



ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

**DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y
TELECOMUNICACIONES**

**CARRERA DE INGENIERÍA EN ELECTRÓNICA Y
TELECOMUNICACIONES**

**TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL
TÍTULO DE INGENIERA EN ELECTRÓNICA Y
TELECOMUNICACIONES**

**TEMA: DESARROLLO DE UN SISTEMA INHIBIDOR DE DRONES EN
LAS BANDAS COMERCIALES 2.4 Y 5.8 GHZ, WIFI.**

AUTOR: OLIVA CEVALLOS, NATALY CATERINE

DIRECTOR: LEÓN VÁSQUEZ, RUBÉN DARÍO MSc.

SANGOLQUÍ

2019



ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que el trabajo de titulación, ***“DESARROLLO DE UN SISTEMA INHIBIDOR DE DRONES EN LAS BANDAS COMERCIALES 2.4 Y 5.8 GHZ, WIFI.”*** fue realizado por la señorita ***Oliva Cevallos, Nataly Caterine*** el mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, julio de 2019

Rubén León Vásquez MSc.

C.C. 1801654284



**DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y
TELECOMUNICACIONES**

**CARRERA DE INGENIERÍA EN ELECTRÓNICA Y
TELECOMUNICACIONES**

AUTORÍA DE RESPONSABILIDAD

Yo, *Oliva Cevallos, Nataly Caterine*, declaro que el contenido, ideas y criterios del trabajo de titulación: *“Desarrollo de un Sistema Inhibidor de Drones en las Bandas Comerciales 2.4 y 5.8 GHz, WIFI”* es de mi autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Consecuentemente el contenido de la investigación mencionada es veraz.

Sangolquí, julio de 2019

A handwritten signature in blue ink, appearing to read 'Nataly Cevallos', is written over a horizontal line.

Nataly Caterine Oliva Cevallos

C.C 1715847404



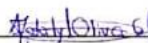
**DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y
TELECOMUNICACIONES**

**CARRERA DE INGENIERÍA EN ELECTRÓNICA Y
TELECOMUNICACIONES**

AUTORIZACIÓN

*Yo, **Oliva Cevallos, Nataly Caterine**, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **“Desarrollo de un Sistema Inhibidor de Drones en las Bandas Comerciales 2.4 y 5.8 GHz, WIFI”** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.*

Sangolquí, julio de 2019



Nataly Caterine Oliva Cevallos

C.C 1715847404

DEDICATORIA

A mis padres, German y Yolita.

Gracias a su apoyo incondicional, he logrado culminar mi formación académica. Mis logros, mis triunfos, mi camino al éxito siempre serán dedicados a ustedes.

Nataly Caterine Oliva Cevallos.

AGRADECIMIENTO

Mi vida es posible gracias a mis padres, que con su amor y dedicación formaron a una persona con valores y realista para desenvolverse en todo ámbito de la vida, y es a ellos que agradezco profundamente desde el fondo de mi corazón y mi alma, por cada consejo, por cada abrazo de fortaleza, por tanto amor. Que dicha tan grande tener a mis padres Yolita Cevallos y German Oliva que son un ejemplo para mí y gracias a ello estoy alcanzando mis metas. ¡Gracias Padres!

Un profundo agradecimiento a mi familia, que con sus muestras de cariño y apoyo han sido para mí el empuje diario. Y a mis amigos gracias por compartir mi vida, con risas, preocupaciones, victorias, todo aquello de las experiencias vividas en la universidad y fuera de ella, quedan grabadas en mi mente como un grato recuerdo, Gracias.

Un agradecimiento especial a las personas que formaron parte integral de este proyecto, mis tutores Rubén León y Alexis Tinoco, y personal del CICTE por la colaboración brindada. Y al laboratorio de antenas y propagación (LAP) del Instituto Tecnológico de Aeronáutica (ITA) por su colaboración en la simulación de las antenas.

ÍNDICE DE CONTENIDO

DEDICATORIA.....	iv
AGRADECIMIENTO.....	v
INDICE DE FIGURAS.....	xi
INDICE DE TABLAS	x
RESUMEN.....	xiii
ABSTRACT	xiv
CAPITULO I.....	1
INTRODUCCIÓN	1
1. Antecedentes	1
2. Justificación e Importancia	3
3. Alcance del Proyecto.....	4
4. Objetivos	5
4.1 Objetivo General	5
4.2 Objetivo Específico	5
CAPITULO II	6
FUNDAMENTOS TEÓRICOS	6
2.1 Introducción	6
2.2 Estándar IEEE 802.11 para redes de área local inalámbricas (WLAN)	12
2.3 Sistema de posicionamiento global (<i>Global Positioning System</i> – GPS)	14
2.4 Vehículo Aéreo no Tripulado (UAV) – Drones.....	17
2.4.1 UAV de ala rotatoria.....	18
2.4.2 Principales sistemas de comunicación de UAV comerciales	19
2.5 Guerra electrónica.	21
2.5.1 Definición.	21
2.5.2 Clasificación.	22
2.5.2.1 Medidas de apoyo electrónico (<i>Electronic Support Measures</i> - ESM)	22
2.5.2.2 Contramedidas electrónicas (<i>Electronic Countermeasures</i> - ECM)	22
2.5.2.3 Contra contra medidas electrónicas (<i>Electronic Counter-Countermeasures</i> - ECM).....	23
2.6 Estrategias para generar interferencias intencionales o <i>Jamming</i>	24

	vii
2.6.1	Generación de señales de interferencia por la adición de ruido24
2.6.2	Generación de señales de interferencia por tonos.26
2.6.3	Generación de señales de interferencia por pulsos.26
2.6.4	Generación de señales de interferencia por barrido.....27
2.6.5	Generación de señales de interferencia por seguimiento.....27
2.6.6	Generación de señales de interferencia inteligente.....27
2.7	Clasificación de los generadores de interferencia (<i>jammer</i>).28
2.7.1	Generador constante de interferencia (<i>jammer</i> constante)28
2.7.2	Generador de interferencia de engaño (<i>jammer</i> de engaño).....28
2.7.3	Generador de interferencia aleatorio (<i>jammer</i> aleatorio)28
2.7.4	Generador de interferencia reactivo (<i>jammer</i> reactivo).....29
CAPITULO III29	
DISEÑO DEL SISTEMA INHIBIDOR DE DRONES QUE TRABAJAN EN BANDAS COMERCIALES WIFI.30	
3.1	Elección de las estrategias de <i>jamming</i> y tipo de <i>jammer</i>30
3.2	Descripción del Sistema Inhibidor31
3.2.1	Oscilador controlado por voltaje (VCO)32
3.2.1.1	Oscilador controlado por voltaje 2.4 GHz.....33
3.2.1.2	Oscilador controlado por voltaje 5.8 GHz.....34
3.2.2	<i>Jamming</i>36
3.2.2.1	Descripción del generador de ruido gaussiano (GNG) desarrollado en arduino due36
3.2.2.2	Descripción del circuito generador de ruido.....39
3.2.2.3	Descripción del <i>Jamming</i> por Barrido.....42
3.2.2.3.1	Para 2.4 GHz.....42
3.2.2.3.2	Para 5.8 GHz.....42
3.2.3	Sistema de control43
3.2.4	Sistema de Radiofrecuencia44
3.2.5	Amplificador RF.....46
3.2.6	Antena.....47
CAPITULO IV49	
IMPLEMENTACIÓN DEL SISTEMA PROTOTIPO INHIBIDOR O <i>JAMMER</i> DE DRONES 49	

	viii
4.1 Conexiones del sistema inhibidor de drones	49
4.2 Sistema Adicional de Laboratorio del Inhibidor de GPS y WIFI	53
4.3 Operación del sistema inhibidor de drones	53
4.4 Operación del sistema adicional de laboratorio del inhibidor de GPS y WIFI	54
4.4.1 Para GPS	54
4.4.2 Para WIFI	54
4.5.1 Mediciones.....	55
4.5.1.2 <i>Jamming</i> por ruido mediante circuito	57
4.5.1.3 <i>Jamming</i> por Barrido	58
4.5.1.4 <i>Jamming</i> causado por modulación FM mediante el generador vectorial de señales RF. 59	
4.5.1.4.1 GPS	60
4.5.1.4.2 WIFI.....	60
4.5.2 Pruebas del Sistema Inhibidor	61
4.5.2.1 Escenario 1	64
4.5.2.1.1 <i>Jamming</i> por ruido gaussiano (GNG) desarrollado en arduino due.	64
4.5.2.1.2 <i>Jamming</i> por ruido mediante circuito	66
4.5.2.1.3 <i>Jamming</i> por barrido	67
4.5.2.2 Escenario 2	69
4.5.2.2.1 <i>Jamming</i> por ruido gaussiano (GNG) desarrollado en arduino due.	69
4.5.2.2.2 <i>Jamming</i> por ruido mediante circuito	70
4.5.2.2.3 <i>Jamming</i> por barrido	70
4.5.3 Pruebas con el sistema adicional de laboratorio del inhibidor de banda GPS y WIFI. ...	72
4.5.3.1 Escenario 1 para GPS	72
4.5.3.2 Escenario 2 para GPS	74
4.5.3.3 Escenario 1 para WIFI.....	75
4.5.3.4 Escenario 2 para WIFI.....	77
4.5.3.5 Escenario 3 para WIFI.....	79
CAPITULO V	83
ANÁLISIS DE RESULTADOS	83
CAPITULO VI.....	89

	ix
CONCLUSIONES Y RECOMENDACIONES.....	89
6.1 Conclusiones	89
6.2 Recomendaciones.....	91
BIBLIOGRAFÍA.....	92

INDICE DE TABLAS

Tabla 1 Designación de las bandas 2 hasta la 14 según la CCIR.....	8
Tabla 2 Tabla comparativa de los diferentes estándares 802.11.....	14
Tabla 3 Bandas de operación, plan de uso y modernización de servicio de GPS.....	17
Tabla 4 Lista de drones comerciales que utilizan la bandas de WiFi.....	19
Tabla 5 Datos de Prueba.....	33
Tabla 6 Datos de Prueba.....	34
Tabla 7 Tabla de verdad.....	45
Tabla 8 Datos de Prueba.....	47
Tabla 9 Dispositivos para pruebas.....	56
Tabla 10 Resultados del jamming por ruido en arduino.....	57
Tabla 11 Resultados del jamming por ruido mediante circuito.....	58
Tabla 12 Resultados del jamming por barrido.....	59
Tabla 13 Resultados del jamming por modulación FM en GPS.....	60
Tabla 14 Resultados del jamming por modulación FM en WIFI.....	61
Tabla 15 Resultado de los parámetros de funcionamiento del drone.....	84
Tabla 16 Tiempos de deshabilitación del control remoto.....	85
Tabla 17 Tiempos de deshabilitación del control remoto.....	87

INDICE DE FIGURAS

Figura 1. Ilustración de la dirección de propagación de una onda electromagnética En rojo se representa el campo eléctrico armónico (\vec{E}) y en azul el campo magnético (\vec{B}).	6
Figura 2. Espectro electromagnético de frecuencias.....	8
Figura 3. Representación de un enlace de telecomunicaciones a través de sus bloques funcionales.	9
Figura 4. Distribución de los canales de la banda de frecuencia de 2,4 GHz WiFi.....	20
Figura 5. Estrategias de generar señales de interferencia por la adición de ruido.	25
Figura 6. Diagrama de Bloques del sistema jamming.....	32
Figura 7. Función de transferencia del VCO.	32
Figura 8. Frecuencia Vs Voltaje de Sintonía	34
Figura 9. Frecuencia Vs Voltaje de Sintonía	35
Figura 10. Sintonización aleatoria en banda de 2.4 GHz.....	38
Figura 11. Sintonización aleatoria en banda de 5.8 GHz.....	39
Figura 12. Circuito generador de ruido blanco	40
Figura 13. Señal de salida del circuito de ruido.....	40
Figura 14. Señal de salida amplificada del circuito de ruido.	41
Figura 15. Bias-Tee.....	41
Figura 16. Señal interferente para la banda de 2.4GHz	42
Figura 17. Señal interferente para la banda de 5.8 GHz	43
Figura 18. Conexiones del sistema de control	44
Figura 19. Switch de control HMC321ALP4E.....	45
Figura 20. Antena log periódica.....	48
Figura 21. Estructura interna del sistema inhibidor de drones.....	50
Figura 22. Dip switch, dip 1	50
Figura 23. Conexiones entre el arduino due y switch RF	51
Figura 24. Dip switch, dip 2.....	51
Figura 25. Ingreso del ángulo mediante puerto COM, monitor serie de la plataforma propia de arduino.....	52
Figura 26. Sistema inhibidor de drones.....	53
Figura 27. Ingreso de datos al generador vectorial de señales RF.....	55
Figura 28. Espectro de salida y ancho de banda, Jamming por ruido en arduino	57
Figura 29. Espectro de salida y ancho de banda, Jamming por ruido mediante circuito	58
Figura 30. Espectro de salida y ancho de banda, Jamming por barrido.....	59
Figura 31. Jamming por modulación FM en banda GPS	60
Figura 32. Jamming por modulación FM en banda WIFI.....	61
Figura 33. Phantom 4.....	62
Figura 34. Pantalla de la aplicación DJI GO.....	63
Figura 35. Pantalla de la aplicación DJI GO.....	63
Figura 36. Escenario 1 de Prueba.....	64
Figura 37. Pérdida de los parámetros de funcionamiento entre el dron y el controlador remoto65	65

Figura 38. Pérdida de la transmisión de video en tiempo real	65
Figura 39. Neutralización de la comunicación entre el dron y el controlador remoto en tiempo real	66
Figura 40. Neutralización de la transmisión de video en tiempo real	67
Figura 41. Interferencia de la comunicación entre el dron y el controlador remoto en tiempo real	68
Figura 42. Neutralización de la transmisión de video en tiempo real	68
Figura 43. Interferencia de la comunicación entre el dron y el controlador remoto en tiempo real	69
Figura 44. Interferencia de la comunicación entre el dron y el controlador remoto en tiempo real	70
Figura 45. Interferencia de la comunicación entre el dron y el controlador remoto en tiempo real	71
Figura 46. Pérdida de GPS con 5 dBm	72
Figura 47. Pérdida de GPS con 7 dBm	73
Figura 48. Pérdida de GPS con 10 dBm	73
Figura 49. Pérdida de GPS con 5 dBm	74
Figura 50. Pérdida de GPS con 7 dBm	74
Figura 51. Pérdida de GPS con 10 dBm	75
Figura 52. Neutralización de la comunicación entre el dron y el controlador remoto en tiempo real para 5 dBm	76
Figura 53. Neutralización de la comunicación entre el dron y el controlador remoto en tiempo real para 7 dBm	76
Figura 54. Neutralización de la comunicación entre el dron y el controlador remoto en tiempo real para 10 dBm	77
Figura 55. Neutralización de la comunicación entre el dron y el controlador remoto en tiempo real para 5 dBm	78
Figura 56. Neutralización de la comunicación entre el dron y el controlador remoto en tiempo real para 7 dBm	78
Figura 57. Neutralización de la comunicación entre el dron y el controlador remoto en tiempo real para 10 dBm	79
Figura 58. Prueba negativa ante jamming.....	80
Figura 59. Prueba tendiente a positiva ante jamming	80
Figura 60. Prueba tendiente a positiva ante jamming	81
Figura 61. Prueba positiva ante jamming.....	81
Figura 62. Escenario de Prueba.....	83

RESUMEN

Hoy en día, debido al crecimiento del empleo de las tecnologías inalámbricas en diversos dispositivos y a la facilidad para acceder a ellas, están convergiendo a la utilización de dichas tecnologías de forma incorrecta, como es el caso de varios puntos estratégicos del estado ecuatoriano que están siendo “visitados clandestinamente”, por drones comerciales, encaminándose así en un entorno de Guerra Electrónica para que las aplicaciones en el espectro electromagnético vigilen amenazas y resguarden la seguridad de la soberanía ecuatoriana. El presente proyecto tiene como objetivo desarrollar un sistema inhibidor o *jammer* de drones que trabajen en bandas comerciales WiFi a través de metodologías *Original Equipment Manufacturer* (OEM), lo que permitirá incrementar las capacidades operativas de las Fuerzas Armadas. Los *jammers* son equipos diseñados para bloquear la interacción de dispositivos mediante la emisión de una señal que interrumpe el proceso de comunicación, así como también degradar la calidad de la señal en el receptor del sistema. El desarrollo de este estudio desarrolla conceptos teóricos correspondientes a la radiofrecuencia, análisis de las distintas técnicas de *jamming* con la finalidad de elegir la mejor opción para bloquear la comunicación de los vehículos aéreos no tripulados (drones). Con las técnicas de *jamming* seleccionadas se muestra el diseño por etapas del sistema inhibidor y se expone los resultados obtenidos.

Palabras clave:

- GUERRA ELECTRÓNICA
- ESPECTRO ELECTROMAGNÉTICO
- WIFI

ABSTRACT

Today, due to the growth in the use of wireless technologies in various devices and the ease of access to them, are converging to the use of such technologies incorrectly, as is the case of several strategic points of the Ecuadorian state that are being "clandestinely visited" by commercial drones, thus heading into an environment of Electronic Warfare for applications in the electromagnetic spectrum to monitor security. The present project aims to develop an inhibitor system or jammer of drones working in commercial WiFi bands through Original Equipment Manufacturer (OEM) methodologies, which will increase the operational capabilities of the Armed Forces. Jammers are equipment designed to block the interaction of devices by emitting a signal that interrupts the communication process, as well as degrade the quality of the signal in the system's receiver. The development of this study develops theoretical concepts corresponding to radio frequency, analysis of different techniques of *jamming* in order to choose the best option to block the communication of unmanned aerial vehicles (drones). With the selected *jamming* techniques, the design by stages of the inhibitor system is shown and the results obtained are explained.

Keywords:

- **ELECTRONIC WARFARE**
- **ELECTROMAGNETIC SPECTRUM**
- **WIFI**

CAPITULO I

INTRODUCCIÓN

1. Antecedentes

El auge que han tenido los avances tecnológicos genera desafíos, puesto que el uso que le dan a estas tecnologías están siendo encaminadas para buenas y malas aplicaciones. Una de las preocupaciones es el uso de teléfonos móviles, tabletas o cualquier dispositivo capaz de emitir una señal para la activación de artefactos explosivos o filmación de video en lugares de gran circulación de personas u otros sitios estratégicos del país, mediante la utilización de "drones". A pesar que existe en Ecuador una regulación para el uso de "drones", que fue dictada el 17 de septiembre de 2015 por la Dirección General de Aviación Civil (DGAC, 2015), la misma que menciona que no podrán ser operados en las cercanías de las bases aéreas militares o aeródromos, y no detalla más zonas, por lo que genera incertidumbre y peligro a otras áreas estratégicas.

En los últimos años Ecuador ha sufrido golpes del narcoterrorismo en la frontera de Ecuador-Colombia, en una entrevista a un excolaborador del líder del frente narcoterrorista Óliver Simisterra alias "Guacho", detalla que usan drones para vigilar al Ejército y Policía Ecuatoriana, información proporcionada por el periódico Expreso (López H. , 2018).

Estas vulnerabilidades que disponen los sitios estratégicos de las naciones, han generado investigaciones para determinar mecanismos eficientes y solventar esta grave problemática. Como (Rodrigo Valim, André dos Anjos, 2017), donde realizan una simulación de interferencia, mediante el bloqueo de señales con diferentes tipos de interferencia utilizando el software *VissimCom* en diversos emisores de los sistemas de comunicación digital. (Parlin, 2017) propone

un sistema de neutralización para vehículos aéreos no tripulados (UAV) donde consta de un simulador con diferentes técnicas de interferencia en contra de un sistema que usa espectro ensanchado híbrido el que combina la secuenciación directa y salto de frecuencia, implementado en una plataforma de radio definida por software. El sistema desarrollado es capaz de interferir los sistemas de control remoto del UAV.

(Thomas Multerer, Alexander Ganis y otros, 2017) han desarrollado un sistema de *jamming* de bajo costo contra drones que usan un seguimiento basado en radar MIMO 3D, que mediante un algoritmo de seguimiento se evalúa el movimiento del drone, para interferirlo se utiliza una antena direccional donde la señal de control del avión no tripulado puede ser superpuesta por una fuerte señal de interferencia que hace que el control del drone sea imposible. Actualmente, existen sistemas comerciales encargados en la detección y defensa contra vehículos aéreos no tripulados (UAV), entre ellos están sistemas interferidores de las frecuencias GPS y bandas ISM con el fin que pierda el control del drone, desarrollado por la compañía (Battelle, 2018). En Estados Unidos (Aviación, 2016) han creado el sistema *Anti-UAV Defense System (AUDS)*, que detecta y neutraliza drones alrededor de un radio de 10 kilómetros, por medio de un radar electrónico, una cámara normal y otra infrarroja que realizan el seguimiento de la trayectoria y una antena que lanza un haz direccional que corta las señales de radio del drone. También en Reino Unido desarrollaron un sistema que ubica el drone, y con una antena direccional envía una señal de radio para inmovilizar al drone en el aire, con la colaboración de (Dynamics, 2018). La empresa (Hertz Systems , 2018) ha desarrollado un arma de tiro tradicional que emite una señal de disrupción, por lo que el drone pierde la conexión. (Rohde & Schwarz, 2018) ha creado ARDRONIS, sistema que detecta e identifica el avión no tripulado, determina las direcciones del avión no tripulado y su piloto, e interrumpe el enlace de control de radio (RC).

2. Justificación e Importancia

El presente proyecto de investigación busca desarrollar un sistema inhibidor de drones comerciales que trabajan en las bandas no concesionadas WiFi. El sistema permite actuar en la inhibición de la señal de datos y comando y control del dron, pero requiere de un proceso previo de detección, discriminación y localización. Esta solución es un aporte importante para mejorar las condiciones de seguridad de áreas estratégicas del Estado.

En la actualidad, se conoce que desde hace algunos años, varios puntos estratégicos del estado ecuatoriano están siendo “visitados clandestinamente”, por drones identificados visualmente como comerciales, así como también se conoce que al no disponer de ningún sistema automático de detección y peor aún de inhibición, los organismos públicos de seguridad pública se ven imposibilitados a tomar acciones inmediatas en estas situaciones de riesgo.

