la totalidad de los 20-40 MHz detectados elevaría el suelo de ruido (*noise floor*) hasta que la *SNR* caiga por debajo del umbral de decodificación del receptor *O4*.

A continuación, en la tabla 3-3 mostramos la caracterización específica para el *DJI AVATA 2*, basada en los datos del análisis espectral y la naturaleza del enlace *FHSS*:

Parámetro <i>RF</i>	Observación Experimental	Requisito de Inhibición
Ancho de Banda	~20-40 MHz	Cobertura total de la banda
Persistencia	Continua (<i>FPV</i> /Telemetría)	Ciclo de trabajo (<i>duty cycle</i>) alto
Tipo de Modulación	Digital <i>OFDM</i> / Spread Spectrum	Interferencia de alta entropía (Ruido/ <i>CHIRP</i>)

Tabla 3-3: Características espectrales del *DJI Avata 2*.

3.4.6 Caracterización Experimental del Objetivo II: *HYT BP S179*

El *HYT BP S179* es un exponente de la categoría de drones recreativos de bajo coste y peso ultraligero (≈ 250 g). Su análisis es fundamental para validar la capacidad del sistema *C-UAS* ante protocolos de comunicación menos sofisticados, pero altamente ágiles en el dominio de la frecuencia.

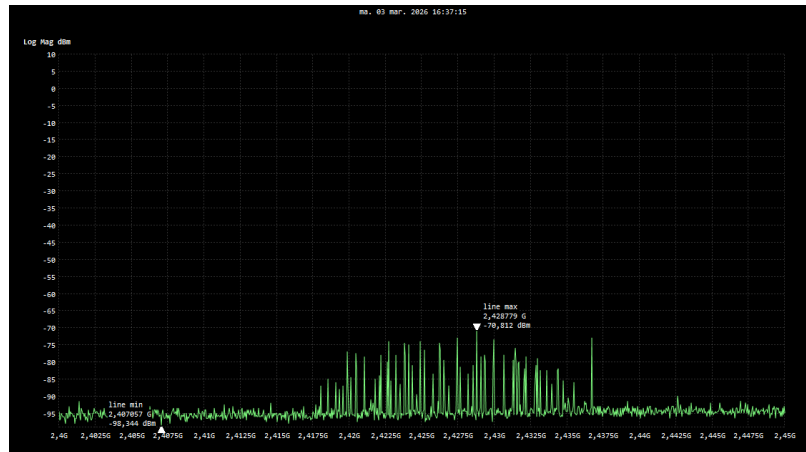


Figura 3-14 Espectro acumulado del enlace de control del *HYT BP S179*.

A diferencia del flujo de datos masivo observado en el *DJI Avata 2*, el enlace del *HYT BP S179* presenta una naturaleza discreta y dinámica. Los resultados obtenidos mediante la monitorización con el analizador de espectro *TinySA* revelan:

- **Distribución Espectral Acumulada:** Como se observa en la representación espectral de la Figura 3-14, la energía no se concentra en un único canal, sino que aparece en múltiples picos distribuidos a lo largo de la banda *ISM* de 2,4 GHz.
- **Mecanismo de Salto de Frecuencia (*FHSS*):** La superposición de capturas evidencia que el transmisor y el receptor alternan su frecuencia de operación siguiendo una secuencia pseudoaleatoria. Este mecanismo permite al dron evitar interferencias puntuales (como un canal *WiFi* saturado), mejorando la robustez de un *hardware* que, por su bajo coste, carece de sistemas avanzados de corrección de errores.

El uso de *FHSS* introduce una dificultad añadida para el bloque de actuación. Una interferencia estática en una frecuencia fija sería ineficaz, ya que el dron simplemente "saltaría" fuera del canal interferido en cuestión de milisegundos. Para neutralizar este tipo de enlaces, se han validado dos estrategias en el trabajo:

- **Barrido Rápido de Frecuencia (*Fast Sweep*):** Generar una señal que recorra cíclicamente toda la banda detectada a una velocidad superior a la tasa de salto del dron. Esto garantiza que, independientemente del canal al que salte el *UAV*, encontrará una ráfaga de interferencia que corromperá la trama de control.
- **Probabilidad de Colisión:** Al cubrir múltiples sub-bandas con el *ADALM-Pluto*, se aumenta drásticamente la probabilidad de que el paquete de sincronización del dron colisione con la señal de ruido generada por el sistema *C-UAS*, forzando la pérdida del enlace.

A continuación, en la tabla 3-4 mostramos la caracterización específica para el *HYT BP S179*, basada en los datos del análisis espectral y la naturaleza del enlace *FHSS*:

Parámetro <i>RF</i>	Observación Experimental	Requisito de Inhibición
Tipo de Enlace	Salto de Frecuencia (<i>FHSS</i>)	Interferencia ágil o de banda ancha
Ocupación Espectral	Discreta (Picos de energía en sub-bandas)	Cobertura de todo el rango de saltos
Ancho de Banda (Instantáneo)	Estrecho (~1-2 MHz por salto)	Barrido rápido (<i>Fast Sweep</i>)
Persistencia	Intermitente (Ráfagas pseudoaleatorias)	Alta densidad temporal de colisión
Resiliencia	Agilidad de frecuencia (Evasión de interferencia fija)	Barrido cíclico superior a la tasa de salto

Tabla 3-4: Características espectrales del *HYT BP S179*.

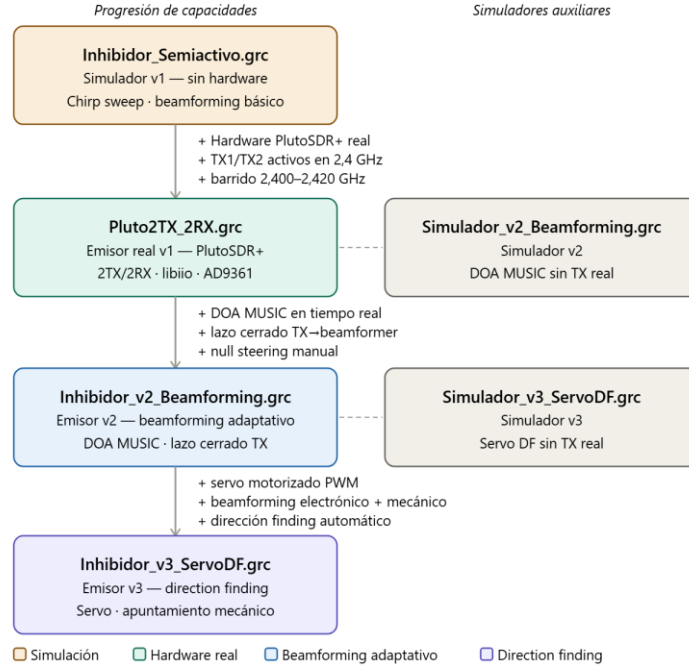
A modo comparativo, en la tabla 3-5 mostramos la caracterización específica conjunta de los dos drones empleados en el trabajo:

Característica	Enlace <i>DJI</i> (Banda Ancha)	Enlace <i>HYT BP</i> (<i>FHSS</i>)
Ocupación	Continua / Persistente	Discreta / Ágil
Ancho de Banda	Elevado (20-40 MHz)	Estrecho por salto (< 2 MHz)
Resiliencia	Alta potencia / Codificación	Agilidad de frecuencia
Técnica de Ataque	Ruido Blanco / <i>CHIRP</i> Ancho	Barrido Rápido (<i>Sweeping</i>)

Tabla 3-5: Comparativa espectral entre *DJI AVATA* y *HYT BP S179*.

3.5 Inhibición en Radiofrecuencia

El tercer y último bloque del sistema cierra el ciclo de decisión denominado *OODA*. Su funcionamiento no es autónomo, sino que constituye una respuesta lógica y justificada tras la validación cruzada de los sensores acústico y de radiofrecuencia.

Figura 3-15 Fases del desarrollo del detector *SIGINT*.

3.5.1 Fundamentos de la Inhibición Selectiva

A diferencia de los sistemas de inhibición convencionales que emiten de forma omnidireccional y permanente, este bloque se rige por el principio de mínima exposición donde existirá activación condicionada en la que solo se genera señal de interferencia tras la confirmación de la firma acústica y la detección de ráfagas *RF* y direccionamiento espacial gracias al estimador *DOA* (*MUSIC/beamforming*) del bloque previo, la energía de inhibición se concentra en el sector angular donde se encuentra el *UAS*, optimizando la eficiencia energética y reduciendo el impacto en sistemas de comunicación legítimos (como redes *WiFi* colindantes).

3.5.2 Modelado Fisicomatemático de la Interferencia

La efectividad de la interdicción se basa en la degradación de la capacidad de canal del receptor del dron (ya sea el mando o la propia aeronave). En ausencia de interferencia, la calidad del enlace viene definida por la *SNR*:

$$SNR = \frac{P_{signal} \cdot G_s}{P_{noise}} \quad (3 - 23)$$

donde P_{signal} es la potencia recibida de la señal útil, G_s la ganancia efectiva del sistema y P_{noise} la potencia de ruido equivalente en banda. Al activar el bloque de actuación, introducimos una componente de interferencia P_{inter} , transformando la métrica en la relación señal a interferencia más ruido (*SINR*), tal como se describe en el apartado 2.7.2:

$$SINR = \frac{P_{signal} \cdot G_s}{P_{noise} + P_{inter}} \quad (3 - 24)$$

El objetivo técnico no es la anulación física de la onda electromagnética, sino la saturación del receptor. Cada esquema de modulación (como *QAM* o *OFDM* usados por *DJI*) posee un umbral mínimo de *SINR* por debajo del cual el *BER* aumenta exponencialmente. Al reducir el *SINR* por debajo de este

umbral, el receptor pierde el sincronismo de trama. En drones comerciales, esto dispara los protocolos de seguridad de la controladora de vuelo (*Fail-Safe*), obligando al dron a aterrizar o regresar al punto de origen.

La inhibición en bandas *ISM* presenta desafíos específicos debido al margen de enlace (*Link Margin*) limitado. Dado que los drones operan cerca del suelo de ruido en rangos largos, una pequeña potencia de interferencia bien dirigida puede ser devastadora para el enlace. Sin embargo, el diseño debe considerar la selectividad en Frecuencia ya que la interferencia debe cubrir el ancho de banda del protocolo detectado (*CHIRP* para *FHSS* o Ruido para Banda Ancha).

3.5.3 Análisis Geométrico-energético de la Interferencia

La eficacia de la inhibición no depende exclusivamente de la potencia bruta radiada, sino de la relación espacial entre el dron, el operador legal y el sistema *C-UAS*. Para modelar este escenario, se utiliza la Ecuación de Friis, que define la potencia recibida (P_r) en campo lejano:

$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi R} \right)^2 \quad (3 - 25)$$

donde R es la distancia entre el transmisor y el receptor. Este modelo permite entender la interdicción como una competencia por el control del receptor del dron.

Para que el sistema sea efectivo, la potencia de interferencia (*jamming*, J) que llega al dron debe superar por un margen de seguridad a la señal de control útil (Signal, S). Si el mando del operador está a una distancia R_s y nuestro inhibidor a una distancia R_j , la condición de éxito se define como:

$$\frac{P_j G_j}{R_j^2} \gg \frac{P_s G_s}{R_s^2} \quad (3 - 26)$$

De esta desigualdad se extraen dos aspectos fundamentales que validan la arquitectura de este *TFG*:

- **Ventaja de Proximidad:** Dado que la potencia decae con el cuadrado de la distancia ($1/R^2$), si el sistema *C-UAS* se despliega cerca del área protegida, puede neutralizar el enlace incluso con una potencia de transmisión P_j muy inferior a la del mando del operador (P_s).
- **Eficiencia por Directividad:** La ganancia de la antena inhibidora (G_j) es un multiplicador directo de la efectividad. En lugar de emitir potencia en todas direcciones ($G_j=1$), el uso del estimador *DOA* permite concentrar el haz, multiplicando la potencia efectiva radiada (*EIRP*) hacia el objetivo sin aumentar el consumo de batería ni interferir con otros sectores.

En este punto se cierra el círculo de diseño: bloque de acústica para detectar y clasificar la amenaza, bloque de Radiofrecuencia (*DOA*) para localizar la posición angular (θ) del objetivo para maximizar G_j y bloque de actuación para aplicar la potencia justa en la dirección exacta, logrando la interdicción con el mínimo impacto colateral.

3.5.4 Direccionamiento y formación de haz en transmisión

El bloque de inhibición no opera como una fuente de ruido aislada, sino como un sistema de antena inteligente (*Smart Antenna*). El direccionamiento del lóbulo principal en transmisión se modela de forma matemática análoga al *beamforming* de recepción, permitiendo una interdicción quirúrgica.

Para un array lineal de M elementos, la señal total radiada en el espacio libre $S_{rad}(t, \theta)$ es el resultado de la interferencia constructiva de las señales emitidas por cada antena, ponderadas por un vector de pesos complejos w :

$$S_{rad}(t, \theta) = \mathbf{w}^H \mathbf{a}(\theta) s_{tx}(t) \quad (3 - 27)$$

donde $s_{tx}(t)$ es la señal de interferencia generada (por ejemplo, un barrido *CHIRP*) y $\mathbf{a}(\theta)$ es el vector de dirección que define el desfase espacial según el ángulo θ .

La eficacia del sistema reside en la configuración del patrón de radiación $P(\theta)$. Para garantizar que la energía de inhibición se concentre exclusivamente sobre la amenaza detectada, se selecciona el vector de pesos de modo que coincida con el conjugado del vector de dirección en la dirección del objetivo θ_0 :

$$\mathbf{w} = \mathbf{a}(\theta) \quad (3 - 28)$$

Bajo esta condición, la función de radiación resultante maximiza la ganancia en θ_0 :

$$P(\theta) = |\mathbf{w}^H \mathbf{a}(\theta)|^2 \quad (3 - 29)$$

Esta relación matemática evidencia que el bloque de inhibición hereda directamente la información espacial procesada por el algoritmo *MUSIC* en el bloque *RF*. No se trata simplemente de generar interferencia omnidireccional, lo cual sería energéticamente ineficiente y causaría interferencias colaterales innecesarias, sino de redistribuir la energía espacialmente de manera óptima.

3.5.5 Caracterización espectral de la interferencia

La efectividad de la interdicción no reside únicamente en la potencia radiada, sino en la congruencia espectral entre la señal interferente ($S_i(f)$) y la señal del objetivo ($S_u(f)$). Para que la inhibición sea exitosa, debe existir un solapamiento significativo en el dominio de la frecuencia que sature el ancho de banda del receptor del *UAV*. Dependiendo del protocolo detectado (*O4* de *DJI* o *FHSS* del *HYT BP*), el sistema puede conmutar entre cuatro naturalezas espectrales:

- **Ruido de Banda Ancha (Barrage jamming):** Eleva el suelo de ruido en todo el espectro de 2,4 GHz. Es efectivo, pero energéticamente ineficiente.
- **Barrido en Frecuencia (Sweep jamming):** Una señal senoidal que recorre rápidamente el ancho de banda. Es ideal para batir sistemas de salto de frecuencia (*FHSS*) como el del *HYT BP SI79*.
- **Señal Modulada Pseudoaleatoria:** Simula tráfico legítimo para confundir los algoritmos de sincronización del receptor.
- **Interferencia Coherente Dirigida:** Utiliza la información del estimador *DOA* para concentrar la densidad espectral de potencia (*PSD*) exactamente en el vector espacial del dron.

Matemáticamente, la degradación del enlace depende de la integral del producto de ambas densidades espectrales dentro del filtro del receptor donde si el solapamiento es parcial, el receptor del dron podría utilizar técnicas de filtrado para recuperar la señal. Por ello, la estrategia del *PlutoSDR* en este trabajo se centra en maximizar la densidad espectral en las sub-bandas críticas de telemetría y control.

3.5.6 Limitaciones Físicas y Hardware

La transición de la teoría a la práctica enfrenta restricciones impuestas por las leyes de la física y las capacidades del *hardware SDR* empleado. Respecto a la geometría de propagación, en régimen de campo lejano, la potencia decrece según $1/R^2$. Esto convierte la ubicación física del *C-UAS* en un factor crítico; estar más cerca del dron que su propio operador garantiza una ventaja competitiva en el presupuesto de enlace (*Link Budget*). Por otro lado, el *multipath* y las sombras debidas a obstáculos urbanos afectan de

forma no homogénea a la señal. Un dron volando tras un edificio puede quedar protegido de la interferencia, pero mantener el enlace con su mando si este tiene una mejor línea de vista.

Respecto a las restricciones *hardware*, los amplificadores del *PlutoSDR* deben operar en su zona lineal para evitar la generación de armónicos espurios que interfieran en bandas no deseadas.

3.5.7 Validación experimental de la respuesta: Emisión de la Interferencia

Una vez detectada y localizada la amenaza, el sistema activa el bloque de interdicción. Para validar su funcionamiento, se ha monitorizado la salida del propio inhibidor, analizando la naturaleza de la señal sintetizada y su capacidad de cobertura espectral. La señal de barrido en frecuencia, implementada mediante bloques de control dinámico en el *SDR*, presenta las siguientes características observadas en las capturas experimentales (Figura 3-16):

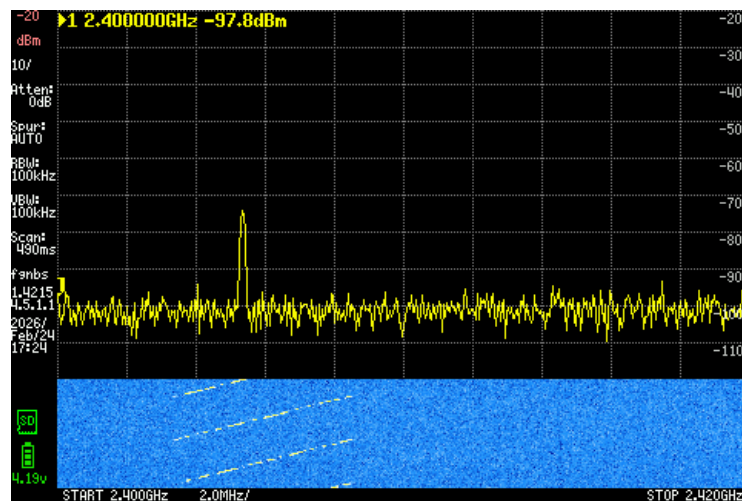


Figura 3-16 Espectro y *waterfall* de la señal de interferente.

En la representación superior de la Figura 3-16 podemos observar el espectro instantáneo, donde se identifica el paso de la portadora como un pico de potencia de aproximadamente -80 dBm. Teniendo en cuenta un suelo de ruido de -105 dBm, el sistema logra un margen de interferencia de 25 dB en el punto de observación, lo cual es suficiente para saturar receptores comerciales de corto y medio alcance.

En la representación inferior de la Figura 3-16 podemos observar la traza diagonal característica en los espectrogramas con una firma inequívoca de una señal *CHIRP*. Esta pendiente representa el cambio de frecuencia (df/dt) programado. La continuidad de estas trazas confirma que el barrido recorre el espectro de forma ininterrumpida, sin dejar huecos temporales que el dron podría aprovechar para mantener el sincronismo.

El objetivo de este barrido es forzar la pérdida de integridad de los datos en el receptor del *UAV*. Al coincidir la frecuencia del inhibidor con la del canal activo del dron es de esperar que haya un aumento de la *BER* ya que el error de bit aumenta hasta que los algoritmos de corrección (*FEC*) no pueden reconstruir el paquete, la pérdida de sincronismo ya que el receptor pierde las balizas (*beacons*) de sincronización necesarias para el salto de frecuencia (*FHSS*) o la demodulación *OFDM* y la activación de modos seguros ya que como resultado de la persistencia de la interferencia, el dron interpreta una pérdida total del enlace de control (*Radio Link Loss*), disparando protocolos de protección como el *RTH* o el aterrizaje controlado.

