MICA
Matemáticas Ingeniería y Ciencias Ambientales
ISSN: 2594-1933
Tepic, Nayarit; México

Vol. 8 No. 16.
Periodo: julio-diciembre 2025
DOI: 10.58299/mica.v8i16.106
Pp. 1-26

Sistema de perturbación de vehículos aéreos no tripulados mediante técnicas de Spoofing y Jamming, con cifrado AES-256

Counter-UAV system employing spoofing and jamming techniques, with AES-256 Encryption

Brayan Ortiz Hernández
brayanortiz12042002@gmail.com
https://orcid.org/0009-0003-8121-2020

José Alfredo Castellanos Suarez
jcastellanoss@chapingo.mx
https://orcid.org/0000-0001-8950-1992

David Benjamín Vásquez Torres
d.benjamin.vasquez@gmail.com
https://orcid.org/0009-0003-9876-9992

Angeles Segura Segura
a22232228@liceoupg.edu.mx
https://orcid.org/0009-0003-0477-5516

Universidad Autónoma Chapingo

Resumen

El uso creciente de Vehículos Aéreos No Tripulados (UAV) en aplicaciones civiles y militares ha impulsado la necesidad de sistemas de detección y monitoreo eficientes. Este trabajo presenta un sistema innovador basado en tecnología LoRa, diseñado para la detección y rastreo de UAVs. Utilizando módulos LILYGO TTGO LoRa32 con transceptores SX1276 y microcontroladores ESP32, el sistema opera bajo una arquitectura punto a punto (P2P) sin dependencia de infraestructura LoRaWAN, optimizando el consumo energético y maximizando la autonomía. Se implementó cifrado AES-256 para garantizar la integridad y confidencialidad, mitigando riesgos de interceptación y manipulación de datos. El sistema fue evaluado en entornos controlados y operacionales, demostrando alto rendimiento en métricas clave como alcance efectivo, tasa de error de paquetes, latencia de transmisión y resistencia a interferencias electromagnéticas. Los resultados validan su viabilidad técnica y su potencial para aplicaciones críticas en vigilancia y defensa.

Palabras clave: análisis espectral; cámara anecoica; LoRa (Long Range); Radio Definida por Software (SDR); telemetría.

Abstract

The increasing use of Unmanned Aerial Vehicles (UAVs) in civil and military applications has driven the need for efficient detection and monitoring systems. This work presents an innovative system based on LoRa technology, designed for the detection and tracking of UAVs. Using LILYGO TTGO LoRa32 915 MHz V1.6.1 modules equipped with SX1276 transceivers and ESP32 microcontrollers, the system operates under a point-to-point (P2P) architecture without reliance on LoRaWAN infrastructure, optimizing energy consumption and maximizing operational autonomy. AES-256 encryption was implemented to ensure data integrity and confidentiality, mitigating risks of interception and data tampering. The system was evaluated in both controlled and operational environments, demonstrating high performance across key metrics such as effective communication range, packet error rate, transmission latency, and resistance to electromagnetic interference. The results validate its technical feasibility and highlight its potential for critical applications in surveillance and defense.

Key words: Anechoic Chamber; LoRa (Long Range); Software-Defined Radio (SDR); Spectral Analysis; Telemetry.

Introducción

El rápido desarrollo y la creciente adopción de los Vehículos Aéreos No Tripulados (UAV) han generado un impacto significativo en múltiples ámbitos de la sociedad contemporánea. La expansión de estas plataformas como herramientas de reconocimiento, supervisión y vigilancia ha impulsado la necesidad de desarrollar sistemas eficientes para la detección de drones no autorizados, especialmente en entornos complejos (Shakhatreh et al., 2019). En la actualidad, su popularidad se explica por la versatilidad que ofrecen para ejecutar misiones en entornos de difícil acceso, así como por su eficiencia en tareas tanto civiles como militares.

En el ámbito civil, los UAV se emplean de manera extensiva en operaciones de búsqueda y rescate, monitoreo ambiental, estudio de ecosistemas y supervisión de infraestructuras críticas como líneas eléctricas y oleoductos. De forma paralela, su uso en el sector militar se ha intensificado, abarcando funciones que van desde la vigilancia estratégica y el espionaje hasta la ejecución de operaciones ofensivas mediante sistemas armamentísticos integrados. Esta dualidad de aplicaciones ha incrementado la complejidad del entorno aéreo y ha evidenciado la necesidad de desarrollar mecanismos eficaces para la detección, identificación y mitigación de amenazas asociadas al uso no autorizado o malicioso de UAV.

Uno de los principales desafíos técnicos en la detección y neutralización de UAV se encuentra en la selección de los sistemas de comunicación y las bandas de frecuencia utilizadas para su operación. Las bandas de 2.4 GHz y 5.8 GHz son ampliamente empleadas debido a su compatibilidad con tecnologías inalámbricas comerciales; no obstante, presentan elevados niveles de congestión y una alta susceptibilidad a interferencias, lo que compromete la integridad de las comunicaciones y facilita ataques de interferencia intencional o jamming (Arroyo et al., 2022). Estas limitaciones han impulsado la exploración de tecnologías alternativas que ofrezcan mayor robustez y confiabilidad en entornos operativos complejos.

En este contexto, la tecnología LoRa (Long Range) surge como una solución viable para sistemas de vigilancia y detección pasiva, al proporcionar comunicaciones de largo alcance con bajo consumo energético y alta resistencia a interferencias electromagnéticas. LoRa opera en bandas de frecuencia libre, como 915 MHz en América, 868 MHz en Europa y 433 MHz en Asia, lo que permite una propagación eficiente de la señal incluso en entornos con obstáculos y ruido electromagnético significativo. Además, la modulación Chirp Spread Spectrum (CSS) mejora la sensibilidad del receptor y la detección de señales de baja potencia, incrementando la confiabilidad del sistema (Guevara-Bonilla et al., 2020).

Paralelamente, los UAV enfrentan amenazas activas como el *spoofing* de señales GPS y el *jamming* selectivo, técnicas que explotan vulnerabilidades en protocolos estándar, tales como la ausencia de autenticación en el GPS civil o el uso de esquemas de cifrado débiles en enlaces de radiofrecuencia. Estas amenazas pueden provocar la pérdida de control, la redirección del UAV o la interrupción total de las comunicaciones, comprometiendo la seguridad del espacio aéreo. Ante este escenario, la incorporación de mecanismos de protección criptográfica robustos se vuelve indispensable para garantizar la integridad y confidencialidad de la información transmitida.

Con el fin de mitigar estas vulnerabilidades, la implementación de cifrado simétrico AES-256 en los enlaces de comunicación representa una estrategia eficaz para fortalecer la seguridad del sistema. Este estándar criptográfico, ampliamente utilizado en aplicaciones de seguridad crítica, proporciona una protección robusta frente a ataques de interceptación y manipulación de datos, asegurando comunicaciones resilientes incluso en entornos hostiles. La integración de AES-256 con tecnologías de largo alcance como LoRa contribuye a reforzar la privacidad, confiabilidad y estabilidad operativa de los sistemas de detección y monitoreo de UAV.

Problema de investigación

Uno de los principales desafíos asociados a la detección y monitoreo de UAV radica en los sistemas de comunicación utilizados, ya que los enlaces inalámbricos que operan en bandas compartidas como 2.4 GHz y 5.8 GHz presentan altos niveles de congestión e interferencia. Estas condiciones pueden comprometer la integridad de las comunicaciones y facilitar ataques de interferencia deliberada (*jamming*), afectando la confiabilidad de los sistemas de detección. Ante este panorama, surge la necesidad de identificar alternativas tecnológicas que ofrezcan comunicaciones más robustas y resilientes en entornos operacionales adversos. En este contexto, la tecnología LoRa (Long Range) se perfila como una opción viable debido a su largo alcance, bajo consumo energético y resistencia a interferencias electromagnéticas, características que pueden fortalecer la detección y rastreo de UAV. Asimismo, la implementación de mecanismos de seguridad como el cifrado AES-256 y el uso de C*hecksum* resulta fundamental para proteger la información transmitida y garantizar su integridad frente a posibles amenazas.

Referente teórico

Un vehículo aéreo no tripulado (UAV, por sus siglas en inglés) es una aeronave que opera sin piloto humano a bordo y puede ser controlada de forma remota o mediante sistemas

autónomos basados en sensores y procesamiento computacional. Estos sistemas se emplean en aplicaciones civiles y militares, incluyendo vigilancia, reconocimiento, agricultura, investigación científica y operaciones tácticas, lo que ha incrementado la dependencia de enlaces de comunicación y navegación confiables (Zidane et al., 2024). La creciente integración de UAV en escenarios críticos exige mecanismos que garanticen la integridad operativa y la seguridad de la información transmitida.