Igualmente, los principales problemas que se presentan a la hora de usar sistemas inhibidores ya existentes en el mercado de Inteligencia de Señales, son: altos costos de los existentes y de alta reserva (en la mayoría propietarios), muchas veces la falta de soporte, así como también la deficiencia en la transferencia de tecnología por ser sistemas cerrados de producción. Contrariamente los sistemas endógenos como el presente proyecto, que se desarrollan en base a la investigación aplicada e ingeniería inversa pueden subsanar estos inconvenientes con costos muy reducidos y con garantía de una transferencia de tecnología real (al usuario) dentro de todos los procesos de concepción, diseño, implementación y operación. Por lo tanto, el desarrollo propuesto supera estas dificultades, puesto que a través de la investigación y desarrollo pueden ser solventadas dando como resultado mejores

herramientas que sobretodo son parte intrínseca y propietaria del sistema general de vigilancia y seguridad. Esto permitirá hacer efectivas la aplicación de políticas y planes para el desarrollo de las tecnologías de información y comunicación en el ámbito de la seguridad nacional, aumentando la eficiencia y la efectividad de respuesta del Ejército Ecuatoriano en situaciones de riesgo que requieran atención inmediata principalmente en zonas declaradas estratégicas.

3. Alcance del Proyecto

Este proyecto de investigación tiene como finalidad el desarrollo de un prototipo de un sistema inhibidor de drones en las bandas comerciales 2.4 y 5.8 GHz, mediante técnicas de *jamming* que generan señales en torno a la misma frecuencia en las que opera el dron, con el objetivo de interferir la señal de radio control, interrumpir el vuelo del aparato y cancelar la transmisión de video. Las frecuencias seleccionadas corresponden a bandas comerciales WiFi, que son los estándares que manejan los drones comerciales.

En la primera etapa del proyecto de investigación, se analizó las distintas técnicas de *jamming* y mediante una comparación entre la complejidad-beneficios, se optó por las técnicas de *jamming* por barrido y por ruido de banda ancha; las cuales son implementadas en el sistema. En la segunda etapa se elaboró el diseño e implementación de las técnicas de *jamming* seleccionadas, las cuales corresponden a algoritmos desarrollados en Arduino C++ y circuitos electrónicos. Una vez elaboradas las estrategias de *jamming* se acoplan los distintos dispositivos como son: osciladores controlados por voltaje (VCO), *switch* de control, amplificador y antena, los cuales conforman el sistema para obstruir a las bandas de frecuencia en las que opera el dron.

4. Objetivos

4.1 Objetivo General

Desarrollar un sistema inhibidor de drones que trabajan en bandas comerciales WIFI para neutralizar y bloquear sus objetivos de vigilancia en zonas estratégicas del estado ecuatoriano.

4.2 Objetivos Específicos

- Analizar las diversas técnicas de inhibición de señales existentes, principalmente aquellas orientadas a sistemas que utilizan *spread spectrum*
- Concebir y diseñar técnicas propias de inhibición de las señales de control de drones, a partir de los datos entregados por el sistema que detecta, monitorea, discrimina y localiza estos dispositivos.
- Implementar y operar el sistema de inhibición de drones desarrollado, para determinar su desempeño y fundamentalmente el alcance en distancia efectiva a obtener.
- Reducir peso, volumen, costo computacional y precio del sistema en relación a los existentes en el mercado.
- Proveer a las instituciones vinculadas con la prestación de servicios de emergencias, información relevante que permita coordinar la respuesta ante un incidente o emergencia.

CAPITULO II

FUNDAMENTOS TEÓRICOS

2.1 Introducción

En esta sección se presenta una visión general de los vehículos aéreos no tripulados (*Unmanned Aerial Vehicle* - UAV), comúnmente denominados drones, sus principales técnicas de control a distancia y las diferentes técnicas empleadas para inserir señales de interferencia intencionales (*jamming*) en el canal de telecontrol. Adicionalmente, una breve revisión de las técnicas de *spread spectrum* (o dispersión controlada del espectro) y del sistema de posicionamiento global (*Global Positioning System*– GPS) serán presentadas.

Fue a mediados del siglo XIX cuando James Clerk Maxwell, en su obra *A Dynamical Theory of the Electromagnetic Field*, sentó las bases teóricas - matemáticas de teoría electromagnética, clave indiscutible de la implementación/consolidación de los actuales sistemas de telecomunicación. Esa teoría establece que, de forma general, fuentes electromagnéticas dinámicas generan campos electromagnéticos dinámicos que se propagan en el interior de un medio o a través del vacío (Balanis, 2012). Considerando campos armónicos linealmente polarizados y un medio lineal, homogéneo, no dispersivo e isotrópico, el mecanismo de propagación de los campos electromagnéticos es ilustrado en la figura 1.

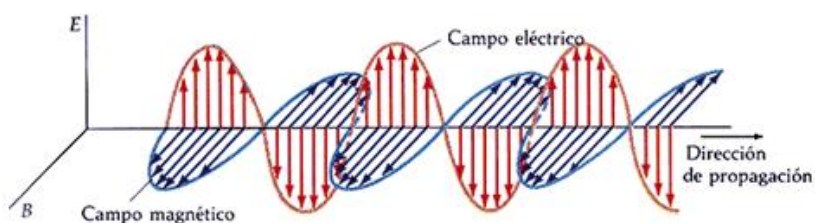


Figura 1. Ilustración de la dirección de propagación de una onda electromagnética. En rojo se representa el campo eléctrico armónico (\vec{E}) y en azul el campo magnético (\vec{B}).

Fuente: (Ureña, 2009)

El mecanismo de propagación presentado en la figura 1, a pesar de ser el más simple, es un buen ejemplo de cómo la dirección de propagación se relaciona con los campos (regla de la mano derecha). Existe una variedad de fenómenos que pueden producirse cuando una onda electromagnética se propaga en un medio cualquiera. Esas interacciones dependen de las propiedades del medio, de la polarización de la onda y de posibles objetos que se encuentren en su interior, de la geometría de la superficie y características de la superficie. Entre ellos, la reflexión, refracción, interferencia y difracción son efectos más conocidos que pueden afectar la propagación de una onda electromagnética (Seybold, 2005).

Con base a la teoría electromagnética se sabe que en el espacio libre o en el vacío la velocidad de propagación de una onda electromagnética es igual a la velocidad de la luz y que esta velocidad se relaciona con los parámetros característicos del medio a través de:

$$c_0 = 1/\sqrt{\mu_0 \varepsilon_0} \cong 2,998 \times 10^8 \text{ [m/s]} \quad (1)$$

donde μ_0 y ε_0 son la permeabilidad magnética y permitividad eléctrica en el vacío, respectivamente.

Uno de los parámetros que caracteriza una onda electromagnética es denominado longitud de onda, λ , y está relacionada con la frecuencia de onda, f , y con la velocidad de propagación de dicha onda en el medio, v , a través de:

$$\lambda = v/f \text{ [m]} \quad (2)$$

en el caso donde el medio de propagación es el vacío se tiene que v es igual a c_0 .

Considerando la frecuencia, o la longitud de onda λ , el espectro electromagnético va desde las ondas subsónicas hasta los rayos cósmicos. Una representación de las principales subdivisiones o bandas se muestra en la figura 2.

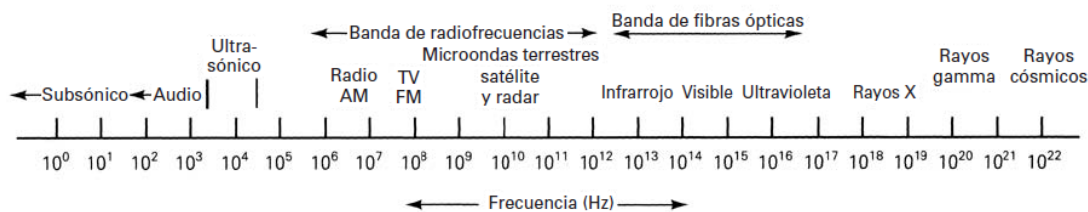


Figura 2. Espectro electromagnético de frecuencias.

Fuente: (Tomasi., 2003)

Diversos organismos internacionales definen el espectro de radiofrecuencias como una sub-sección del espectro de la figura 2 y han separado bandas de frecuencia específicas para la operación y regulación de los diversos sistemas de telecomunicaciones. A título de ejemplo, las designaciones de las bandas según la Unión Internacional de Telecomunicaciones (UIT) se muestran en la Tabla 1.

Tabla 1

Designación de las bandas 2 hasta la 14 según la UIT.

Número de banda	Intervalo de frecuencias	Designación
2	30 Hz – 300 Hz	ELF - frecuencias extremadamente bajas
3	300 Hz – 3 kHz	ULF – frecuencias ultra bajas (voz)
4	3 kHz – 30 kHz	VLF – frecuencias muy bajas
5	30 kHz – 300 kHz	LF – frecuencias bajas
6	300 kHz – 3 MHz	MF – frecuencias intermedias
7	3 MHz – 30 MHz	HF – frecuencias altas
8	30 MHz – 300 MHz	VHF – frecuencias muy altas
9	300 MHz – 3 GHz	UHF – frecuencias ultra altas
10	3 GHz – 30 GHz	SHF – frecuencias super altas
11	30 GHz – 300 GHz	EHF – frecuencias extremadamente altas
12, 13, 14	300 GHz – 300 THz	Luz infrarroja

Fuente: (UIT, 2016)

En este punto se debe mencionar que el presente trabajo, por el propio objetivo planteado, estará restringido a las bandas de UHF y SHF (bandas 9 y 10). De forma general podemos representar un enlace de telecomunicaciones, desde un punto de vista de diagramas de bloques, por medio del gráfico de la figura 3.

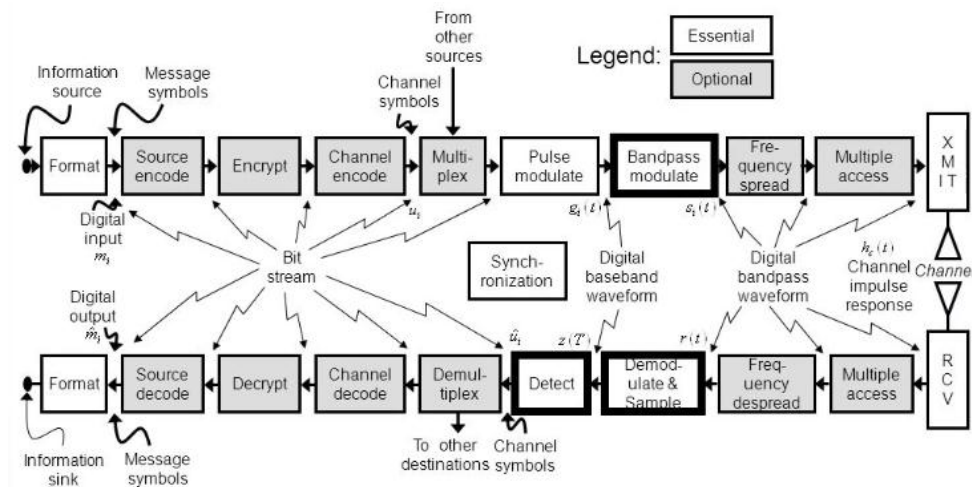


Figura 3. Representación de un enlace de telecomunicaciones a través de sus principales bloques funcionales.

Fuente: (Sklar, 2001)

En la figura 3 se puede observar que la información generada en la fuente de la información (*information source*) es transmitida a través del canal (*channel*) hacia el destinatario (*information sink*) después de la ejecución de diversos procesos, cada uno de los cuales es representado por un bloque en la figura 3. En función del tipo de transmisor/receptor, i.e. si es análogo o digital, los bloques arriba mencionados son esenciales u opcionales. El bloque *frequency spread* que, si bien es cierto es opcional, introduce un cierto grado de inmunidad al *jamming*. De forma análoga, el bloque que realiza el proceso inverso en el receptor es denominado de *frequency despread*. Estos dos bloques, ampliamente estudiados en los sistemas de comunicación digital, es una técnica que implementa la dispersión controlado del espectro (*spread spectrum - SS*).

En sistemas de comunicación *spread spectrum*, la señal que es transmitida suele tener un ancho de banda mucho mayor que el ancho de banda mínimo necesario para su transmisión (Posiel, 2011). El concepto básico utilizado es dispersar el ancho de banda de la señal de información, de forma controlada, sobre todo el ancho de banda disponible, para que en vez de agrupar la energía de la señal alrededor de una portadora específica lo realice sobre toda la banda. Al no tener un pico notoriamente identificable en su espectro, la señal se torna casi indistinguible del ruido y, por lo tanto, más difícil de identificar, interceptar o bloquearla (Instruments, 2014).

De forma general para que un sistema sea considerado *spread spectrum* debe presentar una de las siguientes características (Sklar, 2001):

- El ancho de banda que ocupa la señal excede en mucho el mínimo ancho de banda necesario para transmitir la información deseada.
- La dispersión del espectro es obtenida por medio de una señal denominada de señal de dispersión (*spreading signal*), usualmente denominada de secuencia código, la misma que es independiente de los datos a ser transmitidos.
- En el receptor la operación inversa a la dispersión, o recuperación de los datos originales, es implementada por la correlación entre la señal recibida (*spread signal*) y una réplica sincronizada de la secuencia código usada en el transmisor.

Al considerar una señal con ancho de banda W y duración T su dimensión dentro del espacio de señales es aproximadamente $2WT$ (Haykin, 2001). Para incrementar la dimensión de ese espacio de señales se puede incrementar W , por la dispersión controlada del espectro, o incrementar el T por la dispersión temporal o salto temporal (*time hopping*). La dispersión en

el dominio de la frecuencia es obtenida con la dispersión controlada de la señal, en cuanto, en el dominio temporal es implementada a través del salto temporal (*time hopping*). Las dos técnicas más populares para implementar la dispersión espectral es la secuencia directa (*direct sequence* – DS) y salto de frecuencia (*frequency hopping* – FH).

- Dispersión controlada del espectro por secuencia directa (DS-SS)

En los sistemas DS-SS, todos los usuarios transmiten simultáneamente con la misma portadora y dentro del mismo ancho de banda del canal asignado (Posiel, 2011). La información de banda base se distribuye sobre el ancho de banda del canal, el mismo que es mucho mayor al necesario para transmitir la señal de banda base, en virtud de la utilización de una secuencia denominada pseudo-aleatoria. Esa secuencia está constituida de símbolos denominados *chip*, cada uno de ellos con período mucho menor al período de los símbolos de la señal de banda base, y conforman el denominado código *chipping*. La razón entre el período del símbolo de la señal de banda base al período del *chip* es denominado ganancia del código y está estrechamente relacionada con la cantidad de dispersión que se aplica al espectro original de la señal de banda base.

Esta característica es obtenida por la multiplicación de la señal mediante la convolución con una secuencia de números pseudo-aleatorios de unos y ceros. Por otro lado, en el receptor se utiliza una réplica sincronizada del mismo código *chipping* utilizado en la transmisión para recuperar el mensaje original (Prabakaran, 2003).

- Dispersión controlada del espectro por salto de frecuencia (FH-SS)

Se basa en transmitir una sección de la información en una frecuencia determinada, durante un intervalo de tiempo (*dwell time*). Después de este tiempo se modifica la frecuencia

de emisión y se continúa transmitiendo otra sección del mensaje original en otra frecuencia diferente. De este modo cada sección de información utiliza una frecuencia diferente de intervalos de tiempos cortos.

En la sección de recepción se mantiene un registro sincronizado de la actual frecuencia de transmisión y de sus próximos saltos que serán realizados (López F. , s.f). Se debe resaltar que la selección de la frecuencia de salto es controlada por una secuencia pseudo-aleatoria.

2.2 Estándar IEEE 802.11 para redes de área local inalámbricas (WLAN)

Redes de área local inalámbricas (*Wireless Local Area Network – WLAN*) están normadas por el estándar IEEE 802.x que define el uso de los niveles de capa física y capa de enlace de datos (definidas en la arquitectura del modelo OSI – *Open System Interconnection*). El Instituto de Ingenieros Eléctricos y Electrónicos (*Institute of Electrical and Electronics Engineers – IEEE*) publicó en 1997 el primer estándar de la norma, el mismo que se responsabiliza de su mantenimiento. Los productos con redes inalámbricas del sello *Wi-Fi Alliance* utilizan las especificaciones de este estándar, ya que aporta la base de su desarrollo.

Los estándares de 802.x establecen la tecnología de redes de área local (*Local Area Network – LAN*) y redes de área metropolitana (*Metropolitan Area Network– MAN*). Por ejemplo, el estándar 802.11 define en su capa de control de acceso al medio (*Medium Access Control – MAC*) la gestión y conservación de las comunicaciones entre estaciones 802.11, ya sean puntos de acceso a adaptadores de red. La capa MAC también coordina el acceso a un canal de radio compartido y la utilización de su capa física (*Physical Layer – PHY*) para detectar la portadora y la transmisión/recepción de tramas. (Seide, 2005)

La capa física (PHY) en una red 802.11 realiza las siguientes funciones:

- Opera como la interfaz entre la capa MAC en dos o más puntos geográficos.
- Lleva a cabo la detección real de los sucesos causados por el algoritmo de acceso múltiple con escucha de portadora y detección de colisiones (*Carrier Sense Multiple Access with Collision Detection – CSMA/CD*).
- Realiza la modulación y demodulación de la señal entre dos puntos geográficos en los equipos 802.11. Entre los esquemas de modulación están DS-SS o FH-SS (Seide, 2005).

La capa MAC controla la conectividad de dos o más puntos a través de un esquema de direcciones, presenta las siguientes funcionalidades:

- Servicios de control de acceso y entrega de datos al nivel MAC para las capas superiores de la pila de protocolos de red.
- Los datos del usuario que se transmiten a través del medio inalámbrico deben poseer seguridad y privacidad, en el intercambio de información.
- Controla aspectos de movilidad de una red 802.11.

Los productos 802.11 usan técnicas de dispersión controlada del espectro (SS) para operar legalmente en la banda ISM (*Industrial, Scientific and Medical*) de 2.4 GHz. Existen dos modos soportados por el 802.11 y 802.11b, estos son: dispersión controlada del espectro por secuencia directa (DS-SS) y la dispersión controlada del espectro por saltos de frecuencia (FH-SS). Generalmente DS-SS tiene un mejor desempeño, en tanto que FH-SS es más robusto a la interferencia no intencional o intencional (*jamming*). Aunque OFDM (*Orthogonal Frequency Division Multiplexing*) es una técnica para modular la señal a través de un ancho de banda determinado, no es una técnica spread spectrum, los estándares 802.11a

y 802.11g usan OFDM como su técnica de modulación (Seide, 2005). El protocolo 802.11 contiene varios estándares que se detallan en la Tabla 2.

Tabla 2

Tabla comparativa de los diferentes estándares 802.11

Stan.	Banda	Ancho de banda	Modulación	Canal	Max. Tasa de datos	Distan.	Poten. máxima
802.11	2,4GHz	20 MHz	BPSK a 256 QAM	DS-SS, FH-SS	2 Mbps	20 m	100 mW
b	2,4GHz	21 MHz	BPSK a 256 QAM	CCK, DS-SS	11 Mbps	35 m	100 mW
a	5 GHz	22 MHz	BPSK a 256 QAM	OFDM	54 Mbps	35 m	100 mW
g	2,4GHz	23 MHz	BPSK a 256 QAM	DD-SS, OFDM	54 Mbps	70 m	100 mW
n	2,4GHz 5 GHz	24 MHz 40 MHz	BPSK a 256 QAM	OFDM	600 Mbps	70 m	100 mW
ac	5 GHz	20, 40, 80, 80+80 =160 MHz	BPSK a 256 QAM	OFDM	6,93 Gbps	35 m	160 mW
ad	60 GHz	20 MHz	BPSK a 64 QAM	SC, OFDM	6,76 Gbps	10 m	10 mW
af	54-790 MHz	20 MHz	BPSK a 256 QAM	SC, OFDM	26,7 Mbps	>1000 m	100 mW
ah	900 MHz	20 MHz	BPSK a 256 QAM	SC, OFDM	40 Mbps	1000 m	100 mW

CCK = Complementary code keying, SC = Single-carrier

Fuente: (Seide, 2005)

2.3 Sistema de posicionamiento global (*Global Positioning System – GPS*)

El sistema de posicionamiento global (GPS) fue idealizado, diseñado e implementado por el gobierno de los Estados Unidos en un consorcio entre Universidades Norte Americanas, el Departamento de Defensa (DoD) y empresas del sector privado. Inicialmente, diseñado para

uso militar, su uso fue extendido al campo civil por las innumerables aplicaciones prácticas que fueron desarrolladas posteriormente. El primer satélite GPS fue lanzado en 1978 y la operación total del sistema fue completada a mediados de la década de los noventa. Como se infiere del texto anterior el sistema GPS se basa en la tecnología Satelital. Su principio de funcionamiento es la determinación de la distancia entre el receptor y algunos pocos satélites observables por el usuario de forma simultánea. Esa distancia es generalmente conocida con el nombre de pseudo-distancia. La posición de cada uno de los satélites observables es transmitida dentro de la señal GPS generadas por cada satélite hacia todos los usuarios. Básicamente, conociendo las posiciones de pocos satélites, su pseudo-distancia y aplicando la técnica de trilateración se puede calcular la posición del usuario (Parkinson BW, 1996).

El sistema GPS está constituido por un conjunto de 24 satélites geoestacionarios distribuidos en seis planos orbitales. El ángulo de ascensión orbital entre planos es igualmente distribuido e igual a 60° . Cada uno de los satélites se auto-orienta para garantizar que sus paneles solares estén direccionados hacia el sol y sus antenas estén orientadas hacia la superficie de la tierra. Cada satélite transporta cuatro relojes atómicos y pesa aproximadamente 1000 kg. La estabilidad en frecuencia a largo plazo de cada uno de los relojes es superior a 10^{-13} partes por día. Con base a las señales originadas por los relojes atómicos una base de tiempo de referencia de 10.23 MHz, extremadamente estable, está disponible internamente en los satélites. (Scherrer, 1985)

Todos los satélites GPS son monitoreados por cinco estaciones bases. La estación base principal está en Colorado Spring, Colorado – USA. Las otras cuatro estaciones son la de Ascension Island (Océano Atlántico), Diego Garcia (Océano Indico), Kwajalein y Hawaii (en el Océano Pacífico). Todas las estaciones cuentan con un reloj de Cesio y receptores para

calcular las efemérides que serán transmitidas a los usuarios y para modelar los relojes de los satélites. Los ajustes de las efemérides y de la sincronización de los relojes son transmitidos a cada uno de los satélites, los mismos que, actualizan la señal GPS que se envía, nuevamente, a los receptores de los usuarios posicionados en la superficie de la Tierra.