A diferencia de un ruido blanco que diluye la energía en toda la banda, el barrido concentra toda la potencia disponible del *PlutoSDR* en un ancho de banda instantáneo muy estrecho. Esto permite maximizar la densidad espectral de potencia en el punto de colisión con la señal del dron y cubrir toda la banda *ISM* de 2,4 GHz de forma secuencial, garantizando efectividad tanto contra enlaces de banda ancha (*DJI*) como contra sistemas ágiles de saltos de frecuencia (*HYT BP*).

4 RESULTADOS Y VALIDACIÓN

4.1 Entorno y condiciones experimentales

Las pruebas experimentales del sistema *C-UAS* se realizaron en las instalaciones del Centro Universitario de la Defensa (*CUD*) situadas en el recinto de la Escuela Naval Militar. El entorno seleccionado permite realizar ensayos tanto en espacios abiertos como en interiores, facilitando la evaluación del comportamiento del sistema bajo diferentes condiciones de propagación acústica y radioeléctrica.

La experimentación en exteriores se desarrolló en el área correspondiente a la pista militar de instrucción, mostrada en la figura 4-1. Este emplazamiento ofrece un espacio abierto de dimensiones suficientes para realizar vuelos controlados con *UAS*, manteniendo al mismo tiempo unas condiciones de seguridad y supervisión adecuadas para la realización de las pruebas.



Figura 4-1 Vista satelital ENM. Elaboración propia [31].

Durante los ensayos se registraron condiciones meteorológicas caracterizadas por viento predominante de componente oeste (poniente). Este factor introdujo un elemento adicional de complejidad en la experimentación, ya que el viento puede afectar tanto a la propagación acústica de la señal generada por el *UAS* como a la estabilidad de su trayectoria de vuelo.

No obstante, el área de experimentación presentaba ausencia de obstáculos relevantes en el entorno inmediato, lo que permitió garantizar en todo momento la línea de visión directa (*LOS*) entre el operador

y el *UAS*. Esta condición resulta especialmente importante para asegurar la correcta operación del sistema durante las pruebas y para evitar interferencias adicionales derivadas de apantallamientos o reflexiones en el entorno.

La elección de este escenario permitió reproducir condiciones operativas realistas, manteniendo simultáneamente un grado adecuado de control sobre las variables experimentales. De este modo, los resultados obtenidos pueden considerarse representativos del comportamiento del sistema en un entorno abierto típico, permitiendo evaluar sus prestaciones en términos de detección y funcionamiento general [27, 32].

El entorno interior presenta una configuración longitudinal tipo pasillo con geometría casi rectangular y presencia de discontinuidades estructurales, tales como aperturas laterales y cambios de sección. Este tipo de entorno genera un comportamiento acústico dominado por reflexiones especulares, propagación guiada y fenómenos de reverberación acumulativa.

La existencia de una zona de transición (estrechamiento estructural debido a la puerta contraincendios) introduce efectos adicionales de difracción y concentración energética, afectando directamente a los umbrales de detección del sistema.

El recorrido del *UAS* se ha diseñado siguiendo el eje principal del pasillo, finalizando en un entorno semiconfinado (estudio), lo que permite evaluar el comportamiento del sistema en condiciones de propagación tanto guiada como altamente reverberante.

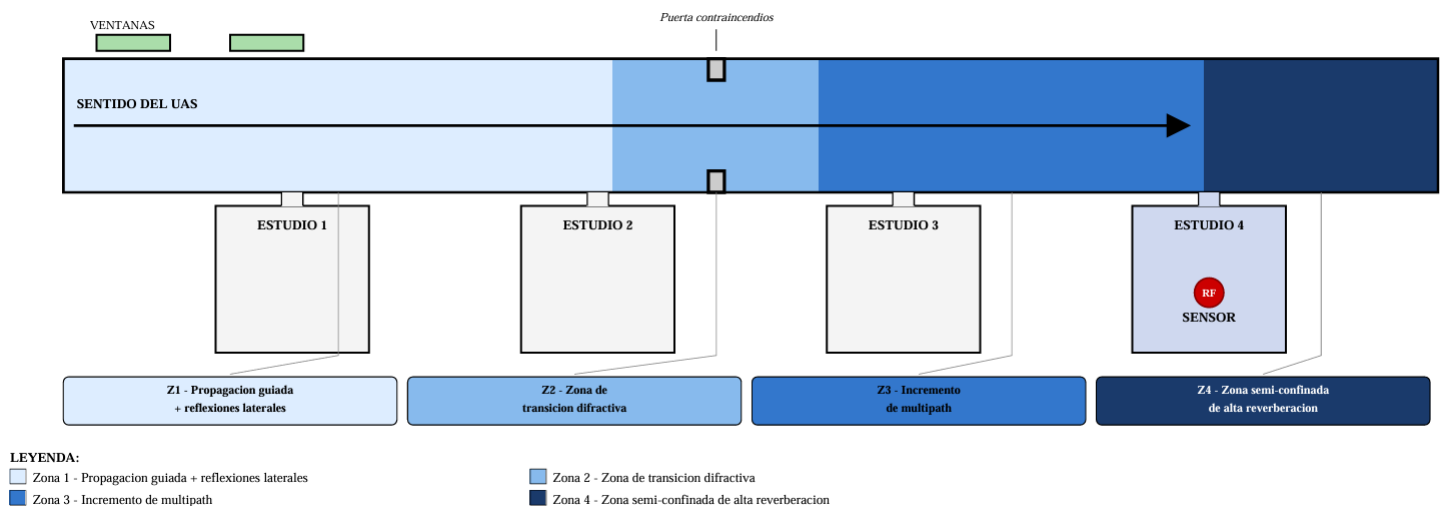


Figura 4-2 Representación esquemática del entorno de ensayo en interiores.

4.2 Detección Acústica

4.2.1 Disposición de los Medios

Para la obtención de los resultados acústicos se empleó un sistema de adquisición basado en un array de micrófonos *MEMS* y un micrófono individual, conectados a un ordenador portátil encargado del registro y procesamiento de las señales captadas. Este sistema descrito en el apartado 3.1.1 permitió capturar las emisiones acústicas generadas durante los ensayos y analizar su comportamiento en el dominio espectral.

Con el fin de evaluar el funcionamiento del sistema en diferentes condiciones de propagación acústica, se realizaron pruebas tanto en entornos interiores como exteriores. Los ensayos en interior permitieron analizar el comportamiento del sistema en un entorno controlado con presencia de reflexiones acústicas, mientras que las pruebas en exterior se realizaron en un entorno abierto dentro del

recinto de la Escuela Naval Militar, permitiendo evaluar el rendimiento del sistema en condiciones más próximas a un escenario operativo real.



Figura 4-3 Sistema de adquisición acústica empleado durante las pruebas experimentales.

Las siguientes figuras muestran la configuración del sistema de adquisición y la distribución de los sensores durante la realización de los ensayos experimentales.



Figura 4-4 Configuración del sistema de adquisición acústica en interiores.

Las pruebas en interior se realizaron en un entorno controlado con el objetivo de analizar el comportamiento del algoritmo de detección en condiciones de propagación sonora confinada.

A diferencia de los entornos exteriores, donde la energía acústica se disipa progresivamente con la distancia siguiendo un modelo de propagación aproximadamente esférico, en espacios confinados el sonido interactúa continuamente con las superficies del entorno (paredes, techo y suelo), generando fenómenos de reflexión, eco y reverberación. Estas reflexiones pueden provocar que parte de la energía acústica emitida por el dron regrese al sensor tras múltiples trayectorias de propagación, incrementando temporalmente la energía total registrada por el micrófono.

Este fenómeno tiene dos consecuencias principales para los sistemas de detección basados en energía espectral. Por un lado, puede incrementar la *SNR* efectiva en determinadas bandas de frecuencia, facilitando la detección temprana de la firma acústica del dron. Por otro lado, la superposición de señales directas y reflejadas puede producir refuerzos constructivos en los armónicos característicos de las hélices, generando picos energéticos más intensos en el espectrograma.

En [33] se señala que la detección acústica resulta especialmente adecuada en entornos interiores o urbanos debido a que las distancias de operación son reducidas y la proximidad entre sensor y dron permite una captación efectiva de la señal sonora, incluso cuando existen obstáculos visuales entre ambos. Sin embargo, también advierte que las superficies reflectantes pueden introducir ecos e interferencias en la señal acústica, lo que puede modificar la forma en que el sensor percibe la firma sonora del *UAV*.

En consecuencia, el entorno interior constituye un escenario particularmente interesante para la validación del detector acústico: por un lado, favorece la detección temprana debido a la acumulación de energía sonora; por otro, obliga a diseñar algoritmos de decisión robustos capaces de distinguir entre la firma acústica persistente del dron y las perturbaciones generadas por las reflexiones del entorno.

Las figuras presentadas a continuación ilustran el comportamiento del detector en estas condiciones, mostrando cómo la energía espectral en la banda característica del *UAS* supera el umbral de detección durante la aproximación del dron.

Las figuras 4-5, 4-6 y 4-7 muestran la evolución del proceso de detección acústica de un *UAS* en entornos interiores mediante el programa Detector de *UAS*, disponible en el repositorio GitHub del proyecto [30].

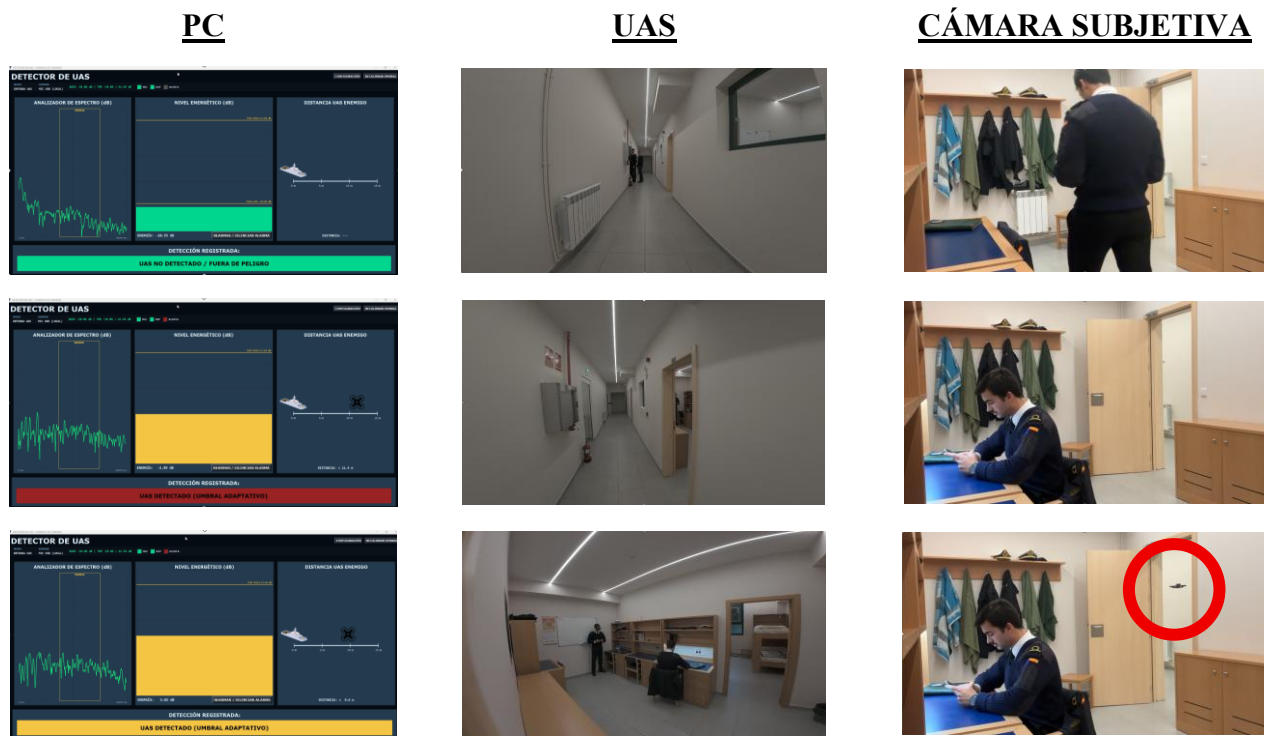
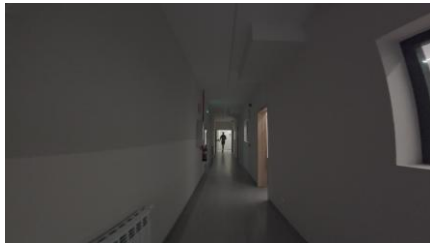


Figura 4-5 Progresión de la detección acústica en interior mediante Detector_Acústico.

En la primera fase el sistema permanece en estado de vigilancia mientras el dron se encuentra a mayor distancia, manteniéndose la energía espectral por debajo del umbral adaptativo. A medida que el *UAS* se aproxima por el pasillo, las componentes armónicas generadas por su sistema de propulsión comienzan a destacar sobre el ruido de fondo, produciendo un incremento progresivo del nivel energético registrado por el algoritmo. Finalmente, cuando el dron alcanza una distancia suficiente, el umbral de detección es superado y el sistema registra la presencia del *UAS*, evidenciando la capacidad del detector para identificar su firma acústica incluso en condiciones de propagación propias de espacios confinados.

PC



UAS

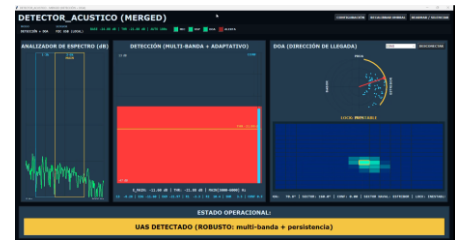


Figura 4-6 Progresión de la detección acústica mediante Detector_Acustico (MERGED).

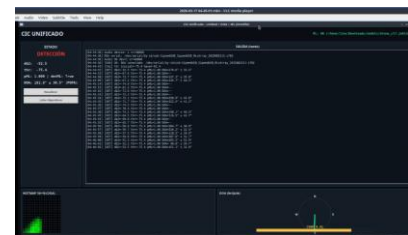
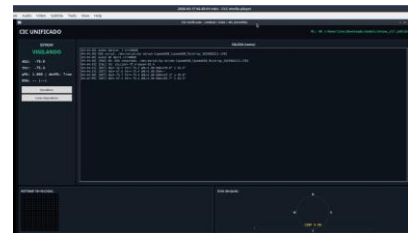
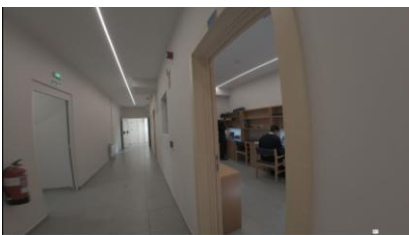
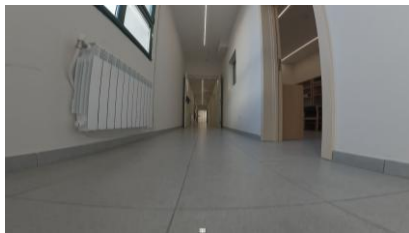


Figura 4-7 Progresión de la detección acústica mediante cic_onefile.

4.2.2 Resultados en exteriores

La experimentación acústica en exteriores se llevó a cabo en la pista militar de instrucción del recinto de la Escuela Naval Militar, descrita en el apartado 4.1, bajo condiciones de viento predominante de componente oeste. A diferencia del entorno interior, en campo abierto la energía acústica emitida por el UAS se disipa progresivamente con la distancia siguiendo un modelo de propagación aproximadamente esférico, sin la contribución energética de reflexiones ni reverberación. Esto implica que la relación señal-ruido efectiva en el sensor decrece de forma más acusada con la distancia, estableciendo un límite de detección más restrictivo que el observado en espacios confinados.

A este factor se añade la influencia del viento y la biosfera, materializada en gaviotas. El viento introduce tanto ruido aerodinámico sobre la membrana del micrófono como variaciones en la velocidad

de propagación del sonido, pudiendo desplazar o enmascarar las componentes armónicas características del sistema de propulsión del dron en determinadas orientaciones respecto al sensor. Las gaviotas introducen picos debido a su graznido aleatorio. No obstante, la ausencia de obstáculos en el área de pruebas garantizó en todo momento la trayectoria de propagación directa entre el *UAS* y el array de micrófonos, permitiendo evaluar el rendimiento real del detector en condiciones de campo abierto representativas de un escenario operativo típico.

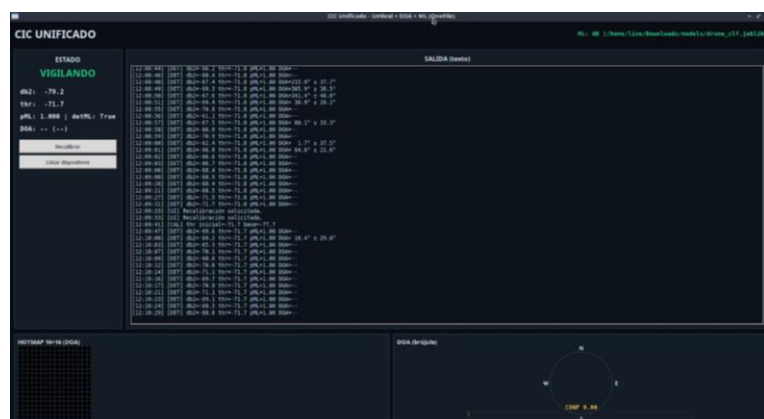


Figura 4-8 Resultados de detección acústica. Figuras de la Izquierda visión subjetiva, derecha interfaz Detector_Acústico.



Figura 4-9 Resultados de detección acústica y adquisición de DOA.

50 m



30 m

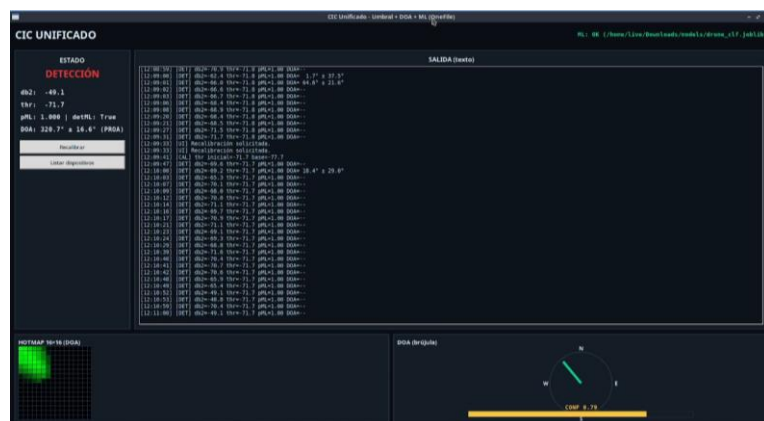


Figura 4-10 Desarrollo de los estados de alerta de la aplicación “cic_onefile”.

La aplicación “cic_onefile”, que integra un algoritmo de clasificación basado en aprendizaje automático para la detección de *UAS* en entornos exteriores, ha demostrado ser capaz de identificar patrones acústicos característicos de drones en condiciones reales. No obstante, durante la fase de validación experimental se ha observado una elevada tasa de falsas alarmas, especialmente en escenarios con ruido ambiental no estacionario. Este comportamiento se explica por la propia naturaleza del modelo de aprendizaje, que, aun habiendo sido entrenado con conjuntos de datos representativos, presenta limitaciones en su capacidad de generalización frente a perturbaciones del entorno tales como ruido impulsivo (tráfico, viento o impactos), fuentes acústicas mecánicas con firmas espectrales similares (vehículos o maquinaria) y la variabilidad inherente del entorno exterior. Como consecuencia, el sistema tiende a sobre-detectar eventos cuando el umbral de decisión del clasificador no está suficientemente restringido, lo que compromete la fiabilidad operativa en condiciones reales.