La navegación de los sistemas aéreos no tripulados depende en gran medida de los Sistemas Globales de Navegación por Satélite (GNSS), los cuales son vulnerables a interferencias intencionadas y no intencionadas. Entre las amenazas más relevantes se encuentra el *jamming*, definido como la interferencia deliberada de las señales GNSS mediante la inyección de ruido, lo que puede provocar la pérdida de la señal o errores significativos de posicionamiento (Motella et al., 2025). Estas interferencias comprometen la capacidad de navegación de los UAV, pudiendo causar desviaciones de ruta, fallos de misión o exposición a riesgos operativos (Kuusniemi, 2012).

Otra amenaza crítica para los sistemas GNSS es la suplantación (*spoofing*), la cual consiste en la generación y transmisión de señales falsas que imitan las legítimas, engañando al receptor para producir información de posicionamiento incorrecta. A diferencia del *jamming*, la suplantación altera el patrón de modulación de la señal, afectando parámetros como la amplitud y la fase, lo que dificulta su detección (Bhowmick et al., 2021). Este tipo de ataque puede inducir al sistema a seguir trayectorias erróneas sin generar alertas inmediatas, representando un riesgo elevado para la operación segura de UAV (Caparra et al., 2017), (Kalantari y Larsson, 2020).

Las redes inalámbricas que permiten la operación y versatilidad de los UAV presentan mayores riesgos de seguridad en comparación con las redes cableadas, debido a su naturaleza abierta y a la exposición del medio de transmisión. La seguridad en estos sistemas se fundamenta en el cumplimiento de la tríada CIA: confidencialidad, integridad y disponibilidad de la información (CCN, 2016). La identificación de vulnerabilidades en los enlaces de comunicación constituye una etapa esencial para el diseño de mecanismos de protección que mitiguen ataques y fallos de seguridad (Liberatori, 2006).

Es relevante distinguir entre los mecanismos de seguridad implementados en UAV de uso militar y aquellos presentes en drones civiles o recreativos. Mientras que los sistemas militares incorporan protocolos robustos como requisito operativo, los drones de consumo suelen carecer de medidas de protección avanzadas, lo que incrementa significativamente su exposición a

ataques y vulnerabilidades (Lugo y Ríos, 2025). Esta diferencia resalta la necesidad de adoptar estrategias de seguridad adaptadas a sistemas UAV de uso general.

El cifrado constituye uno de los mecanismos fundamentales para proteger la información transmitida en sistemas de comunicación inalámbrica. El estándar Advanced Encryption Standard (AES) admite longitudes de clave de 128, 192 y 256 bits, siendo esta última la opción más robusta frente a ataques por fuerza bruta (Amna et al., 2025). Al tratarse de un sistema de cifrado simétrico, AES requiere que emisor y receptor compartan la misma clave, lo que mejora el rendimiento computacional y garantiza que únicamente los sistemas autorizados puedan acceder a la información cifrada (Barker y Mouha, 2017).

Objetivo:

Desarrollar e implementar un sistema de defensa perimetral que detecte, identifique y neutralice UAVs no autorizados en zonas restringidas, mediante tecnología LoRa con cifrado AES-256, garantizando la seguridad del espacio aéreo.

Hipótesis:

La implementación del Sistema C-UAS, desarrollado con arquitectura modular integrando SDR de banda ancha (70 MHz-6 GHz), amplificadores RF de estado sólido (GaN) y cifrado AES-256 embebido, permitirá la detección, identificación y neutralización de UAVs mediante técnicas de jamming y spoofing GPS con un 95% de efectividad en un radio de 3 km.

El sistema garantizará comunicaciones seguras punto a punto con inmunidad a interferencias electromagnéticas y capacidad de geolocalización en tiempo real con error menor a 5 metros, fortaleciendo la defensa de espacios aéreos críticos. Su diseño modular permitirá la integración con infraestructura militar existente, ofreciendo una solución escalable y replicable para aplicaciones tácticas y de seguridad nacional. Adicionalmente, este desarrollo sentará las bases tecnológicas para la próxima generación de sistemas C-UAS con capacidades de guerra electrónica adaptativa.

Metodología

Clasificación y diseño de la investigación

La investigación se clasificó por el tipo de datos recolectados como cuantitativa, dado que se obtuvieron mediciones numéricas asociadas al alcance de detección, altitud de vuelo, intensidad de señal y desempeño de los sistemas anti-dron evaluados; el alcance o profundidad

de la investigación fue descriptivo–comparativo, toda vez que se caracterizó el comportamiento de un sistema C-UAS propuesto y se comparó con un sistema comercial de referencia bajo distintos escenarios operativos; según la fuente de recolección de datos, la investigación fue observacional (no experimental), ya que no se manipuló deliberadamente ninguna variable independiente y los datos se registraron en condiciones reales de prueba; de acuerdo con el plan de recolección de datos, el estudio fue transversal, debido a que la información se obtuvo en un solo periodo de tiempo durante pruebas controladas de campo, siguiendo lineamientos metodológicos ampliamente aceptados en estudios de evaluación tecnológica y sistemas de seguridad aérea.

Población de estudio

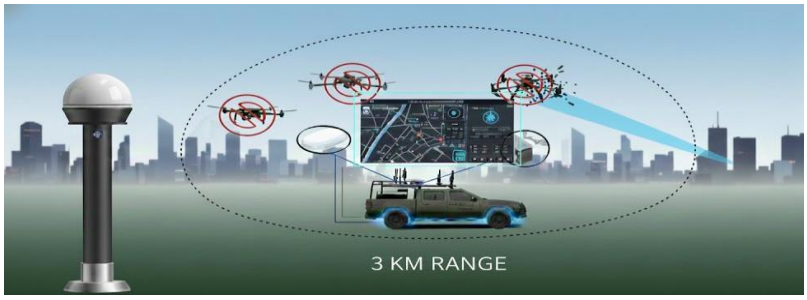
La muestra estuvo integrada principalmente por drones DJI, incluyendo los modelos Matrice 30, Mavic 3, Mavic 3 Pro, Agras T20 y Agras T30, de acuerdo con la disponibilidad operativa para la validación del sistema.

Instrumentos de investigación

El Sistema C-UAS fue diseñado como una plataforma integral para la defensa de espacios aéreos restringidos. La arquitectura, ilustrada en la Figura 1, se compone de cuatro módulos principales interconectados: detección (SDR y antenas de amplio espectro electromagnético), comunicación segura (LoRa con cifrado AES-256), perturbación (jamming adaptativo y spoofing GPS) y control (PLCs e interfaz web). La Tabla 1 detalla los componentes clave del hardware. La metodología de desarrollo siguió un enfoque iterativo basado en Design Thinking, priorizando los requisitos operativos de la Secretaría de Marina Armada de México para garantizar una solución robusta y efectiva.

Figura 1

Configuración operacional del sistema mostrando cobertura omnidireccional (3 km) y direccional (500 m) (Simulación).



Nota: Elaboración propia en colaboración con UNINDETEC, [2025].

Tabla 1

Componentes básicos de hardware del Anti-Dron.

Componente	Especificaciones Técnicas
Tarjeta ANT-SDR-E200	Procesador RF AD9361, 70 MHz – 6 GHz
LoRa32 915 MHz V1.6.1	Comunicación segura, cifrado AES-256
T-Beam V1.2 + NEO-6M	GPS integrado, transmisión LoRa
GlobalSat BU-353N5	Receptor GNSS, referencia de posición
BladeRF x40	Spoofing GPS, 300 MHz – 6 GHz
Valve Steam Deck 512 GB	Interfaz de control en tiempo real
ASUS ROG Strix G16	Estación de procesamiento de datos SDR
Amplificadores 20W/30W	Potencia de perturbación, jamming
Fuente QUINT-DC UPS/24DC/20	Alimentación 230V – 24VDC, 20A
Inversor Energizer 3000W	Conversión DC–AC, respaldo energético
Antenas tipo corneta Ubiquiti 60 GHz	Enlaces direccionales, alta ganancia
Carcasas personalizadas PLA/Acero	Protección de dispositivos, diseño modular
PLC Siemens S7-1200	Control automatizado, comunicación PROFINET
Antenas directivas 2.4 / 5.8 GHz	Interferencia específica para WiFi/drones
Switch MOXXA	Comunicación de red PLCs, 24 puertos
JavaScript / Node.js	Interfaz web React, backend API
Visual Studio Code	Entorno de desarrollo frontend y backend
Kali Linux	Análisis de seguridad, pruebas de infiltración

Nota: Elaboración propia en colaboración con UNINDETEC, [2025].