Cada satélite GPS transmite datos en tres frecuencias de la banda L. Esas frecuencias son L1 (1575,42 MHz = $154 f_0$), L2 (1227,60 MHz = $120 f_0$) y L5 (1176,45 MHz = $115 f_0$), donde f_0 es la frecuencia de referencia de 10,23 MHz. Las informaciones del código pseudorandómico (*Pseudorandom Noise* – PRN), efemérides del satélite, modelo ionosférico y las correcciones al relojes del satélite son superpuestas en las portadores de L1, L2 y L5. La banda L5 está reservada para aumentar la redundancia del sistema y mejorar su robustez.

Como fue mencionado anteriormente la banda L5 está reservada para incrementar la robustez del sistema, por tanto, se centrará la explicación de la señalización solo en las bandas L1 y L2. Los datos de navegación contienen información respecto al satélite. Esta información es subida para todos los satélites a partir de las estaciones de tierra del segmento de control y son retransmitidos a los usuarios a una tasa de transmisión de 50 bps. Cada satélite posee dos secuencias pseudo-aleatoria o códigos. El primer es conocida como código de adquisición grueso (*Coarse Acquisition Code* – C/A) y el segundo es el código de precisión encriptado (*Encrypted Precision Code* – P(Y)).

El código C/A es una secuencia de 1023 *chirps*. Este código es repetido cada 1 ms con una tasa de repetición de *chirps* de 1,023 MHz.

El código P(Y) es un código extremadamente grande, aproximadamente de $2,35 \times 10^4$ *chirps*, que es transmitido a una tasa de *chirps* de 10,23 MHz. Su período de repetición es alrededor de 1 semana, iniciando con la semana GPS. El código C/A es modulado solamente en la

banda L1, mientras que el código P(Y) es modulado en la banda L1 y L2 (Kai, 2007). Las informaciones presentadas anteriormente son mostradas, de forma resumida, en la Tabla 3.

Tabla 3

Bandas de operación, plan de uso y modernización de servicio de GPS

Banda	Frecuencia (MHz)	Fase	Uso original	Modernizado
L₁	1575,42 154 f_0	I	Código de precisión encriptada P(Y)	
		Q	Código de adquisición grueso C/A	C/A, civil L1 y código militar (M)
L₂	1227,60 120 f_0	I	Código de precisión encriptada P(Y)	
		Q	Portadora no modulada	Código civil L2 y código militar (M)
L₅	1176,45 115 f_0	I	No disponible	Señal de datos de seguridad de la vida (SoL)
		Q		Señal de datos de seguridad de la vida (SoL)

$$f_0 = 10,23 \text{ MHz.}$$

Fuente: (Kai, 2007)

La Tabla 3 es una versión resumida de cómo los códigos de adquisición gruesa y el código de precisión encriptado son transportados en las bandas L1, L2 y L5. Se debe resaltar, en este punto, que el sistema GPS es un elemento clave en los UAV y que a través de él le permite conocer su posición actual y recorrer trayectorias predefinidas automáticamente.

2.4 Vehículo Aéreo no Tripulado (UAV) – Drones

Un vehículo aéreo no tripulado (UAV), como fue mencionado anteriormente, es un dispositivo aéreo capaz de mantener de manera autónoma un nivel de vuelo controlado y sostenido. Con el auxilio de sensores, sistemas de posicionamiento, plataformas inerciales, un enlace de comunicación y un sistema de procesamiento, el UAV es capaz de ser manejado y

controlado de forma remota por un operador en tierra o auto guiarse para cumplir una misión pre-programada (G. Zhou, 2005).

Al contar con una serie de sensores en el vehículo UAV este es capaz de notificar de manera remota al usuario de lo que sucede a su alrededor (control mediante sensores). Igualmente, al disponer de unidades de GPSs, el UAV es capaz de proporcionar información de las coordenadas geográficas del dron en tiempo real. Aparte de rastrear la posición del UAV, permite a la aeronave dirigirse una ruta establecida por el usuario de manera automática entre una serie de ubicaciones (Carrasco, 2015). En vista de la capacidad de control, movilidad y facilidad de acceso a lugares inaccesibles estos vehículos puede grabar imágenes (filmación de eventos). Adicionalmente, pueden realizar mediciones de campos electromagnéticos, sistemas de radar, visión de infrarrojos y sensores tanto biológicos como químicos.

Actualmente el uso de drones abarca muchos campos y ha crecido exponencialmente en todas las naciones. Su uso puede ser legal para favorecer el avance de la sociedad o, por otro lado, facilitar los actos delictivos y servir como apoyo a los grupos ilegales. Para conocer sus principales características se menciona a continuación:

2.4.1 UAV de ala rotatoria

Se caracterizan por utilizar un motor que impulsan una o más hélices del conjunto denominado rotor. Este sistema es el responsable de suministrar el impulso necesario para el despegue y maniobrabilidad de la aeronave. Dispone de una autonomía máxima, alrededor de veinte minutos y con la habilidad de volar a una velocidad media en torno a 60 km/h (Carrasco, 2015). Estos UAV son aptos para quedarse suspendidos en el aire, inmóviles, por la

acción de los rotores. Por tanto, pueden realizar tareas de control sobre un objetivo fijo a una distancia adecuada del mismo. Con la incorporación de un dispositivo de grabación son utilizados en trabajos de vigilancia y monitorización de elementos, ya sean éstos fijos o móviles. Además pueden llevar una carga adicional hasta un punto geográfico predefinido.


2.4.2 Principales sistemas de comunicación de UAV comerciales

La característica particular que presenta los drones comerciales es la comunicación en la banda de WiFi. A seguir en la Tabla 4 se proporciona una lista de las bandas utilizadas su comunicación por drones comerciales.

Tabla 4

Lista de drones comerciales que utilizan la bandas de WiFi

Modelo	Fabricante	Frecuencia [GHz]	Peso [gramos]	Costo [\$ USA]
Phantom 4	Dji	2.4	1380	2000
Phantom 4 Advanced	Dji	2.4	1368	1750
Phantom FC40	Dji	2.4 y 5.8	1200	700
AR.Drone	Parrot	2.4	420	320
Bebop 2	Parrot	2.4	500	580
Disco FPV	Parrot	2.4	750	1390
Jumping Race	Parrot	2.4 y 5.8	205	170
Mambo	Parrot	2.4	100	130
Swing	Parrot	2.4	295	150
Typhoon H	Yuneec	5.8	1950	1280
H501A X4 Air Pro	Hubsan	2.4	1300	230
H507A X4 Star Pro	Hubsan	2.4	162	99
X8SW	Syma	2.4	1500	155
X8SC	Syma	2.4	1500	150
X5UW	Syma	2.4	127	75

Continúa 

U818A Discovery	UdiRc	2.4	132	100
U29W	UdiRc	2.4	100	60

Fuente: (Igor Bisio, Chiara Garibotto y otros, 2018)

Los drones se comunican con la estación de control terrestre a través de transmisiones de RF. La gran mayoría de los UAV comerciales (más del 90%) se comunican hoy en día en las bandas ISM (*Industrial, Scientific and Medical radio bands*) no sujetas a licencia. Las frecuencias asignadas para las transmisiones ISM es de 2.4 GHz y 5.8 GHz, las mismas bandas utilizadas por los dispositivos WiFi. Se debe resaltar que los UAVs cuando están equipados con cámaras normalmente transmiten video a su controlador en uno de los canales inalámbrico asignados a la banda de 5.8 GHz (Igor Bisio, Chiara Garibotto y otros, 2018).

La banda 2.4 GHz dispone de 14 canales superpuestos con un salto de 5MHz entre cada canal y con un ancho de banda cada uno de 22 MHz. Mientras que la banda de 5.8 GHz posee hasta 24 canales sin superposición. Adicionalmente, la velocidad de transmisión de 54 Mbps y hasta de 1.3 Gbps, para el protocolo 802.11ac, son tasas de transmisión comunes en la actualidad. Una representación de los canales disponibles para la frecuencia de 2.4 GHz se presenta en la figura 4.

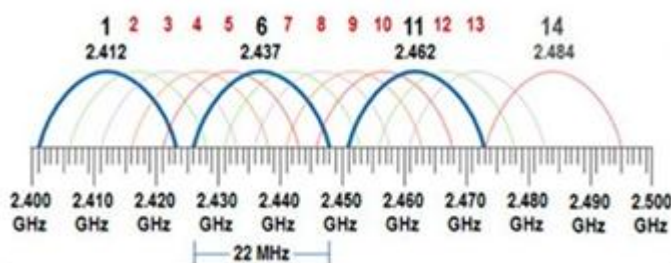


Figura 4. Distribución de los canales de la banda de frecuencia de 2,4 GHz WiFi.

Fuente: (Drones, 2018)

La figura 4 ejemplifica las alternativas de control en los canales asignados a la banda de 2.4 GHz disponibles actualmente. Los métodos que son más utilizados (> 80 %) para el control remoto de los drones son la de secuencia directa (DS-SS) y la dispersión controlada del espectro por salto de frecuencia (FH-SS) con diferentes características según sus fabricantes. Los dos procedimientos FH-SS/DS-SS se han implantado para el control de drones a modo de estándar que adoptan la mayoría de los fabricantes (Phuan, 2017). La red global de comunicación entre la estación base y el dron por lo general se origina en el propio vehículo ya que posee su propia red WiFi en modo ad-hoc a la cual se conecta la estación base. La manipulación de drones con este tipo de tecnología resulta sencillo y factible, ya que se requiere solamente de un smartphone o tablet para manejar y/o visualizar este vehículo aéreo no tripulado. (Fernández, 2016).

2.5 Guerra electrónica.

2.5.1 Definición.

Guerra electrónica (*Electronic Warfare - EW*) es la representación general de acciones militares que involucran la utilización de energía electromagnética con el fin de determinar, aprovechar, explotar, reducir o prevenir el empleo hostil del espectro electromagnético por parte del enemigo y a su vez apropiarse del espectro en beneficio propio, logrando obtener un reconocimiento inmediato de una amenaza (Valderrama, 1980). El uso de equipos electrónicos abarca completamente los niveles y modalidades de combate.

La guerra electrónica se identifica por mantener el control del espectro electromagnético y por la explotación tecnológica de los Sistemas de Armas dirigidos a la reducción o destrucción de las capacidades de los sistemas enemigos y a oponerse a los ataques, creando

sistemas de protección, cuya conservación dependerá de la aplicación sistemática y coordinada de los sistemas electrónicos en el momento y lugar adecuados a fin de contrarrestar las acciones del enemigo (Valderrama, 1980).

2.5.2 Clasificación.

Las diferentes acciones a realizar dentro del campo de la guerra electrónica, se agrupan en tres áreas fundamentales para identificar cualquier tipo de amenaza y evitar ataques sorpresas (Arcangelis, 1983).

2.5.2.1 Medidas de apoyo electrónico (*Electronic Support Measures- ESM*)

Área que comprende las acciones de búsqueda, intercepción, identificación de fuentes de energía electromagnética con el propósito de obtener un reconocimiento inmediato de la amenaza (Arcangelis, 1983).

Las ESM tienen aplicación en una amplia gama de actividades, como son: alarma temprana de amenazas, detección y localización de la amenaza, forma de eludir las emisiones, adquisición de blancos y destrucción o supresión de defensas (Instrucción a la Guerra Electronica Aérea, 1983).

Para resumir, se puede decir que ESM trata con la expansión de las operaciones militares a través del estudio del espectro electromagnético.

2.5.2.2 Contramedidas electrónicas (*Electronic Countermeasures - ECM*)

Área que basa sus acciones para impedir o reducir el uso enemigo del espectro electromagnético y ejercer el comando, empleo de las armas y comunicaciones, mediante la utilización del bloqueo o engaño electrónico. A su vez pueden ser activas o pasivas.

Las ECM activas presentan dos funciones:

- **Perturbación:** Es la irradiación o reflexión de la energía electromagnética para reducir el empleo del enemigo, de equipos o sistemas electrónicos. Esto se genera modulando una onda portadora con una señal de ruido.
- **Engaño o Señuelo:** Irradiación, alteración, absorción o reflexión de energía electromagnética con el fin de aturdir al adversario en la interpretación de la información recibida por medio de sus sistemas electrónicos (Arcangelis, 1983).

Las ECM pasivas emplean medios no electrónicos, se clasifican en:

- **Mecánicas:** Estas son cintas de estaño, las cuales reflejan las emisiones del radar, produciendo ecos falsos en sistemas de Radar.
- **Químicos:** Son sustancias como pinturas especiales diseñadas para absorber las ondas electromagnéticas con el objetivo de disminuir el parámetro denominado de sección recta de radar (*Radar Cross Section - RCS*) (Arcangelis, 1983).

2.5.2.3 Contra contra medidas electrónicas (*Electronic Counter-Countermeasures - ECM*)

Los ECCM son sistemas que permiten eludir a las ECM y tienen la capacidad de proteger los sistemas amigos ante una acción ECM tomada por un enemigo potencial (Arcangelis, 1983).

2.5.3 Otras actividades de la Guerra Electrónica.

Otra actividad de la EW que se realiza en cualquier momento y para cualquier aplicación es denominada inteligencia de señales SIGINT (*Signal Intelligence*). Esta actividad no se realiza, necesariamente en medio de un conflicto bélico, si no en cualquier momento para

recoger, evaluar, analizar, interceptar y valorar informaciones relativas a países extranjeros considerados potencialmente hostiles o áreas de operaciones significativas para guerra electrónica (Arcangelis, 1983). Tradicionalmente se subdividen en:

- Inteligencia de Comunicaciones COMINT (*Communications Intelligence*): Capta señales radioeléctricas del adversario para transformarlas en información técnica y operativa.
- Inteligencia Electrónica ELINT (*Electronic Intelligence*): Estudio de las emisiones electromagnéticas presentes en un posible escenario de actividades.

2.6 Estrategias para generar interferencias intencionales o *Jamming*

Jamming se define como una actividad que afecta directamente la comunicación sobre los enlaces de RF de un adversario en un tiempo específico. Es decir, logra que la información no llegue al usuario (Poisel, 2004). Existen diferentes estrategias de *jamming* que se puede implementar para atacar diversas aplicaciones, entre ellas tenemos:

2.6.1 Generación de señales de interferencia por la adición de ruido

Esta técnica utiliza una fuente de ruido aleatorio para generar una señal de interferencia intencional que se transmite en el mismo espectro que es ocupada por la señal que se pretende bloquear. El propósito es interrumpir la comunicación del sistema identificado por medio de la inserción de ruido en el receptor. El ancho de banda de la señal puede ser tan extenso como todo el espectro utilizado por el sistema a ser interferido o más estrecho, ocupando solo un canal (Poisel, 2004). Suele ser dividido en:

- *Jamming* por ruido de banda-ancha o banda completa: Conocido como ruido de banda ancha (*Broad band noise- BBN*) introduce energía a través de todo el ancho de banda

del espectro asignado al sistema enemigo. Este tipo de interferencia aumenta el nivel de ruido de fondo en el receptor, creando un ambiente mucho más ruidoso para ese sistema. Al incrementar el nivel de ruido en el receptor su sensibilidad empeora y exige un mayor desempeño al proceso de detección, desempeño que, posiblemente, se encuentre fuera de sus características de proyecto.

- *Jamming* por ruido de banda-parcial: Conocido como PBN (*Partial-band noise*) introduce energía a través de una parte delimitada del espectro, cubriendo algunos canales. Canales que pueden ser o no consecutivos. Desde el punto de vista de energía este tipo *jamming* no desperdicia potencia al insertar interferencia en bandas o canales no utilizados.
- *Jamming* por ruido de banda angosta: Conocido como NBN (*Narrowband noise*), produce una señal de interferencia introduciendo energía en sólo un canal. El ancho de banda de dicha energía podría contener todo el canal o solamente una parte de él. De esta forma la potencia puede ser concentrada a una pequeña parte del espectro, lo que es una ventaja en términos de eficiencia y efectividad (Poisel, 2004). Una representación gráfica de estas técnicas de *jamming* es ilustrada en la figura 5.

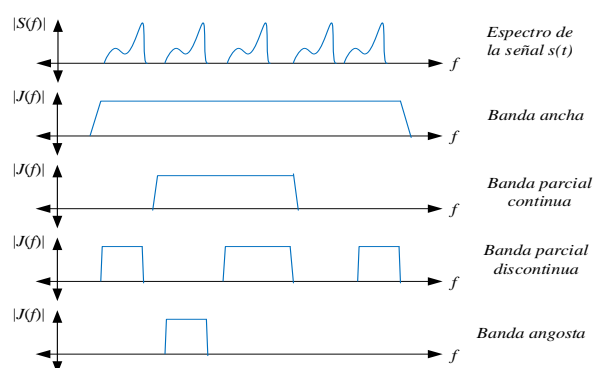


Figura 5. Estrategias de generar señales de interferencia por la adición de ruido.

Fuente: (Poisel, 2004).

2.6.2 Generación de señales de interferencia por tonos.

En esta técnica la generación de señales de interferencia se basa en la adición de un tono (*single tone- ST*) o múltiples tonos (*multiple tone- MT*) a lo largo del ancho de banda donde se encuentre la señal que se desea interferir. En este esquema se asume que el tono se coloca precisamente en una frecuencia en el espectro, de modo que el tono de interferencia pasa a través de los filtros del receptor sin distorsión ni atenuación. En sistemas con dispersión controlada del espectro por DS-SS es factible usar un tono simple para cambiar el offset en los receptores y provocar que exceda el nivel máximo de la señal, logrando así la pérdida de información. La relación entre la fase del tono emitido por el *jammer* y la fase de la señal es un factor relevante. Al enviar un solo tono, éste estará en la frecuencia del cero o del uno. Si está en la frecuencia del uno, su fase representa una complicación, puesto que si el tono no se está en fase no se lograría interferir la transmisión del símbolo. Por el contrario si el tono está en la frecuencia del cero, entonces se podrá bloquear la transmisión al símbolo considerando que la potencia sea apropiada sin depender de la fase. En el caso de múltiples tonos, si se ubican los tonos en canales continuos, la capacidad de la interferencia sería equivalente a la capacidad de la interferencia generada por ruido de banda parcial. Puesto que los tonos se sitúan en canales continuos, se los conoce como *comb jamming* (Poisel, 2004).

2.6.3 Generación de señales de interferencia por pulsos.

Similar a la generación de señales de interferencia por ruido de banda parcial, en este caso corresponde a una porción de tiempo que la interferencia está activa. El tiempo que está encendido la señal de interferencia se abarca una parte amplia del espectro. Aquí la señal de interferencia puede tener potencias promedio más bajas, cuando comparadas con las otras

señales generadas por las técnicas enumeradas anteriormente. Esta característica la hace eficiente si se diseña correctamente el ciclo del trabajo (Poisel, 2004). El ciclo de trabajo determina la relación entre la potencia media y la potencia máxima. Los efectos de interferencia dependen de la potencia máxima y de la frecuencia con la que la señal llega al receptor.

2.6.4 Generación de señales de interferencia por barrido.

Radica en inyectar ruido en una parte del espectro, después de ubicar esa señal, se procede a efectuar un barrido por todo el ancho de banda que ocupe la señal que se desea interferir. Esta estrategia optimiza el uso de la potencia, puesto que emplea la máxima potencia en un determinado lugar y en un determinado momento (León, 2010).

2.6.5 Generación de señales de interferencia por seguimiento.

Se aplica en sistemas que utilizan la tecnología FH-SS. Primero se debe conocer la frecuencia a la que ha saltado la señal objetivo. Un posible algoritmo para determinar el nuevo salto de frecuencia es monitorear la potencia en puntos específicos, a partir de esa medida se podría deducir que esa es la nueva frecuencia del salto cuando la potencia sobrepase algún determinado valor. Este procedimiento no siempre produce buenos resultados ya que la velocidad del salto de frecuencias es alto, tornando difícil estimar la frecuencia del nuevo salto (Poisel, 2004).

2.6.6 Generación de señales de interferencia inteligente

Se refiere al estudio de la señal enemiga (objeto adversario) para lograr mejores resultados en la toma de decisión de cual tipo de interferencia debe ser utilizada. Un ejemplo de esto es

el *jamming* de engaño, en el cual se envía mensajes falsos para mantener a una de los puntos terminales del enlace de comunicación en estado de recepción permanente. Logrando así que no haya confirmación de que se recibió el mensaje y se genere una interrupción del enlace.

2.7 Clasificación de los generadores de interferencia (*jammer*).

Con base a las estrategias que pueden ser utilizadas para generar una señal de interferencia se pueden derivar cuatro tipos principales de generadores de interferencias o *jammer*:

2.7.1 Generador constante de interferencia (*jammer* constante)

El principal beneficio es la facilidad de implementarse, aunque en aplicaciones donde se desea que el *jamming* pase inadvertido no es recomendable utilizar un *jammer* constante.

2.7.2 Generador de interferencia de engaño (*jammer* de engaño)

Envía señales que parecen ser auténticas, pero no incluye una señalización de fin de mensaje. Esto produce que el receptor permanezca en estado de recepción indefinidamente. Como ventaja es ser menos propenso a la detección pero el consumo de potencia requerida es considerable (Xu, 2005).

2.7.3 Generador de interferencia aleatorio (*jammer* aleatorio)

Este *jammer* opera en períodos de tiempo aleatorios, fuera de esos el deja de generar la señal de interferencia. El ciclo de trabajo es programado de acuerdo a su aplicación. Se puede utilizar para generar señales de interferencia por ruido, por pulsos, por tonos e incluso por barrido (Poisel, 2004). El consumo de potencia requerida es menor ya que no se encuentra en funcionamiento todo el tiempo.

2.7.4 Generador de interferencia reactivo (*jammer* reactivo)

Su principio de trabajo radica en censar la actividad de su entorno para conocer en qué momento debe ejecutarse la operación de interferencia. El consumo de potencia es mínimo, sin embargo, a pesar de no ser excesivo si se requiere determinada potencia para estar supervisando la actividad de su ambiente de trabajo (Xu, 2005).

Las estrategias ideales para el proyecto son: ruido y barrido, teniendo en cuenta que al comparar entre rendimiento y aplicación, estas resultaron ser las más óptimas.