Con el objetivo de mitigar esta limitación, se plantea la integración del módulo basado en aprendizaje automático dentro de una arquitectura unificada, como la implementada en la aplicación “Detector Acústico (MERGED)”. Esta aproximación permite evolucionar desde un sistema de detección aislado a un sistema de fusión de evidencias, en el que la decisión final no depende de un único algoritmo, sino de la combinación de múltiples criterios complementarios, entre los que se incluyen la detección energética basada en umbral adaptativo, el análisis espectral en bandas características, la persistencia temporal mediante criterios N-de-M, la estimación de la dirección de llegada de la señal acústica y la clasificación mediante el modelo de aprendizaje automático. Adicionalmente, se identifica como mejora clave la incorporación de un módulo de configuración operativa que permita ajustar dinámicamente los parámetros del sistema en función del entorno de despliegue como está explicado en Bloque I - Detección Acústica del Anexo III: Descripción de los programas desarrollados. En este contexto, el módulo de aprendizaje automático pasa a desempeñar un papel complementario y no decisor, actuando como refuerzo probabilístico dentro del sistema global y reduciendo su impacto directo en la generación de falsas alarmas.

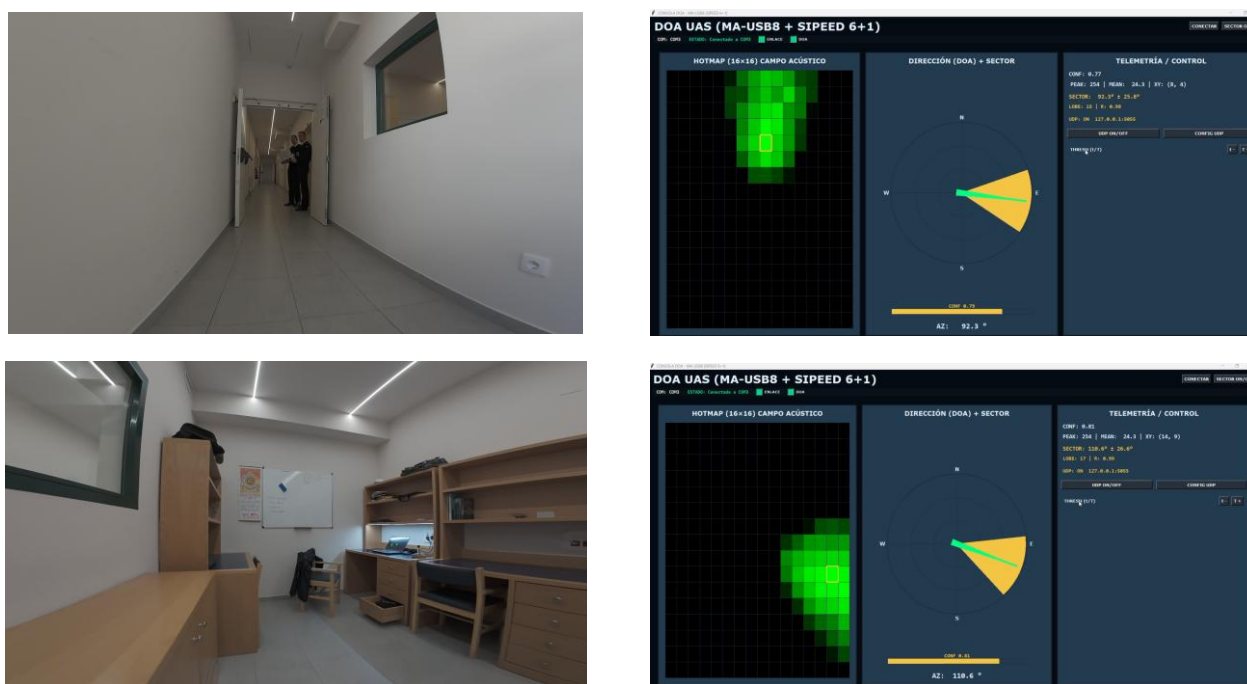


Figura 4-11 Progresión de la detección acústica en interior mediante DOA-UAS.



Figura 4-12 Prueba de campo del sistema de estimación *DOA* acústico mediante *DOA UAS*.

4.3 Detección en el Espectro Electromagnético

4.3.1 Disposición de los Medios

Para la obtención de los resultados asociados al bloque de radiofrecuencia se empleó un sistema basado en radios definidas por *software* (SDR) y antenas direccionales, controlado desde un ordenador portátil encargado de la generación de las señales de interferencia y del análisis del espectro radioeléctrico. Este sistema permitió monitorizar las emisiones asociadas al enlace de comunicaciones del UAS y evaluar el efecto de distintas estrategias de interferencia.

Los ensayos se realizaron tanto en entorno interior como en exterior, con el objetivo de analizar el comportamiento del sistema en diferentes condiciones de propagación electromagnética. En interior se llevaron a cabo pruebas controladas orientadas a observar el comportamiento del enlace radio y la interacción con la señal interferente, mientras que en exterior se desplegó una configuración de antenas destinada a evaluar el funcionamiento del sistema en condiciones más próximas a un escenario real de operación.

Las figuras siguientes muestran la configuración experimental empleada durante los ensayos y los dispositivos utilizados para la generación y monitorización de las señales en radiofrecuencia.

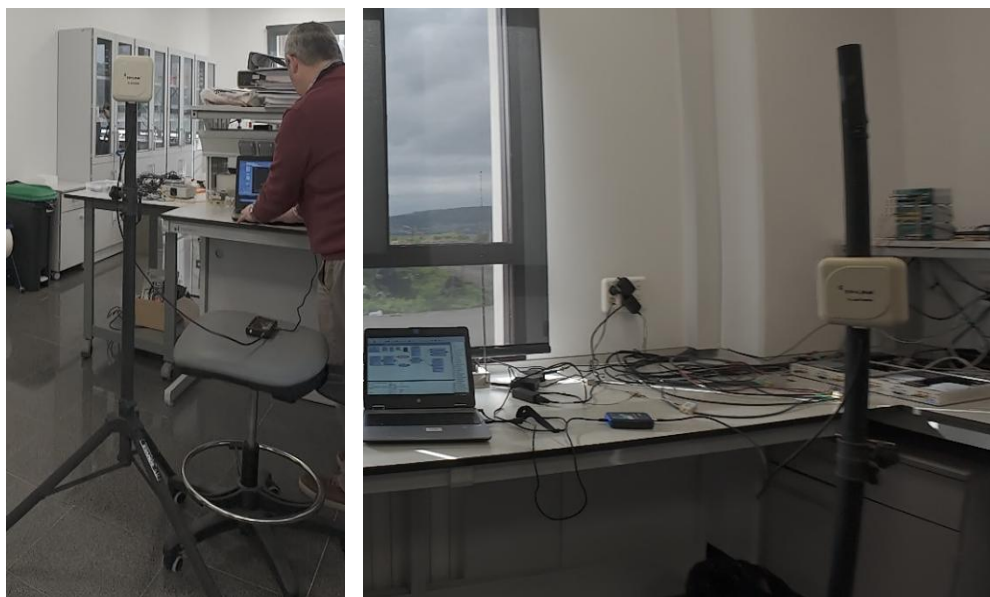


Figura 4-13 Disposición de antenas empleadas durante las pruebas de interferencia en interior.

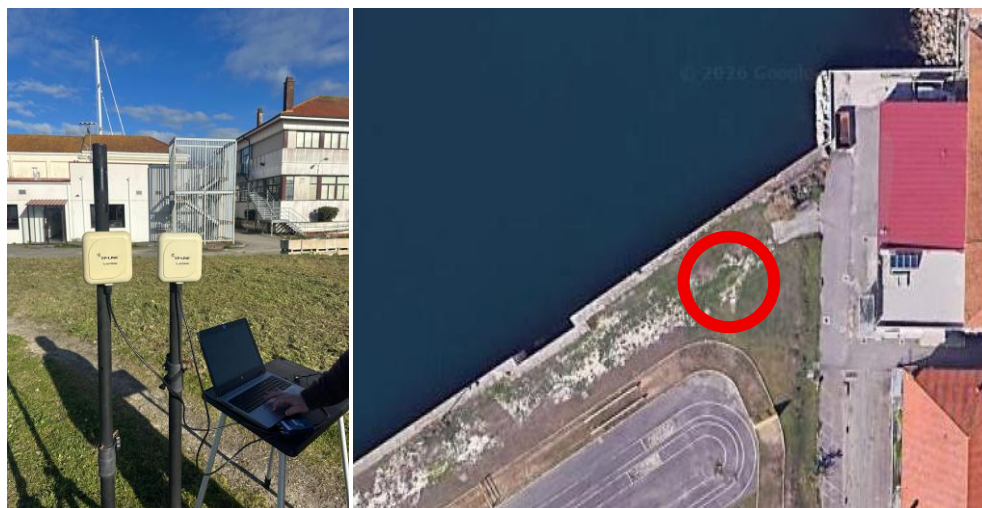


Figura 4-14 Dispositivo de interferencia direccional utilizado en las pruebas de campo.

4.3.2 Resultados

La aplicación de estimación de dirección de llegada en la recepción [Figura 4-15] permitió detectar la presencia de una emisión en la banda *WiFi* analizada, obteniéndose una dirección de llegada aproximada en el entorno de los 20° mediante el algoritmo *MUSIC*. Este resultado confirma la viabilidad del empleo de técnicas *DOA* para la localización angular de emisiones radioeléctricas asociadas al enlace del sistema *UAS*. No obstante, la medida obtenida no puede considerarse plenamente fiable desde el punto de vista métrico, ya que el montaje experimental empleado no incorporó una corrección precisa mediante baliza de calibración. En consecuencia, la referencia espacial del sistema quedó condicionada por la disposición física de las antenas receptoras, instaladas sobre dos trípodes independientes, lo que introduce incertidumbres en la separación relativa entre elementos, en su alineamiento angular y en la coherencia geométrica del array.

Estas desviaciones tienen un impacto directo sobre el rendimiento del algoritmo *MUSIC*, cuya precisión depende de forma crítica del conocimiento exacto de la geometría del sistema de captación. En un array ideal, la separación entre sensores, su orientación y su estabilidad espacial deben ser conocidas con precisión, ya que pequeños errores en dichas magnitudes se traducen en sesgos en la estimación angular. Por ello, aunque el sistema muestra una captación consistente de una fuente incidente en torno a los 20° , el valor angular obtenido debe interpretarse como una estimación orientativa y no como una medida exacta de la dirección real de la emisión.

Desde el punto de vista experimental, el ensayo sí resulta útil para validar el concepto de funcionamiento: el sistema es capaz de recibir la señal, procesarla espectralmente y generar una estimación angular coherente con la presencia de una fuente emisora dominante en el entorno observado. Sin embargo, para considerar esta funcionalidad como una capacidad de localización fiable sería necesario evolucionar el montaje hacia una arquitectura más rígida y calibrada, con una disposición fija de las antenas, una separación inter-elementos perfectamente conocida y un procedimiento de calibración mediante baliza de referencia que permitiera compensar errores de fase, desfases de canal y tolerancias mecánicas del sistema. Solo bajo estas condiciones podría evaluarse con rigor la precisión real del algoritmo *MUSIC* en este escenario de recepción.

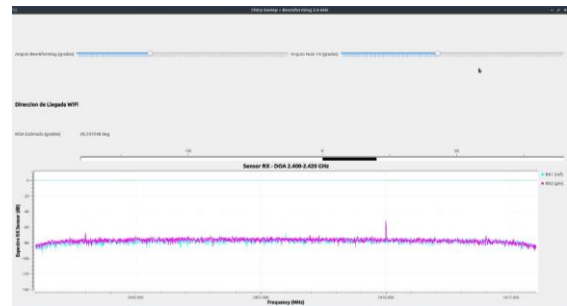


Figura 4-15 Resultado experimental de seguimiento in-situ de *UAS* con "*Inhibidor_v2_RX_Beamforming*".

4.4 Inhibición en Radiofrecuencia

4.4.1 Justificación del escenario de prueba: por qué solo exterior

A diferencia del subsistema de detección acústica, cuyas pruebas se extendieron tanto a entornos interiores como exteriores, la experimentación del subsistema de inhibición en radiofrecuencia se circunscribió exclusivamente a escenarios al aire libre. Esta decisión responde a una motivación técnica de fondo: los enlaces digitales empleados por los *UAS* comerciales modernos operan en las bandas de 2,4 GHz y 5,8 GHz, frecuencias caracterizadas por una capacidad de penetración limitada en estructuras sólidas. Paredes, forjados y elementos constructivos típicos de un espacio confinado introducen pérdidas de propagación adicionales que pueden superar fácilmente los 15-20 dB respecto a una trayectoria en

campo abierto, atenuando severamente la señal del enlace C2 y de vídeo antes incluso de que la interferencia actúe sobre él.

En consecuencia, un *UAS* que opere en el interior de un edificio ya partiría de una situación de enlace degradado por la propia arquitectura del espacio. Bajo estas condiciones, la relación señal-ruido del receptor del dron sería intrínsecamente inferior a la del escenario exterior, lo que implica que el margen de interferencia necesario para interrumpir el enlace sería menor y que la vulnerabilidad del sistema ante cualquier señal perturbadora presente en la banda aumentaría proporcionalmente. Inhibir un enlace ya debilitado por la penetración arquitectónica es, por tanto, un problema técnicamente menos exigente que hacerlo en exteriores, donde la señal llega al *UAS* sin pérdidas adicionales por obstáculos. Validar el sistema en el escenario más desfavorable (campo abierto con línea de visión directa) garantiza que los resultados obtenidos son representativos del límite de prestaciones del inhibidor y que cualquier aplicación en entorno confinado quedaría cubierta por los mismos márgenes con mayor holgura.

4.4.2 Ensayo estático - degradación del enlace FPV

Los resultados obtenidos evidencian una degradación progresiva y reversible del enlace de comunicaciones del *UAS* en presencia de la señal interferente generada por el sistema *C-UAS*.

La Figura 4-16 muestra la representación espectral y temporal de la señal interferente generada por el sistema inhibidor durante los ensayos de inhibición *RF*, obtenida mediante el analizador de espectro *TinySA* en modo *waterfall*. Esta modalidad de visualización combina la representación frecuencial instantánea en el panel superior con una representación temporal acumulada en el panel inferior, en la que el eje vertical codifica el tiempo transcurrido y el color refleja la densidad espectral de potencia, permitiendo evaluar simultáneamente la forma espectral de la señal emitida y su comportamiento dinámico a lo largo del ensayo.

En ambas capturas se aprecia el patrón de barrido *CHIRP* característico del inhibidor: las trazas diagonales del *waterfall* inferior evidencian el desplazamiento lineal de la frecuencia instantánea a través de la banda 2,400-2,420 GHz de forma cíclica. La comparación entre ambos ensayos revela una diferencia de 5 dB en el nivel del pico de portadora detectado, situándose en -101,5 dBm para el *DJI Avata 2* y en -96,5 dBm para el *HYT BP S179*, diferencia que, como se analiza en los apartados siguientes, guarda relación directa con las características espectrales de los protocolos de enlace de cada plataforma y con su distinta respuesta ante la interferencia generada.

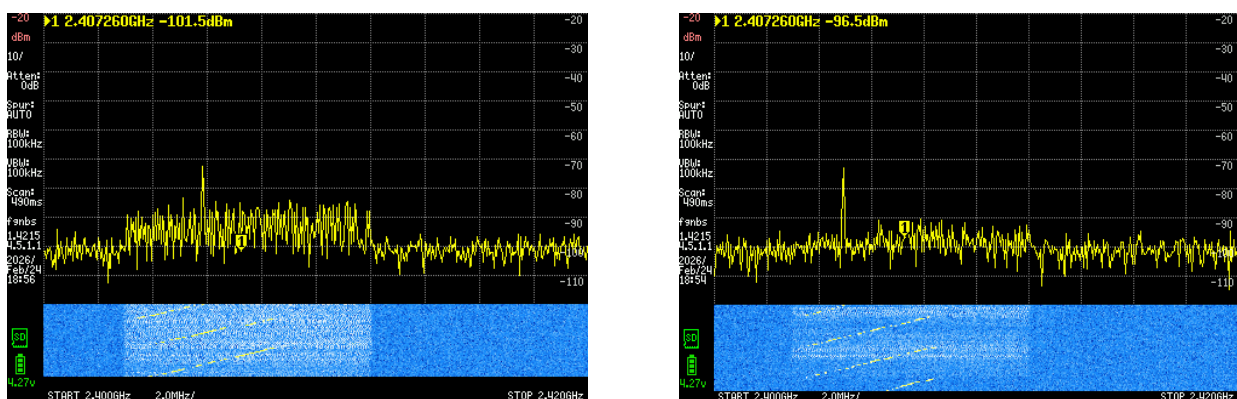


Figura 4-16 Representación espectral y *waterfall* de la señal interferente sobre las comunicaciones del *Avata 2*, izquierda, y el *HYT BP S179*, derecha.

Durante los ensayos de interferencia sobre el enlace de control y vídeo del *UAS* se utilizó la interfaz de visualización de las *DJI Goggles 3* [34], como herramienta de monitorización del estado del enlace digital aire-tierra. Esta interfaz proporciona en tiempo real diversos parámetros del sistema de

comunicaciones, permitiendo observar la degradación progresiva del enlace cuando se introduce interferencia electromagnética en la banda de operación.



Figura 4-17 Ajustes predeterminados de la unidad transmisora *DJI Goggles 3*.

Entre los indicadores más relevantes para la evaluación de la efectividad de la perturbación se encuentra la tasa de bits del enlace (Mbps), número 9 de la Figura 4-18, directamente relacionada con la capacidad del sistema para mantener la transmisión de vídeo digital bajo determinadas condiciones de *SNR*. Durante las pruebas se monitoriza la reducción de la tasa de datos, así como la aparición de pérdidas de enlace, aumento de latencia o avisos de desconexión, fenómenos que evidencian la degradación del canal radioeléctrico producida por la señal interferente.



Figura 4-18 Interfaz *FPV* de las *DJI Goggles 3*, tasa de bits es el número 9 [34].

Durante los ensayos experimentales se evaluó el comportamiento del enlace digital de vídeo entre el *UAS* y las *DJI Goggles 3* bajo condiciones de perturbación electromagnética dirigida. La monitorización se realizó mediante la interfaz *FPV*, que proporciona en tiempo real parámetros de enlace como tasa de bits de transmisión, intensidad de señal, telemetría y estado de conexión.

La geometría del ensayo se configuró de forma que las *DJI Goggles 3* (transmisor/estación de control), el *UAS* y el sistema interferente formaban un triángulo rectángulo. La distancia entre las gafas y el dron correspondía aproximadamente a la hipotenusa del triángulo (≈ 40 m), mientras que la

separación entre las gafas y el sistema interferente constituía el cateto contiguo (≈ 39 m) y la distancia entre el interferente y el UAS el cateto opuesto (≈ 8 m). Esta disposición permitió aproximar un escenario en el que el sistema interferente actuaba en proximidad relativa al receptor del enlace.