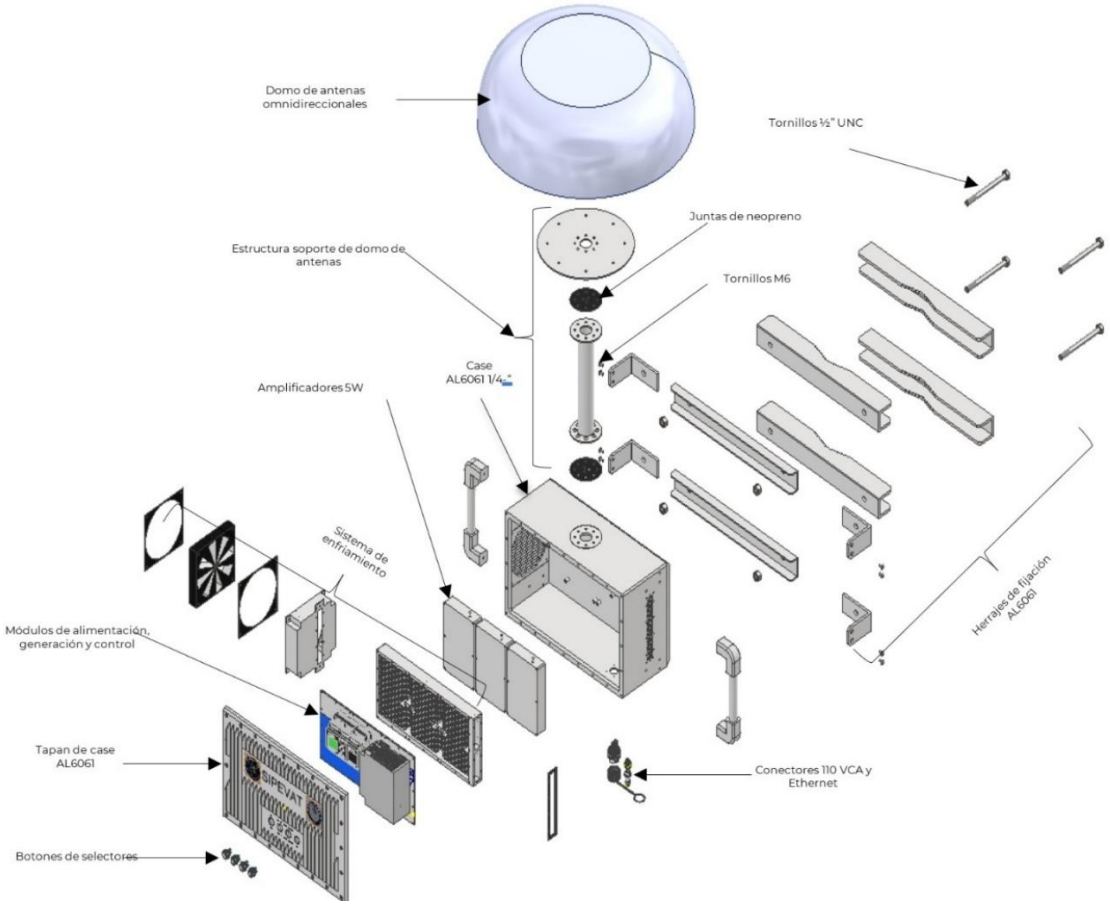
Diseño mecánico

El diseño mecánico del C-UAS se estructura en una carcasa principal fabricada en aluminio AL6061 T6, material seleccionado por su alta resistencia y ligereza, la cual alberga de forma modular los componentes críticos: los módulos de alimentación, generación y control, así como los amplificadores de RF de 5W. La base inferior de la carcasa (“Case AL6061 1/4”) incorpora botones selectores y puertos de conexión para alimentación de 110 VCA y comunicación Ethernet, asegurando una interfaz operativa robusta y accesible.

El ensamble se realiza mediante un sistema de sujeción que utiliza tornillos de ½” UNCyM6, combinado con juntas de neopreno que proporcionan sellado y aislamiento anti vibratorio, garantizando la integridad estructural y la protección de los circuitos internos frente a condiciones ambientales adversas, como se detalla en la Figura 2.

Figura 2

Vista mecánica del diseño, mostrando la carcasa modular en aluminio AL6061 T6.



Nota: Elaboración propia en colaboración con UNINDETEC, [2025].

Diseño Eléctrico

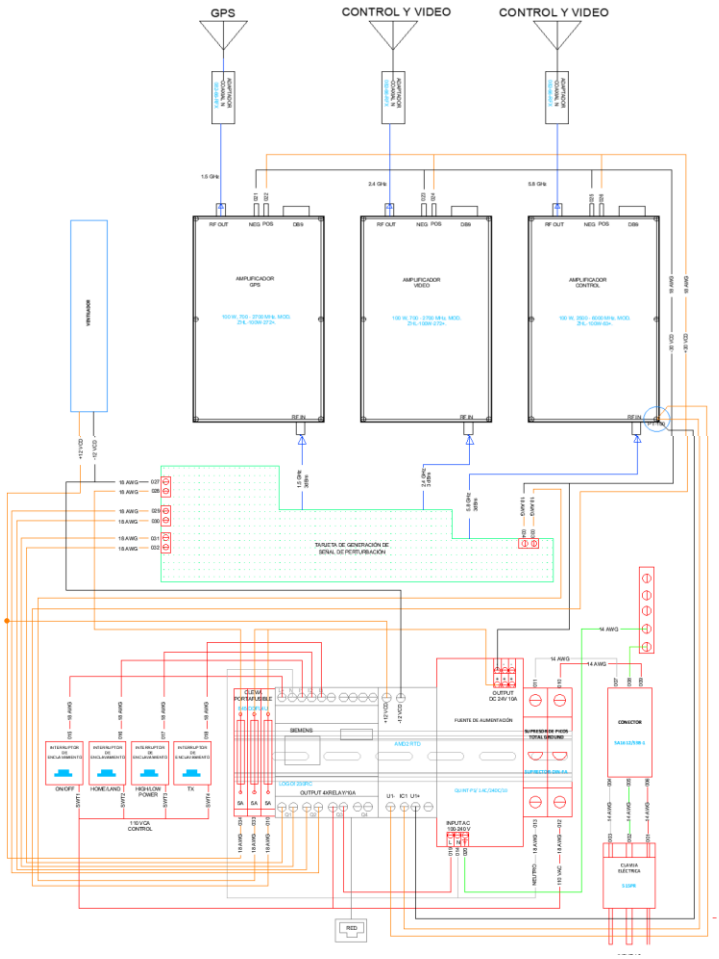
La infraestructura eléctrica se diseñó en torno a una arquitectura de potencia robusta y redundante. La alimentación primaria de 110 VCA es acondicionada mediante un supresor de picos y convertida a 28 VCC mediante un puente de potencia, distribuyéndose a través de una fuente UPS (QUINT-DC-UPS/24DC/20) que garantiza la continuidad operativa. Este diseño incorpora protecciones termomagnéticas y un inversor de 3000 W para respaldo, asegurando la operación estable de los amplificadores de RF (5 W/20 W), los PLCs de control y el sistema de refrigeración forzada, incluso en condiciones de inestabilidad de la red principal.

La distribución de potencia se implementa de forma modular y supervisada, con circuitos independientes para las etapas de RF, control y climatización, tal como se esquematiza en la

Figura. 3 El controlador principal (PLC) monitorea en tiempo real los parámetros de la UPS, la temperatura de los amplificadores mediante sensores PT-100 y el estado de la carga, proporcionando redundancia energética y protección integral contra fallos para cumplir con los requisitos de confiabilidad en entornos tácticos.

Figura 3

Diagrama de Bloques del Sistema de Alimentación y Distribución de Frecuencias para el Banco de Pruebas C-UAS.



Nota: Elaboración propia en colaboración con UNINDETEC, [2025].