CAPITULO III

DISEÑO DEL SISTEMA INHIBIDOR DE DRONES QUE TRABAJAN EN BANDAS COMERCIALES WIFI.

De acuerdo con lo mencionado en el capítulo II sobre las bandas UHF y SHF, tecnología WIFI, vehículo aéreo no tripulado (UAV), así como también las estrategias de *jamming*, el objetivo del presente capítulo es unificar estos tópicos para el desarrollo del sistema inhibidor de drones en las bandas comerciales WIFI, para lo cual en este capítulo se muestran conceptos ligados a la elección de las técnicas de *jamming*, descripción de elementos a utilizar y explicación de la elaboración de los subsistemas que conforman el sistema global inhibidor, como se visualiza en la figura 6.

Con la investigación previa realizada sobre las diversas estrategias de *jamming*, estudiadas en el capítulo II, a continuación se indica las técnicas que se eligieron para formar parte del sistema inhibidor del presente proyecto de grado.

3.1 Elección de las estrategias de *jamming* y tipo de *jammer*

Previamente con el conocimiento referente a las estrategias y tipos de *jamming*, se optó que las estrategias ideales para el proyecto son: las estrategias por ruido y barrido, teniendo en cuenta que al comparar las diversas técnicas entre complejidad, rendimiento y aplicación, estas resultaron ser las más óptimas, así como por la experiencia que tiene el CICTE en el desarrollo de sistemas de *jamming* para COMINT realizadas en el proyecto de guerra electrónica del año 1996.

La estrategia de *jamming* por ruido de banda parcial se eligió visto que cubre solamente algunos canales, y no desperdicia tanta potencia. Otra estrategia elegida es la estrategia de *jamming* por barrido la cual emplea la máxima potencia en un determinado lugar y en un determinado momento. Estas estrategias trabajan con el tipo de *jammer* constante por las ventajas que proporciona.

Las demás estrategias que no se seleccionaron presentan ciertas complicaciones al elaborarlas, así como también el requerimiento de mucha potencia. A continuación se detalla algunas de las limitaciones:

- El *jamming* por pulsos al caracterizarse por encenderse y apagarse, no es adecuado para nuestra aplicación puesto que se requiere que esté encendido en todo instante.
- El *jamming* de ruido por banda-ancha demanda mucha potencia, lo que llevaría a la elaboración de varias etapas de ganancia para la antena.
- El *jamming* de tonos no es funcional ni eficaz en sistemas que manejan “Frequency Hooping” (FH).
- El diseño de *jamming* por seguimiento es muy complejo así como su implementación.

Ahora con las técnicas de *jamming* ya seleccionadas se parte a realizar la implementación del sistema inhibidor de drones, la cual presenta varias etapas, que se muestran a continuación.

3.2 Descripción del Sistema Inhibidor

La figura 6 detalla los componentes del sistema inhibidor, cada uno de los bloques presentan acciones importantes que se relacionan entre sí para un funcionamiento coordinado. En este apartado se explica cada uno de los bloques.

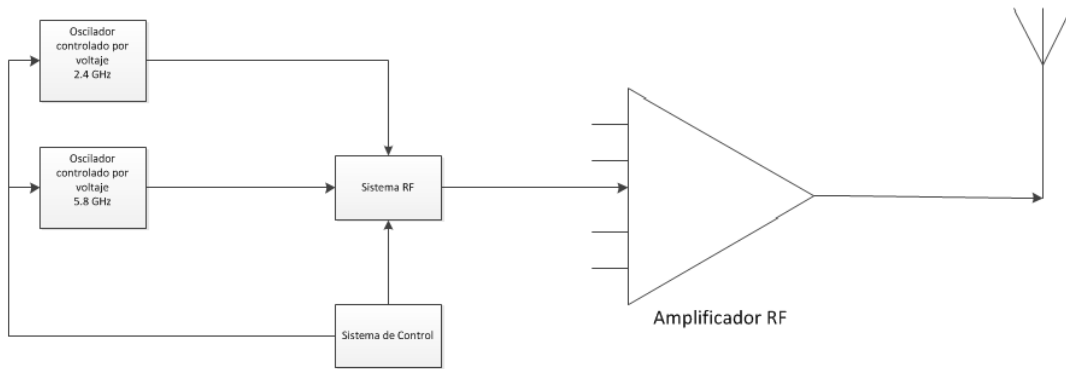


Figura 6. Diagrama de Bloques del sistema *jamming*

Para iniciar se debe considerar unos de los elementos más importantes del sistema que son los osciladores controlados por voltaje (VCO), los cuales nos van proporcionar de frecuencias portadoras para interferir las bandas comerciales WIFI del drone.

3.2.1 Oscilador controlado por voltaje (VCO)

El oscilador controlado por voltaje (VCO), es el elemento principal del sistema. La función de transferencia del VCO es:

$$f(t) = f_o + K_o V_c(t) \quad (3)$$

La grafica que detalla el comportamiento de la ecuación 3, se visualiza en la figura 7.

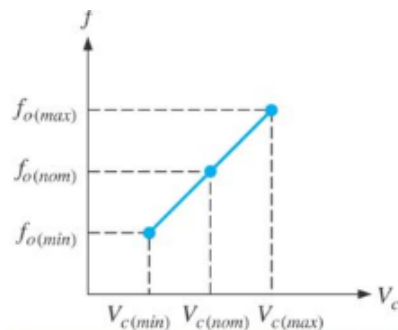


Figura 7. Función de transferencia del VCO.

Fuente: (Comunicaciones, 2016)

Por definición se admite que el VCO es lineal y que el coeficiente K_o es constante. En la práctica, no siempre es así (Dieuleveult, 1999).

Para el sistema inhibidor de drones, se conoce que opera el drone en las bandas de 2.4 GHz y 5.8 GHz para su transmisión con el comando de control, tratado en el capítulo II, lo cual se dispone de VCO's en el rango de esas frecuencias.

3.2.1.1 Oscilador controlado por voltaje 2.4 GHz

Se utiliza el oscilador ZX95-2536C-S+, de la empresa minicircuit, que trabaja desde 2.31 GHz hasta 2.53 GHz. Para más detalle de sus especificaciones, observar el [Anexo 1](#).

Para corroborar dichos datos del Anexo 1 que proporciona (MiniCircuits), se realizó pruebas del funcionamiento del VCO ZX95-2536C-S+. Considerando 3 parámetros: voltaje de sintonía (V. Tune), frecuencia y potencia. Se tomaron datos desde 0.5 V hasta 5 V con pasos de 0.25 V, en la Tabla 5 se indica los resultados obtenidos.

Voltaje de alimentación: 5 V

Corriente: 42 mA-44 mA

Tabla 5
Datos de Prueba

V. Tune [V]	Frecuencia [GHz]	Potencia [dBm]
0.5	2.294	4.3
0.75	2.311	4.5
1	2.328	4.6
1.25	2.345	4.7
1.5	2.362	5
1.75	2.379	5
2	2.397	4.7
2.25	2.416	4.7
2.5	2.435	4.7
2.75	2.453	4.7
3	2.470	4.9
3.5	2.504	5.1
4	2.539	5.2
4.5	2.569	5.1
5	2.595	5.1

En la figura 8 se visualiza el comportamiento real del VCO ZX95-2536C-S+, considerando que con un determinado valor de voltaje se obtiene una determinada frecuencia.

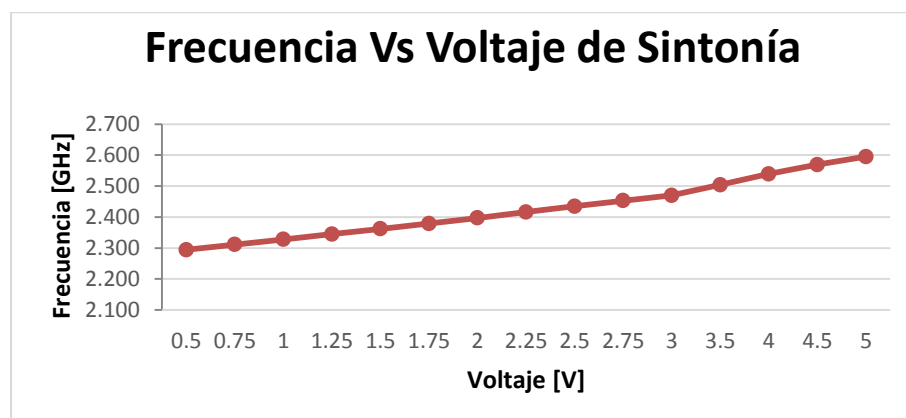


Figura 8. Frecuencia Vs Voltaje de Sintonía

3.2.1.2 Oscilador controlado por voltaje 5.8 GHz

Se utiliza el oscilador ZX95-5776+, de la empresa minicircuit, que trabaja desde 5.72 GHz hasta 5.82 GHz. Para más detalle de sus especificaciones, observar el [Anexo 2](#).

Para corroborar dichos datos del Anexo 2 que proporciona (MiniCircuits), se realizó pruebas del funcionamiento del VCO ZX95-5776+. Considerando 3 parámetros: voltaje de sintonía (V. Tune), frecuencia y potencia. Se tomaron datos desde 0.5 V hasta 5 V con pasos de 0.25 V, en la Tabla 6 se indica los resultados obtenidos.

Voltaje de alimentación: 5 V

Corriente: 23 mA

Tabla 6
Datos de Prueba

V. Tune [V]	Frecuencia [GHz]	Potencia [dBm]
0.5	5.689	-3.6
0.75	5.706	-4.8
1	5.722	-4.7
1.25	5.737	-3.6

Continúa

1.5	5.752	-1.7
1.75	5.767	-1
2	5.783	-2.3
2.25	5.801	-3.8
2.5	5.819	-3.5
2.75	5.837	-1.8
3	5.856	-0.3
3.25	5.873	-1.6
3.5	5.894	-3.6
3.75	5.913	-4.1
4	5.933	-2.6
4.25	5.951	-0.6
4.5	5.968	-1.4
4.75	5.984	-3.7
5	5.999	-4.9

En la figura 9 se visualiza el comportamiento real del VCO ZX95-5776+, considerando que con un determinado valor de voltaje se obtiene una determinada frecuencia.

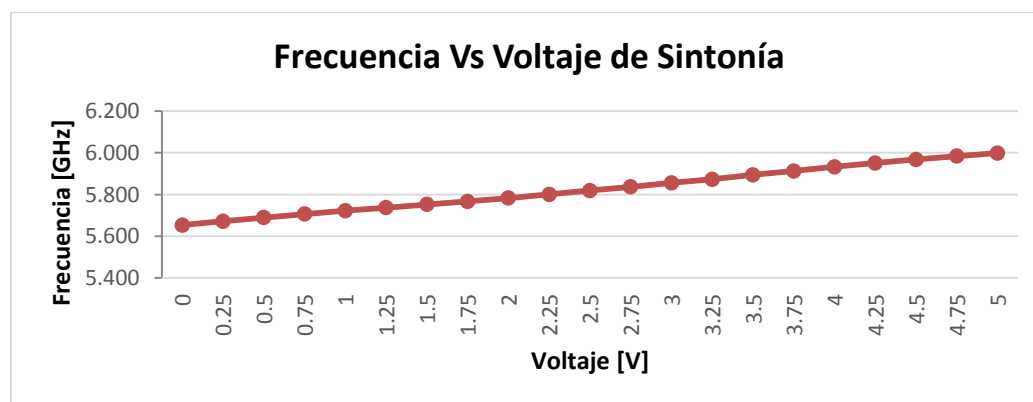


Figura 9. Frecuencia Vs Voltaje de Sintonía

Conociendo el comportamiento de los VCO's anteriormente detallados y con cuales se trabajarán, ahora se debe plantear el control que va a regir a dichos VCO's, para nuestra finalidad, que es interferir con las técnicas ya seleccionadas. De lo estudiado en el capítulo II sobre el estándar WIFI de las bandas de 2.4 GHz y 5.8 GHz, se considera trabajar con un ancho de banda de 80 MHz en cada una de las bandas de frecuencias.

Es decir en el caso de los VCO's se va a manejar entre 2 V a 3 V para obtener el ancho de banda de 80 MHz. Dato primordial para desarrollar las técnicas de *jamming*, para la técnica de ruido se plantearon dos métodos: a) una de ellas es desarrollado tanto en software como hardware mediante Arduino Due que se encuentra en parte del sistema de control y b) la otra solamente en hardware. A continuación se presenta la elaboración de las estrategias de *jamming*.

3.2.2 Jamming

De las estrategias seleccionadas que son de barrido y ruido, la de ruido presenta dos métodos, y se ha optado por generar ruido gaussiano, estos métodos se detallan en las secciones 3.2.2.1 y 3.2.2.2.

3.2.2.1 Descripción del generador de ruido gaussiano (GNG) desarrollado en arduino due

Se opta por algoritmos utilizados en los GNGs como son los métodos Wallace, Box-Muller (BM) (D. Lee, 2006), teorema del límite central (CLT) e inversión. Para la elaboración del GNG de nuestro sistema se utilizó el método de Box-Muller. El método BM genera un par de números aleatorios gaussianos independientemente, transformando un número aleatorio distribuido uniformemente, proporcionando así un rendimiento relativamente alto en el hardware GNG (Jaejoon Choi, 2016). El procedimiento de conversión requiere funciones como: seno, coseno, logaritmo y raíz cuadrada. Este método hace el análisis accesible debido a las propiedades analíticas deseables de la distribución gaussiana.

Al tratar con ruido gaussiano se sabe que éste es un tipo de ruido que posee distribución gaussiana de media cero, característica fundamental para utilizar herramientas que nos

permita dicho comportamiento, (Carlson, 2002). La implementación del GNG con el método Box-Muller (BM) se desarrolla en el IDE de Arduino DUE, esta tarjeta tanto en hardware como software permite la realización del programa por la diversidad de funciones que posee.

3.2.2.1.1 Método Box Muller

Primero se inicia con la creación de dos variables aleatorias independientes y uniformes, u_0 y u_1 , en el intervalo (0,1). Posterior a ello se realizan las siguientes operaciones matemáticas para generar dos muestras, x_0 y x_1 . (D. Lee, 2006)

$$e = -2 \ln(u_0) \quad (4)$$

$$f = \sqrt{e} \quad (5)$$

$$g_0 = \sin(2\pi u_0) \quad (6)$$

$$g_1 = \sin(2\pi u_1) \quad (7)$$

$$x_0 = f * g_0 \quad (8)$$

$$x_1 = f * g_1 \quad (9)$$

Las variables x_0 y x_1 son números generados con distribución normal de media 0 y variancia 1.

3.2.2.1.2 Generador de ruido gaussiano

Al obtener las variables con distribución normal de media 0 y variancia 1, que modelan el ruido gaussiano, ahora deben sintonizarse con el voltaje que controlarán los VCO's, para ello la tarjeta de Arduino Due tiene pines DAC (Conversión Digital- Análogo) de 12 bits que proporciona voltajes analógicos según la resolución en bits. Por lo cual se debe unir las variables x_0 y x_1 del método de Box Muller con una variancia "Var" y los valores de 12 bits

que están en el rango de 0 a 4095, cada uno de estos representan su valor en analógico, por ejemplo: 1023 equivale a 1.2V. Es así que se eligió el valor de 1345 (para situar el valor de 1.5V en el arduino) y con 116 (para que se encuentre en el rango de 1 a 2V) logrando así en conjunto la oscilación de valores analógicos entre 1 V a 2 V, para posteriormente incrementar en una etapa de amplificación de 2 V a 3 V, voltajes requeridos para sintonizar al VCO de 2 GHz entre 2.39 GHz a 2.48 GHz y al VCO de 5 GHz entre 5.78 GHz a 5.85 GHz.

A continuación se presenta en las figuras 10 y 11 el espectro de la señal de salida del VCO, según el valor de voltaje aleatorio correspondiente.

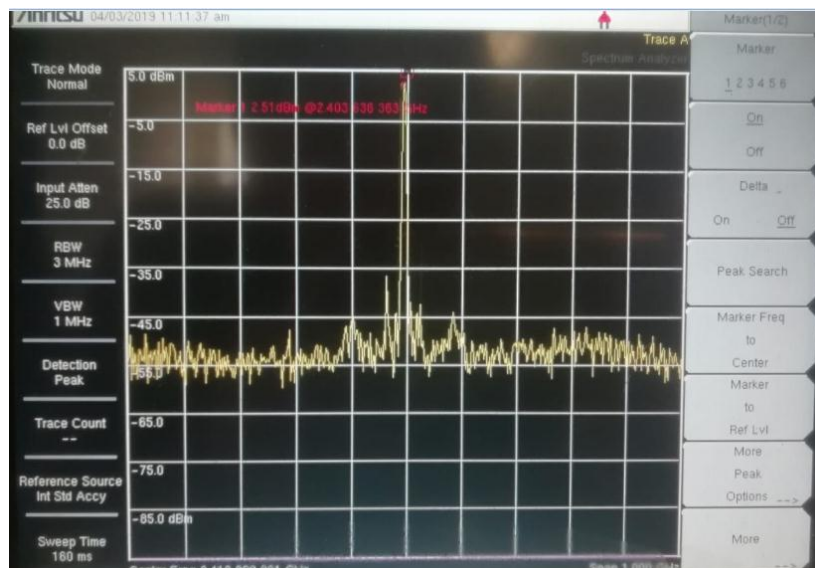


Figura 10. Sintonización aleatoria en banda de 2.4 GHz

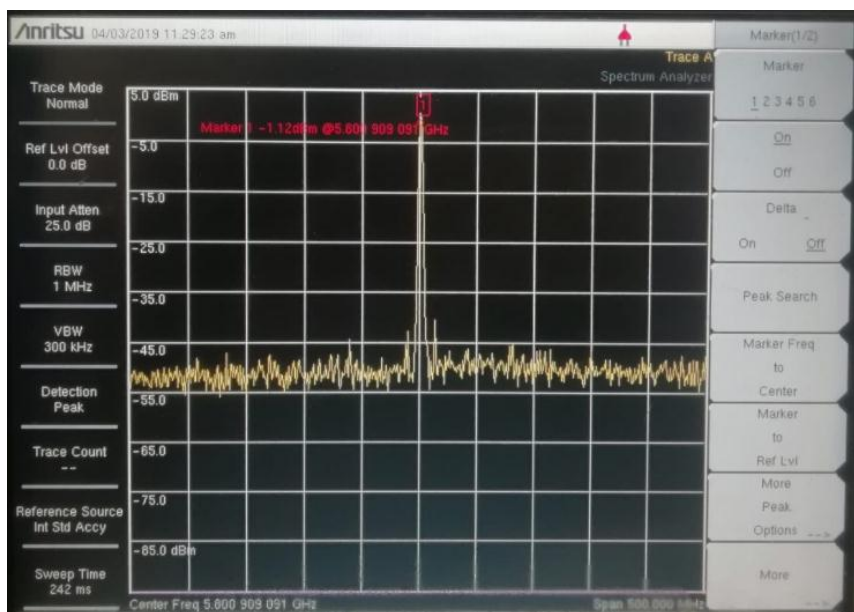


Figura 11. Sintonización aleatoria en banda de 5.8 GHz

3.2.2.2 Descripción del circuito generador de ruido

Para generar el ruido, se opta por la elaboración de un circuito de ruido gaussiano blanco, el cual consta de transistores NPN, y al polarizar un transistor inversamente, de tal manera que su juntura no conduzca ninguna corriente, aun así existe la circulación de una pequeña cantidad de portadores de cargas y se aprovecha esta unión para la producción de ruido a partir del movimiento térmico de los portadores de carga. También cuenta con etapas de amplificación. Este generador de ruido es de nivel regulable por medio del potenciómetro de 10k. Las resistencias son de 1/4W con 5 o 10% de tolerancia y los capacitores pueden ser de poliéster o de cerámica. El esquema para obtener el ruido deseado se muestra en la figura 12.

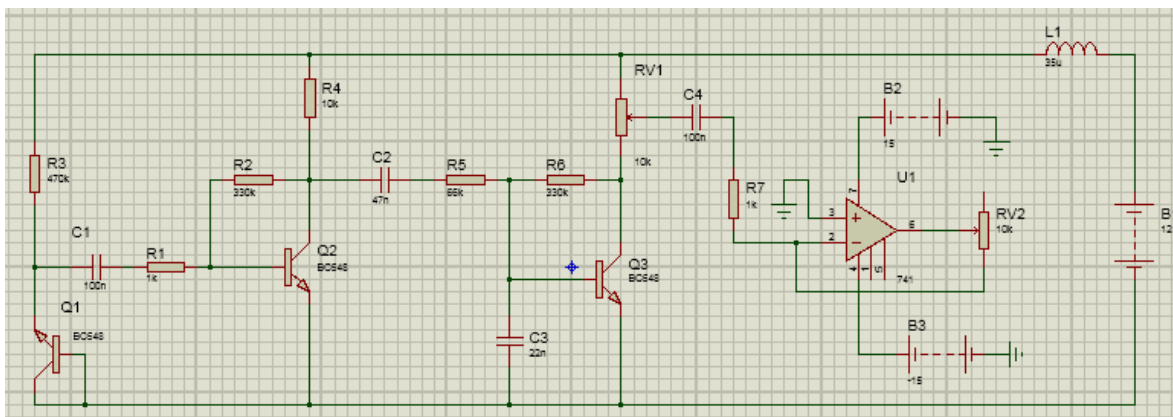


Figura 12. Circuito generador de ruido blanco

La señal de salida presenta una baja intensidad, alrededor de 36 mV de amplitud, como se visualiza en la figura 13, por lo que la salida de esta señal debe ser amplificada.

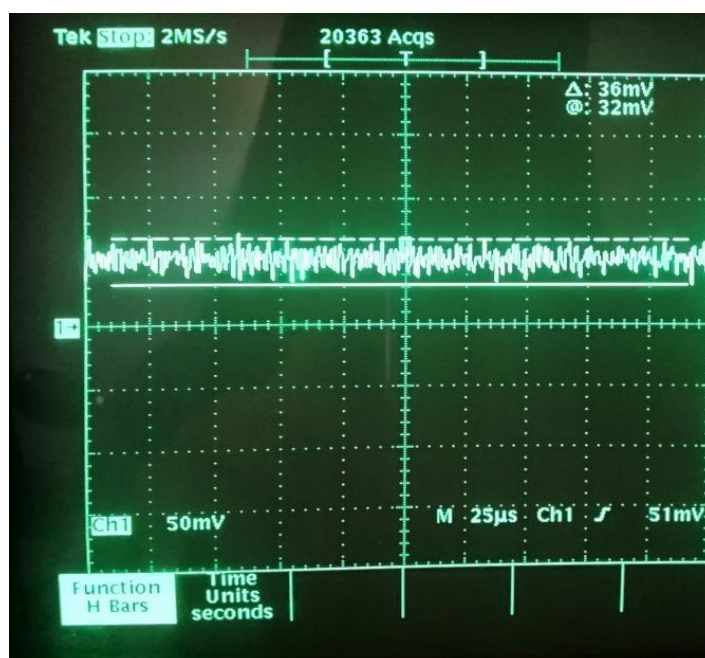


Figura 13. Señal de salida del circuito de ruido.