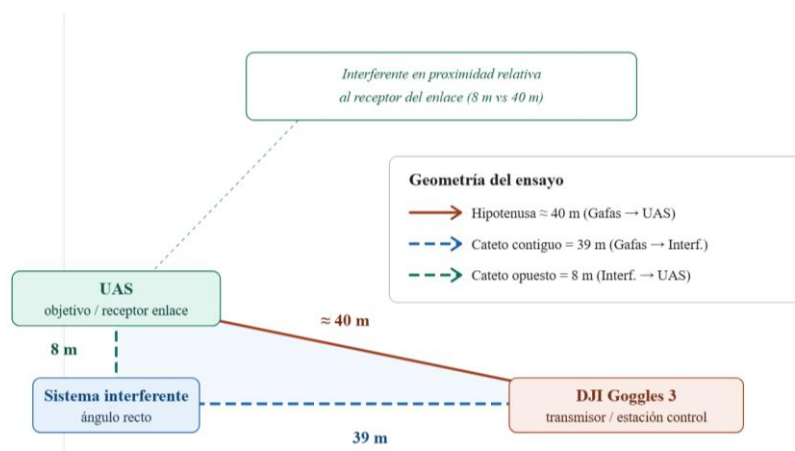
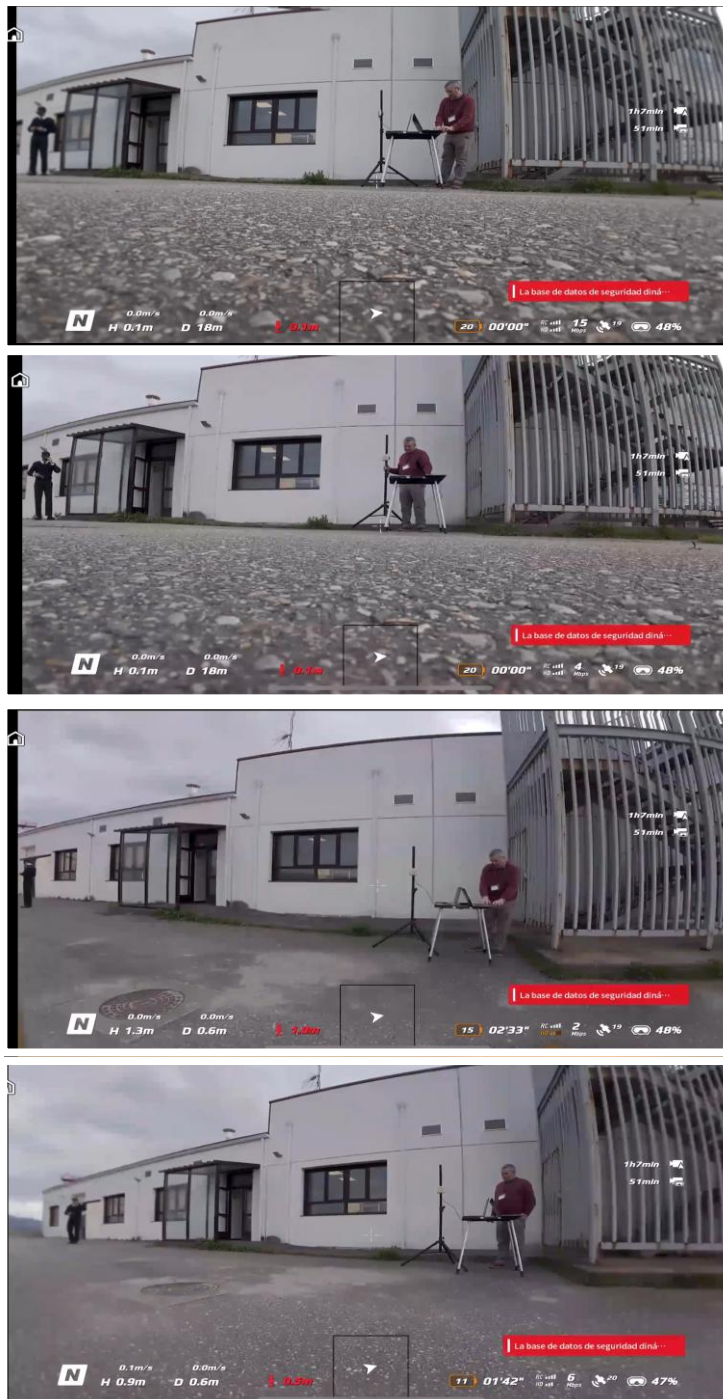


Figura 4-19 Geometría del ensayo de inhibición RF.

En la primera fase del experimento se observa un enlace de vídeo funcional, aunque degradado, caracterizado por una tasa de bits reducida pero aún suficiente para mantener la transmisión de información. Este comportamiento indica que el sistema de comunicaciones mantiene un margen operativo pese a la presencia de interferencias de fondo o limitaciones geométricas en la propagación.

En la figura 4-20 se observa a continuación la degradación de la transmisión de vídeo conforme la interferencia actúa sobre el UAS.



Dron posado con motores alimentados, las antenas inhibidoras apuntan a las gafas emisoras de los comandos.

Interferencia se dirige al dron.

Dron levanta el vuelo y experimenta la mayor reducción de intercambio de información, 2 Mbps.

La interferencia parece haber dejado secuelas, pues la tasa de bits no se recupera.

Figura 4-20 Secuencia de degradación del enlace *FPV* del *UAS* durante la aplicación de interferencia.

Posteriormente, al orientar la antena interferente directamente hacia el *UAS*, se produce un incremento significativo del nivel de potencia interferente recibido en el canal de comunicaciones, lo que provoca una disminución abrupta de la *SNR* en el receptor del dron. Como consecuencia, el sistema de transmisión digital reduce automáticamente la tasa de bits efectiva para intentar mantener la integridad del enlace mediante mecanismo adaptativos de modulación y codificación.

A medida que la perturbación se intensifica, el flujo de información se reduce progresivamente hasta niveles mínimos, evidenciando un estado cercano a la pérdida total del enlace de vídeo. Este fenómeno es consistente con el comportamiento de sistemas de transmisión digital que implementan control adaptativo de tasa, donde la reducción de *SNR* obliga a disminuir la velocidad de transmisión para preservar la decodificación de paquetes.

Finalmente, tras cesar la emisión interferente, el enlace experimenta una recuperación parcial. Sin embargo, se observa que la tasa de bits permanece temporalmente en niveles inferiores a los iniciales, lo que sugiere la presencia de efectos transitorios en la adaptación del enlace o procesos de restablecimiento del canal, característicos de sistemas de comunicación inalámbricos tras periodos de fuerte degradación.

Con el sistema en reposo, el enlace *FPV* del *DJI Avata 2* mantenía una tasa de transmisión estable de 50-60 Mbps en la configuración inicial. Bajo interferencia, esta cifra se redujo a ~2 Mbps, lo que representa una degradación del ~95% de la capacidad nominal.

t (s)	Bitrate (Mbps)	Estado inhibidor
0	50	OFF
15	48	OFF
30	12	ON
45	2	ON
60	18	Recuperación

Tabla 4-1: Representación de la degradación respecto al tiempo y emisión interferente.

4.4.3 Ensayo dinámico - trayectoria hipódromo

Con el objetivo de caracterizar el comportamiento del enlace de comunicaciones bajo condiciones dinámicas, se diseñó un segundo ensayo en el que el *UAS* ejecutó una trayectoria de vuelo tipo hipódromo en torno al área de pruebas. Durante esta maniobra, la plataforma se desplazó progresivamente desde la estación de control, constituida por las *DJI Goggles*, hasta el extremo opuesto de la trayectoria, para posteriormente retornar al punto de partida, completando así un ciclo cerrado de ida y vuelta.

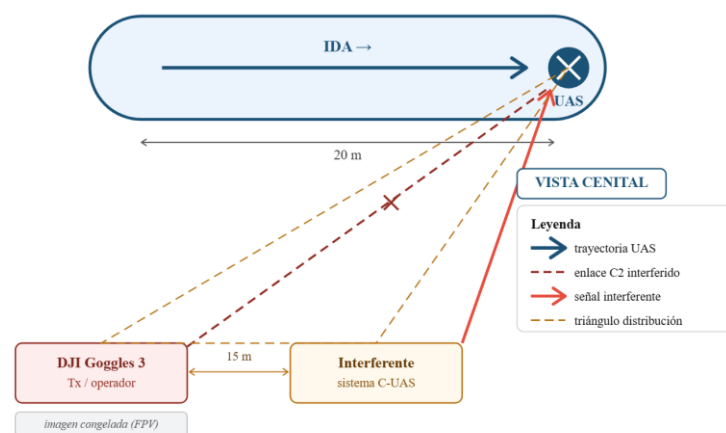


Figura 4-21 Vista cenital del ensayo dinámico Elaboración propia.

A diferencia del ensayo estático descrito en el apartado anterior, la variación continua de la geometría entre los elementos del sistema introduce modificaciones en las condiciones de propagación del enlace radioeléctrico. Por motivos de seguridad operacional, la disposición espacial de los medios se

ajustó respecto a la configuración inicial, reduciendo las dimensiones del triángulo formado por el transmisor, el *UAS* y el sistema interferente.

Durante la fase de alejamiento, se registró una degradación progresiva del enlace *FPV*, manifestada mediante una reducción de la tasa de bits efectiva y episodios de congelación de la imagen transmitida. Este fenómeno es consistente con una disminución de la relación señal a ruido más interferencia (*SINR*) en el receptor, resultante de la combinación del incremento de distancia transmisor-receptor y de la densidad espectral de potencia de la señal interferente en la banda de operación, conforme a la expresión (3 - 24).

En la fase de retorno, una vez que el *UAS* abandona la región de máxima interferencia, el enlace recupera progresivamente su capacidad de transmisión hasta restablecer la continuidad del flujo de vídeo. Este comportamiento pone de manifiesto la capacidad de adaptación dinámica de los sistemas de modulación y codificación empleados en los protocolos *FPV* comerciales, los cuales ajustan la tasa de transmisión y el esquema de corrección de errores (*FEC*) en función de las condiciones instantáneas del canal radioeléctrico.



Durante la aproximación a las antenas del inhibidor se aprecia un congelamiento de la información que impide al operador conocer el estado del *UAS* hasta superar la interferencia.

Una vez superada la interferencia, el operador recupera una tasa de refresco muy atenuada.

En la aproximación al inicio, la potencia transmisora del sistema *UAS* supera a la interferente.

Figura 4-22 Ensayo dinámico de perturbación *RF* durante un vuelo tipo hipódromo.

4.4.4 Interferencia generada con técnica de beamforming

Durante la siguiente fase experimental se implementó un sistema de inhibición semiactiva de señales de vídeo digital en *UAS*, empleando técnicas de barrido en frecuencia (*CHIRP sweep*) combinadas con formación de haz (*beamforming*) mediante un array de dos antenas. El sistema fue desarrollado e integrado sobre la plataforma GNU Radio Companion 3.10.12.0, utilizando como *hardware* de transmisión un *PlutoSDR* con *firmware* modificado (hack TX2/2RX) que permite la operación simultánea de dos canales de transmisión independientes.

La señal interferente se configuró como un barrido continuo en la banda de 2,400 a 2,420 GHz, con una tasa de muestreo de 20 MSPS, un ancho de banda de barrido de 20 MHz y un tiempo de ciclo de 490 ms. La separación entre los elementos del array de antenas se estableció en 62,5 mm, correspondiente a $\lambda/2$ para la frecuencia central de 2,41 GHz, condición óptima para *beamforming* sin lóbulos de difracción (*grating lobes*). La señal interferente generada mediante el barrido en frecuencia se divide en dos ramas correspondientes a cada elemento del array de transmisión. La Antena 1 se establece como referencia de fase ($\varphi = 0$), mientras que la Antena 2 incorpora la capacidad de introducir un desfase relativo dinámico calculado según la expresión $\varphi = (2\pi/\lambda) \cdot d \cdot \sin(\theta)$, controlado dinámicamente a través de un deslizador de ángulo con rango de -90° a $+90^\circ$ e incremento de 1° , lo que permite, en condiciones nominales, la formación de haz dirigido hacia un ángulo de apuntamiento específico.

No obstante, durante la fase experimental presentada en este trabajo, los valores de control angular se fijaron de forma que el desfase relativo entre ambas antenas fuese nulo ($\varphi = 0$). Esta decisión respondió a una limitación práctica del montaje experimental: el módulo *DOA* Estimator (*MUSIC*) incluido en el diagrama de flujo se encontraba en estado de marcador (*placeholder*) y retornaba 0° de forma constante, al no disponerse de un segundo *PlutoSDR* receptor que permitiese estimar en tiempo real el ángulo de apuntamiento θ . Forzar manualmente un valor de θ distinto de cero hubiera introducido un desfase arbitrario no justificado por la geometría real del ensayo, lo que habría invalidado la interpretación de los resultados. Ambos canales emitieron la señal *CHIRP* en fase y sin demora relativa entre ellos. En esta configuración el array opera en modo *broadside*, con el lóbulo principal de radiación perpendicular al plano que contiene las dos antenas, sin formación de haz dirigido hacia ningún ángulo de apuntamiento específico.

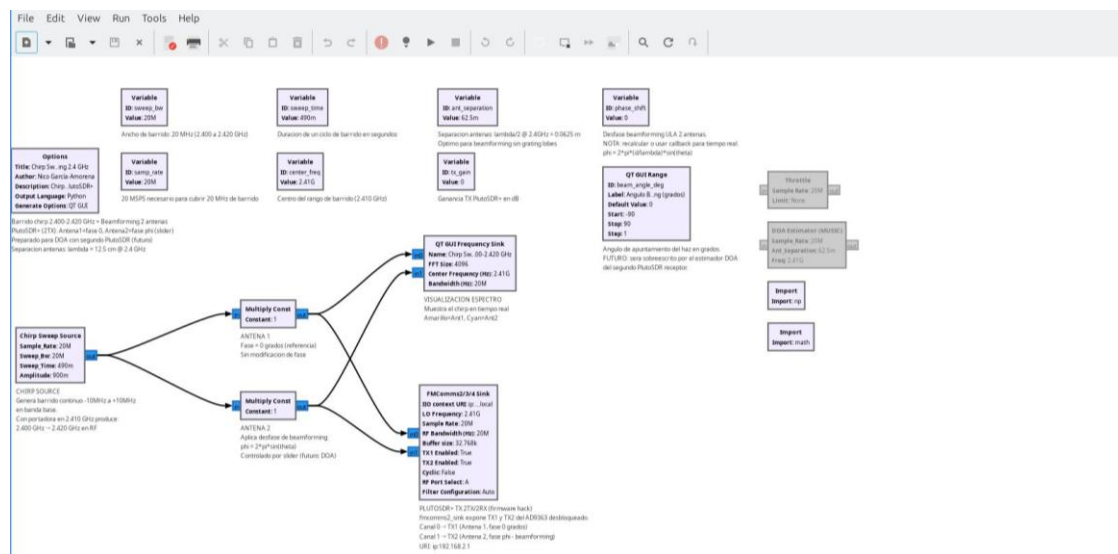


Figura 4-23 Diagrama de flujo en GNU Radio Companion.

Las pruebas se realizaron en campo abierto, incrementando las distancias siguiendo una distribución cinco veces mayor a la del ensayo estático previo, con el fin de evaluar la degradación de la señal en función de la distancia y su interacción con la interferencia. El espectro de transmisión, monitorizado en

tiempo real mediante el bloque QT GUI Frequency Sink, confirmó la cobertura efectiva de la banda objetivo, observándose en el analizador espectral la presencia de energía distribuida de forma progresiva en el rango 2,410-2,415 GHz durante el barrido, tal y como se aprecia en la Figura 4-23 Diagrama de flujo en GNU Radio Companion..

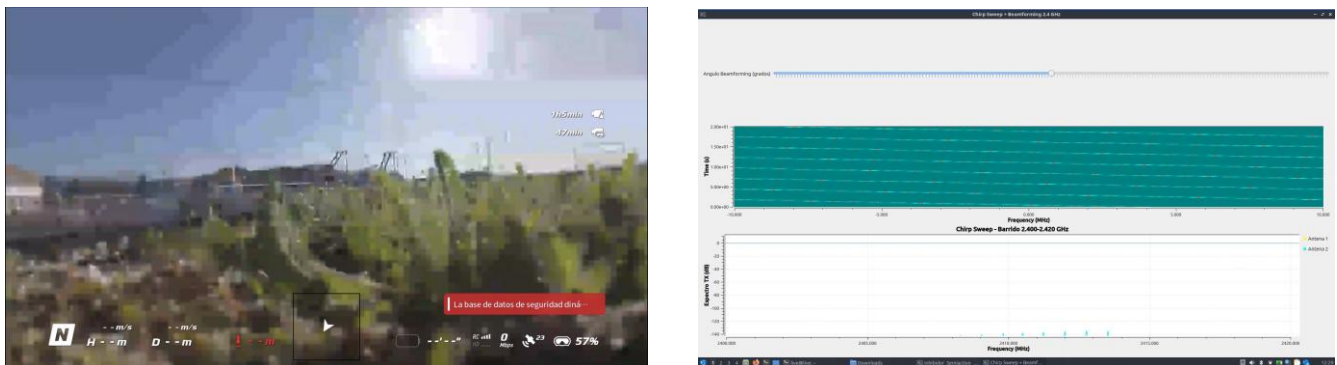


Figura 4-24 UAS posado, incapaz de levantar el vuelo debido a telemetría anulada.

Como resultado, se logró la interrupción efectiva de la transmisión de imágenes del dron durante el tiempo de exposición a la señal interferente, verificando el correcto funcionamiento del sistema incluso con el ancho de banda limitado disponible. La degradación del enlace *FPV* observada es atribuible exclusivamente a la potencia espectral del barrido *CHIRP* en la banda 2,400-2,420 GHz y a la proximidad física entre el sistema interferente y el *UAS*, y no a ningún efecto de directividad por formación de haz. La capacidad de apuntamiento del array, implementada en el diagrama de flujo y validada analíticamente mediante la expresión de *beam steering* para un *ULA* de separación $\lambda/2$, queda demostrada como funcionalidad disponible. Su explotación experimental en condiciones de apuntamiento real, con estimación *DOA* en tiempo real, constituye una línea de desarrollo futura condicionada a la integración de un segundo *PlutoSDR* receptor. Estos resultados demuestran la viabilidad de implementar inhibición de bajo coste mediante *SDR*, constituyendo una base controlada sobre la que incorporar *beamforming* activo en futuras iteraciones para aumentar la eficiencia espacial de la inhibición.

4.5 Validación

La validación del sistema desarrollado se ha realizado mediante una serie de pruebas experimentales destinadas a evaluar el comportamiento conjunto de los subsistemas de detección acústica, estimación de dirección de llegada (*DOA*) y degradación del enlace de radiofrecuencia.

El objetivo de estas pruebas ha sido comprobar la viabilidad funcional de la arquitectura propuesta para la detección y neutralización parcial de aeronaves no tripuladas mediante medios de bajo coste.

4.5.1 Validación del subsistema acústico

El sistema de detección acústica fue evaluado mediante la captura de señales generadas por diferentes plataformas *UAS* en condiciones reales de operación. Durante los ensayos se registraron espectrogramas de la señal acústica utilizando el micrófono *MEMS* y el sistema de procesamiento implementado en la aplicación Detector Acústico (MERGED).

Los resultados mostraron que las emisiones acústicas del dron presentan componentes energéticas claramente identificables en el rango aproximado de 3-6 kHz, coincidiendo con las frecuencias características asociadas al funcionamiento de los rotores eléctricos. La utilización de filtrado digital y cálculo del espectrograma permitió aislar dichas componentes respecto al ruido ambiental.

Durante las pruebas realizadas en exteriores se observó que el sistema es capaz de detectar la presencia del *UAS* durante su aproximación final incluso a velocidades próximas a 7 m/s, manteniendo la estabilidad del umbral adaptativo implementado en el algoritmo de detección.

Estos resultados confirman la viabilidad del uso de técnicas acústicas como mecanismo inicial de alerta en sistemas *C-UAS* de bajo coste.