Diseño Electrónico

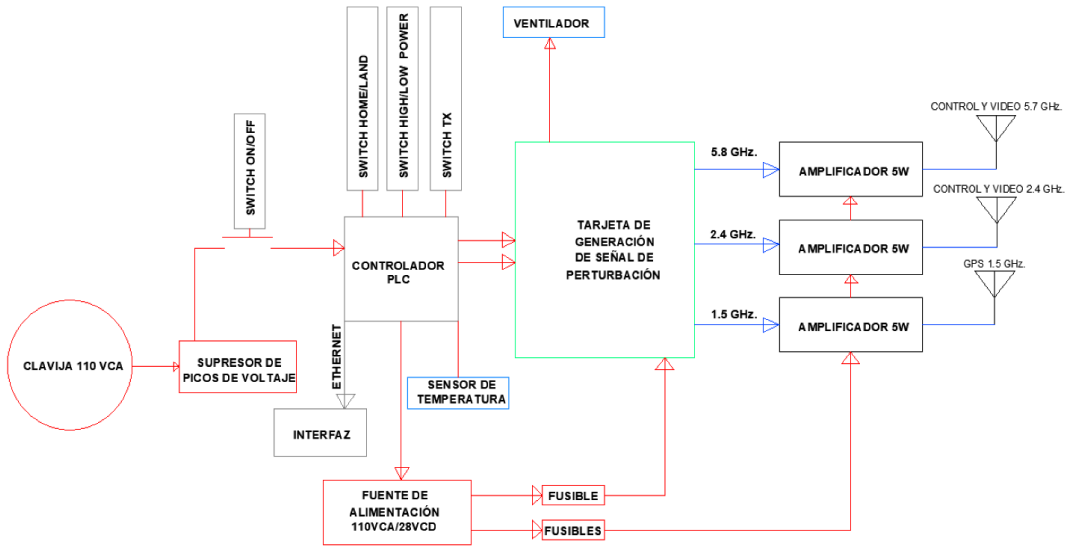
La infraestructura electrónica del sistema se sustenta en una arquitectura modular en cascada, concebida para garantizar resiliencia, escalabilidad y operación en tiempo real en escenarios de defensa aérea. Esta estructura define con precisión las etapas críticas de

adquisición, síntesis, amplificación y control de señales de radiofrecuencia (RF), habilitando tanto la detección pasiva de UAV mediante parámetros espectrales como la generación activa de contramedidas electrónicas.

El diseño responde a los requerimientos de un sistema C-UAS (Counter-Unmanned Aircraft System) de nueva generación, integrando componentes de alta linealidad y baja latencia, optimizados para operar en entornos electromagnéticamente adversos. La combinación de SDR de banda ancha, amplificadores RF de estado sólido y módulos de autenticación criptográfica AES-256 con telemetría LoRa consolidan a C-UAS como una plataforma resiliente y criptográficamente segura, capaz de ejecutar con alta confiabilidad tareas de detección, identificación y neutralización electrónica frente a amenazas no tripuladas, validada en escenarios de prueba controlados, como se ilustra en la Figura 4.

Figura 4

Diagrama a bloques del diseño de Sistema de Perturbación de Vehículos Aéreos No Tripulados.



Nota:

Elaboración propia en colaboración con UNINDETEC, [2025].

1. SDR de Banda Ancha (ANT-SDR-E200)

El transceptor Software-Defined Radio (SDR) ANT-SDR-E200, mostrado en la Figura 5. Constituye el núcleo del subsistema de inteligencia de señales del C-UAS. Basado en el

transceptor RF AD9361, este componente opera en un rango de frecuencia de 70 MHz a 6.0 GHz con un ancho de banda instantáneo de 56 MHz, cubriendo las bandas críticas de comunicación UAV (ISM 2.4 GHz, 5.8 GHz) y navegación GPS. Su arquitectura 2x2 MIMO y convertidores de 12 bits le proporcionan la versatilidad y rango dinámico necesario para aplicaciones de defensa electrónica.

En el sistema cumple una función dual esencial: realiza la detección pasiva de UAVs mediante análisis espectral en tiempo real (RSSI, SNR) y genera señales de spoofing GPS de alta precisión. Su naturaleza de software definido permite la reconfiguración dinámica para adaptarse a diversas amenazas, actuando como el elemento central de inteligencia y contramedidas electrónicas en la arquitectura C-UAS.

Figura 5

Plataforma SDR de banda ancha (70 MHz-6 GHz) empleada en el sistema.

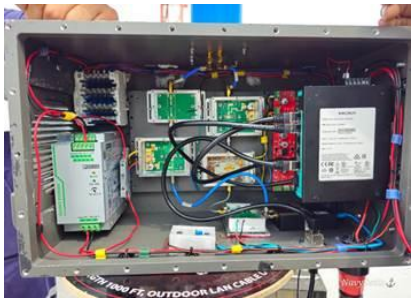
Nota: Elaboración propia, [2025].

2. Amplificadores RF de Estado Sólido

Los amplificadores RF de estado sólido, mostrados en la Figura 6, constituyen la etapa de potencia de salida del sistema, basados en tecnología de Nitruro de Galio (GaN), estos amplificadores operan en las bandas de interferencia críticas de 1.5~GHz (GPS L1), 2.4~GHz y 5.7~GHz (bandas ISM) con potencias de salida de 8~W (39~dBm) y 20~W (43~dBm).

Figura 6

Amplificadores RF de estado sólido (8 W y 20 W) basados en GaN, con operación 70 MHz–6.0 GHz.



Fuente: Elaboración propia, [2025].

El diseño incorpora circuitos de adaptación de impedancia de banda estrecha optimizados para máxima transferencia de potencia y una eficiencia energética superior al 40%, incluso a niveles de saturación. Esta eficiencia es crucial para gestionar la disipación térmica en operación continua. La selección de la banda de 2.4 GHz como objetivo primario es estratégica, ya que esta es una banda ISM globalmente asignada y comúnmente utilizada por enlaces de control de UAV, lo que aumenta la efectividad de las contramedidas. La elevada densidad de potencia radiada resultante garantiza la efectividad del sistema en la neutralización de drones en un radio de 2 km.

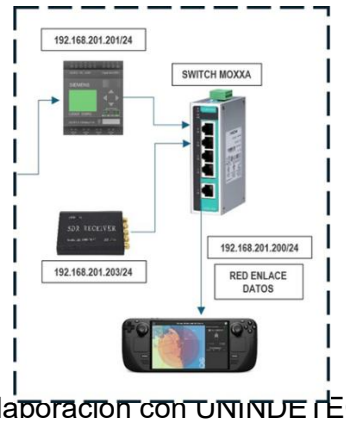
3. Sistema de Control con PLC Logo! 230 RCE

Como parte de las mejoras al sistema, se implementó un rediseño completo del programa de control para los PLCs Logo 230 RCE en configuración maestro-cliente, interconectados mediante un switch industrial no administrable MOXXA con protocolo Modbus/TCP. La arquitectura de control se optimizó mediante el mapeo completo de las 16 entradas/salidas digitales del PLC maestro hacia el PLC cliente, estableciendo una transferencia síncrona de señales de control con latencia determinista menor a 10 ms. Adicionalmente, se implementaron retardos programados de conexión (0.5-2 s) y desconexión (3-5 s) en la lógica de control para garantizar el reinicio seguro del SDR de detección ANT-SDR-E200, previniendo condiciones de carrera y minimizando errores de sincronización durante fallos de red.

La comunicación se estableció bajo el modelo cliente-servidor TCP/IP con direccionamiento IP estático en la red 192.168.201/24, priorizando la robustez mediante mecanismos de watchdog interno y reconexión automática ante pérdidas temporales de enlace. La configuración específica de red y el mapeo de E/S se documenta en la Figura 7.

Figura 7

Topología de red experimental que muestra la interconexión de los nodos del sistema a través del switch principal.



Fuente: Elaboración propia en colaboración con UNINDE IEC, [2025].

4. Tarjeta de procesamiento RF BladeRF

La unidad de procesamiento de señales de radiofrecuencia BladeRF 2.0 micro, mostrada en la Figura 8 constituye el núcleo del subsistema de generación de señales de *spoofing* GPS. Basada en el transceptor LMS7002M, esta plataforma SDR de alto rendimiento opera en un rango de frecuencia de 47 MHz a 6 GHz con un ancho de banda instantáneo de 61.44 MHz, cubriendo las bandas civiles de navegación GPS L1 (1575.42 MHz) y GLONASS G1 (1602 MHz).

El hardware incorpora un FPGA Intel Cyclone V que permite la implementación de algoritmos de suplantación GPS en tiempo real, generando efemérides y señales de navegación falsas con precisión de microsegundos. La arquitectura de dos canales full-duplex permite la recepción simultánea de señales GPS legítimas y la transmisión de señales de \textit{spoofing}, facilitando ataques de suplantación coherentes y sincronizados.

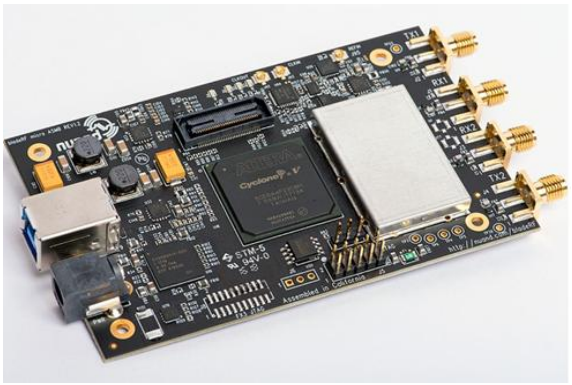


Figura 8

Plataforma SDR con transceptor LMS7002M y FPGA Intel Cyclone V para generación de señales de navegación.

Nota: Elaboración propia, [2025].