La figura 14 muestra la magnitud del ruido generado por el circuito, con la etapa de amplificación unificada que es de alrededor de 108 mV de amplitud.

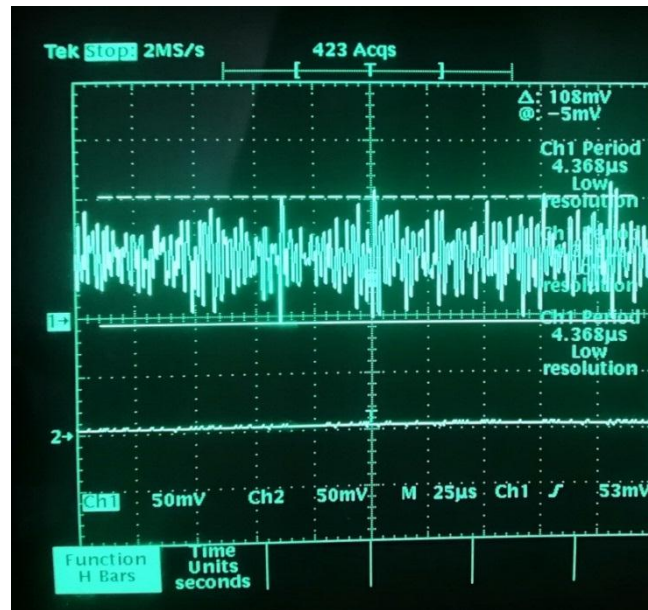


Figura 14. Señal de salida amplificada del circuito de ruido.

Para acoplar el circuito se requiere de un Bias-Tee (figura 15) en el cual se introduce un voltaje entre 2 V a 3V (voltaje de sintonía de los VCO's en las bandas de 2.4 GHz o 5.8 GHz) y la salida del circuito de la figura 12. La salida del Bias-Tee ingresa al VCO correspondiente y se obtiene ruido blanco en las banda de frecuencia sea en 2.4 GHz o 5.8 GHz.



Figura 15. Bias-Tee

3.2.2.3 Descripción del *Jamming* por Barrido

La técnica de *jamming* por barrido se elabora mediante la utilización del generador de señales, modelo AFG2020 Sony Tektronix, la cual permite crear una señal del tipo triangular o rampa, como se indica en la figura 16. Esta señal presenta las siguientes características, dependiendo del tipo de frecuencia a interferir:

3.2.2.3.1 Para 2.4 GHz

Voltaje High: 1.5 V

Voltaje Low: 1V

Offset: 1.25 V

Amplitud: 0.5 Vpp

Frecuencia: 8 KHz

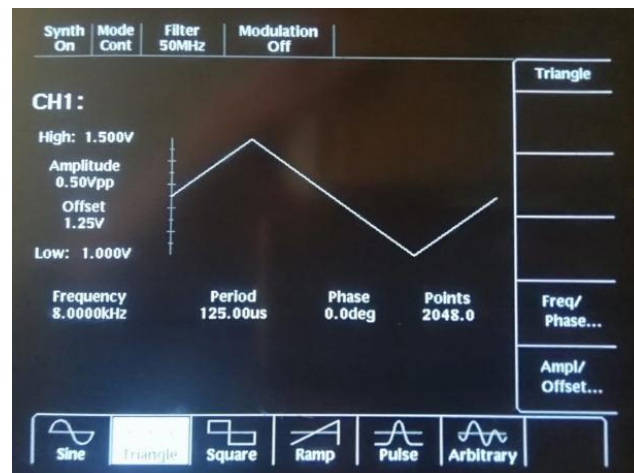


Figura 16. Señal interferente para la banda de 2.4GHz

3.2.2.3.2 Para 5.8 GHz

Voltaje High: 1.5 V

Voltaje Low: 1 V

Offset: 1.25 V

Amplitud: 0.5 Vpp

Frecuencia: 8 KHz

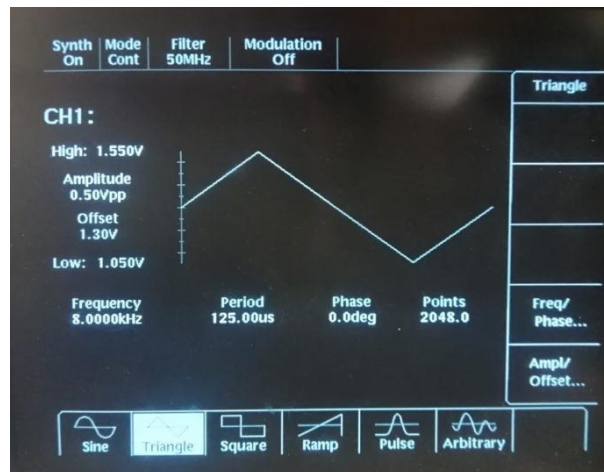


Figura 17. Señal interferente para la banda de 5.8 GHz

En cada una de las señales generadas de las figuras 16 y 17 estas barren todas las frecuencias comprendidas entre los valores *Low* y *High*, cada determinado periodo. La salida del generador de señales se conectan con los voltajes de sintonía de los VCO's correspondientes.

Con las estrategias de *jamming* ya desarrolladas y al estar ya acopladas con los VCO's, se procede a unir con los sistemas de control y radiofrecuencia, cada uno de estos sistemas se trata a continuación.

3.2.3 Sistema de control

El sistema de control tiene la funcionalidad de recibir información correspondiente a las frecuencias de 2.4 GHz y 5.8 GHz y ejecuta determinadas instrucciones para una de las frecuencias seleccionadas, mencionadas a continuación:

- Activa el sistema de radiofrecuencia para dar el paso de la señal interferente, ya sea ésta correspondiente a las bandas de 2.4 GHz o 5.8 GHz.
- Genera la técnica de *jamming* por ruido, considerando que en este proceso constan los voltajes que sintonizan las frecuencias correspondientes para el funcionamiento de los VCO's, para ello se utiliza las tablas de frecuencias de los VCO's de 2.4 GHz y 5.8 GHz.

Cada una de estas instrucciones es desarrollada en Arduino Due.

La figura 18 presenta la conexión general del sistema de control con el sistema de radiofrecuencia y VCO's.

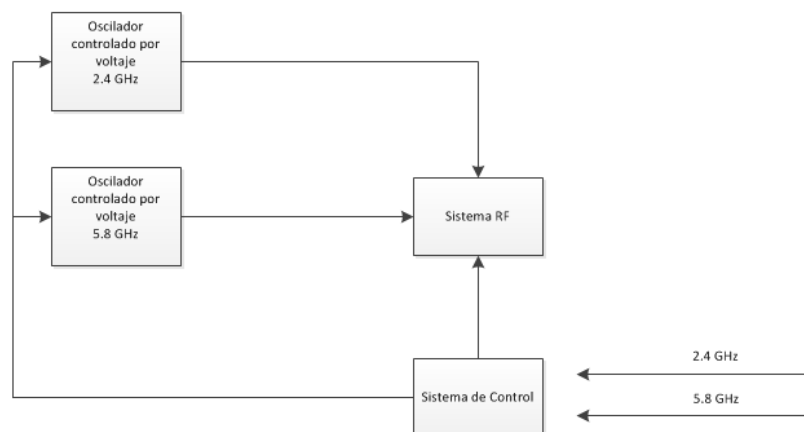


Figura 18. Conexiones del sistema de control

3.2.4 Sistema de Radiofrecuencia

El sistema de radiofrecuencia permite el paso de las señales interferentes generadas por los VCO's, para lo cual el sistema lo compone un interruptor de control HMC321ALP4E de la empresa (Analog Devices) como se muestra en la figura 19, el cual permite la conmutación de las señales a utilizar. Sus principales características son:

- Rendimiento de banda ancha: DC-8 GHz.
- Incluye un circuito de decodificador binario integrado, lo que reduce las líneas de control lógico necesarias a tres.
- El interruptor funciona con una tensión de control positiva de 0/+5 voltios.
- Para el uso de sistemas de 50 Ohm o 75 Ohm.
- Alto aislamiento: >30 dB a 6 GHz




Figura 19. Switch de control HMC321ALP4E
Fuente: (Analog Devices)

La conmutación del *switch* es controlado por un circuito binario, el cual requiere una combinación de 3 bits para seleccionar una de sus salidas, la Tabla 7 presenta la tabla de verdad:

Tabla 7
Tabla de verdad

Control Input			Signal Path State
A	B	C	RFC:
Low	Low	Low	RF1
High	Low	Low	RF2
Low	High	Low	RF3
High	High	Low	RF4
Low	Low	High	RF5
High	Low	High	RF6

Continúa 

Low	High	High	RF7
High	High	High	RF8

Fuente: (Analog Devices)

Al contener dos señales interferentes que proporcionan los VCO's, se toma las entradas RF2 y RF3 que se conectan con el VCO de 2.4 GHZ y el VCO de 5.8 GHZ, respectivamente.

Este sistema de radiofrecuencia está ligado al sistema de control puesto que la conmutación del *switch* depende de combinaciones digitales que va a realizar el sistema de control para que la señal de uno de los VCO's se muestre a la salida RFC y ésta sea amplificada.

3.2.5 Amplificador RF

Para alcanzar la potencia de salida deseada, la etapa de amplificación es necesario, el amplificador que trabaja en el rango de frecuencia de 2000 a 8000 MHz y el que se uso es el modelo ZVE-3W-83+, de la empresa minicircuit. Sin embargo de sus especificaciones es posible utilizarlo para la banda L1 de GPS con una pequeña perdida en el rendimiento pero útil. Entre sus características están:

- Máxima potencia, 3 W
- Figura de ruido, 5.8 dB típ.
- Alta IP3, +42 dBm typ.
- Alto rango dinámico
- Alta ganancia, 35 dB típ. y buena directividad, 35 dB tip.
- Tensión interna regulada de 13 a 18 VDC.

Para mayor detalle de sus especificaciones observar el [Anexo 3](#). Para corroborar dichos datos del anexo que proporciona (MiniCircuits), se realizó pruebas del funcionamiento del

amplificador ZVE-3W-83+. Considerando 3 parámetros: frecuencia, potencia de entrada y potencia de salida. Se tomaron datos desde 1.5 GHz hasta 6 GHz con pasos de 1 GHz, en la Tabla 8 se indica los resultados obtenidos.

Voltaje de alimentación: 15 V

Corriente: 0.849 mA

Tabla 8

Datos de Prueba

Frecuencia [GHz]	Potencia In [dBm]	Potencia Out [dBm]
1.5	5	35.6
	10	40.8
2	-50	-18.76
	-40	-8.7
3	-50	-20.19
	-40	-10.23
4	-50	-19.75
	-40	-9.77
5	-50	-20.9
	-40	-11.96
6	-50	-24.75
	-40	-14.9

3.2.6 Antena

La antena log periódica con 11 dipolos, presentada en la figura 20, al presentar mayor directividad, permite emitir la señal interferente, para causar un mayor impacto hacia el drone, la banda de operación es 900 MHz a 2300 MHz, impedancia de 50Ω. Para mayor detalle de su desempeño observe los resultados de las simulaciones en ANSYS HFSS [Anexo](#)

[4.](#)

Función Directividad, $D(\theta, \phi)$, tridimensional para 2,4 GHz

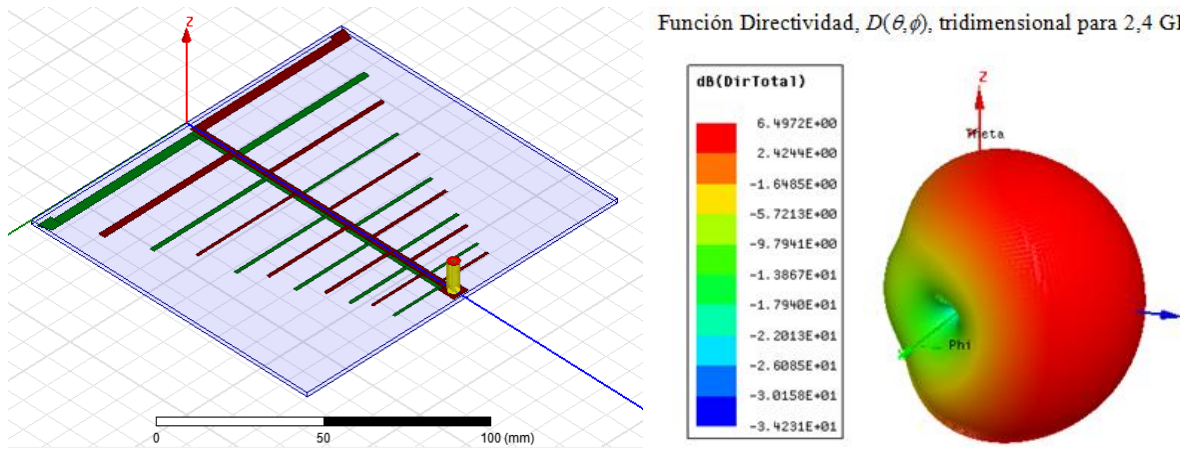


Figura 20. Antena log periódica

CAPITULO IV

IMPLEMENTACIÓN DEL SISTEMA PROTOTIPO INHIBIDOR O *JAMMER* DE DRONES

El objetivo del presente capítulo radica en la implementación y puesta en operación del sistema prototipo inhibidor de drones en las bandas comerciales WIFI, mediante pruebas de campo, cuyo sistema es detallado en el capítulo III. Se detallan las conexiones del sistema para su implementación, así como también el manejo del mismo, el cual permitirá conocer la correcta manipulación del sistema inhibidor para dar inicio a las pruebas de campo, que son expuestas a diversos escenarios, cuyos resultados son presentados en este capítulo y en el respectivo manual de usuario (documento de exclusivo uso del CICTE).

4.1 Conexiones del sistema inhibidor de drones

El sistema inhibidor de drones consiste en una estructura que integra todos los elementos (VCO's, *switch* RF, circuito ruido, arduino, amplificador, antena) detallados en el capítulo III (figura 21) y que son necesarios para cumplir la función principal del sistema: interferir al vehículo no tripulado (drone). Cada técnica de *jamming* se adapta al sistema ya sea por lógica de programación o conexiones físicas, y se especifican a continuación:

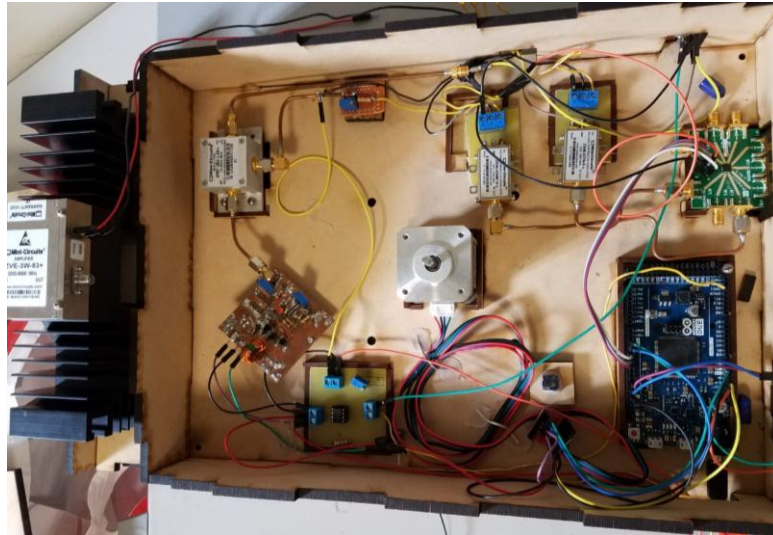


Figura 21. Estructura interna del sistema inhibidor de drones.

Primero, mediante un *dip switch*, denominado dip 1, se permite seleccionar la frecuencia a trabajar, estas son: 2.4 GHz y 5.8 GHz (figura 22), al elegir una de ellas, se ejecutarán determinadas instrucciones como: activación del sistema radiofrecuencia y la generación de la técnica de *jamming* por ruido generado en Arduino. Aquí se presentan las primeras conexiones, las salidas digitales del Arduino hacia los pines de activación del *switch* de control, como se indica en la figura 23



Figura 22. Dip switch, dip 1

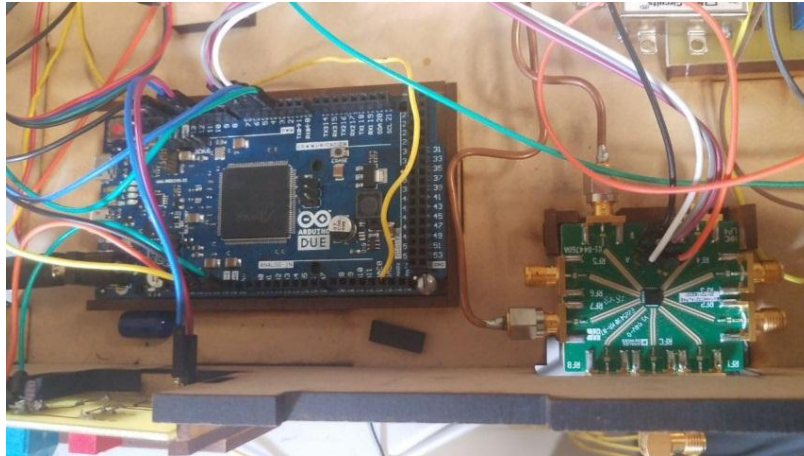


Figura 23. Conexiones entre el arduino due y *switch* RF

La salida analógica del arduino due se conecta con la etapa de amplificación para posteriormente conectarse con otro *dip switch*, denominado dip 2. Las conexiones se realizaron mediante cables dupont.

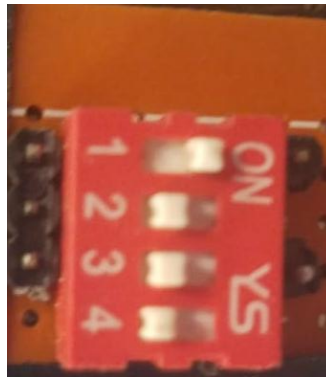


Figura 24. *Dip switch*, dip 2

Segundo, el dip 2 es el encargado de la selección de las técnicas de *jamming*, visualizada en la figura 24, la primera técnica es por ruido generado en arduino, cuya conexión es detallada anteriormente. La segunda técnica es ruido generado mediante un circuito, cuya salida se conecta con el Bias-Tee, el cual está conectado a una fuente de voltaje entre 2 V a 3 V, la salida del Bias-Tee se conecta con otro pin del dip 2. Las respectivas conexiones se realizaron con cable coaxial rígido y conectores tipo SMA.

La tercera técnica es por barrido, la cual es elaborada por el generador de señales AFG2020, cuya señal de salida se conecta con otro pin del dip 2 mediante cable coaxial rígido y conectores tipo BNC a SMA con adaptación a cable dupont.

El pin de salida del dip2 se conecta con los voltajes tune de los VCO's de 2.4 GHz y 5.8 GHz mediante cables dupont. Posteriormente, la salida de los VCO's se conectan a los puertos del *switch* de control, donde su salida se conecta con la entrada del amplificador ZVE-3W-83+, y finalmente la salida del amplificador conectada a la antena. Las conexiones se realizaron mediante cable coaxial de bajas pérdidas y conectores tipo SMA.

Tercero, la antena tiene la característica de movilidad, la cual le permite desplazarse a la dirección donde se encuentra el drone, esto se realiza por medio de la conexión de un motor programado por arduino, el cual permite el movimiento en grados. El ingreso del ángulo se realiza mediante el puerto COM, monitor serie de la plataforma propia de Arduino, como se indica en la figura 25.

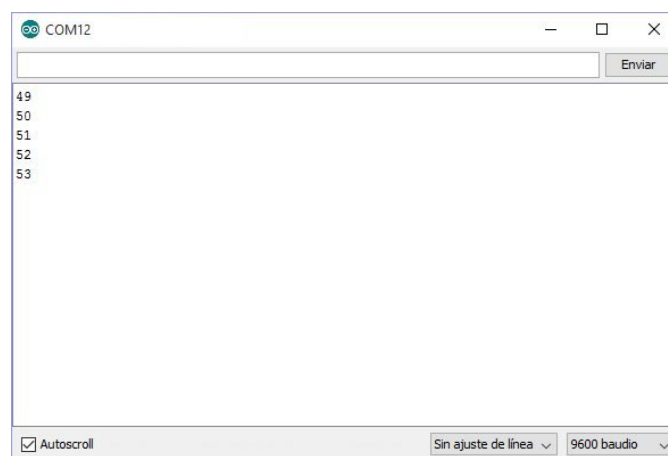


Figura 25. Ingreso del ángulo mediante puerto COM, monitor serie de la plataforma propia de arduino

La estructura que conforma el sistema inhibidor se indica en la figura 26.