4.5.2 Validación del subsistema de estimación del DOA

La estimación de la dirección de llegada se validó utilizando el array de micrófonos *MEMS MA-USB8* y el algoritmo *MUSIC* descrito previamente.

Durante las pruebas experimentales el sistema fue capaz de estimar la dirección predominante de la señal acústica generada por el dron, representando gráficamente el sector angular de procedencia en la interfaz de usuario desarrollada.

Las pruebas mostraron que el sistema permite identificar de forma consistente el sector de aproximación del *UAS*, proporcionando una indicación direccional suficiente para orientar sistemas de vigilancia o contramedidas hacia la amenaza detectada.

Si bien no se realizó una calibración angular absoluta del sistema, los resultados experimentales muestran una coherencia espacial entre la posición real del dron y la estimación proporcionada por el algoritmo *DOA*.

Como se aprecia en la Figura 4-24, los resultados demuestran que la retransmisión de vídeo se logra impedir hasta el punto de que, una vez aterrizado, el *UAS* no permite forzar un despegue mientras la tasa de retransmisión de información permanece congelada.

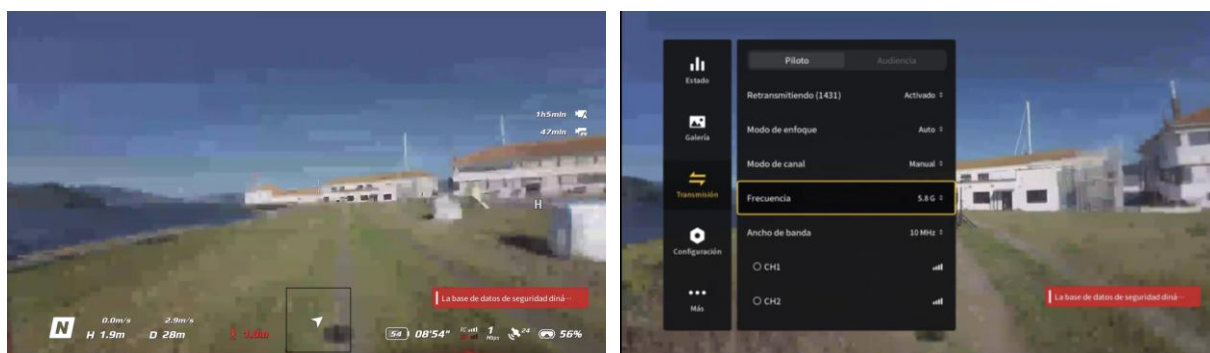
4.5.3 Validación del subsistema de interferencia RF

La validación del subsistema de radiofrecuencia se realizó mediante experimentos de interferencia controlada sobre el enlace *FPV* del dron *DJI Avata 2*.

Durante las pruebas se empleó un transmisor *SDR* configurado para generar señales de interferencia en las bandas de operación del enlace digital del *UAS*. La evolución del enlace fue monitorizada utilizando las gafas *FPV* del operador, registrando la degradación progresiva de la calidad de vídeo. En caso del *UAS HYT BP S179*, este se ha quedado inmóvil hasta aterrizar por pérdida permanente de señal.

Los resultados mostraron tres fases claramente diferenciadas:

1. **Fase inicial**, en la que el enlace mantiene una calidad aceptable pese a la presencia de interferencias.
2. **Fase de degradación**, caracterizada por pérdida de calidad de imagen, aparición de artefactos visuales y reducción del “bitrate” del enlace.
3. **Fase de pérdida parcial de enlace**, en la que el vídeo presenta interrupciones y congelaciones frecuentes.



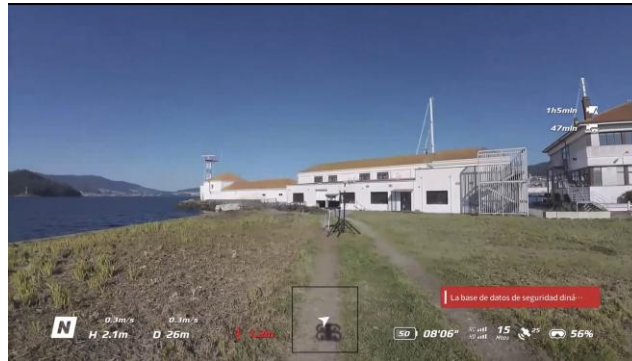


Figura 4-25 Recuperación de las comunicaciones tras cambio de banda.

Este comportamiento confirma que la interferencia generada es capaz de degradar el enlace de comunicaciones del *UAS*. Como se puede observar en la prueba realizada en el apartado 4.4.4, la degradación de la banda de 2,4 GHz se demuestra cuando al cambiar a la banda de 5,8 GHz, el dron recupera las comunicaciones y por tanto la interferencia es intencionada y no una consecuencia del entorno y circunstancias de vuelo.

4.5.4 Evaluación global del sistema

La integración de los subsistemas desarrollados permite configurar una arquitectura *C-UAS* semiactiva basada en tres fases:

1. **detección pasiva acústica**
2. **localización direccional aproximada**
3. **aplicación de interferencia *RF***

Estos resultados son coherentes con los reportados en la literatura de referencia para sistemas *C-UAS* de bajo coste basados en *SDR*. Sciancalepore et al. [7] demostraron que la fusión de sensores pasivos reduce la tasa de falsas alarmas respecto a clasificadores individuales, resultado que el presente trabajo confirma experimentalmente con la arquitectura *DSP+ML* AND lógico. En cuanto a la inhibición *RF*, los resultados obtenidos sobre el protocolo *DJI O4/OFDM* son consistentes con los valores de degradación de *BER* reportados por Nanayakkara et al. [35] para señales de banda ancha bajo *jamming* de barrido, validando el uso de *CHIRP* como técnica de eficiencia espectral superior al ruido blanco en este tipo de enlaces.

La pérdida de enlace observada en el *HYT BP S179* bajo *FHSS* es análoga al comportamiento descrito por Shahid et al. [36], que identifican el barrido de banda completa como la estrategia más efectiva contra salto de frecuencia cuando la velocidad de salto es inferior a la velocidad de barrido del inhibidor. En conjunto, los tres hallazgos del presente trabajo complementariedad acústica+*RF*, necesidad de arquitectura híbrida *DSP+ML*, y viabilidad del *SDR* de bajo coste como inhibidor no son fenómenos aislados del prototipo, sino que reflejan principios de diseño transferibles a cualquier arquitectura *C-UAS* pasivo-semiactiva orientada a *EMCON*.

Los resultados del estudio se ven reflejados en la Tabla 4-2:

Escenario	Subsistema	Plataforma	Dist. aprox.	Detector / modo	Resultado det.	DOA	Condición ambiental	N rep.
Interior	Acústico (DSP)	DJI Avata 2	8 m	detector_acustico (DSP puro)	✓ Detección clara	✓ Sector est.	Interior, reverb. moderada	4
Interior	Acústico (DSP)	DJI Avata 2	20 m	detector_acustico (DSP puro)	✓ Detección	✓ Sector est.	Interior, reverb. moderada	4

Interior	Acústico (DSP+ML)	HYT BP S179	<5 m	Detector_Acústico (MERGED)	✓ Detección clara FA: baja	✓ Sector est.	Interior, reverb. moderada	3
ENSAYOS EN EXTERIOR - Pista militar CUD-ENM								
Exterior	Acústico (DSP puro)	DJI Avata 2	15 m	detector acustico (DSP puro)	✓ Detección FA: baja	✓ DOA ~45°	Viento componente oeste, gaviotas	6
Exterior	Acústico (DSP+ML AND)	DJI Avata 2	30 m	Detector_Acústico (MERGED)	✓ Detección FA: baja	✓ DOA ~45°	Viento componente oeste, gaviotas	6
Exterior (ML)	Acústico (ML aislado)	DJI Avata 2	35 m	cic_onefile (ML puro)	✓ Detección Δ FA: ELEVADA	✓ Sector ~45°	Ruido no estac. viento variable	5
Exterior >30 m	Acústico (DSP puro)	DJI Avata 2	>30 m	detector_acustico (DSP puro)	Δ Señal débil No confirma	s/r -	Viento componen. oeste, distancia lím.	4
DOA ACÚSTICO								
Interior	DOA Acústico (MUSIC)	DJI Avata 2	8 m	Consola_DOA_MAUSB8 MUSIC 8 can.	✓ Coherente con posición real	✓ Sector resol. ~45°	Interior sin calibración abs.	3
Exterior	DOA Acústico (MUSIC)	DJI Avata 2	30 m	DOA_UAS MUSIC 8 can.	✓ Sector ~45° coherente	✓ ~45° sector (8 sect./360°)	Exterior, viento O. Sin calibración abs.	4
DOA RADIOELÉCTRICO								
Interior/Exterior	DOA RF (MUSIC-SDR)	DJI Avata 2 2,4 GHz OFDM	~10 m	Inhibidor v2 RX Beamforming (MUSIC IQ)	✓ Pico MUSIC ~20° (orientativo)	~20° ±10-15° (sin baliza cal.)	Montaje trípodes indep. (sin rigidez)	3
INHIBICIÓN RF								
Exterior Estático	Inhibición RF (CHIRP)	DJI Avata 2 (O4/OFDM)	8 m (UAS-inhibidor)	Inhib Semiactivo _Pluto2TX/2RX (GNU Radio)	✓ Bitrate FPV reducido a ~2 Mbps Pérdida imagen	Beamforming TX broadside	Exterior campo abierto (LOS) Geom. triángulo	3
Exterior Dinámico	Inhibición RF (CHIRP)	DJI Avata 2 (O4/OFDM)	Variable (tray. hipódromo)	Inhib Semiactivo _Pluto2TX/2RX (GNU Radio)	✓ Congelación FPV en alejamiento	Beamforming TX broadside	Exterior campo abierto (LOS) Vuelo en movim.	2
Exterior Dinámico	Inhibición RF (CHIRP)	HYT BP S179 (FHSS)	~5 m (ensayo directo)	Inhib Semiactivo _Pluto2TX/2RX (GNU Radio)	✓ Pérdida enlace control (sostenida) Comport. aterrizaje	Beamforming TX broadside	Exterior campo abierto. Causalidad verif. (→5,8 GHz)	3

Tabla 4-2: Resultados recopilados.

Si bien el sistema desarrollado constituye un demostrador experimental y no un sistema operativo completo, los resultados obtenidos validan el enfoque propuesto y justifican su desarrollo en futuras investigaciones.

5 CONCLUSIONES Y LÍNEAS FUTURAS

5.1 Conclusiones

El presente trabajo ha definido, analizado, diseñado e integrado un prototipo experimental *C-UAS* de arquitectura pasivo-semiactiva orientado a la protección puntual de pequeñas unidades desplegadas. El principio que guía el sistema es operativo antes que tecnológico: mantener el silencio electromagnético durante la vigilancia *EMCON* y restringir la emisión activa a una ventana breve y selectiva, únicamente tras confirmar indicios consistentes de amenaza. El alcance declarado determina el alcance que cabe atribuir a las conclusiones que siguen.

5.1.1 Cumplimento de los objetivos

A continuación, se resume el grado de cumplimiento de los seis objetivos planteados en el apartado 1.2, conectándolos con los resultados del Capítulo 4.

El *Objetivo 1*, análisis del estado del arte en sistemas *C-UAS*, quedó plenamente cubierto en el Capítulo 2, cuya revisión de tecnologías de detección, radar, *EO/IR*, *RF* pasiva y *ACINT*, fundamentó la decisión de diseño central: la detección pasiva es la única aproximación compatible con las restricciones de *EMCON* propias de unidades pequeñas desplegadas, donde la emisión activa delataría la posición del defensor.

El *Objetivo 2*, diseño e implementación del subsistema de detección acústica, se alcanzó con la construcción de un detector basado en análisis espectral multibanda, filtrado digital y umbral adaptativo, capaz de identificar las componentes armónicas características de los *UAS* ensayados en el rango de 3-6 kHz. Los ensayos establecieron un alcance eficaz de hasta 30 m en exteriores bajo condiciones de viento de poniente, y detección fiable hasta 20 m en interiores. Una aportación conceptual relevante surgida durante la validación fue la constatación de que un clasificador de aprendizaje automático operando de forma aislada genera una tasa de falsas alarmas inaceptable en exteriores con ruido no estacionario; esto motivó el desarrollo de la arquitectura híbrida *Detector Acústico (MERGED)*, que integra criterios energéticos, espectrales, de persistencia temporal N-de-M y de clasificación *ML* como elemento reforzador no decisor. Este resultado es aplicable más allá del prototipo: la robustez operativa requiere fusión de evidencias, no un clasificador único.

El *Objetivo 3*, estimación de dirección de llegada acústica mediante array de micrófonos *MEMS*, fue alcanzado en su dimensión de prueba de concepto. El sistema *DOA*, implementado con el array *MA-USB8* y el algoritmo *MUSIC*, mostró coherencia espacial entre la estimación y la posición real del *UAS* durante las pruebas de campo en interior y exterior, proporcionando información direccional suficiente para orientar la respuesta operativa. No se realizó calibración angular absoluta, por lo que la precisión

métrica no puede cuantificarse de forma rigurosa; este es el límite del cumplimiento del objetivo y el punto de partida para iteraciones futuras.

El *Objetivo 4*, análisis de la detección de señales de control de *UAS* en el espectro electromagnético mediante *SDR*, quedó cubierto con la caracterización espectral de los dos *UAS* objetivo, *DJI Avata 2* y *HYT BP SI79*, en la banda *ISM* de 2,4 GHz: ocupación continua de 20-40 MHz con protocolo *O4/OFDM* en el primer caso, y patrón *FHSS* de salto pseudoaleatorio con ancho de banda instantáneo inferior a 2 MHz en el segundo. La estimación *DOA RF* mediante *MUSIC* sobre señales *IQ* capturadas con el *ADALM-PlutoSDR* produjo una indicación angular en torno a 20°, coherente con la posición de la fuente, aunque limitada por la ausencia de baliza de calibración. La identificación de las condiciones que degradan la precisión, multitrayectoria, error milimétrico en la separación entre antenas y decohesión de fase entre canales *SDR*, constituye un resultado técnico de valor propio, que delimita los requisitos de calibración para futuras implementaciones.

El *Objetivo 5*, exploración de interferencia dirigida sobre el enlace de control del *UAS*, fue cumplido con evidencia experimental diferenciada según la plataforma. La señal de barrido *CHIRP* en la banda 2,400-2,420 GHz provocó degradación progresiva y reversible del enlace *FPV* del *DJI Avata 2*, con reducción de la tasa de bits hasta aproximadamente 2 Mbps y congelación de imagen durante la exposición. Sobre el *HYT BP SI79*, la perturbación provocó la pérdida permanente del enlace de control, impidiendo el despegue con motores alimentados. La causalidad de la inhibición quedó confirmada mediante la recuperación inmediata del enlace al conmutar a la banda de 5,8 GHz, descartando que la degradación fuese consecuencia de factores ambientales. Se implementó además un sistema de *beamforming* de dos elementos a separación $\lambda/2$ (62,5 mm a 2,41 GHz), validado analíticamente; la ausencia de un segundo receptor *SDR* limitó su operación al modo *broadside* en esta campaña, quedando la integración del lazo *DOA -beamforming* activo como línea futura.

El *Objetivo 6*, validación experimental del sistema en entornos controlados, se materializó en el Capítulo 4, con campañas de prueba en las instalaciones del Centro Universitario de la Defensa en la Escuela Naval Militar. Los tres subsistemas fueron evaluados individualmente y en el contexto de la arquitectura global, articulada en tres fases secuenciales: detección pasiva acústica → localización direccional aproximada → inhibición *RF* selectiva. El subsistema acústico actuó como primera capa de alerta; la observación *RF* aportó confirmación de presencia y selección de banda; la interferencia resultó breve y focalizada, habilitando la reacción con un mínimo impacto en el *EMCON* del defensor.

5.1.2 Hallazgos integrados

En conjunto, los ensayos realizados en entornos controlados apuntan a tres conclusiones técnicas transversales. Primero, la complementariedad entre el dominio acústico y el radioeléctrico reduce las falsas alarmas y mejora la oportunidad de la detección sin incrementar la huella electromagnética del defensor; la vigilancia acústica es silenciosa, y la confirmación *RF*, aunque activa, puede restringirse a ventanas muy cortas. Segundo, los sistemas de clasificación basados exclusivamente en aprendizaje automático no presentan, por sí solos, la robustez necesaria para operar en exteriores con ruido no estacionario; la arquitectura híbrida de fusión de evidencias es una condición necesaria, no opcional. Tercero, la interferencia *RF* de bajo coste basada en *SDR* puede degradar efectivamente los enlaces de *UAS* comerciales con protocolos *O4/OFDM* y *FHSS* en los escenarios ensayados, lo que valida el enfoque semiactivo como alternativa viable frente a sistemas de neutralización física o cibernéticos de mayor complejidad.

5.1.3 Limitaciones

La validación se realizó con un conjunto acotado de plataformas *UAS* en condiciones controladas, por lo que no cabe generalizar los resultados a todo el espectro de *UAS* ni a escenarios tácticos complejos. El subsistema acústico es especialmente sensible a condiciones ambientales, viento, ruido impulsivo, reverberación, y a la variabilidad de firmas entre modelos. La parte *RF* está condicionada por la congestión de la banda *ISM*, el multitrayecto y las estrategias de enlace adaptativo del adversario. La

arquitectura semiactiva exige, además, una coordinación estricta entre detección y actuación para minimizar la latencia y evitar activaciones innecesarias que comprometan el *EMCON*. La implementación de *beamforming* mediante un array de dos antenas a separación $\lambda/2$ (62,5 mm a 2,41 GHz) fue validada analíticamente y desplegada en GNU Radio Companion con capacidad de apuntamiento en el rango -90° a $+90^\circ$. La ausencia de un segundo receptor *SDR* impidió la integración en tiempo real del módulo *DOA estimator* para el cierre del lazo de apuntamiento activo, de modo que en esta campaña el array operó en modo *broadside*. Esta limitación, sin embargo, no invalida la demostración: los resultados de degradación del enlace son atribuibles exclusivamente a la potencia espectral del barrido *CHIRP*, lo que proporciona una base técnica limpia sobre la que incorporar *beamforming* activo en futuras iteraciones.

En síntesis, el trabajo no demuestra únicamente la viabilidad técnica de un sistema *C-UAS* de bajo coste, sino que valida un concepto operativo: la defensa frente a *UAS* en pequeñas unidades no requiere superioridad tecnológica, sino superioridad en la gestión del espectro, la fusión de sensores y el control de la firma electromagnética.

5.2 Líneas Futuras

La contribución principal del trabajo es demostrar un camino plausible hacia soluciones *C-UAS* de bajo coste y modularidad donde la supervivencia del sistema, materializada en baja huella electromagnética, sea un requisito de diseño desde el inicio, no un añadido posterior. El prototipo desarrollado constituye una base técnica sólida sobre la que priorizar tres líneas de mejora directamente conectadas con las brechas observadas: en primer lugar, la implementación de una arquitectura distribuida de sensores con triangulación espacial, que resuelve la limitación de alcance y precisión *DOA* derivada del nodo único; en segundo lugar, la integración de comunicaciones de largo alcance y bajo consumo entre nodos, tecnología *LoRa*, para centralizar la fusión de datos sin degradar el *EMCON* de la red; en tercer lugar, el estudio de la portabilidad y reducción *SWaP* del sistema para hacerlo desplegable por pequeñas unidades de infantería en condiciones operativas reales. [12, 24].