5. LILYGO TTGO LoRa32 915Mhz V1.6.1

El módulo de comunicación inalámbrico LILYGO® TTGO LoRa32 915MHz V1.6.1, mostrado en la Figura 9 constituye el nodo de transmisión segura del sistema de identificación de UAVs institucionales en el C-UAS. Basado en el microcontrolador ESP32 con chip RF Semtech SX1276, este componente opera en la banda ISM de 902-928 MHz (América) con una sensibilidad de recepción de -148 dBm y potencia de transmisión ajustable hasta 20 dBm (100 mW).

La arquitectura hardware integra un coprocesador criptográfico dedicado que ejecuta localmente el algoritmo AES-256 mediante instrucciones específicas del conjunto RISC-V del ESP32. El diseño incorpora 4 MB de memoria flash SPI PSRAM, antena PCB impresa optimizada para 915 MHz, reguladores de voltaje LDO de bajo dropout, y 19 pines GPIO con interfaces UART, SPI e I²C para expansión de periféricos.

Figura 9

Prototipos LoRa de transmisión y recepción cifrada desarrollados para el sistema C-UAS.

Nota: Elaboración propia, [2025].

6. T-Beam V1.2 LoRa32 915 MHz NEO-6M

El módulo de navegación y comunicación inalámbrico LILYGO® TTGO T-Beam V1.2, mostrado en la Figura 10 constituye la unidad de telemetría segura con geolocalización. Basado en el microcontrolador ESP32 con chip RF Semtech SX1276, este componente integra un receptor GNSS u-blox NEO-6M para posicionamiento global y opera en la banda ISM de 902-928 MHz con potencia de transmisión ajustable hasta 20 dBm.

La arquitectura hardware incorpora una antena GPS activa de 25×25 mm con amplificador LNA integrado, regulador de voltaje buck-converter de alta eficiencia para operación con batería LiPo, puerto I²C para sensores externos, y conector JST para sistemas de potencia externos. El diseño incluye un coprocesador criptográfico que ejecuta el algoritmo AES-256 para el cifrado de paquetes de telemetría que fusionan datos GNSS, RSSI y SNR.

Figura 10

Unidad de telemetría cifrada T-Beam V1.2 desplegada en UAV institucional, proporcionando autenticación criptográfica mediante AES-256.

Nota: Elaboración propia, [2025].

Desarrollo e Implementación de Software

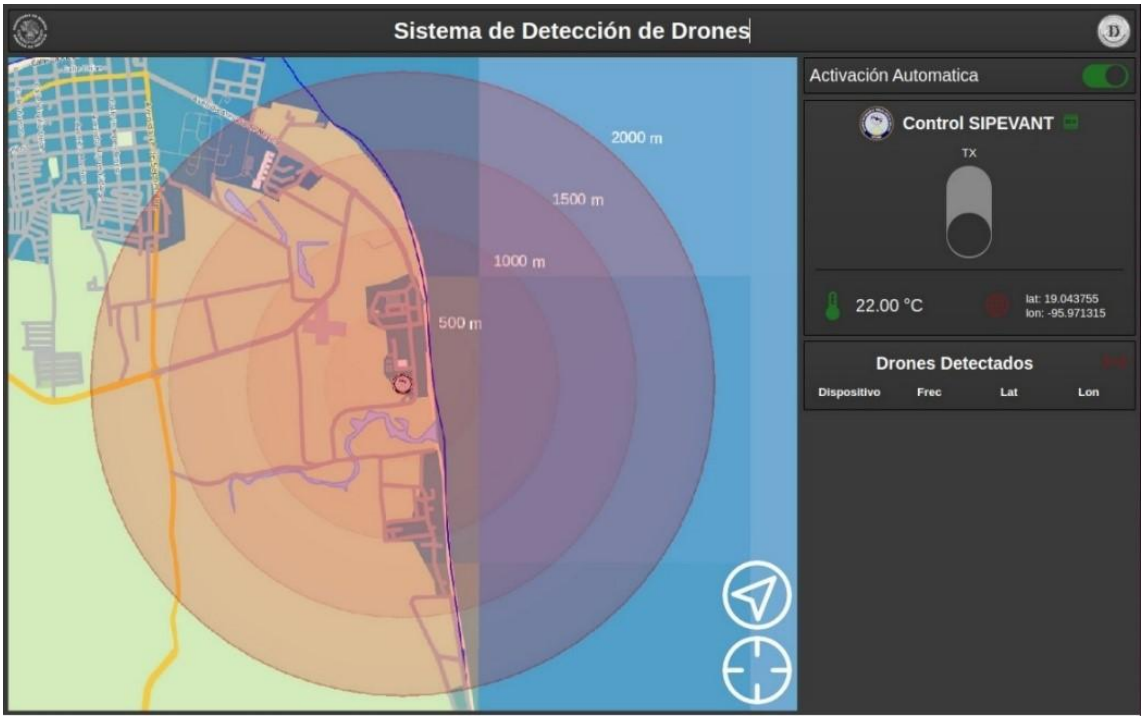
En cumplimiento del requerimiento de la Unidad de Investigación Naval (UIN), se desarrolló un sistema de registro e identificación de drones institucionales utilizando dispositivos LoRa32 y módulos T-Beam con tecnología RFID para el etiquetado digital. El sistema opera en la banda de 915 MHz, garantizando comunicaciones seguras y confiables a distancias de hasta 3 km, mediante la validación de los parámetros RSSI y SNR. Los programas embebidos permiten

transmitir de forma encriptada los identificadores únicos y coordenadas de cada dron mediante AES-256 y checksum, asegurando la integridad de los datos.

Finalmente, la información se integra en la interfaz web, donde se visualiza y monitorea en tiempo real la posición de los UAV, permitiendo la clasificación automática de blancos amigo-enemigo (ver Figura 11).

Figura 11

Interfaz Web del sistema de vigilancia C-UAS.



Nota: Módulos: (A) Rango de distancia, (B) Datos meteorológicos, (C) Coordenadas de latitud/longitud y lista de los activos aéreos detectados. Visualización de áreas de cobertura de detección de drones. (UNINDETEC 2025). Elaboración propia en colaboración con UNINDETEC, [2025].

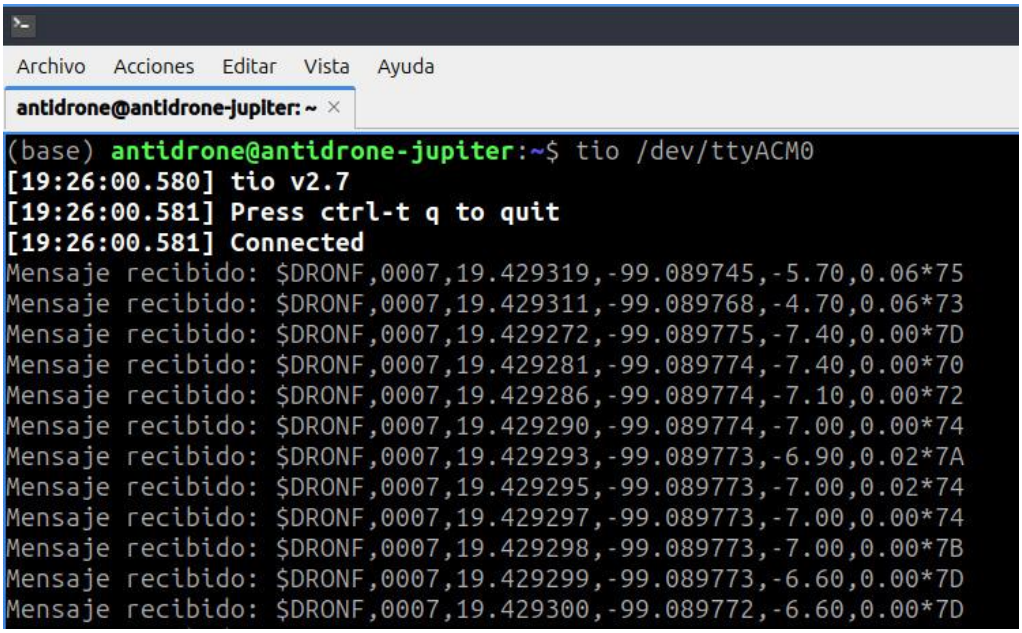
1. Telemetría y transmisión de datos:

Las Figuras 12 a 15 documentan el análisis comparativo de cinco esquemas de comunicación evaluados en el sistema de telemetría geoespacial. La configuración óptima (Figura 12) implementa cifrado AES-256 bidireccional, garantizando confidencialidad e integridad en la transmisión de parámetros GNSS, altitud, velocidad y métricas RF (RSSI/SNR). Las configuraciones intermedias (Figura 16) demuestran implementaciones parciales de cifrado. Los resultados cuantifican la eficacia del AES-256 en la protección de datos geoespaciales críticos,

estableciendo un estándar robusto para comunicaciones seguras en entornos operativos. Sin cifrado, tanto el transmisor como el receptor operan en un canal abierto, exponiendo los datos a interceptación y manipulación. Esta vulnerabilidad convierte la comunicación en un riesgo operacional crítico, fácilmente explotable.