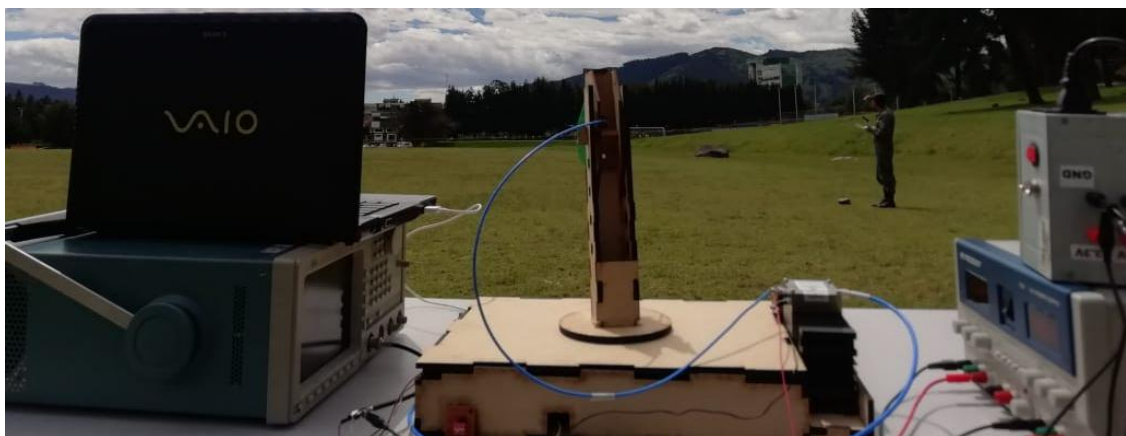


Figura 26. Sistema inhibidor de drones

4.2 Sistema Adicional de Laboratorio del Inhibidor de GPS y WIFI

Adicional al sistema realizado, se implementó con equipos de laboratorio, la generación de una señal que permite interferir la banda GPS (1.575 GHz), por medio del generador vectorial de señales RF E4438C de Agilent, con un ancho de banda de 10 MHz. En esta etapa, a modo de comparación se realizaron pruebas de interferencia a las bandas de WIFI de 2.4 GHz y 5.8 GHz con un ancho de banda de 32 MHz, cuyos resultados fueron de ayuda para verificar la correcta funcionalidad del sistema prototipo diseñado en el actual proyecto.

La señal de salida del generador se conecta directamente con el amplificador y este a su vez se conecta con la antena, mediante cables coaxial de bajas pérdidas y conectores tipo SMA.

4.3 Operación del sistema inhibidor de drones

Una vez realizadas las conexiones pertinentes de todos los elementos con sus respectivas alimentaciones, a seguir se enumeran los pasos a ejercer:

1. Localizar el objetivo (drone)
2. Orientar la antena en la dirección del objetivo (drone), mediante el ingreso del ángulo.
3. Seleccionar en el dip 1, la opción 1 para la frecuencia de 2.4 GHz y opción 2 para la de 5.8 GHz.
4. Seleccionar en el dip 2, la opción 1 para *jamming* por ruido de Arduino, opción 2 para *jamming* por ruido de circuito y opción 3 para *jamming* por barrido.

4.4 Operación del sistema adicional de laboratorio del inhibidor de GPS y WIFI

Para la generación de la señal de *jamming* utilizando el generador vectorial de señales de RF se procede a colocar las siguientes instrucciones:

4.4.1 Para GPS

- Frecuencia: 1.575 GHz
- Amplitud: 5-10 dBm
- Tipo de modulación: FM
- Desvío de frecuencia (equivalente a ancho de banda): 10 MHz
- Rate FM: 2.5 KHz (señal interna del generador)

4.4.2 Para WIFI

- Frecuencia: 2.44 GHz
- Amplitud: 5-10 dBm
- Tipo de modulación: FM
- Desvío de frecuencia (equivalente a ancho de banda): 32 MHz
- Rate FM: 15 KHz (señal interna del generador)

En la figura 27 se indica el ingreso de datos en el generador vectorial de señales RF con las respectivas características para GPS y WIFI.

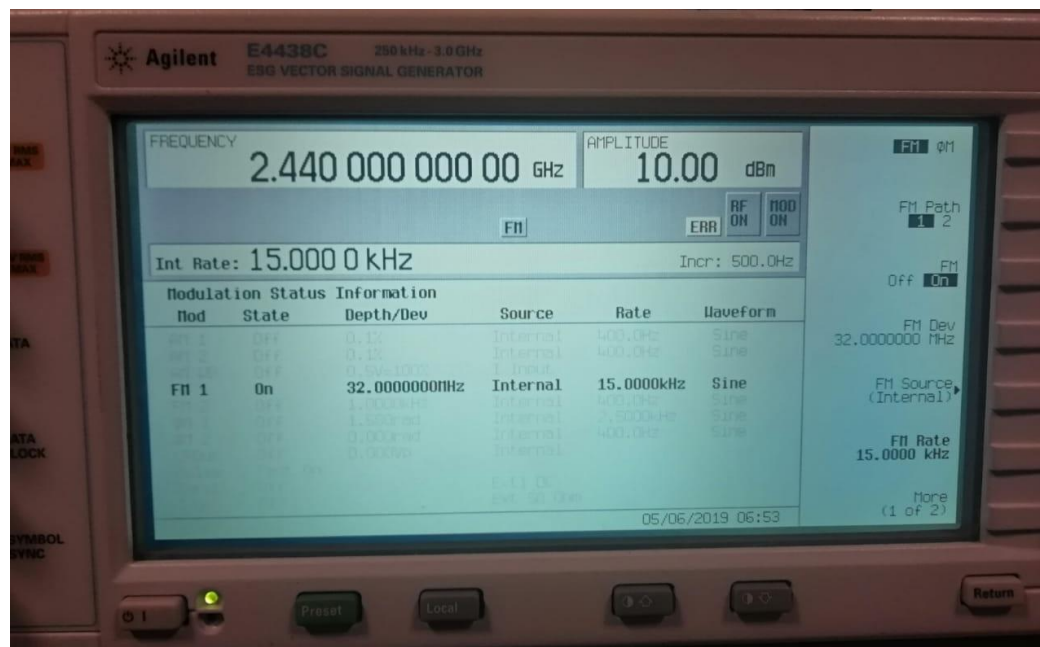


Figura 27. Ingreso de datos al generador vectorial de señales RF

4.5 Pruebas de Funcionamiento del Sistema Inhibidor de Drones.

4.5.1 Mediciones

Las mediciones realizadas en el sistema inhibidor prototipo desarrollado son fundamentalmente una estimación de la potencia de salida del amplificador y el ancho de banda. Para la toma de datos de potencia se debe añadir un atenuador de 18dB para protección del equipo de medición. A continuación se detallan los equipos utilizados para las mediciones, en la Tabla 9:

Tabla 9
Equipos utilizados para las mediciones

Equipos	
	Sistema inhibidor de drones
	Fuente variable BK precision 1760A
	Analizador de espectros, Aritsu MS2712E
	Generador vectorial de señales, Agilent E4438C

4.5.1.1 *Jamming* por ruido gaussiano (GNG) desarrollado en arduino due

En la figura 28 se muestra el espectro de la señal de salida del amplificador de RF, cuando el sistema es excitado con una señal de potencia de alrededor de 9 dBm.

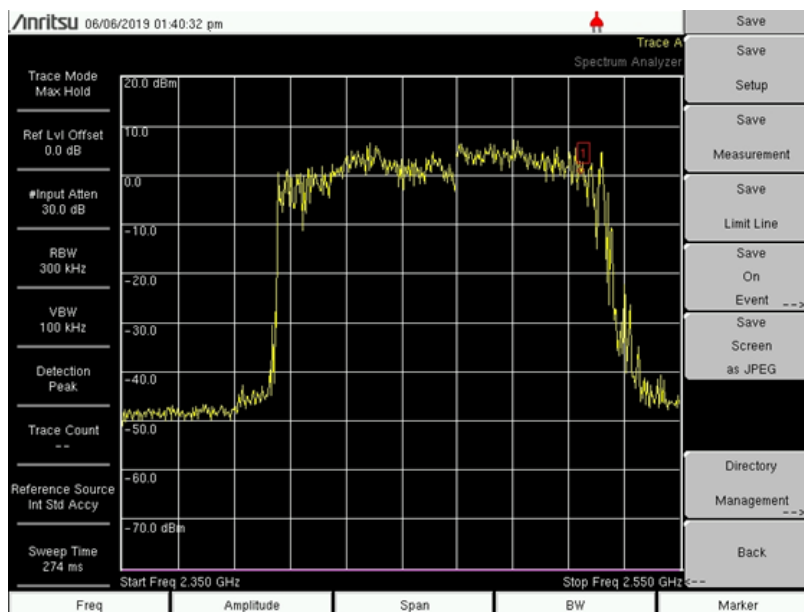


Figura 28. Espectro de salida y ancho de banda, *Jamming* por ruido en arduino

En la Tabla 10 se muestran los resultados respectivos del *jamming* por ruido en arduino. Se puede observar que la potencia total generada por el amplificador de potencia de RF, se distribuye en el ancho de banda generado, es decir, a mayor ancho de banda menor es el nivel máximo del espectro.

Tabla 10

Resultados del jamming por ruido en Arduino.

Nivel máximo del espectro	27 dBm
Frecuencia Inicial	2.40GHz
Frecuencia Final	2.505 GHz
Ancho de Banda	105MHz

4.5.1.2 *Jamming* por ruido mediante circuito

En la figura 29 se muestra el espectro de la señal de salida del amplificador de RF, cuando el sistema es excitado con una señal de potencia de alrededor de 8 dBm.

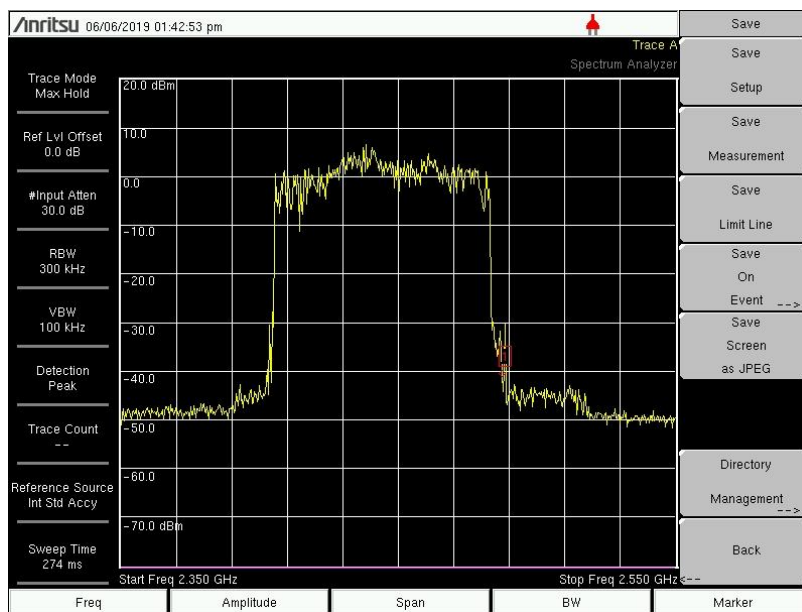


Figura 29. Espectro de salida y ancho de banda, *Jamming* por ruido mediante circuito

En la Tabla 11 se muestran los resultados respectivos del *jamming* por ruido mediante circuito.

Tabla 11

Resultados del jamming por ruido mediante circuito.

Nivel máximo del espectro	26 dBm
Frecuencia Inicial	2.404 GHz
Frecuencia Final	2.483 GHz
Ancho de Banda	79 MHz

4.5.1.3 *Jamming* por Barrido

En la figura 30 se muestra el espectro de la señal de salida del amplificador de RF, cuando el sistema es excitado con una señal de potencia de alrededor de 0 dBm

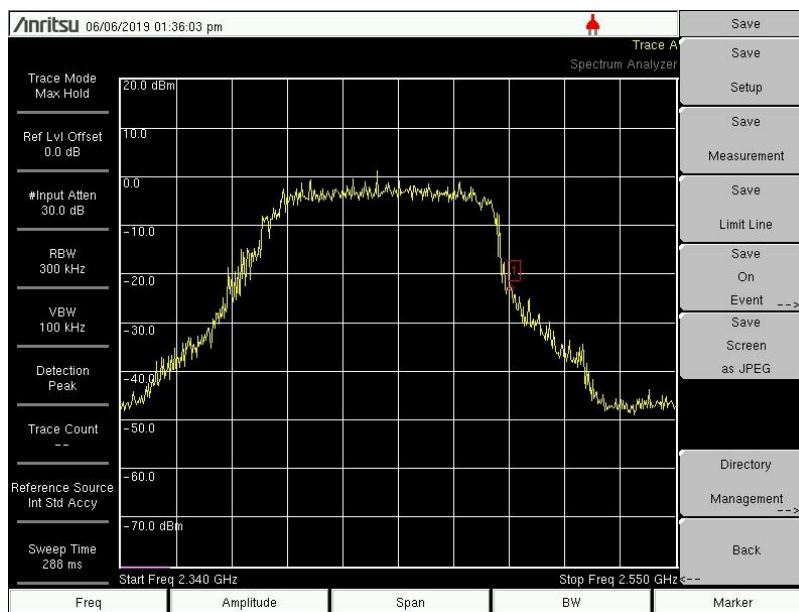


Figura 30. Espectro de salida y ancho de banda, *Jamming* por barrido

En la Tabla 12 se muestran los resultados respectivos del *jamming* por barrido.

Tabla 12

Resultados del jamming por barrido.

Nivel máximo del espectro	18 dBm
Frecuencia Inicial	2.402 GHz
Frecuencia Final	2.487 GHz
Ancho de Banda	85MHz

4.5.1.4 *Jamming* causado por modulación FM mediante el generador vectorial de señales RF.

Para la medición de potencia del sistema usando el generador vectorial de señales RF, se utilizan 16 dB y 18 dB de atenuación, para GPS y WIFI, respectivamente. A continuación se presentan los datos obtenidos.

4.5.1.4.1 GPS

La figura 31 muestra el espectro de la señal de salida del amplificador de RF, cuando el amplificador es excitado con una señal de potencia de alrededor de 10 dBm.

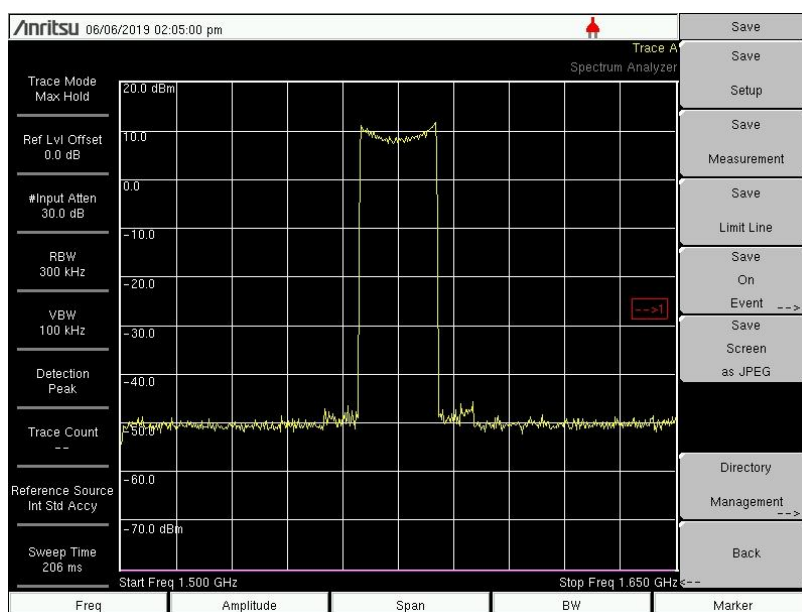


Figura 31. Jamming por modulación FM en banda GPS

En la Tabla 13 se muestran los resultados respectivos del *jamming* por modulación FM en GPS.

Tabla 13

Resultados del jamming por modulación FM en GPS.

Nivel máximo del espectro	26 dBm
Frecuencia Inicial	1.565 GHz
Frecuencia Final	1.585 GHz
Ancho de Banda	10 MHz

4.5.1.4.2 WIFI

La figura 32 muestra el espectro de la señal de salida del amplificador de RF, cuando el sistema es excitado con una señal de potencia de alrededor de 7 dBm

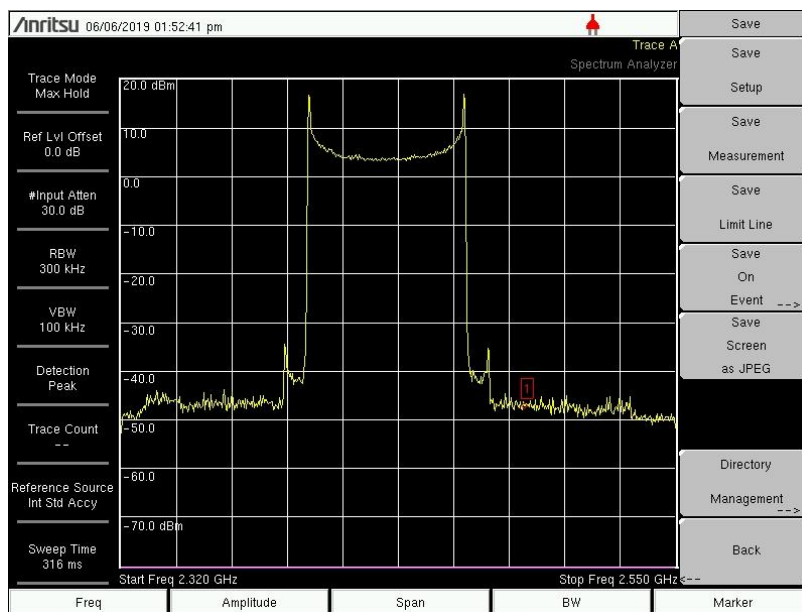


Figura 32. Jamming por modulación FM en banda WIFI

En la Tabla 14 se muestran los resultados respectivos del *jamming* por modulación FM en WIFI.

Tabla 14

Resultados del jamming por modulación FM en WIFI.

Nivel máximo del espectro	25 dBm
Frecuencia Inicial	2.411 GHz
Frecuencia Final	2.475 GHz
Ancho de Banda	32 MHz

4.5.2 Pruebas del Sistema Inhibidor

Para realizar las pruebas en exteriores se utilizó como objetivo el dron Phantom 4, del cual, los sistemas de transmisión de vídeo y de control remoto de la aeronave funcionan a 2.4 GHz, el dispositivo se visualiza en la figura 33.



Figura 33. Phantom 4

Fuente: (Dji, 2016)

Mediante la aplicación DJI GO que posee la tablet del controlador remoto, se permite observar los parámetros de funcionamiento entre el drone y el control remoto. Como se indica en la figura 34, los principales parámetros de funcionamiento son los siguientes:

1. Modo de vuelo [1].
2. Intensidad de señal GPS [2].
3. Sensor de detección de obstáculos [3].
4. Señal del controlador remoto [6].
5. Intensidad de señal de transmisión de vídeo HD [7].
6. Mapa [11].
7. Posicionamiento visual [12].
8. Telemetría de vuelo [13].

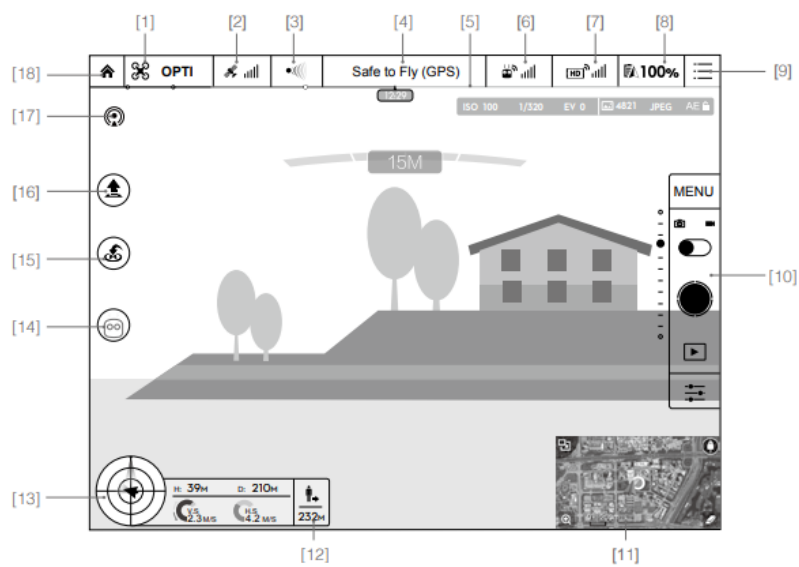


Figura 34. Pantalla de la aplicación DJI GO
Fuente: (Dji, 2016)

Para comprobar que todos los parámetros se encuentren operando correctamente, se inició el vuelo del dron, cuya interfaz se indica en la figura 35.

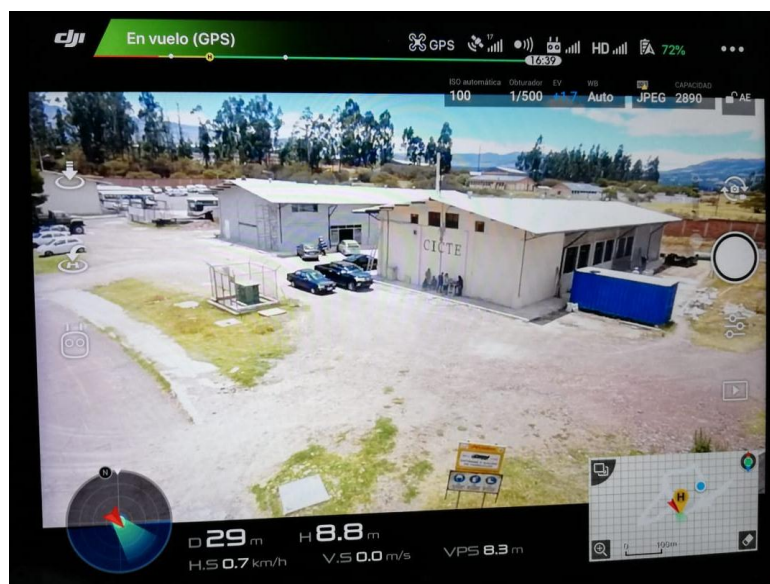


Figura 35. Pantalla de la aplicación DJI GO

Como se puede ver en la figura 35, en la parte superior se evidencian que todos sus parámetros están en óptimas condiciones, así como también en la parte inferior se indica la

telemetría del vuelo y la posición en el mapa de la ubicación del drone. Conociendo todas las características del drone, se procedió a realizar las pruebas en los diferentes escenarios.

4.5.2.1 Escenario 1

A una distancia de 100m y 80m de altura, del *jamming*, se ubica al drone. La antena del sistema de *jamming* se orienta al drone. Como se indica en la figura 36



Figura 36. Escenario 1 de Prueba

4.5.2.1.1 *Jamming* por ruido gaussiano (GNG) desarrollado en arduino due.

Al activar el sistema inhibidor de drones y seleccionar la opción 1 (2.4 GHz) del dip 1, así como también la opción 1 (*Jamming* por Ruido en Arduino) del dip 2 y orientar la antena hacia el drone, se pierden los parámetros de funcionamiento entre el controlador remoto y el drone, la cual se puede constatar en la pantalla de la tablet, mostrada en la figura 37.