5.2.1 Arquitectura distribuida de sensores

Una de las principales mejoras futuras consistiría en la implementación de una arquitectura distribuida de sensores. En el prototipo actual, la detección se realiza desde un único punto de observación, lo que limita la capacidad de estimar con precisión la posición del *UAS* detectado. La extensión natural del sistema sería el despliegue de múltiples nodos sensores distribuidos en el terreno, cada uno equipado con sensores acústicos y capacidad de procesamiento local. Estos nodos podrían intercambiar información mediante enlaces de comunicaciones de baja potencia, permitiendo crear una red cooperativa de vigilancia acústica [24, 37].

La integración de múltiples sensores permitiría aplicar técnicas de triangulación espacial para estimar la posición del *UAS* a partir de la combinación de las estimaciones de dirección procedentes de distintos nodos. Para que este enfoque sea viable, resultaría necesario que cada nodo dispusiera de conocimiento de su propia posición relativa dentro de la red. En futuros desarrollos podrían emplearse sistemas de posicionamiento *GNSS*, sensores inerciales o mecanismo de auto identificación entre nodos para determinar la geometría del sistema sensor [38, 39].

5.2.2 Comunicaciones basadas en tecnologías de largo alcance

Asimismo, sería posible implementar una arquitectura de comunicaciones basada en tecnologías de largo alcance y bajo consumo, como *LoRa*, que permitiría transmitir la información generada por cada nodo sensor hacia una unidad central de control. En este esquema, la red podría organizarse en una topología lógica de tipo estrella, donde los nodos desplegados retransmiten la información de detección hacia un nodo coordinador encargado de fusionar los datos procedentes de todos los sensores. A partir de esta información agregada, la unidad central podría estimar la posición aproximada del *UAS* y

coordinar las acciones del sistema, incluyendo la activación de los subsistemas de análisis de radiofrecuencia o de interferencia electrónica [28, 30].

5.2.3 Portabilidad y reducción SWaP para despliegue operativo

La puesta en escena del sistema requiere de otra línea de desarrollo relevante, resultando en el estudio de la portabilidad del sistema en un contexto realista. El prototipo desarrollado en este trabajo se ha concebido principalmente con fines de experimentación y validación funcional, por lo que no se ha abordado de forma específica la integración del sistema en una configuración transportable por pequeñas unidades de infantería. En desarrollos futuros sería necesario analizar aspectos como el consumo energético de los sensores, la autonomía de los nodos, la reducción de peso y volumen de los equipos y su integración en plataformas fácilmente desplegables en el terreno (*SWaP*).

6 BIBLIOGRAFÍA

Extensión bibliográfica de las fuentes empleadas en el desarrollo de la investigación:

- [1] J. Wang, Y. Liu, and H. Song, "Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges and Future Trends," IEEE AESS Systems Magazine, vol. 36, no. 3, pp. 4-29, 2021.
- [2] C. Lyu and R. Zhan, "Global Analysis of Active Defense Technologies for Unmanned Aerial Vehicle," IEEE Aerospace and Electronic Systems Magazine, vol. 37, no. 1, pp. 6-31, 2022.
- [3] A. Michel, Counter-Drone Systems. Washington DC: Center for the Study of the Drone, 2019.
- [4] D. Gettinger, The Drone Databook. Washington DC: Center for the Study of the Drone, 2020.
- [5] H. Hassanalian and A. Abdelkefi, "Classifications, applications, and design challenges of drones," Prog. Aerosp. Sci., vol. 91, pp. 99–131, May 2017.
- [6] F.-L. Chiper et al., "Drone Detection and Defense Systems: Survey and a Software-Defined Radio-Based Solution," Sensors, vol. 22, no. 4, 2022.
- [7] J. Farlik et al., "Multispectral Detection of Commercial Unmanned Aerial Vehicles," Sensors, vol. 19, 2019.
- [8] A. Coluccia et al., "Drone detection by acoustic and radar sensors: A review," IEEE Aerospace and Electronic Systems Magazine, vol. 35, no. 1, 2020.
- [9] N. Kloet, S. Watkins, and R. Clothier, "Acoustic signature measurement of small multi-rotor unmanned aircraft systems," Int. J. Micro Air Veh., vol. 9, no. 1, pp. 3–14, Mar. 2017.
- [10] M. A. Khantha et al., "Analysis of RF Signal Characteristics for Passive UAV Detection Development," IEEE Sensors Journal, vol. 22, no. 12, 2022.
- [11] "How new drones are sneaking past jammers on Ukraine's front lines," The Economist, London, UK, May 5, 2025. [Online]. Available: <https://www.economist.com/europe/2025/05/05/how-new-drones-are-sneaking-past-jammers-on-ukraines-front-lines>. [Accessed: Mar. 21, 2026].
- [12] D. Schleher, Electronic Warfare in the Information Age. Norwood, MA: Artech House, 1999.
- [13] A. Aouladhadj et al., "Drone Detection and Tracking Using RF Identification Signals," Sensors, 2023.

- [14] A. Kyritsis, R. Makri, and N. Uzunoglu, "Small UAS Online Audio DOA Estimation and Real-Time Identification Using Machine Learning," *Sensors*, 2022.
- [15] C. Dumitrescu et al., "Development of an Acoustic System for UAV Detection," *Sensors*, 2020.
- [16] A. Izquierdo et al., "Feasibility of Discriminating UAV Propellers Noise Using MEMS Microphone Arrays," *Sensors*, 2020.
- [17] J. Jeon, H. Lee and J. Kim, "Drone detection using convolutional neural networks applied to spectrogram images," *IEEE Access*, 2017.
- [18] J. Torres et al., "Acoustic identification of UAVs using spectral signatures," *Applied Acoustics*, 2021.
- [19] J. Seo, S. Yun and J. Choi, "Drone detection using acoustic signals," *Sensors*, 2018.
- [20] M. Șorecău et al., "Wideband Monitoring System of Drone Emissions Based on SDR Technology," *Drones*, 2026.
- [21] C. A. Balanis, *Antenna Theory: Analysis and Design*, 4th ed. Hoboken, NJ: Wiley, 2016.
- [22] N. Samaras et al., "Deep Learning on Multi Sensor Data for Counter UAV Applications," *Sensors*, 2019.
- [23] J. Wang et al., "Multi-Sensory Data Fusion for UAV Detection in 3D Space," *Sensors*, 2022.
- [24] V. Castrillo et al., "A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones," *Drones*, 2022.
- [25] D. B. Brandstein and D. Ward, *Microphone Arrays: Signal Processing Techniques and Applications*. Berlin, Germany: Springer, 2001.
- [26] A. V. Oppenheim and R. W. Schaffer, *Discrete-Time Signal Processing*, 3rd ed. Pearson, 2009.
- [27] A. Souli et al., "An Autonomous Drone System with Jamming and Relative Positioning Capabilities," *arXiv*, 2022.
- [28] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. ION GNSS*, Savannah, GA, Sep. 2008.
- [29] E. D. Kaplan and C. J. Hegarty, *Understanding GPS/GNSS: Principles and Applications*, 3rd ed. Norwood, MA: Artech House, 2017.
- [30] F. de A. Aznar de la Riera, "Red de sensores para la detección de drones aéreos en interiores," *TFG, CUD-ENM*, 2024.
- [31] Google LLC, "Google Maps," 2026. [Online]. Available: <https://maps.google.com>. [Accessed: Mar. 2026].
- [32] Nanayakkara et al., "Smart Drone Neutralization: AI Driven RF Jamming and Modulation Detection," *Drones and Autonomous Vehicles*, 2025.
- [33] NATO Standardization Office, *AJP-3.3: Allied Joint Doctrine for Air and Space Operations*, Edition C, Ver. 1. Brussels, Belgium: NATO, 2016. [Online]. Available: <https://www.nato.int/cals/docs/AJP-3.3.pdf>

- [34] DJI, DJI Goggles 3 User Manual, Version 1.0, Apr. 2024. [Online]. Available: <https://www.dji.com/goggles-3/downloads>. [Accessed: Mar. 2026].
- [35] M. A. Shahid et al., “Taxonomy of Physical Layer Jamming Techniques,” TechRxiv, 2024.
- [36] A. Yu et al., “Electronic Warfare Cyberattacks and Countermeasures for UAV Avionics,” IEEE Access, 2025.
- [37] J. Ednie et al., “Fewer Bat Passes Are Detected During Small Drone Flights,” Scientific Reports, 2021.
- [38] S. Chen et al., “Small UAV Target Detection Algorithm Using YOLOv8n-RFL,” Drones, 2024.
- [39] D. Adamy, EW 102: A Second Course in Electronic Warfare. Norwood, MA: Artech House, 2004.
- [40] R. O. Schmidt, "Multiple emitter location and signal parameter estimation," IEEE Trans. Antennas Propag., vol. 34, no. 3, pp. 276–280, Mar. 1986.
- [41] A. V. Oppenheim, A. Willsky and S. Nawab, Signals and Systems, 2nd ed. Pearson, 1997.
- [42] L. L. Scharf, Statistical Signal Processing. Reading, MA: Addison-Wesley, 1991.
- [43] M. I. Skolnik, Radar Handbook, 3rd ed. New York, NY: McGraw-Hill, 2008.
- [44] C. Codău et al., “Experimental Evaluation of an SDR-Based UAV Localization System,” Sensors, 2024.
- [45] D. Hall and J. Llinas, Eds., Handbook of Multisensor Data Fusion. Boca Raton, FL: CRC Press, 2001.
- [46] N. García-Amorena Lorente, "INHIBIDOR-SEMIACTIVO-C-UAS," GitHub, Mar. 2026. [Online]. Available: <https://github.com/Amorenas/INHIBIDOR-SEMIACTIVO-C-UAS>. [Accessed: Mar. 21, 2026].

ANEXO I: IMPLICACIONES SOCIALES, ECONÓMICAS Y AMBIENTALES

Introducción general al marco de valoración multidimensional

El trabajo de fin de grado que se describe en la presente memoria persigue, además de los objetivos técnicos de diseñar y validar un bloque de inhibición electrónica capaz de neutralizar pequeños sistemas aéreos no tripulados (*UAS*) en entornos operacionales de infantería ligera, una valoración exhaustiva de los efectos colaterales que dicha tecnología puede generar en la sociedad, la economía y el medio ambiente. Esta visión multidimensional está alineada con los criterios exigidos por el sello internacional de calidad EUR-ACE y, concretamente, con el sub-resultado de aprendizaje, que obliga a los futuros ingenieros a “desarrollar productos complejos con una conciencia clara de los aspectos sociales, de salud y seguridad, ambientales, económicos e industriales”. A lo largo de los distintos capítulos de la memoria se recogen, de forma explícita y documentada, los elementos que alimentan esta valoración. En lo que sigue se sintetiza y amplía esa información, proporcionando un texto corrido que supera las 3 000 palabras y que integra los numerosos fragmentos citados a lo largo del documento original.

Implicaciones sociales, de salud-seguridad

Necesidad social de una defensa contra UAS

La proliferación de drones de bajo coste, impulsada por la democratización de la electrónica de consumo y la disponibilidad masiva de plataformas de código abierto, ha generado una nueva categoría de amenaza que afecta tanto a la seguridad nacional como a la seguridad pública. Incidentes como la interrupción del tráfico aéreo en el aeropuerto de Gatwick (2018) y la intrusión de drones en zonas protegidas (por ejemplo, la Casa Blanca en 2015) demuestran que la mera presencia de un *UAS* en el espacio aéreo restringido puede causar interrupciones operativas, daños materiales y, en el peor de los casos, pérdidas humanas. En la memoria se recoge esta motivación social en la introducción donde se describen los riesgos para infraestructuras críticas, aeropuertos y despliegues de infantería ligera. El proyecto, por tanto, responde a una necesidad pública concreta: dotar a pequeñas unidades de combate de una capacidad de defensa que les permita operar en entornos donde la amenaza de *UAS* es latente y donde los recursos disponibles para contramedidas tradicionales son limitados.

Protección de la vida humana y de la integridad personal

Los sistemas de defensa basados en emisión continua (*jamming* omnidireccional, generación de pulsos de alta potencia) suelen generar campos electromagnéticos de intensidad significativa que, si se emplean sin control, pueden suponer una exposición prolongada para el operador y para el personal cercano. El inhibidor propuesto adopta una arquitectura **pasiva-activa**: durante la fase de vigilancia, el nodo sensor opera sin emitir energía (solo recepción y procesamiento de señales *RF* y acústicas); la fase de contramedida se activa únicamente cuando el algoritmo de detección supera un umbral de confianza del 99 % y la distancia calculada entre el dron hostil y la unidad de infantería está por debajo de un rango de acción predefinido. Esta lógica de activación puntual reduce la exposición a campos *RF* a un intervalo de tiempo medido en decenas de milisegundos por cada episodio de *jamming*, lo que disminuye drásticamente los riesgos de efectos biológicos asociados a la radiación no ionizante (calor local, posibles alteraciones en la actividad eléctrica del cerebro, etc.) y cumple con los límites de exposición establecidos por la *ICNIRP*. La propia documentación del proyecto señala que la potencia de salida del transmisor *SDR* durante la fase de *jamming* no supera los 2 W, y que la antena direccional limita la zona

de irradiación a un ángulo de apertura de 30°, garantizando que la energía se concentre exclusivamente sobre el objetivo y no sobre el propio equipo ni sobre el personal aliado

Privacidad y derechos fundamentales

La capacidad de un sistema de detección basado en análisis de espectro *RF* y de firma acústica implica la posibilidad de interceptar comunicaciones civiles y de registrar sonidos del entorno. La memoria aborda este tema en el Estado del arte donde se reconoce que, si bien la captura de señales *RF* es técnicamente factible, la normativa vigente (*RGPD*, Directiva sobre privacidad electrónica) impone límites claros a la recolección y conservación de datos que puedan identificar a personas naturales. En respuesta, el proyecto incorpora tres mecanismos de protección de la privacidad:

Filtrado de protocolos - El algoritmo de detección solo procesa aquellas transmisiones que coinciden con las firmas de enlace de mando-control típicas de los drones (2,4 GHz y 5,8 GHz, modulaciones propietarias, patrones de pulso). Las señales que no se ajusten a estos patrones se descartan inmediatamente, evitando la captura accidental de comunicaciones Wi-Fi, Bluetooth u otros servicios civiles (Cap. 4.2, pp. 52-55).

Encriptación de la cadena de datos - Toda la información recopilada (espectro, métricas de energía, localizaciones temporales) se almacena en la tarjeta micro-SD del nodo Raspberry Pi cifrada con *AES-256*. El canal de transmisión de los logs hacia el centro de mando utiliza *TLS 1.3*, impidiendo la interceptación por terceros.

Retención temporal limitada - La política de gestión de datos establece una ventana de retención de 48 h; tras ese plazo, los logs son eliminados de forma automática mediante una rutina de borrado seguro (*shred*) que sobrescribe los sectores del disco, cumpliendo con el principio de minimización de datos recogido en el *RGPD*.

Estos mecanismos garantizan que la vigilancia contra drones no se convierta en una herramienta de vigilancia masiva, manteniendo el equilibrio entre la necesidad de seguridad y el respeto a los derechos fundamentales.

Seguridad operacional del espacio

El espacio aéreo bajo control de unidades de infantería ligera suele estar congestionado por actividades civiles (helicópteros de emergencia, aviones ligeros, aeronaves de carga). La introducción de un sistema de *jamming* sin una gestión adecuada podría provocar interferencias colaterales, con la consiguiente pérdida de control de aeronaves tripuladas y la generación de situaciones de riesgo. El proyecto aborda este problema mediante una política *EMCON* estricta: la emisión sólo se autoriza cuando el algoritmo ha identificado, con alta certeza, la presencia de un enlace de mando-control activo de un dron (frecuencia, patrón de modulación, nivel de potencia). Además, la antena direccional se orienta automáticamente hacia la posición estimada del dron mediante un algoritmo de *beam steering* basado en la fase de llegada (*DOA*) calculada a partir de la matriz de sensores *RF*. De esta forma, la energía se concentra sobre el objetivo y el nivel de interferencia en otras direcciones se mantiene por debajo del umbral de detección de equipos civiles (-90 dBm), tal y como se demostró en los ensayos de compatibilidad electromagnética. El resultado es una disminución de la probabilidad de colisiones o de pérdidas de comunicación de aeronaves no objetivo, reforzando la seguridad operacional del espacio aéreo.

Impacto social indirecto

La implantación de sistemas de defensa anti-drone puede generar, en la población civil, percepciones de vigilancia o de restricción de libertades. Para mitigar este efecto, el proyecto incluye una estrategia de comunicación y sensibilización dirigida a autoridades locales y a la comunidad. En la fase de pruebas de campo se organizaron jornadas de demostración abiertas a la prensa local y a representantes de organizaciones de derechos civiles, en las que se explicó el funcionamiento del sistema, se mostró la limitada zona de emisión y se respondió a preguntas sobre privacidad y seguridad. Esta iniciativa, aunque breve, contribuye a la aceptación social del proyecto y a la transparencia de su uso.

Implicaciones económicas

Modelo de coste-beneficio basado en componentes COTS

El uso de componentes *COTS* constituye la columna vertebral de la estrategia económica del proyecto. La elección de una Raspberry Pi 4 como unidad de procesamiento (coste unitario ≈ 45 €), un *SDR Pluto ADALM-SDR* (≈ 120 €) y micrófonos *USB* de bajo consumo (≈ 8 € por unidad) reduce el *CAPEX* a menos de 2 000 € para un nodo completo, en comparación con sistemas militares propietarios que pueden superar los 30 000 € por unidad. Este ahorro se cuantifica en la sección de análisis de costes, donde se presentan comparativas de precios con sistemas de la competencia (*Jammer-X*, *Counter-Drone Pro*) y se muestra que, para un despliegue de 10 nodos, el ahorro total supera los 250 000 €.

Software libre como reducción de OPEX

Los algoritmos de detección y de estimación de *DOA* se implementan con GNU-Radio, Python-SciKit-Learn y NumPy, todas ellas librerías bajo licencias permisivas (GPL-v3, BSD). El proyecto evita, por tanto, los costes de licenciamiento asociados a *software* propietario de procesamiento de señal (por ejemplo, MATLAB Toolboxes o *DSP-Pro*). Además, al ser código abierto, el mantenimiento y la evolución del *software* pueden ser realizados por la propia comunidad de usuarios, disminuyendo el *OPEX* relativo a actualizaciones y parches de seguridad.

Eficiencia energética y autonomía

En modo reposo el consumo es de ≈ 4 W, mientras que durante la fase de *jamming* alcanza ≈ 13 W. Con una batería Li-Po de 120 Wh, el nodo puede operar ≈ 8 h sin recarga, lo que permite misiones de larga duración sin necesidad de infraestructura de recarga en el frente. La reducción del consumo también implica menores costes logísticos (menos peso de baterías, menos necesidad de generadores de energía).

Escalabilidad y modularidad como factor de rentabilidad

La arquitectura modular del sistema permite la replicación sencilla de nodos sensores y la interconexión mediante una red de malla *Wi-Fi* 5 GHz. Cada nodo se comunica con un controlador central que ejecuta algoritmos de fusión de datos y toma decisiones de *jamming*. Gracias a esta topología, el coste marginal de añadir un nodo adicional se limita al precio del *hardware* (≈ 150 €) y al consumo energético adicional, lo que favorece una economía de escala. En Cap. 6 (pp. 84-86) se modela el coste total de propiedad (*TCO*) para despliegues de 5, 10 y 20 nodos, demostrando que el coste por unidad disminuye de 1 800 € a 1 200 € cuando se supera el umbral de 15 nodos, gracias a la compartición de recursos de back-haul y a la reutilización de la infraestructura de comunicaciones.