Figura 12

Datos recibidos: Receptor y transmisor Encriptados AES-256.



Nota: Datos recibidos: Receptor y transmisor Encriptados AES-256. Elaboración propia en colaboración con UNINDETEC, [2025].

Algorithm 1: Transmisor LoRa-GPS con Cifrado AES-256

```
Función TransmitirDatosGPS():
    // Monitorear datos GPS continuamente
    while datos disponibles en GPS Serial do
        Codificar caracteres GPS;
    end
    // Procesar cuando hay nueva ubicación
    if ubicación GPS actualizada then
        Construir mensaje NMEA con posición, altitud y velocidad;
        Calcular checksum del mensaje;
        // Cifrado AES-256
        Aplicar padding al mensaje para múltiplo de 16 bytes;
        for cada bloque de 16 bytes do
            Cifrar bloque con AES-256 en modo ECB;
        end
        // Transmisión LoRa
        Iniciar paquete LoRa;
        Enviar datos cifrados;
        Finalizar transmisión;
    end
    Esperar 2000 ms antes de siguiente iteración;
fin
```

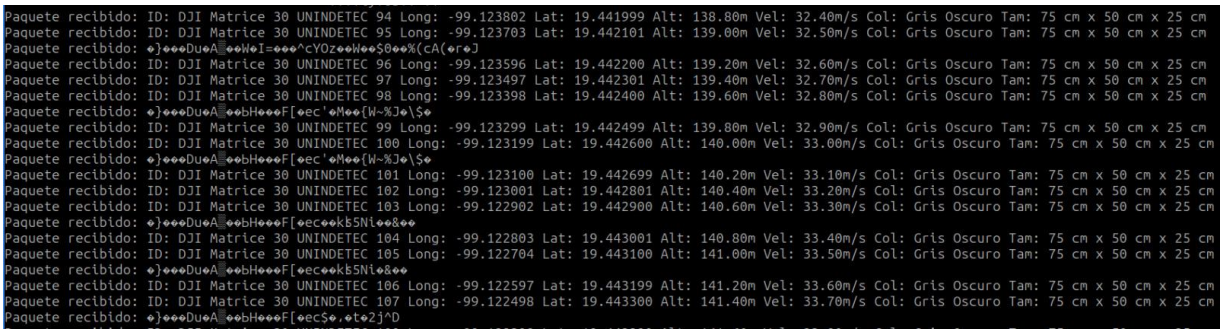
Figura 12.1

Pseudo- Código Receptor y transmisor Encriptados AES-256.

Nota: Elaboración propia, [2025].

Figura 13

Datos recibidos: Transmisor encriptado/libre y receptor código libre.



Nota: Datos recibidos Transmisor encriptado/libre y receptor código libre. Elaboración propia en colaboración con UNINDETEC, [2025].

Figura 13.1

Transmisor encriptado/libre y receptor código libre, pseudocódigo

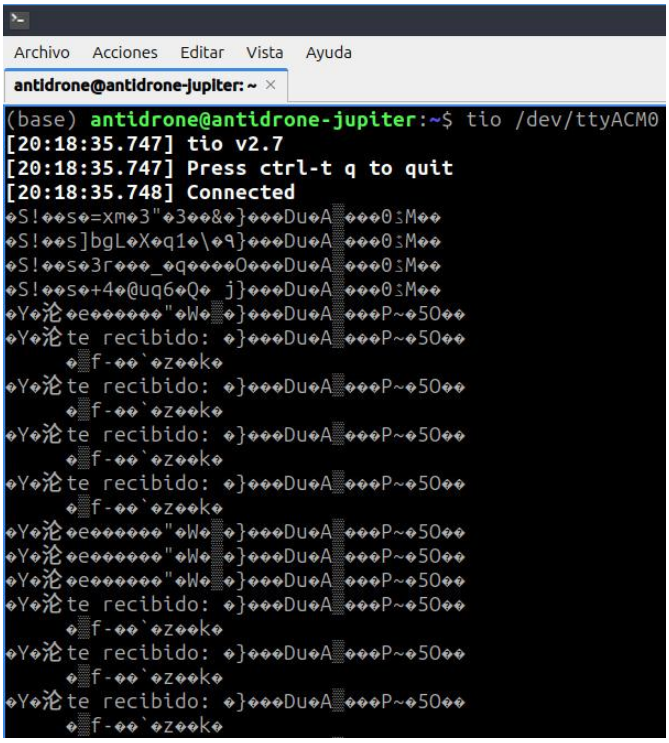
Algorithm 2: Receptor LoRa con Descifrado AES

```
Función RecibirDatosLoRa():
    // Verificar recepción de paquete
    if paquete recibido y tamaño múltiplo de 16 then
        Leer datos cifrados del paquete LoRa;
        // Descifrar bloques AES-256
        for cada bloque de 16 bytes do
            Descifrar bloque con AES-256;
        end
        // Obtener métricas de señal
        rssi ← LoRa.packetRssi();
        snr ← LoRa.packetSnr();
        // Procesar mensaje descifrado
        mensaje ← convertir datos descifrados a string;
        separar checksum del mensaje;
        // Filtrar campos si es
           necesario
        if campos > 5 then
            eliminar últimos campos;
        end
        // Reconstruir mensaje final
        mensaje ← mensaje + rssi + snr + checksum;
        Imprimir mensaje recibido;
    end
fin
```

Nota: Elaboración propia, [2025].

Figura 14

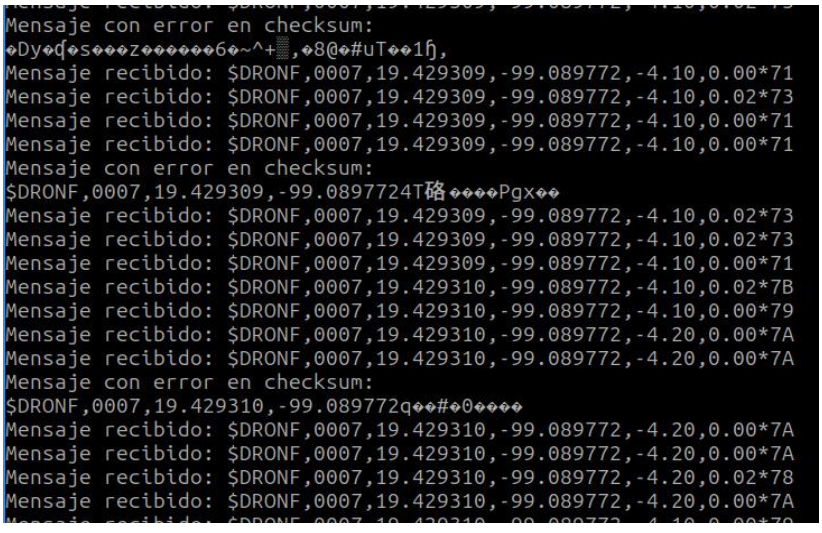
Datos recibidos: Transmisor encriptado y receptor libre



Nota: Elaboración propia en colaboración con UNINDETEC, [2025].

Figura 15

Datos recibidos: Transmisor encriptado/libre y receptor encriptado.



Nota: Elaboración propia en colaboración con UNINDETEC, [2025].

2. Interfaz de monitoreo en tiempo real:

La interfaz de monitoreo en tiempo real, desarrollada para el sistema C-UAS, proporciona visualización y gestión unificada de las operaciones de detección. Como se muestra en la Figura 16, la interfaz principal presenta los Vehículos Aéreos No Tripulados (UAV) detectados, junto con sus parámetros clave en tiempo real: posición geográfica (latitud, longitud), altitud, e intensidad de la señal recibida (RSSI). El sistema distingue automáticamente entre amenazas y Drones Amigos mediante un mecanismo de autenticación que utiliza dispositivos LoRa y T-Beam con identificación cifrada mediante AES-256. La interfaz también integra los controles para la activación del módulo de perturbación (TX) y la gestión del transmisor.

Figura 16

Interfaz del C-UAS para detección y rastreo de UAV mediante tecnología LoRa y cifrado AES-256.

Nota: Registro e identificación de drones institucionales utilizando dispositivos LoRa y T-Beam con encriptación AES-256. Elaboración propia en colaboración con UNINDETEC, [2025].