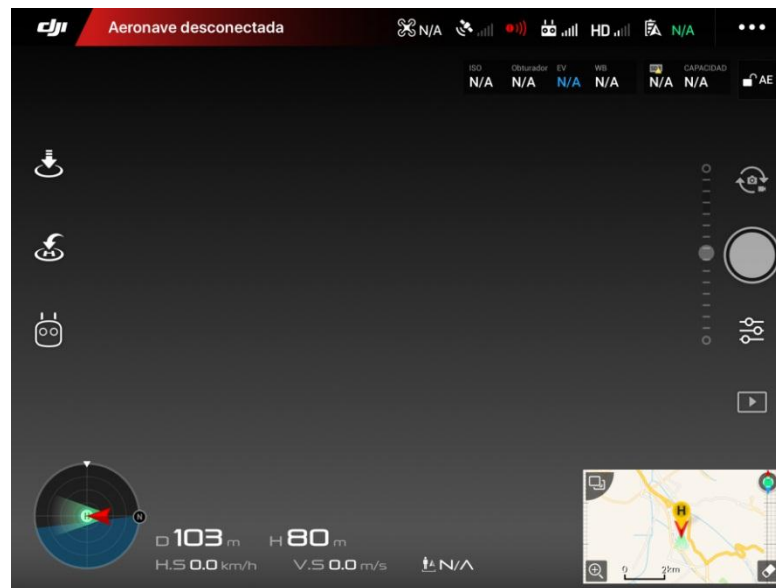


Figura 37. Pérdida de los parámetros de funcionamiento entre el dron y el controlador remoto

Como se observa en la figura 37 en la parte superior izquierda la aeronave se encuentra desconectada, así como también en la parte superior derecha se visualiza la pérdida de parámetros de funcionamiento del vuelo del dron.

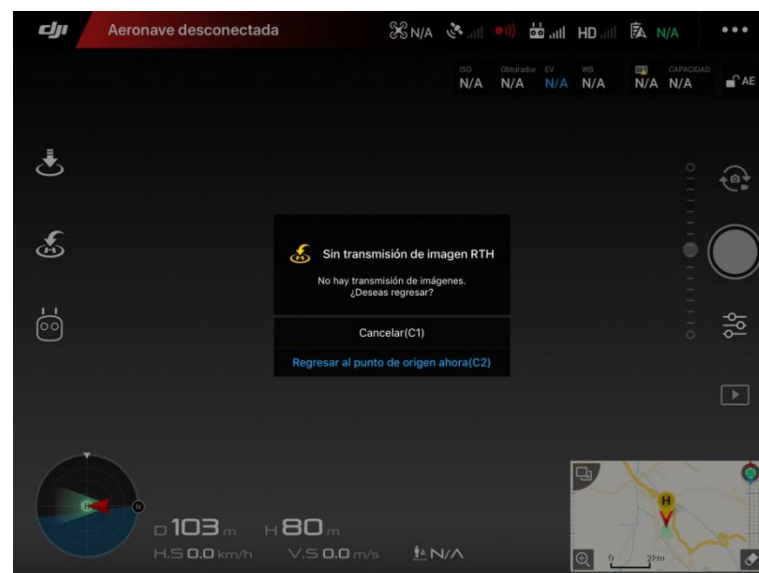


Figura 38. Pérdida de la transmisión de video en tiempo real

La figura 38 indica el momento cuando se pierde la transmisión de video, lo que llevó a no tener maniobrabilidad sobre el dron. También se presenció que el controlador no visualizaba la posición exacta del dron, puesto que, este valor se mantenía en la posición que estaba antes de que fuera interferido. Los parámetros de la parte inferior como mapa, posicionamiento visual y telemetría de vuelo se encuentran deshabilitadas.

4.5.2.1.2 *Jamming* por ruido mediante circuito

Al activar el sistema inhibidor de drones y seleccionar la opción 1(2.4 GHz) del dip 1, así como también la opción 2 (*Jamming* por Ruido) del dip 2 y orientar la antena hacia el dron, se obstruye la comunicación entre el controlador remoto y el dron, la cual se puede constatar en la figura 39.

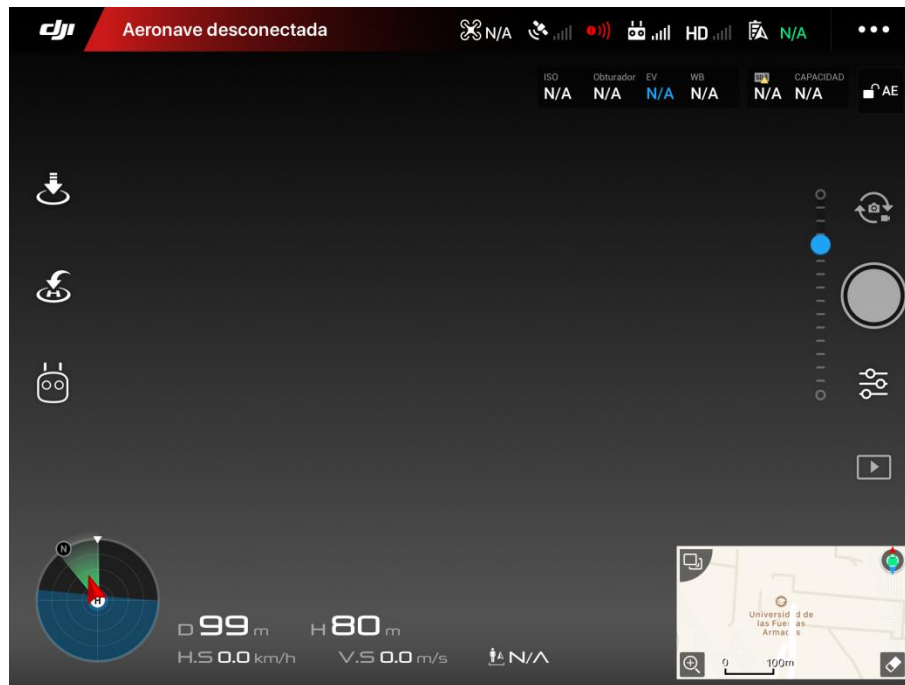


Figura 39. Neutralización de la comunicación entre el dron y el controlador remoto en tiempo real

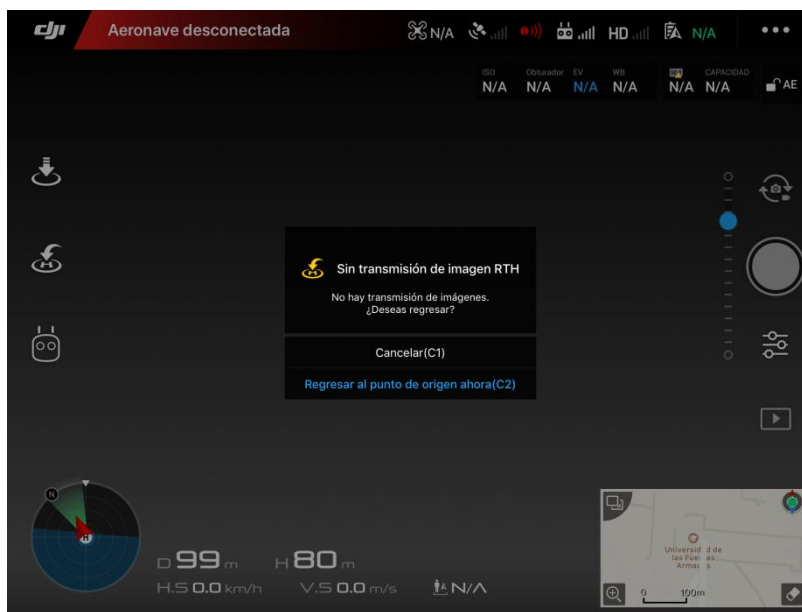


Figura 40. Neutralización de la transmisión de video en tiempo real

Las figuras 39 y 40 indican la obstrucción de los parámetros de funcionamiento del vuelo del drone, visualizadas en la parte superior e inferior de dichas figuras, lo que llevó a no tener maniobrabilidad sobre el drone.

4.5.2.1.3 *Jamming* por barrido

Al activar el sistema inhibidor de drones y seleccionar la opción 1 (2.4GHz) del dip 1, así como también la opción 3 (*Jamming* por barrido) del dip 2 y orientar la antena hacia el drone, se logró neutralizar la comunicación y la funcionalidad entre el controlador remoto y el drone, la cual se puede verificar en la pantalla de la tablet, que se visualiza en la figura 41.

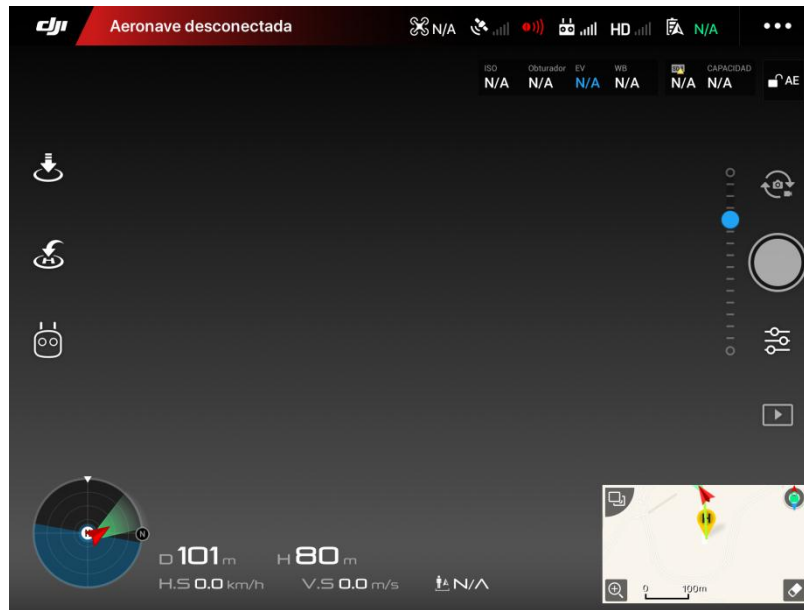


Figura 41. Interferencia de la comunicación entre el drone y el controlador remoto en tiempo real

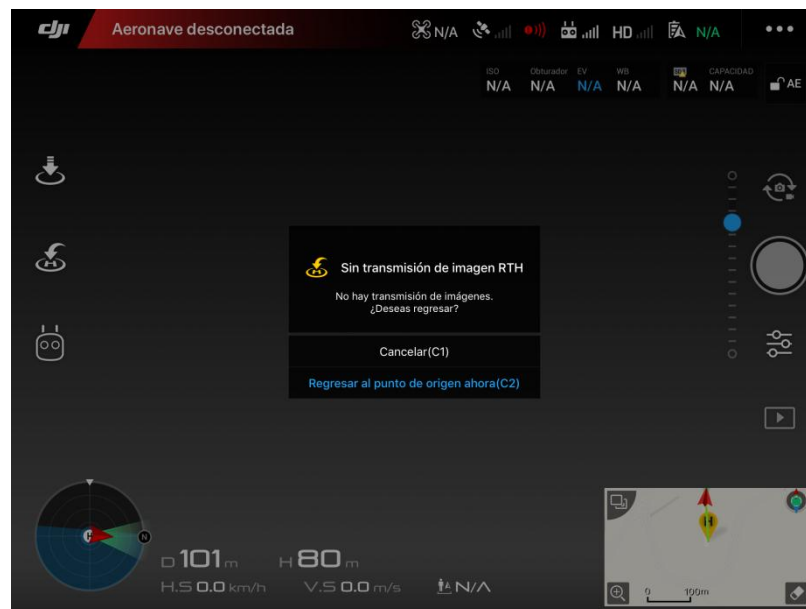


Figura 42. Neutralización de la transmisión de video en tiempo real

Las figuras 41 y 42 detallan en la parte superior e inferior, la obstrucción de los parámetros de funcionamiento del vuelo del drone. El control remoto se deshabilitó, lo que llevó a no tener maniobrabilidad sobre el drone.

4.5.2.2 Escenario 2

A una distancia de 200 m y 80 m de altura, del *jamming*, se ubica al drone, considerando que la antena del sistema de *jamming* está orientada al drone. En las mismas condiciones de selección de cada *dip switch* para las diferentes técnicas de *jamming* en el sistema inhibidor, se obtienen los siguientes resultados:

4.5.2.2.1 *Jamming* por ruido gaussiano (GNG) desarrollado en arduino due.

Se interfiere la comunicación y la funcionalidad de los parámetros del controlador remoto y el drone. El control remoto se deshabilitó, lo que llevó a no tener maniobrabilidad sobre el drone, como se indica en la figura 43.

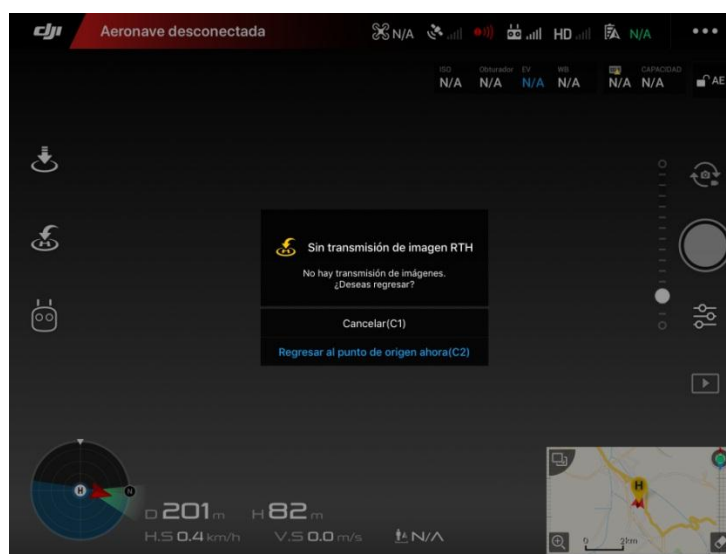


Figura 43. Interferencia de la comunicación entre el drone y el controlador remoto en tiempo real

4.5.2.2.2 *Jamming* por ruido mediante circuito

Los resultados en esta técnica se basan en la obstrucción de las funcionalidades de los parámetros del drone como lo indica la figura 44 en la parte superior e inferior.

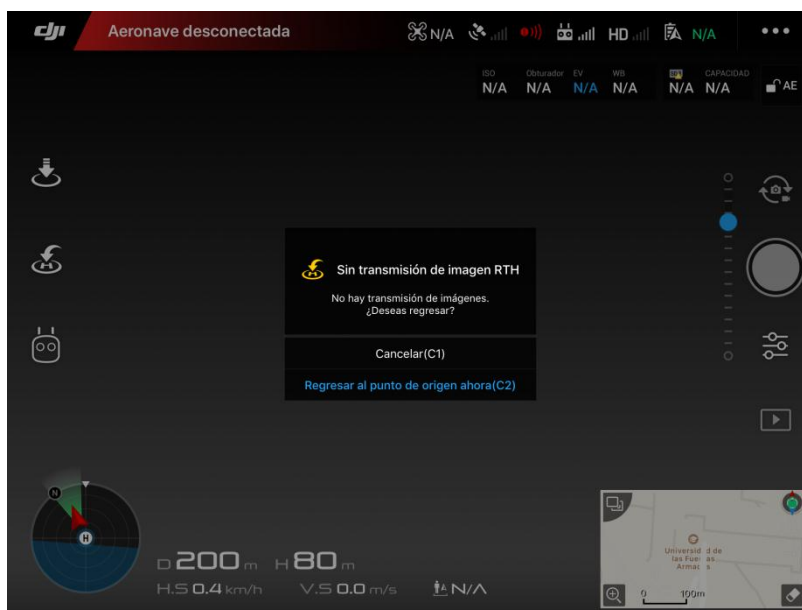


Figura 44. Interferencia de la comunicación entre el drone y el controlador remoto en tiempo real

4.5.2.2.3 *Jamming* por barrido

La figura 45 detalla la obstrucción a la comunicación del drone con el controlador remoto, puesto que pierde funcionalidades vitales para el manejo del drone.

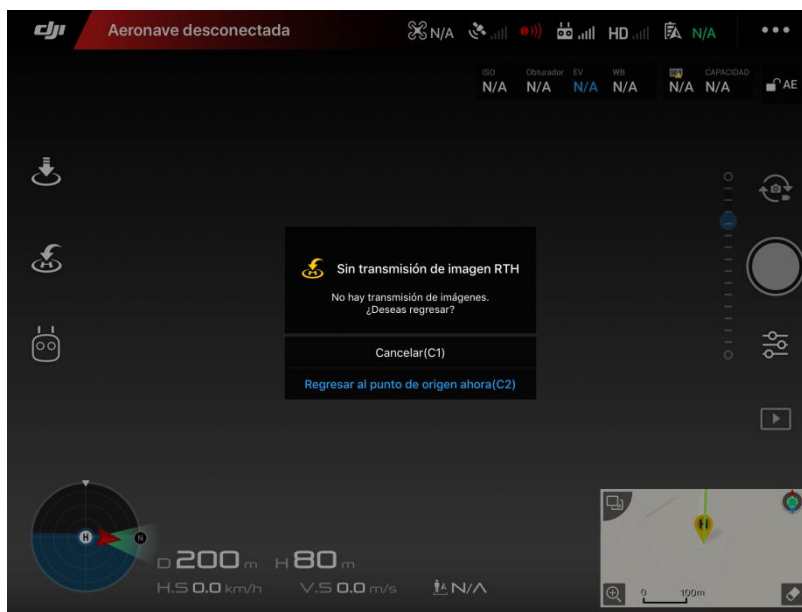


Figura 45. Interferencia de la comunicación entre el drone y el controlador remoto en tiempo real

Como resultado de las pruebas en los dos escenarios y con cada una de las técnicas de *jamming*, se observó como el sistema interfirió a la comunicación entre el drone y el controlador remoto, en la cual, los parámetros de funcionamiento como: modo de vuelo, intensidad de señal GPS, sensor de detección de obstáculos, intensidad de señal de transmisión de vídeo HD, mapa, posicionamiento visual y telemetría de vuelo se deshabilitaron por completo. La señal del controlador remoto se perdió en intervalos de tiempo entre 5 y 15 segundos dependiendo de la técnica de *jamming*, en estos intervalos, se perdía el dominio del controlador remoto sobre el drone.

4.5.3 Pruebas con el sistema adicional de laboratorio del inhibidor de banda GPS y WIFI.

El equipo utilizado para causar interferencia es el generador vectorial de señales E4438C de Agilent, como se mencionó anteriormente, el cual permite modular (modulación FM) una señal que interfiera las bandas de GPS y WIFI.

Anteriormente se presentó los escenarios de pruebas para el sistema inhibidor de drones, en esta sección se mantienen los escenarios especificados.

4.5.3.1 Escenario 1 para GPS

Este escenario corresponde a 100 m de distancia y 80 m de altura, del *jamming*, se ubica al dron, variando la potencia de salida del generador vectorial de señales entre 5dBm, 7dBm y 10dBm.

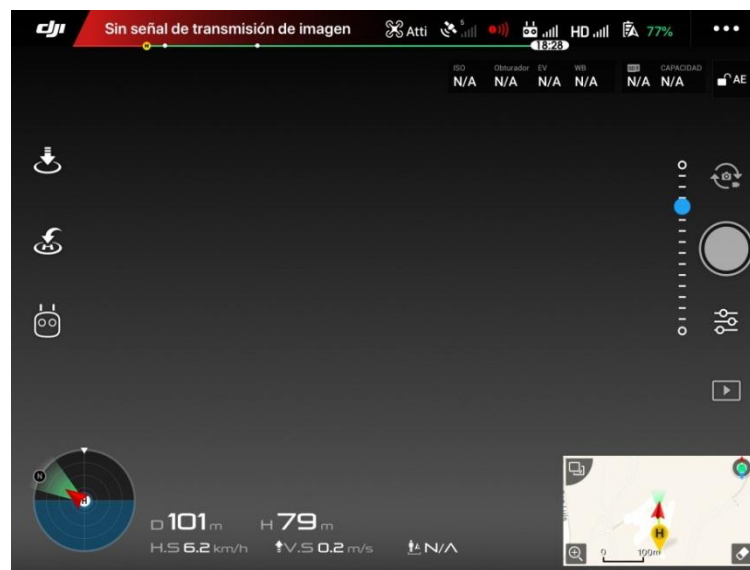


Figura 46. Pérdida de GPS con 5 dBm

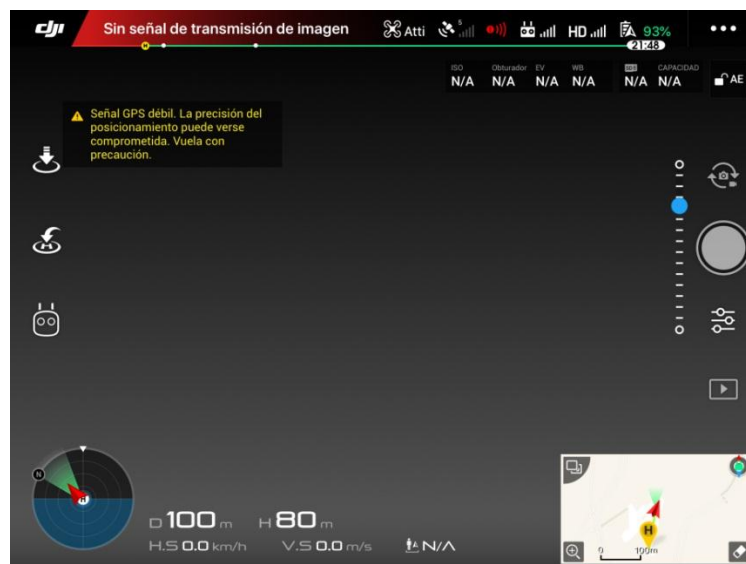


Figura 47. Pérdida de GPS con 7 dBm

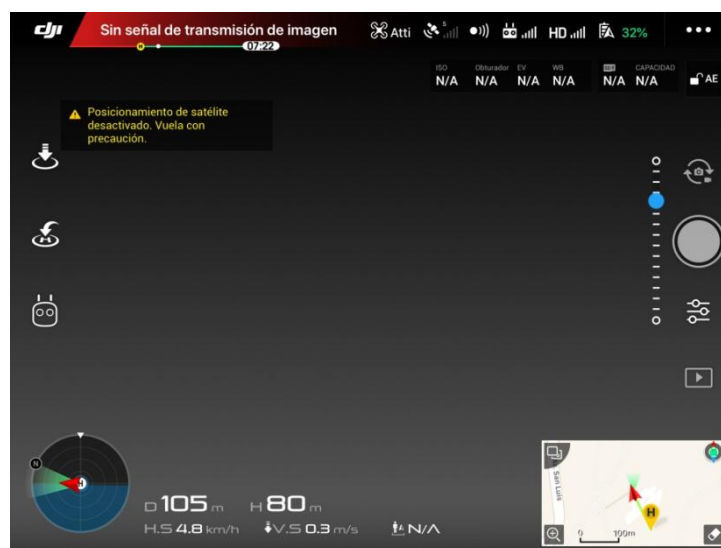


Figura 48. Pérdida de GPS con 10 dBm

Se pudo visualizar en las figuras 46, 47 y 48 que el dron presentó interferencias en la banda de GPS, lo que causó que la aeronave hiciera uso de su barómetro de posicionamiento para controlar la altitud, siendo influenciado por la dirección del viento, lo que se denomina en la aplicación DJI GO como ATTI, como se puede visualizar en la parte superior derecha de cada figura.