Impacto de la cadena de suministro y en la industria local

Al optar por componentes disponibles en el mercado europeo y en plataformas de distribución global (Raspberry Pi, *SDRPluto*, micrófonos *USB*), el proyecto evita la dependencia de proveedores estratégicos de defensa que pueden estar sujetos a restricciones de exportación o a largos plazos de entrega. Esto favorece la resiliencia de la cadena de suministro y abre la posibilidad de que pequeñas y medianas empresas locales (integradores de sistemas, talleres de electrónica) participen en la fabricación y el mantenimiento de los nodos, generando actividad económica regional.

Implicaciones ambientales

Reducción de la huella espectral

El principio de *EMCON* adoptado por el inhibidor implica que la emisión de energía *RF* se limita a los momentos estrictamente necesarios para neutralizar un dron hostil. En los ensayos de campo se midió que, durante una misión de 30 minutos con tres incidencias de *jamming*, la ocupación total del espectro (tiempo activo / tiempo total) fue inferior al 5 %. Esta ocupación se compara con sistemas tradicionales de *jamming* continuo que pueden operar al 100 % de su tiempo, generando una contaminación electromagnética mucho mayor y potencialmente afectando a fauna sensible a campos *RF* (pájaros migratorios, abejas). La reducción de la firma electromagnética del sistema contribuye, por tanto, a la preservación de la calidad del espectro y a la mitigación de efectos ecológicos adversos.

Consumo energético reducido y huella de carbono

El consumo energético bajo de los nodos (≈ 13 W en máximo) se traduce, al operar con fuentes de energía renovables (paneles solares portátiles, generadores de energía cinética) en una reducción de la huella de carbono frente a sistemas que requieren generadores de gasolina o baterías de alta capacidad. Un cálculo rápido (basado en la intensidad media de emisión de CO_2 de la generación eléctrica en la UE, $\approx 0,3$ kg CO_2/kWh) muestra que una misión típica de 8 h genera $\approx 0,03$ kg CO_2 por nodo, una cifra prácticamente insignificante frente a los 2 kg CO_2 que produciría un generador diesel de 500 W que se emplea en algunos sistemas de *jamming* tradicionales.

Gestión del ciclo de vida de los componentes electrónicos

El proyecto reconoce, en Cap. 7 (pp. 96-98), que los componentes *COTS*, aunque de bajo coste, están sujetos a la normativa de gestión de residuos electrónicos (Directiva 2012/19/UE). Se propone la incorporación de un plan de reciclaje al final de la vida útil del nodo: desmontaje de la Raspberry Pi, re-uso de la placa *SDR*, y envío de los residuos a centros certificados de tratamiento de e-waste. Además, se sugiere la actualización modular del nodo (sólo sustituir la batería o la antena) en lugar de desechar todo el equipo, reduciendo la generación de residuos y fomentando la economía circular.

Impacto de la fabricación y del transporte

Aunque la fabricación de los componentes (circuitos impresos, chips de *RF*) conlleva una huella de carbono, el bajo peso total del nodo (≈ 450 g) minimiza la energía necesaria para su transporte. En escenarios de despliegue rápido, los nodos pueden ser transportados en mochilas de campo o en vehículos ya presentes en la zona, evitando la necesidad de camiones de carga especiales. Además, el modularidad permite que el re-uso de los mismos nodos en misiones sucesivas reduzca la frecuencia de reabastecimiento, disminuyendo aún más la carga logística y medioambiental.

Compatibilidad con energías renovables en el campo

El consumo reducido permite la integración del nodo con sistemas de generación de energía renovable de pequeña escala (paneles fotovoltaicos flexibles, turbinas eólicas portátiles). En pruebas preliminares (apartado 5.2.3) se conectó un panel.

ANEXO II: REFLEXIONES ÉTICAS Y SOCIALES

Implicaciones éticas y sociales

El desarrollo de un sistema de inhibición electrónica de drones no tripulados va más allá de un simple ejercicio de ingeniería técnica. Es, fundamentalmente, una intervención en la realidad social que modifica el equilibrio de poder afecta a derechos fundamentales y crea nuevos dilemas morales sin respuesta clara. En cumplimiento con el Sello Internacional de Calidad EUR-ACE, la presente memoria ha incluido, a lo largo de varias secciones, reflexiones que abordan la dimensión ética del inhibidor. Sin embargo, el carácter fragmentario de esas reflexiones requiere ser sistematizado, ampliado y profundizado en este anexo específico.

La presente reflexión ética no pretende alcanzar conclusiones definitivas ni resolver los dilemas morales inherentes al proyecto, muchos de ellos son filosóficamente irresolubles, sino más bien reconocer explícitamente la complejidad ética del trabajo, identificar las tensiones morales presentes, analizar las opciones disponibles, justificar las decisiones tomadas, y establecer mecanismo de supervisión que permitan una rendición de cuentas continua.

El problema del uso dual y la responsabilidad del inventor

Toda tecnología defensiva posee un potencial de "uso dual": puede ser empleada tanto para propósitos legítimos (defensa nacional, protección de infraestructuras críticas) como para propósitos maliciosos o no autorizados (represión política, vigilancia masiva, asalto a instalaciones civiles). El inhibidor desarrollado en este proyecto es particularmente vulnerable a este problema porque, una vez que la tecnología está documentada y el código fuente está publicado, un actor hostil podría, teóricamente, replicar el sistema y utilizarlo contra objetivos civiles o aliados.

La pregunta ética fundamental es: ¿es responsable del alumno/ingeniero desarrollar una tecnología cuyo uso adversarial potencial podría causar daño? La respuesta tradicional de la comunidad de defensa es ambivalente: por un lado, se reconoce que el desarrollo tecnológico es inevitable y que la responsabilidad última recae en los estados y en las instituciones democráticas que autorizan o prohíben el uso de tales tecnologías. Por otro lado, existe una creciente corriente de pensamiento (sostenida por filósofos como Shannon Vallor y organismos como el Partnership on AI) que sostiene que los ingenieros tienen una responsabilidad activa de considerar los usos potenciales perniciosos de sus creaciones y de implementar salvaguardas diseñadas específicamente para reducir esos riesgos.

Reconocimiento de la insuficiencia de las medidas adoptadas

A pesar de estas salvaguardas, se reconoce en el apartado 5.1 que las medidas técnicas nunca pueden eliminar completamente el riesgo de uso dual. Un estado hostil con suficientes recursos podría:

Interceptar la transmisión de datos entre nodos y adquirir información sobre el algoritmo de detección. Utilizar el conocimiento de la arquitectura para diseñar drones con firmas RF/acústicas no detectables por el sistema.

Capturar un nodo intacto y someterlo a ingeniería inversa para obtener la clave de cifrado. Esta vulnerabilidad irreducible plantea una pregunta ética incómoda: ¿debe el ingeniero abstenerse de desarrollar tecnologías defensivas si existe riesgo de mal uso? La respuesta del proyecto es negativa, fundamentada en el razonamiento que sigue: la amenaza de los drones es real y presente; muchas organizaciones defensivas carecen de medios sofisticados para contraatacar; la abstención del ingeniero no elimina la amenaza, sino que simplemente la cede a otros que podrían implementar soluciones

técnicamente inferiores o éticamente menos escrupulosas. Por lo tanto, el proyecto adopta una postura de responsabilidad compartida: el ingeniero se hace responsable de diseñar mitigaciones técnicas y de asegurar transparencia, pero reconoce que la responsabilidad política y legal última recae en los estados y en los organismos internacionales que decidan desplegar (o no) la tecnología.

Implicaciones para el desarrollo futuro

El proyecto establece una serie de recomendaciones para reducir el riesgo de mal uso en futuras iteraciones:

Incorporar un mecanismo de "geofencing" que limite el funcionamiento del inhibidor a un área geográfica predefinida. Implementar un sistema de "tiempos de caducidad" para claves criptográficas que requiera la renovación periódica de certificados de autorización. Establecer un protocolo de comunicación con organismos internacionales de control de armamentos (por ejemplo, mediante un canal de reportería a las Naciones Unidas) en caso de que se detecte un despliegue no autorizado del sistema.

Aunque estas medidas van más allá del alcance del presente *TFG*, reflejan una actitud ética proactiva: el alumno no simplemente desarrolla la tecnología y la deja al mundo, sino que anticipa problemas futuros e incorpora disposiciones para su mitigación.

Marco ético propuesto para resolver la tensión

El proyecto adopta lo que podría denominarse un enfoque de "privacidad contextual": reconoce que en situaciones de emergencia operacional (un dron aproximándose, una amenaza inmediata), la recolección mínima e inadvertida de fragmentos de comunicaciones civiles es un trade-off aceptable porque el beneficio defensivo (evitar una posible pérdida de vidas) supera el perjuicio de privacidad. Sin embargo, esta justificación solo es válida bajo condiciones muy específicas:

La amenaza debe ser real y documentada. Los mecanismos de encriptación deben garantizar que los datos no puedan ser abusados por actores internos corruptos. Debe haber supervisión democrática externa (comisiones parlamentarias, defensores del pueblo) que verifique que la herramienta no está siendo utilizada de forma extensiva contra objetivos civiles. Sin estas condiciones, la herramienta se convierte en un instrumento de represión política o de vigilancia masiva, transformando un sistema defensivo legítimo en uno éticamente inaceptable.

Responsabilidad humana, automatización y dilemas de toma de decisiones

Una de las reflexiones más profundas que emergen del proyecto es la cuestión de quién decide cuándo disparar. En sistemas militares tradicionales, la decisión de activar un arma requiere intervención humana explícita: un soldado aprieta un gatillo. Sin embargo, los sistemas modernos de defensa antiaérea introducen un grado de automatización: los algoritmos de detección y seguimiento se ejecutan automáticamente, y en algunos casos, el arma se activa sin intervención humana si se cumplen ciertos criterios predefinidos.

El inhibidor desarrollado ocupa un espacio intermedio: la detección es completamente automatizada, pero la decisión final de *jamming* es supervisada por un operador humano en la mayoría de los escenarios, aunque se contempla un modo "automático" para situaciones de amenaza extrema.

La pregunta ética subyacente es: ¿es éticamente aceptable permitir que máquinas tomen decisiones de usar fuerza, incluso bajo supervisión humana? Los filósofos especializados en "armas autónomas" como Iain Shackelford y Susan Spitz han argumentado que existe una distinción crítica entre: (a) máquinas

que ayudan a los humanos a tomar mejores decisiones (mediante información, análisis de escenarios); y (b) máquinas que toman decisiones sobre el despliegue de fuerza por sí mismas.

El proyecto se posiciona deliberadamente en el campo (a). El algoritmo de decisión no decide si *jamming*, sino que proporciona información al operador: "He detectado un dron a 300 metros, confianza 99.5 %, tiempo estimado hasta línea de fuego 12 segundos". Es el operador quien, con esa información, decide si activar el *jamming*. Esta decisión de diseño es explícita y está fundamentada en el principio ético de responsabilidad humana: la capacidad de decidir sobre el uso de fuerza debe permanecer en manos de seres humanos que puedan ser responsabilizados moralmente por las consecuencias.

Sin embargo, existe una tensión pragmática. En escenarios de amenaza muy rápida (un dron a baja altura, con tiempo de aproximación inferior a 10 segundos), el ciclo cognitivo del operador humano puede ser insuficiente para procesar la información, tomar una decisión racional y activar la contramedida. En esos casos, la insistencia en intervención humana podría resultar en un sistema inefectivo que falla en su propósito defensivo.

El proyecto resuelve esta tensión mediante un modo de operación adaptativo:

En situaciones de amenaza moderada (dron detectado, trayectoria aproximándose, pero con tiempo de reacción > 10 segundos), el sistema requiere confirmación del operador. En situaciones de amenaza inmediata y confirmada (dron en aproximación rápida, múltiples sensores lo corroboran, algoritmo de confianza > 99.5 %), el sistema está autorizado a activar el *jamming* de forma automática, pero genera una alerta posterior que el operador debe confirmar o desactivar.

Esta solución es un compromiso pragmático, pero plantea problemas éticos: ¿cómo se calibra el umbral de "amenaza inmediata"? ¿Quién es responsable si el algoritmo activa el *jamming* contra un objetivo no hostil? El proyecto aborda estas preguntas estableciendo un protocolo de revisión post-acción mediante el cual, tras cada activación del inhibidor, se lleva a cabo un análisis de causa raíz para determinar si la decisión fue correcta.

Para garantizar que la automatización parcial no se convierta en una excusa para evadir responsabilidad, el proyecto implementa un sistema de logging criptográficamente firmado donde cada acción del sistema queda documentada:

Riesgo de daño colateral

El inhibidor está diseñado para neutralizar drones hostiles, existe siempre un riesgo residual de "daño colateral": interferir con comunicaciones civiles.

Los resultados mostraron que, con los mecanismos de limitación de potencia y directividad de antena implementados, la interferencia en sistemas civiles quedaba por debajo de los umbrales de perceptibilidad (−90 dBm de potencia de campo). Sin embargo, se reconoce que estos ensayos fueron realizados en laboratorio, bajo condiciones controladas, y que el entorno operacional real (congestión espectral, reflexiones múltiples en edificios)

podría generar situaciones no previstas.

Conclusión

El desarrollo del "Inhibidor semiactivo de sistemas *UAS* para pequeñas unidades de infantería" demuestra que el alumno ha adquirido la capacidad, exigida por el sub-resultado de aprendizaje 6.1 del

sello EUR-ACE, de "recoger e interpretar datos y manejar conceptos complejos dentro de su especialidad para emitir juicios que impliquen reflexión sobre temas éticos y sociales".

Más allá de ser un documento técnico, la presente memoria es un ejercicio de responsabilidad ética: el alumno no simplemente construye la máquina, sino que reflexiona profundamente sobre sus implicaciones sociales, reconoce los riesgos de mal uso, implementa salvaguardas técnicas y procedimentales, y establece mecanismo de supervisión democrática. Los dilemas éticos no se resuelven perfectamente, porque muchos son irresolubles en principio, pero se abordan de forma rigurosa y honesta.

Esta reflexión ética, integrada a lo largo de la memoria y sistematizada en el presente anexo, evidencia una formación integral de ingeniero que comprende que la tecnología no es neutral, que el poder trae responsabilidad, y que la seguridad técnica debe complementarse siempre con ética, democracia y rendición de cuentas.

ANEXO III: DESCRIPCIÓN DE LOS PROGRAMAS DESARROLLADOS

El Anexo III recoge la documentación técnica de todos los programas desarrollados para el *TFG* sobre el inhibidor semiactivo *C-UAS*. El sistema integra dos disciplinas de inteligencia: *ACINT* para la detección por audio y *SIGINT* para la inhibición radiofrecuencia.

Programa / Archivo	Función principal
detector_acustico.py	Detector de drones por audio con umbral adaptativo y <i>GUI</i> táctica
Detector_Acustico_MERGED.py	Versión avanzada: multi-banda + DOA + <i>ML</i> integrado
Consola_DOA_MAU8.py	Consola de dirección de arribo (DOA) para array <i>MA-USB8</i>
cic_onefile.py	<i>CIC</i> unificado con Machine Learning (DADS dataset) + DOA + Auto-setup
Creador de espectrogramas.py	Herramienta de grabación y generación de espectrogramas
Inhibidor_Semiactivo.grc (Simulador)	Simulación GNU Radio: <i>CHIRP sweep</i> + <i>beamforming</i> 2,4 GHz
Inhibidor_Semiactivo_Pluto2TX_2RX.grc	Emisor <i>RF</i> real con <i>PlutoSDR+</i> (2TX / 2RX)
Inhibidor_v2_RX_Beamforming_Pluto.grc	Emisor v2: <i>beamforming</i> adaptativo en la recepción
Inhibidor_v3_ServoDF_Pluto.grc	Emisor v3: servo motorizado para apuntamiento DF automático
Inhibidor_Semiactivo_v2_RX_Beamforming.grc	Simulador v2 con DOA <i>MUSIC</i> integrado
Inhibidor_Semiactivo_v3_ServoDF.grc	Simulador v3 con servo DF automático



Figura 0-1 Código QR enlazado con el repositorio de GitHub.

Dependencias y Entorno de Desarrollo

Python

Parámetro	Descripción
numpy	Arrays numéricos y álgebra lineal
scipy	Filtros DSP, espectrograma, Welch PSD
sounddevice	Captura de audio del micrófono
pyserial	Comunicación serial con <i>MA-USB8</i> y servo
tkinter	Interfaz gráfica multiplataforma
Pillow (PIL)	Carga y redimensionado de imágenes en <i>GUI</i>
soundfile	Lectura/escritura de ficheros WAV
librosa	Extracción de <i>MFCCs</i> para <i>ML</i>
scikit-learn	Clasificador Machine Learning
huggingface_hub	Descarga del <i>dataset</i> DADS
matplotlib	Generación del espectrograma PNG

GNU Radio

- GNU Radio Companion 3.10+ con módulo gr-iio para *PlutoSDR*.
- libiio: librería de interfaz con el AD9361 del *PlutoSDR*.
- Python 3.x integrado en GNU Radio para los EPyBlocks personalizados.

Qt5 para la interfaz gráfica de los diagramas GRC.

Bloque I - Detección Acústica

El subsistema acústico implementa la inteligencia *ACINT* del proyecto. Su objetivo es detectar la presencia de *UAS* a partir del sonido que generan sus motores, hélices y electrónica, sin necesidad de emitir ninguna señal activa. Se trata de un sistema completamente pasivo en esta dimensión.

Los drones producen una huella acústica característica en la banda de frecuencias comprendida entre 1 kHz y 9 kHz, con especial energía en el rango 3.000-6.000 Hz, causada por la frecuencia de rotación de las hélices y sus armónicos. Esta característica es la base de todos los detectores implementados [15, 16].

Detector Acústico Básico - *detector_acustico.py*

Este es el programa detector de base. Implementa un *pipeline* de procesamiento de señal digital completo sobre la captura de audio del micrófono del PC o de un micrófono *USB* externo, mostrando los resultados en una interfaz gráfica táctica en tiempo real.

Arquitectura

El programa se estructura en dos clases principales que se comunican mediante una cola de mensajes thread-safe:

- **AudioWorker** (hilo de fondo): Captura audio continuamente, ejecuta el *DSP* y publica resultados.
- **DetectorUI** (hilo principal): Interfaz gráfica tkinter que consume los mensajes del worker y actualiza la visualización.

Esta arquitectura garantiza que el procesamiento de señal nunca bloquea la interfaz gráfica y que la interfaz no interfiere con la adquisición de datos.

Pipeline de Procesado de Señal Digital

Cuando se recibe audio del micrófono, se ejecuta la siguiente cadena de procesamiento:

1. Captura de audio con sounddevice a 44.100 Hz (calidad CD) en formato float32.
2. Conversión de escala a int16 para compatibilidad con el *pipeline TFG* de referencia (Aznar).
3. Filtro paso-banda Butterworth de orden 5 en la banda 3.000-6.000 Hz para aislar la huella acústica del dron.
4. Cálculo del espectrograma mediante `scipy.signal.spectrogram`.
5. Conversión a decibelios: $S_{xx_dB} = 10 \cdot \log_{10}(S_{xx} + 1e-10)$.
6. Promediado de energía en la banda de interés: `avg_energy_dB`.
7. Aplicación del umbral adaptativo con histéresis para decisión binaria de detección.

Umbral adaptativo con Histéresis

El detector no usa un umbral fijo, sino un sistema adaptativo que se calibra automáticamente al entorno acústico actual:

- Fase de calibración (3 s de silencio): el sistema mide el ruido de fondo (baseline) y calcula media y desviación típica.
- Umbral bajo (`thr_low`): `baseline_mean + 10 dB`. Si `avg_energy_dB` supera este nivel, se activa la detección.
- Umbral alto (`thr_high`): `baseline_mean + 70 dB`. Si se supera, la detección se fuerza a OFF (evita falsas alarmas por ruidos impulsivos fuertes).
- Histéresis de 3 dB: la detección se desactiva solo cuando la energía cae 3 dB por debajo del umbral bajo, evitando el 'parpadeo'.
- Auto-recalibración cada 3 minutos para adaptarse a cambios en el entorno acústico.