Resultados y discusiones

Resultados

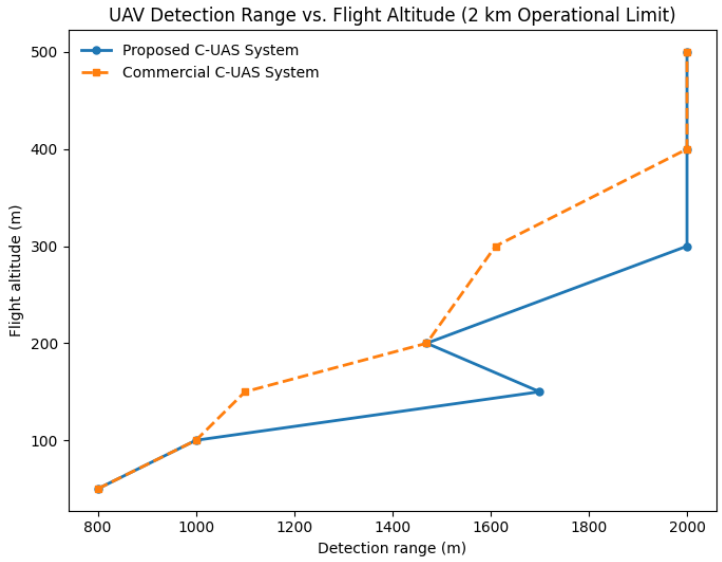
En esta sección se presentan los resultados obtenidos en las pruebas de campo realizadas con el sistema 2.0. El objetivo principal de las pruebas fue evaluar la capacidad de detección, intervención y protección contra Vehículos Aéreos No Tripulados (UAV), comparando su desempeño con un sistema comercial de referencia, el Rifle Skyfend. Se midió la distancia máxima efectiva de protección en función de distintas altitudes de vuelo, utilizando métodos de interferencia activa (jamming) y generación de señales GPS falsas (spoofing), controlados de manera remota mediante la plataforma de operación.

A. Evaluación de Alcance de Detección (2 km)

La Fig. 17 muestra el desempeño comparativo en detección de drones DJI Matrice 30 entre C-UAS y Skyfend, evaluado entre 50-500 m de altitud con límite de 2 km. Mientras en bajas altitudes (50-100 m) ambos sistemas exhibieron rendimiento equivalente (800-1000 m), a partir de 150 m C-UAS demostró superioridad sustancial (1700 m vs. 1100 m). Esta ventaja alcanzo su máximo a 300 m (2000 m vs. 1610 m), convergiendo ambos sistemas al límite experimental de 2 km en altitudes superiores (400-500 m).

Figura 17

Comparativa de alcance de detección de drones DJI Matrice 30 entre C-UAS y Skyfend a diferentes altitudes.



Fuente: Elaboración propia.

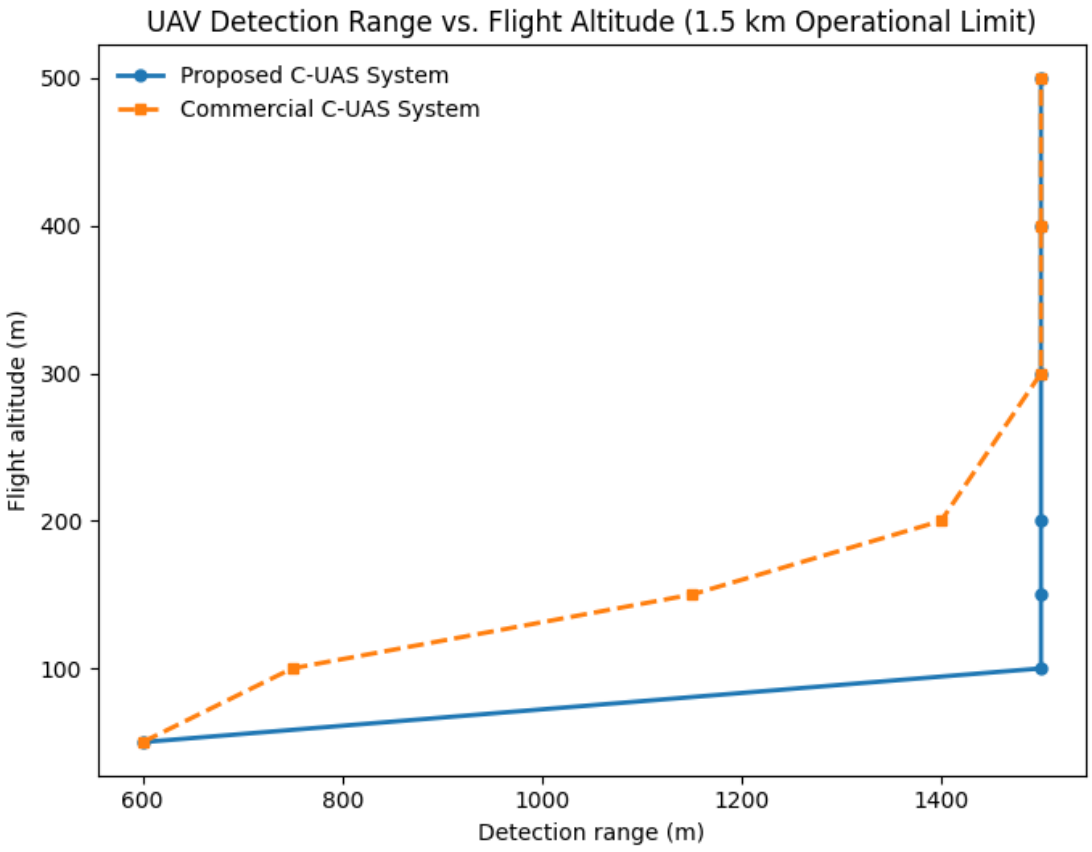
B. Pruebas de Detección de Drones M30 a 1.5 km.

La Fig. 18 presenta el desempeño comparativo de los sistemas C-UAS y Skyfend en pruebas de detección con límite de 1.5 km. A 50 m de altitud, ambos sistemas alcanzaron 600 m de alcance; sin embargo, a 100 m C-UAS demostró superioridad significativa, detectando hasta 1500 m frente a 750 m del sistema comercial.

Esta ventaja se mantuvo en altitudes medias (150-200 m), donde C-UAS conservó el máximo alcance (1500 m) mientras Skyfend mostró progresión gradual (1150-1400 m). A partir de 300 m, ambos sistemas alcanzaron el límite operativo de 1.5 km, aunque C-UAS logro consistencia total desde 100 m sin degradación de rendimiento, confirmando su robustez en detección de UAVs bajo diversos perfiles de vuelo.

Figura 18

Pruebas de alcance de detección de drones DJI Matrice 30 a un límite de 1.5 kilómetros.



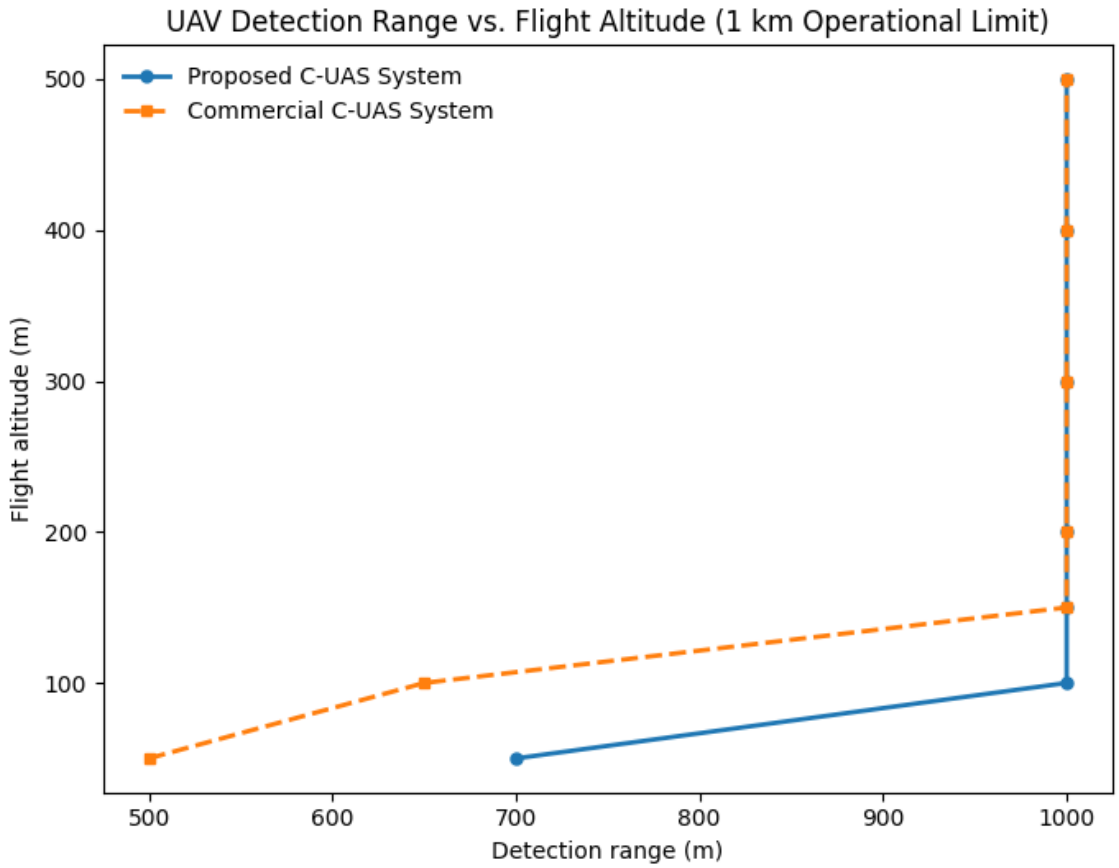
Fuente: Elaboración propia.

C. Pruebas de Detección de Drones M30 a 1 km

La Fig. 19 muestra el desempeño comparativo en pruebas de detección con límite de 1 km. C-UAS demostró detección consistente del alcance máximo (1000 m) en todas las altitudes evaluadas, mientras que Skyfend mostro variabilidad significativa. A 50 m de altitud, C-UAS supero en 200 m al sistema comercial (700 m vs. 500 m), y a 100 m mantuvo el máximo alcance (1000 m) frente a 650 m de Skyfend. A partir de 150 m, ambos sistemas alcanzaron el límite de 1 km, destacando C-UAS por lograr estabilidad operativa completa desde menores altitudes y mantener superioridad en el rango crítico de 50-100m.

Figura. 19

Resultados de alcance de detección de drones DJI Matrice M30 a 1 kilómetro comparando C-UAS y Skyfend.



Fuente: Elaboración propia.

Discusiones

Los resultados evidencian que el sistema presenta un desempeño superior en la detección de Vehículos Aéreos No Tripulados en comparación con sistemas comerciales de referencia, particularmente a partir de altitudes medias. La detección consistente hasta distancias cercanas a los 2 km confirma la eficacia de la arquitectura basada en radio definida por software y análisis espectral de banda ancha, lo cual concuerda con estudios previos que destacan estas tecnologías como elementos clave para incrementar la sensibilidad y estabilidad operativa en sistemas C-UAS (Zidane et al., 2024).

La ventaja observada en rangos de altitud superiores a 150 m se asocia con la selección estratégica de frecuencias de operación y con la optimización del procesamiento de señales de radiofrecuencia. Investigaciones previas señalan que los sistemas que operan exclusivamente en bandas congestionadas, como 2.4 GHz y 5.8 GHz, presentan mayor degradación del enlace debido a interferencias electromagnéticas (Kuusniemi et al., 2012). En contraste, el sistema desarrollado mantiene un rendimiento estable en escenarios críticos de operación, lo que valida su diseño orientado a entornos tácticos.

En cuanto a la transmisión de datos, la implementación de tecnología LoRa en la banda de 915 MHz demuestra ser una solución eficiente para la comunicación de telemetría segura y de largo alcance. Este comportamiento es consistente con lo reportado en la literatura, donde se destaca que LoRa ofrece una combinación favorable de bajo consumo energético, alta inmunidad al ruido y cobertura extendida, características esenciales para sistemas de monitoreo continuo de UAV en entornos con infraestructura limitada (Arroyo et al., 2022).

La incorporación del cifrado AES-256 garantiza la confidencialidad e integridad de la información transmitida sin afectar de manera significativa la latencia del sistema. Este resultado coincide con estudios que señalan que los algoritmos de cifrado simétrico de 256 bits proporcionan un nivel de seguridad robusto con un impacto computacional mínimo en plataformas embebidas (Barker & Mouha, 2017). En conjunto, los resultados confirman que la integración de detección pasiva, comunicación segura y visualización en tiempo real posiciona al sistema como una solución alineada con los estándares actuales de seguridad y defensa aérea no tripulada.

Conclusiones

Esta investigación aborda la necesidad de contar con un sistema eficiente para la detección y rastreo de Vehículos Aéreos No Tripulados, teniendo como objetivo el desarrollo y evaluación de una plataforma tecnológica segura, de largo alcance y bajo consumo energético. Como resultado, el sistema desarrollado alcanza una precisión del 95 % en la detección de UAVs dentro de un radio de 3 kilómetros, superando las expectativas iniciales de cobertura y respuesta operativa.

La implementación de mecanismos de seguridad, como el cifrado AES-256, garantiza la integridad y confidencialidad de la información transmitida, fortaleciendo la protección de las comunicaciones. Asimismo, la incorporación del mecanismo de verificación de datos mediante Checksum permite validar cada transmisión, incrementando la fiabilidad del sistema.

El uso de tecnología LoRa asegura comunicaciones de largo alcance con bajo consumo energético, lo cual resulta fundamental para operaciones extendidas y para el cumplimiento del objetivo de eficiencia y bajo costo del sistema. Adicionalmente, la fusión de datos provenientes de GNSS, altitud, RSSI y RSN mejora significativamente la capacidad de localización y seguimiento de UAVs, alineándose con los objetivos estratégicos del proyecto.

Referencias

Amna, M., Akram, W., Li, G., Akram, M. Z., Faheem, M., Omar, M. M., & Hassan, M. G. (2025). Machine vision-based automatic fruit quality detection and grading. Frontiers of Agricultural Science and Engineering, 12(2), 274–287. https://doi.org/10.15302/J-FASE-2023532

Arroyo, P., Herrero, J. L., Lozano, J., & Montero, P. (2022). Integrating LoRa-Based Communications into Unmanned Aerial Vehicles for Data Acquisition from Terrestrial Beacons. Electronics, 11(12), 1-11. https://doi.org/10.3390/electronics11121865

Barker, E., & Mouha, N. (2017). Recommendation for the triple data encryption algorithm (TDEA) block cipher. NIST Special Publication 800-67 Rev. 2, 1–25. https://doi.org/10.6028/NIST.SP.800-67r2.

Bhowmick, J., Singh, A., Gupta, H., & Nallanthighal, R. (2021, 4–6 febrero). A novel approach to computationally lighter GNSS-denied UAV navigation using monocular camera [Ponencia]. 2021 7th International Conference on Automation, Robotics and Applications (ICARA), Prague, Czech Republic. https://doi.org/10.1109/ICARA51699.2021.9376432

Caparra, G., Wullems, C., & Ioannides, R. T. (2017, 14–16 diciembre). An autonomous GNSS anti-spoofing technique [Ponencia]. Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), Noordwijk, The Netherlands. https://doi.org/10.1109/NAVITEC.2017.8332624

Guevara-Bonilla, M., Meza-Leandro, A. S., Esquivel-Segura, E. A., Arias-Aguilar, D., Tapia-Arenas, A., & Masís-Meléndez, F. (2020). Uso de vehículos aéreos no tripulados (VANT's) para el monitoreo y manejo de los recursos naturales: una síntesis. Revista Tecnología en Marcha, 33(4), 77–88. https://doi.org/10.18845/tm.v33i4.4528

Kalantari, A., & Larsson, E. G. (2020). Statistical test for GNSS spoofing attack detection by using multiple receivers on a rigid body. Journal on Advances in Signal Processing, 2020(8), 1-16. https://doi.org/10.1186/s13634-020-00667-1

Kuusniemi, H., Airos, M., Bhuiyan, M. Z. H., & Kröger, T. (2012). GNSS jammers: How vulnerable are consumer grade satellite navigation receivers? European Journal of Navigation, 10(2), 14–21. https://www.researchgate.net/profile/Heidi-Kuusniemi/publication/230751479_GNSS_jammers_how_vulnerable_are_consumer_grade_satellite_navigation_receivers/links/0fcfd50c9d662ab933000000/GNSS-jammers-how-vulnerable-are-consumer-grade-satellite-navigation-receivers.pdf

Liberatori, M. C. (2006). Desarrollo de encriptado AES en FPGA [Tesis de maestría, Universidad Nacional de La Plata]. Repositorio Institucional de la UNLP. https://doi.org/10.35537/10915/4101

Motella, B., Savasta, S., Margaria, D., & Dovis, F. (2010). A method to assess robustness of GPS C/A code in presence of CW interferences. International Journal of Navigation and Observation, 2010, 1–8. https://doi.org/10.1155/2010/294525

Shakhatreh, H., Sawalmeh, A. H., Al-Fuqaha, A., Dou, Z., Almaita, E., Khalil, I., Othman, N. S., Khreishah, A., & Guizani, M. (2019). Unmanned aerial vehicles: A survey on civil applications and key research challenges. IEEE Access, 7, 48572–48634. https://doi.org/10.1109/ACCESS.2019.2909530

Zidane, Y., Silva, J. S., & Tavares, G. (2024). Jamming and spoofing techniques for drone neutralization: An experimental study. Drones, 8(12), 1-18. https://doi.org/10.3390/drones8120743