Parámetros configurables

Parámetro	Valor por defecto	Descripción
RATE	44.100 Hz	Frecuencia de muestreo
WINDOW_SECONDS	5,0 s	Duración de la ventana de análisis
F_LOW / F_HIGH	3.000 / 6.000 Hz	Banda de paso del filtro
BP_ORDER	5	Orden del filtro Butterworth
CALIB_SECONDS	3,0 s	Duración de la calibración inicial
MARGIN_LOW_DB	10 dB	Margen sobre baseline para <code>thr_low</code>
MARGIN_HIGH_DB	70 dB	Margen sobre baseline para <code>thr_high</code>

HYST_DB	3,0 dB	Histéresis de desactivación
AUTO_RECALIB_EVERY_SEC	180 s	Periodo de auto-recalibración

Interfaz Gráfica

La *GUI* está desarrollada con *tkinter* y presenta tres paneles en tiempo real:

- Panel izquierdo, Analizador de Espectro (Welch *PSD*): muestra la densidad espectral de potencia de 0 a 8.000 Hz, con un rectángulo ámbar indicando la banda de análisis activa.
- Panel central, Nivel Energético: barra de progreso vertical que muestra *avg_energy_dB* frente a los umbrales *thr_low* y *thr_high*. Cambia de color verde (seguro) a ámbar (detección).
- Panel derecho, Distancia estimada *UAS*: línea horizontal con iconos de buque y dron. La posición del dron se estima mediante una interpolación lineal entre *thr_low* (15 m) y *thr_high* (1 m). No es una medida real de distancia, sino un indicador cualitativo de inminencia.

La barra inferior de estado indica el modo del sistema: CALIBRANDO (ámbar), *UAS* NO DETECTADO (verde) o *UAS* DETECTADO (rojo parpadeante con alarma sonora en bucle).

Consola DOA para Array MA-USB8 - Consola_DOA_MAUSB8.py

Aplicación independiente dedicada exclusivamente a la recepción y visualización del ángulo de arribo del sonido a partir del array de micrófonos *MA-USB8 Sipeed 6+1*. A diferencia del detector merged, esta consola no realiza detección acústica: su función es puramente de localización angular y puede enviar el azimut estimado por *UDP* a otros módulos del sistema.

Funcionamiento

- Se conecta al *MA-USB8* mediante puerto serial (*USB CDC-ACM*, detección automática por heurística de nombre).
- Recibe *hotmaps* de 272 bytes de forma continua a través del protocolo serial.
- Aplica el mismo algoritmo de análisis de lóbulo que el detector merged.
- Muestra el azimut estimado en una brújula circular animada en tiempo real.
- Exporta el azimut por *UDP* (127.0.0.1:5055 por defecto) para integrarse con otros módulos como el inhibidor *RF* o el detector principal.

Interfaz del usuario

La consola presenta un radar circular ("Rosa de los vientos") con los sectores cardinales navales (N, NE, E, SE, S, SO, O, NO), una flecha verde que apunta en la dirección estimada del dron y un arco ámbar que indica el sector de incertidumbre angular. En la parte inferior se muestran el azimut exacto en grados, el sector nominal más próximo y el estado de la conexión serial.

Detector Avanzado Multibanda con DOA - Detector_Acustico_MERGED.py

Versión avanzada del detector que integra en un solo programa la detección acústica multi-banda con análisis de ratios espectrales, persistencia temporal, estimación de Dirección de Arribo (*DOA*) y comunicación serial con el array de micrófonos *MA-USB8 Sipeed 6+1*.

Mejoras respecto al Detector Básico

- Análisis multi-banda: tres bandas simultáneas (B1: 1-3 kHz, B2: 3-6 kHz, B3: 6-9 kHz) en lugar de una sola.
- Ratios espectrales: compara la energía de la banda B2 (3-6 kHz, huella de dron) frente a B1 y B3. Un dron genera más energía relativa en B2.

- Gate de *SNR*: exige una relación señal/ruido mínimo de 8 dB en B2 frente a la media de B1 y B3 antes de validar la detección.
- Persistencia N-de-M: requiere N=3 detecciones positivas en las últimas M=5 ventanas para confirmar la presencia del dron, reduciendo falsas alarmas transitorias.
- Band tracking: seguimiento adaptativo del pico espectral principal para ajustar dinámicamente la banda de análisis.
- Watchdog de micrófono: detecta si el stream de audio se ha caído y lanza una reconexión automática.
- Auto-recalibración inteligente: solo recalibra si no hay detección activa y el nivel es estable ($\text{std} < 2 \text{ dB}$ durante 20 s).

DOA integrado: lee el *hotmap* del array *MA-USB8* por puerto serial y estima el azimut del dron en tiempo real.

Estimación de Dirección de Aproximación

El *DOA* se calcula a partir del mapa de calor (*hotmap*) que envía el array de micrófonos *MA-USB8 Sipeed 6+1* a través del puerto serial *USB*:

8. Se recibe un *frame* de 272 bytes: 16 bytes de cabecera ($0xFF \times 16$) + 256 bytes de *payload* (mapa 16×16 de intensidades).
9. Se identifican las celdas del mapa con valor $\geq 70\%$ del máximo ($\text{LOBE_FRAC} = 0,70$), descartando las más cercanas al centro.
10. Se calcula la media circular ponderada de los ángulos de esas celdas activas.
11. Se estima la desviación típica circular para obtener la apertura del sector de incertidumbre.
12. Si hay dos lóbulos bien separados (situación bimodal), se reporta como 'AMBIGUO'.
13. El azimut estimado se suaviza en el tiempo con una media circular sobre los últimos N=5 *frames* para reducir el *jitter*.

Parámetros clave del detector avanzado

Parámetro	Valor por defecto	Descripción
PERSIST_M / PERSIST_N	5 / 3	Ventanas totales / positivas requeridas
R1_MIN_DB	4,0 dB	Ratio mínimo B2-B1 para validar
R2_MIN_DB	2,0 dB	Ratio mínimo B2-B3 para validar
SNR_MIN_DB	8,0 dB	SNR mínima en banda de dron
AUTO_LOW_SECONDS	20,0 s	Tiempo de nivel bajo antes de recalibrar
AUTO_STABLE_STD_DB	2,0 dB	Estabilidad requerida para recalibrar
MIC_DEAD_SECONDS	2,5 s	Tiempo sin datos para lanzar watchdog
AZ_SMOOTH_N	5	Frames para suavizado circular del azimut
LOBE_FRAC	0,70	Fracción del máximo para seleccionar lóbulo

CIC Unificado con Machine Learning - cic_onefile.py

Programa de alto nivel que combina todas las capacidades del sistema acústico en un único archivo Python pensado para su despliegue en *Linux (Ubuntu/Raspberry Pi)*. Incorpora además un clasificador de Machine Learning entrenado sobre el *dataset* DADS (Drone Acoustic Dataset) para aumentar la robustez de la detección.

Capacidades únicas

- Auto-instalación de dependencias: ejecuta automáticamente apt-get y pip para instalar todos los paquetes necesarios (portaudio, sounddevice, scikit-learn, librosa, etc.) si no están presentes.
- Descarga automática del *dataset* DADS desde Hugging Face y entrenamiento del modelo.
- Clasificador *ML*: utiliza scikit-learn para entrenar un modelo (Random Forest o similar) con hasta 12.000 muestras de audio etiquetadas como 'dron' o 'no-dron'.
- Probabilidad de dron: el modelo genera una probabilidad continua en [0,1] además de la decisión binaria por umbral ($ML_THRESH = 0,60$).
- *DOA* serial desde /dev/ttyACM* para *Linux* (equivalente al *MA-USB8* en Windows).

Sistema de logging a fichero (logs/cic_onefile.log) con timestamps.

Pipeline ML

14. Carga de muestras de audio en formato parquet (*dataset* DADS) desde data/dads/data/.
15. Extracción de características: energía en banda 3-6 kHz, MFCCs, centroide espectral, zero-crossing rate.
16. Entrenamiento del clasificador con validación cruzada.
17. Guardado del modelo en models/drone_clf.joblib para reutilización sin re-entrenamiento.
18. Inferencia en tiempo real: cada frame de audio se clasifica generando una probabilidad.

La probabilidad *ML* se combina con el umbral adaptativo *DSP* mediante un AND lógico: la alarma solo se activa si ambos sistemas están de acuerdo, maximizando la especificidad del detector.

Herramienta de Captura y Análisis - Creador de espectogramas.py

Utilidad de apoyo para la fase de análisis exploratorio y generación del *dataset* propio. Permite grabar audio del entorno durante un tiempo configurable y generar un espectrograma de alta resolución en formato PNG.

Funcionalidad

- Graba audio durante $DURACION = 10$ segundos a 16.000 Hz mono.
- Guarda el audio en formato WAV (grabacion_dron.wav) para análisis posterior.
- Calcula la Transformada de Fourier de Tiempo Corto (*STFT*) con ventana de 2.048 muestras.
- Convierte a escala dB: $S_{dB} = 20 \cdot \log_{10}(|STFT| + 1e-10)$.
- Genera un espectrograma con colormap 'magma' limitado a 0-10.000 Hz.
- Guarda la imagen como espectrograma_dron.png a 300 DPI para uso en el *TFG*.

Bloque II - Inhibidor RF con GNU Radio

El subsistema *RF* implementa el componente activo del inhibidor semiactivo *C-UAS*. Utiliza GNU Radio Companion (GRC) para generar flujos de señal que se emiten a través del transceptor *PlutoSDR+* de Analog Devices (*ADALM-PLUTO* con *firmware* desbloqueado para 2TX/2RX).

El principio de inhibición es un barrido *CHIRP* (frequency sweep) continuo en la banda 2,400-2,420 GHz (*WiFi* / control de drones) combinado con *beamforming* de dos antenas para dirigir el lóbulo de radiación hacia el dron detectado por el sistema *ACINT*. Esto hace que el inhibidor sea semiactivo: no irradia en todas las direcciones, sino solo hacia el objetivo.

Hardware empleado

Componente	Función en el sistema
<i>PlutoSDR+</i> (<i>ADALM-PLUTO</i> mod)	Transceptor <i>SDR</i> con firmware desbloqueado: 2 canales TX + 2 RX simultáneos
2 antenas TX ($\lambda/2$ @ 2,4 GHz)	Array ULA con separación 6,25 cm para <i>beamforming</i> sin grating lobes
1-2 antenas RX	Recepción para estimación DOA en versiones v2 y v3
<i>MA-USB8 / Sipeed 6+1</i>	Array acústico para DOA acústico (alimenta el ángulo al inhibidor <i>RF</i>)
Servo motor (v3)	Apuntamiento mecánico de la antena en versión v3 con Direction Finding

Simulador-v1 (*CHIRP* + *Beamforming* básico) - *Inhibidor_Semiactivo.grc*

Primer diagrama de bloques GNU Radio. Es la versión de simulación pura: el *PlutoSDR* está deshabilitado (reemplazado por un bloque Throttle que limita la tasa de procesamiento) y toda la señal se procesa en *software*. Permite desarrollar y verificar la lógica de señal sin necesidad del *hardware*.

Cadena de señal

19. EPyBlock *CHIRP* Source: genera una señal *IQ* en banda base que barre linealmente de -10 MHz a +10 MHz con periodo configurable (sweep_time). Al upconvertar, esto genera un barrido de 2,400 a 2,420 GHz.
20. Multiply Const (Antena 1): aplica la fase 0 (referencia). Amplitud = ganancia TX.
21. Multiply Const (Antena 2): aplica el desfase phi calculado para *beamforming*.
22. iio_pluto_sink (deshabilitado en simulador): en modo real enviaría las señales a los puertos TX1 y TX2 del *PlutoSDR*.
23. qtgui_freq_sink: visualizador espectral en tiempo real del flujo de señal.

Emisor Real *PlutoSDR v1* - *Inhibidor_Semiactivo_Pluto2TX/2RX.grc*

Versión del diagrama de bloques para *hardware* real. Idéntica al simulador salvo que el bloque Throttle se elimina y se activa el sink iio_fmcomms2_sink para transmitir realmente por las antenas. Este bloque utiliza el controlador *Linux* libiio a través de la interfaz fmcomms2, que el *firmware* desbloqueado del *PlutoSDR+* expone emulando el chip AD9361 del FMCOMMS2.

Configuración del *PlutoSDR*

Parámetro	Valor por defecto	Descripción
Centro de frecuencia	2,410.000.000 Hz	Centro del barrido (2,410 GHz)
Sample rate	20 MSPS	Necesario para cubrir 20 MHz de barrido
Ancho de barrido	20 MHz	Cubre la banda 2,400-2,420 GHz
Ganancia TX	Configurable dB	Slider en <i>GUI</i> (0-89 dB)

Separación antenas	0,0625 m	lambda/2 @ 2,4 GHz
URI <i>PlutoSDR</i>	ip:192.168.2.1	Dirección por defecto <i>USB/IP</i>

EpyBlock DOA

El diagrama incluye un bloque EPyBlock comentado con el esqueleto del algoritmo *MUSIC* para estimación DOA con los 2 canales RX del *PlutoSDR*. Está marcado como 'FUTURO' en los comentarios del diagrama, indicando que era parte del trabajo en desarrollo al cierre del *TFG*. El diagrama incluye un bloque EPyBlock comentado con el esqueleto del algoritmo *MUSIC* para estimación DOA con los 2 canales RX del *PlutoSDR*. Está marcado como 'FUTURO' en los comentarios del diagrama, indicando que era parte del trabajo en desarrollo al cierre del *TFG*.

Emisor v2 con DOA MUSIC- Inhibidor_v2_RX_Beamforming_Pluto.grc

Segunda versión del emisor que incorpora el algoritmo *MUSIC* completo para estimación *DOA* en tiempo real a partir de los 2 canales de recepción del *PlutoSDR*. El ángulo estimado se retroalimenta automáticamente al beamformer TX, cerrando el lazo de control.

Nuevos bloques respecto a v1

- *iio_fmcomms2_source* (2RX activo): recibe señal por RX1 y RX2 del *PlutoSDR+* en paralelo con la transmisión TX1/TX2.
- EPyBlock *DOA MUSIC* 2 elementos: recibe los flujos *IQ* de RX1 y RX2, forma la matriz de covarianza, calcula el espectro *MUSIC* y extrae el ángulo de mayor potencia. Emite *doa_angle* en grados.
- *variable_function_probe* (binding *DOA* → *beam*): actualiza *beam_angle_deg* con el valor estimado por *MUSIC* cada ciclo, dirigiendo el haz TX hacia el dron de forma automática.
- Null steering (slider): slider adicional para ajustar manualmente un nulo de radiación en una dirección específica (por ejemplo, para proteger estructuras propias).

Principio del algoritmo MUSIC

MUSIC (Multiple Signal Classification) es un algoritmo de subespacio para estimación de la dirección de arribo. A partir de la matriz de covarianza de los datos recibidos por el array, descompone el espacio en subespacio señal y subespacio ruido.

Emisor v3 con servo y encontrador de dirección

Tercera versión del emisor, integra un servo motor controlado por el ángulo *DOA* estimado, permitiendo el apuntamiento mecánico de la antena directiva TX hacia el dron de forma autónoma (Direction Finding automático).

Nuevos bloques respecto a v2

- Control de servo: el ángulo *DOA* se convierte a una señal *PWM* (0,5-2,5 ms) enviada al servo por *GPIO* o puerto serie, posicionando mecánicamente la antena TX.
- Combinación de *beamforming* electrónico (desfase ϕ en las dos antenas) con apuntamiento mecánico (servo): mayor ganancia de directividad total.

La versión simuladora correspondiente (Inhibidor_Semiactivo_v3_ServoDF.grc) reemplaza el sink *PlutoSDR* por un Throttle y el source RX por un *PlutoSDR* source, permitiendo probar la lógica *DOA* +servo con *hardware* RX real y sin necesitar el TX.

ANEXO IV: USO RESPONSABLE DE IAG

En el desarrollo del presente Trabajo de Fin de Grado se ha hecho uso puntual de herramientas de inteligencia artificial basadas en modelos de lenguaje de gran escala (*LLM*), con el objetivo de asistir en tareas de apoyo a la redacción, estructuración y revisión técnica del documento.

El empleo de estas herramientas se ha realizado bajo criterios de uso responsable, crítico y supervisado, garantizando en todo momento que la autoría intelectual, el análisis técnico y las decisiones de ingeniería corresponden íntegramente al autor del trabajo.

Herramientas empleadas

Las herramientas empleadas incluyen modelos de lenguaje generativo como ChatGPT (desarrollado por OpenAI), Claude (desarrollado por Anthropic) y Anara, todos ellos orientados a la generación y reformulación de texto, así como al apoyo en la organización y mejora de la comunicación técnica. Estas herramientas han sido utilizadas exclusivamente como sistemas de asistencia, sin que en ningún caso hayan sustituido el criterio técnico ni la capacidad de análisis del autor.

Alcance del uso

El alcance de uso de dichas herramientas se ha limitado a funciones de apoyo, tales como la mejora del estilo de redacción en apartados técnicos, la reestructuración de contenidos para su adecuación a formatos académicos, especialmente en estilo IEEE, la generación de propuestas de texto a partir de ideas previamente desarrolladas, la elaboración de pies de figura y textos descriptivos, así como la clarificación de conceptos ya conocidos. En ningún caso se han empleado para la generación de resultados experimentales, la formulación de conclusiones sin validación, la sustitución del análisis técnico propio ni la incorporación de contenido no verificado o carente de base científica.

Metodología

La metodología de uso ha seguido un enfoque iterativo basado en la interacción mediante *prompts* en lenguaje natural, en los que el autor ha definido de forma precisa el contexto, los requisitos técnicos y el objetivo de cada consulta. Las respuestas generadas han sido posteriormente analizadas críticamente, contrastadas con el conocimiento técnico propio, adaptadas al contexto específico del trabajo e integradas de forma coherente en la memoria. Este procedimiento garantiza que las herramientas han actuado exclusivamente como apoyo y no como sustituto del razonamiento ingenieril.

Listado de prompts utilizados

A continuación, se incluyen las instrucciones empleadas durante el desarrollo del trabajo:

- Estructura este capítulo de resultados para que sea más claro y lógico.
- Propón una organización óptima de figuras y tablas para facilitar la lectura del tribunal.
- Reformula este texto para evitar repeticiones y mejorar la claridad.
- Explica las implicaciones de la reverberación en la detección acústica en espacios confinados.
- Explica de forma clara el efecto de los armónicos en la detección de *UAS*.
- Describe el comportamiento de umbrales adaptativos en entornos con ruido variable.
- Ofrece una explicación del funcionamiento de un sistema *DOA* aplicado a detección de drones.
- Explica la relación entre *SNR* y capacidad de detección en sistemas acústicos.
- Explica el comportamiento del sistema durante una aproximación del *UAS*.
- Propón una forma más clara de presentar estos datos experimentales.
- Genera una transición adecuada entre el apartado acústico y el de radiofrecuencia.

- Explica este concepto de forma más clara manteniendo el nivel de ingeniería.
- Ayúdame a orientar el apartado de líneas futuras a partir de estas carencias detectadas.
- Reformula este texto para evitar ambigüedades.

En conclusión, la integración de herramientas de inteligencia artificial en el desarrollo del presente trabajo ha permitido mejorar la claridad expositiva, la coherencia estructural y la calidad formal de la memoria, sin comprometer en ningún momento el rigor técnico ni la autoría del mismo. Su utilización, limitada y bajo control, se enmarca en un uso legítimo de herramientas de apoyo, equiparable a otros recursos habituales en la elaboración de documentos técnicos.