4.5.3.2 Escenario 2 para GPS

A 200 m de distancia y 80 m de altura, del *jamming*, se ubica al drone, cada una de las pruebas se realizó variando el nivel de potencia de la señal de salida del generador vectorial de señales RF entre 5dBm, 7dBm y 10dBm.

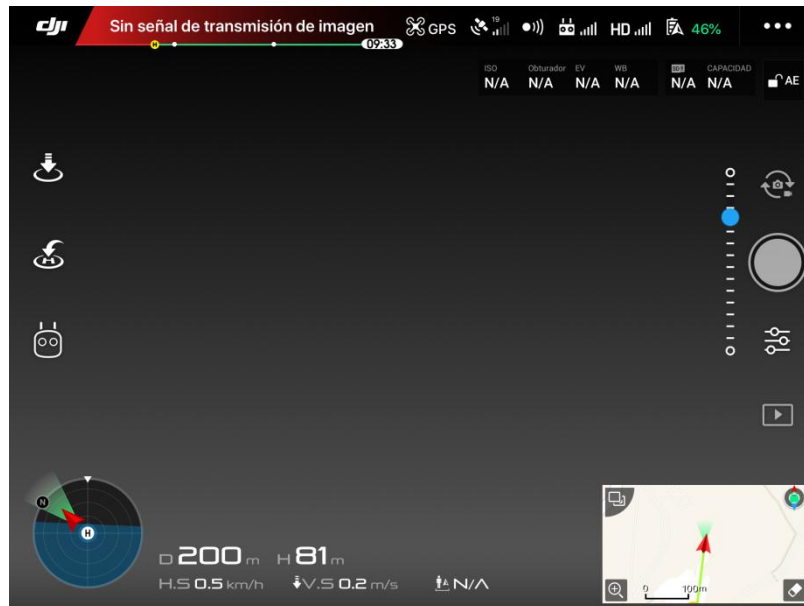


Figura 49. Pérdida de GPS con 5 dBm

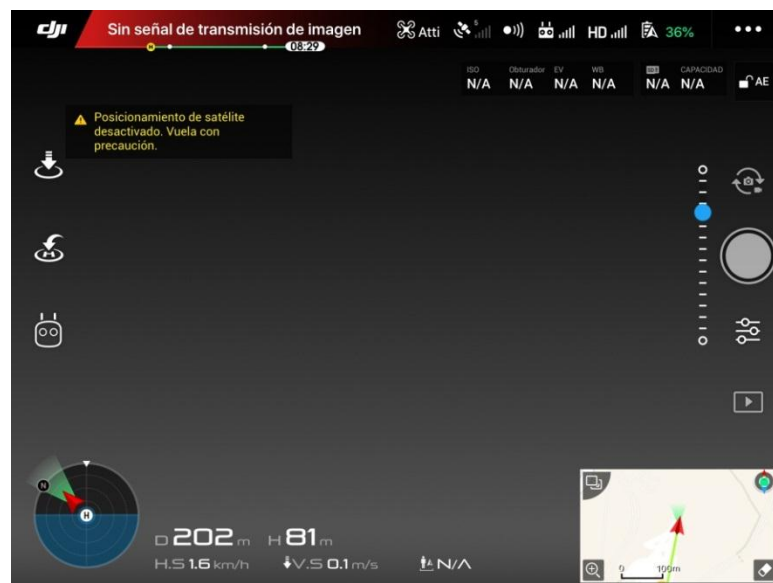


Figura 50. Pérdida de GPS con 7 dBm

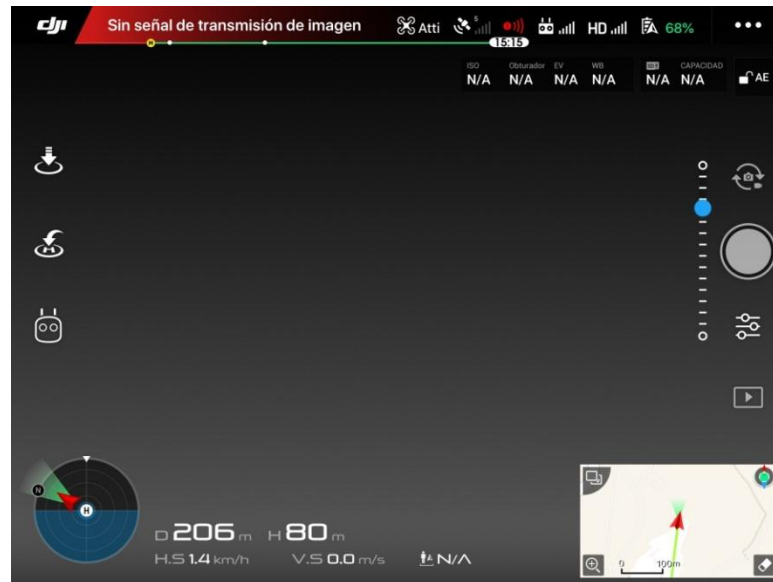


Figura 51. Pérdida de GPS con 10 dBm

Las figuras 49, 50 y 51, indican la pérdida de GPS y al no disponer de ellos, la aeronave hace uso de su barómetro de posicionamiento para controlar la altitud, siendo influenciado por la dirección del viento lo que se denomina en la aplicación DJI GO como ATTI, cada una de ellas se consideró variando la potencia del generador vectorial de señales RF.

4.5.3.3 Escenario 1 para WIFI

A 100m de distancia y 80m de altura, del *jamming*, se ubica al drone, donde se varió la potencia de salida del generador vectorial de señales entre 5dBm, 7dBm y 10dBm.

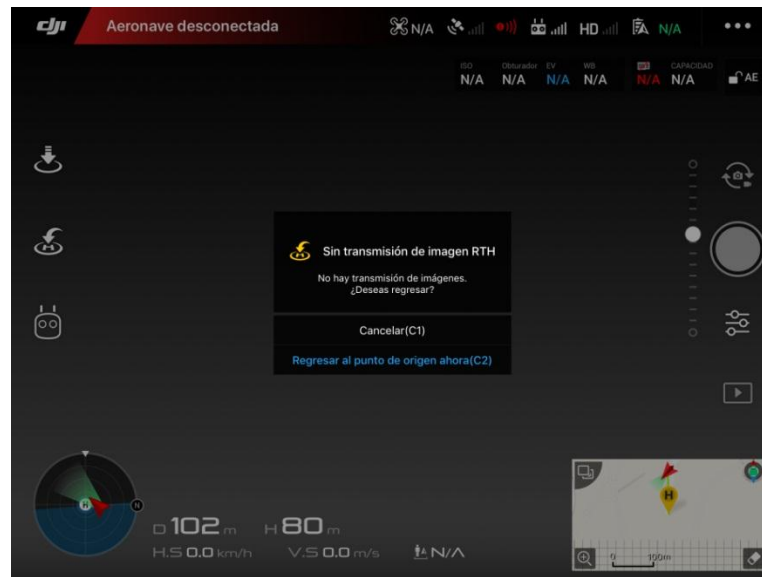


Figura 52. Neutralización de la comunicación entre el drone y el controlador remoto en tiempo real para 5 dBm

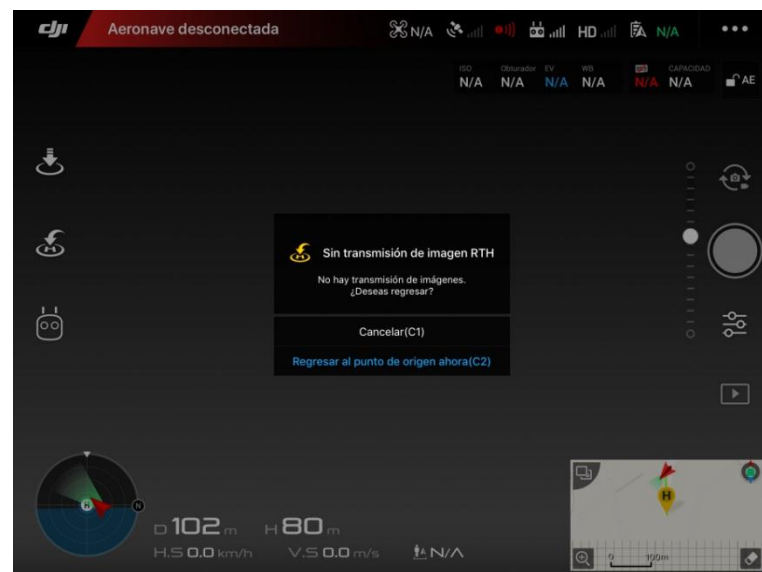


Figura 53. Neutralización de la comunicación entre el drone y el controlador remoto en tiempo real para 7 dBm

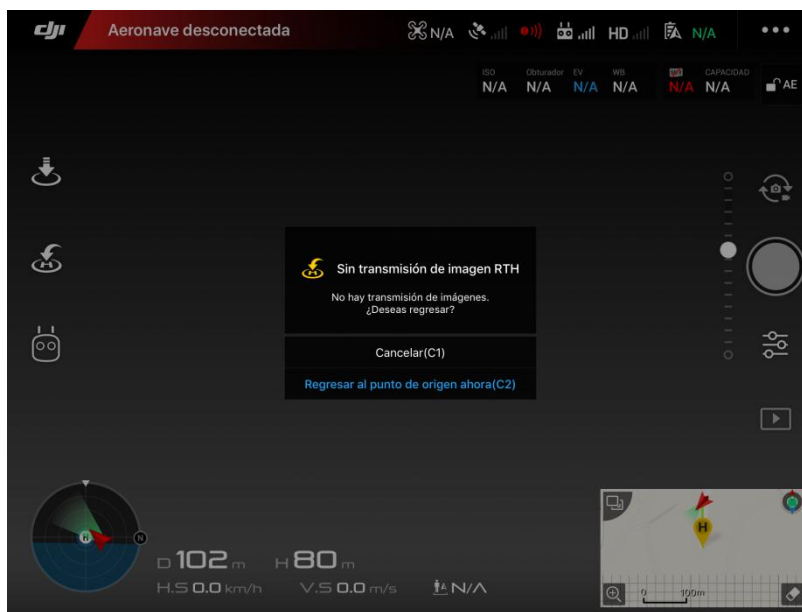


Figura 54. Neutralización de la comunicación entre el drone y el controlador remoto en tiempo real para 10 dBm

En las figuras 52, 53 y 54, se observa la neutralización de la funcionalidad de sus parámetros, visualizadas en la parte superior e inferior de las figuras.

4.5.3.4 Escenario 2 para WIFI

A 200 m de distancia y 80 m de altura, del *jamming*, se ubica al drone, variando la potencia de salida del generador vectorial de señales entre 5dBm, 7dBm y 10dBm. En las figuras 55, 56 y 57, se observa la neutralización de la funcionalidad de sus parámetros, visualizadas en la parte superior e inferior de las figuras. También se presencié la pérdida del control en la maniobrabilidad del drone en intervalos de tiempo alrededor de 10 segundos.

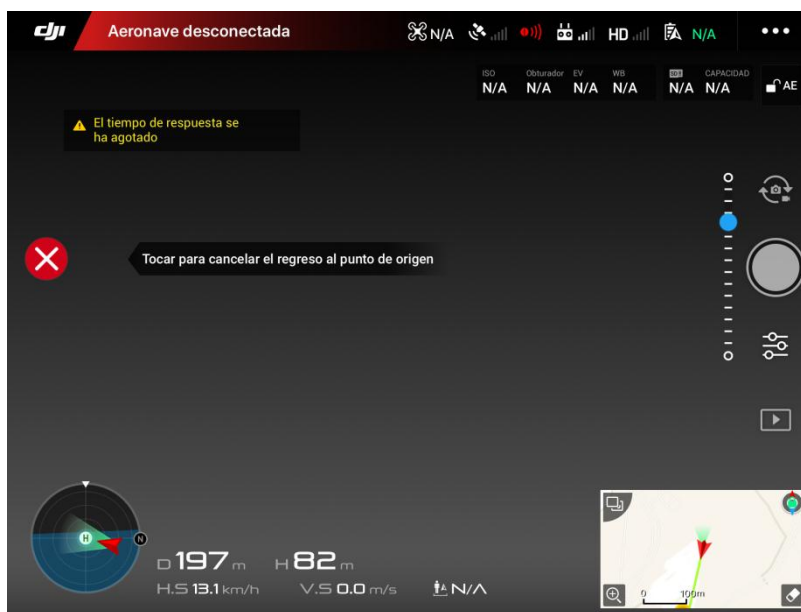


Figura 55. Neutralización de la comunicación entre el dron y el controlador remoto en tiempo real para 5 dBm

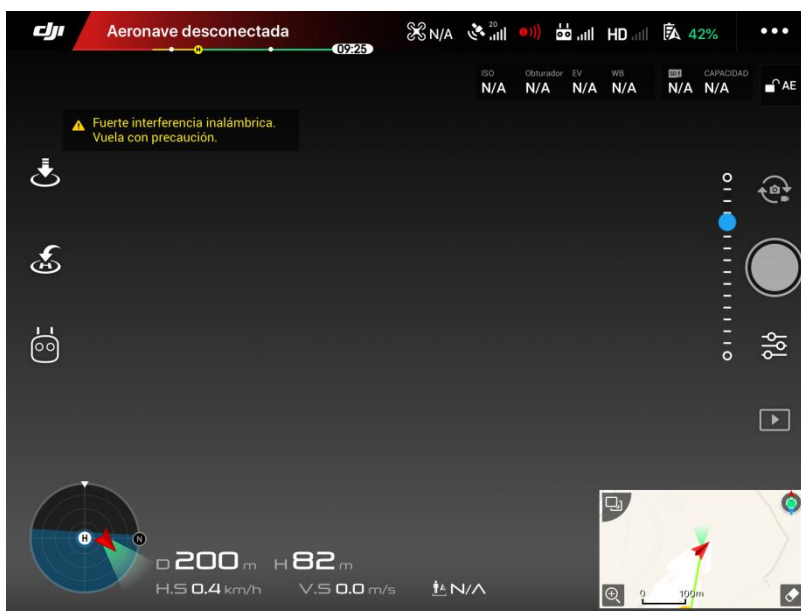


Figura 56. Neutralización de la comunicación entre el dron y el controlador remoto en tiempo real para 7 dBm

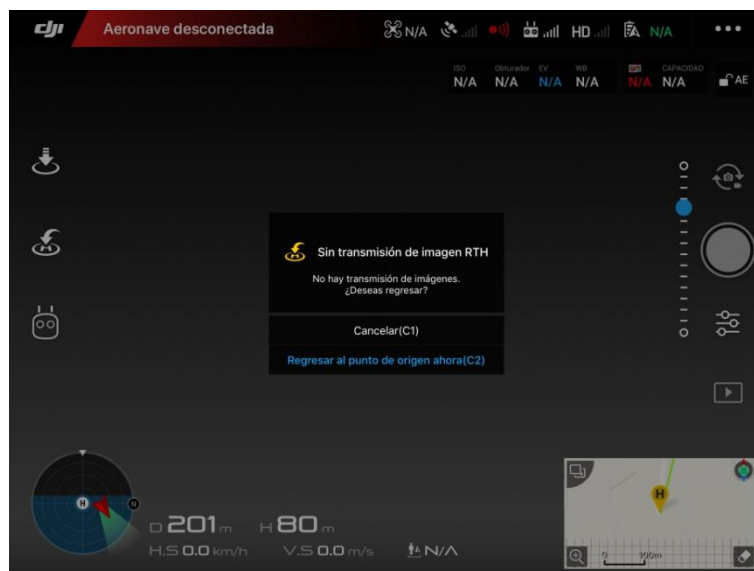


Figura 57. Neutralización de la comunicación entre el drone y el controlador remoto en tiempo real para 10 dBm

Para la interferencia en la banda de WIFI se consigue la obstrucción de la comunicación entre el drone y el controlador remoto, en las cuales, los parámetros de funcionamiento como: modo de vuelo, intensidad de señal GPS, sensor de detección de obstáculos, intensidad de señal de transmisión de vídeo HD, mapa, posicionamiento visual y telemetría de vuelo se han deshabilitado por completo. La señal del controlador remoto se perdía en intervalos de tiempo y de duración reducida alrededor de 5 a 10 segundos, lo que llevaba a no tener dominio para movilizar el drone.

4.5.3.5 Escenario 3 para WIFI

En este escenario el controlador remoto debe estar alejado alrededor de 300 m del sistema adicional, el cual usa una potencia respectiva de 10 dBm de salida del generador. En estas pruebas, el drone vuela alrededor de la estación de interferencia, haciendo que la altura varié hasta tener resultados positivos ante la interferencia. Es así que se obtienen los siguientes resultados:

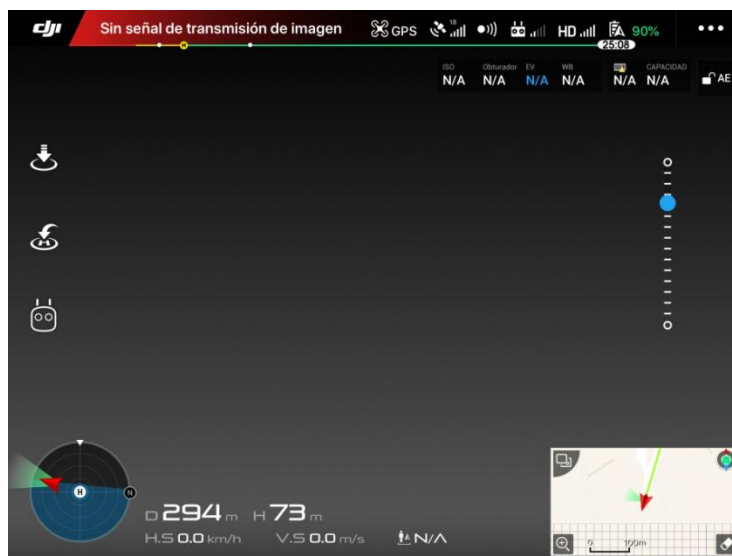


Figura 58. Prueba negativa ante *jamming*

La figura 58 indica en la parte inferior izquierda la localización del dron, la cual detalla que se encuentra alrededor 73 m de altura de la estación de interferencia, en esta prueba sus parámetros de funcionamiento se encuentran en condiciones óptimas para el vuelo, lo que implica a que no se está interfiriendo al dron. Para que el dron sea interferido se procede a disminuir la altura de vuelo, acercándose a la estación de interferencia.

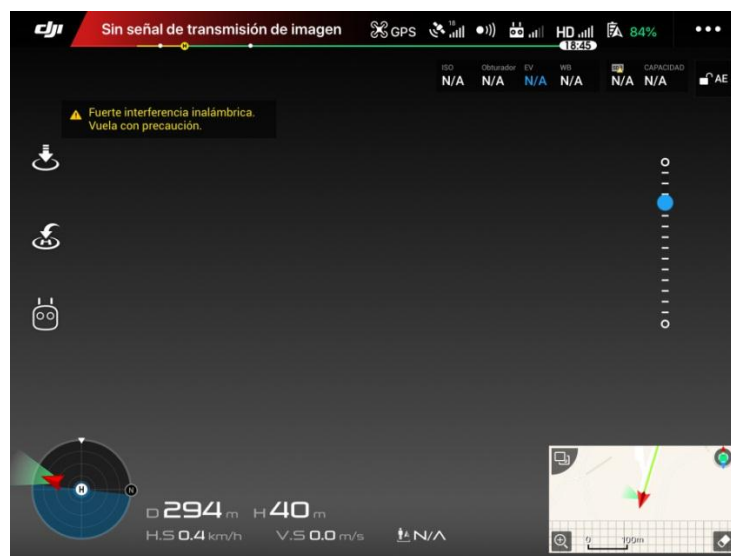


Figura 59. Prueba tendiente a positiva ante *jamming*

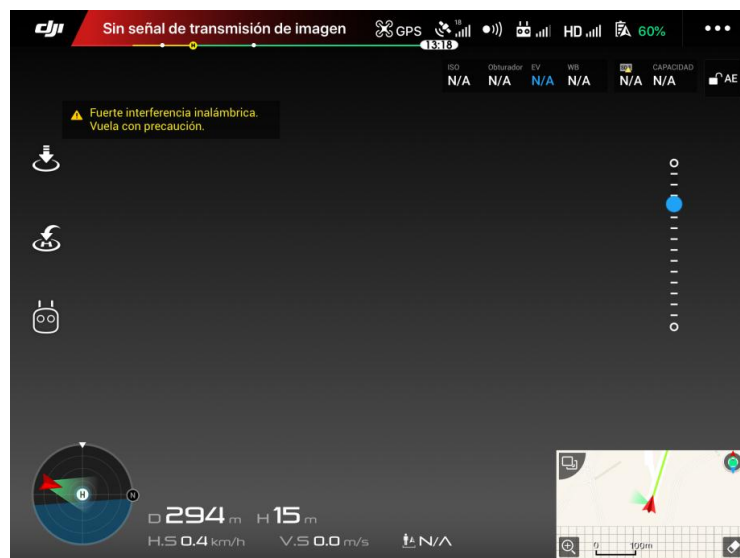


Figura 60. Prueba tendiente a positiva ante *jamming*

En la figura 59 y 60 se observa que el dron se encuentra a 40 m y 15 m de altura de la estación de interferencia respectivamente, en estas condiciones los parámetros del dron aún se encuentran en modo óptimo de vuelo, sin embargo se detecta una alerta de *Fuerte interferencia inalámbrica. Vuela con precaución*, la cual indica que se está perdiendo levemente la comunicación.

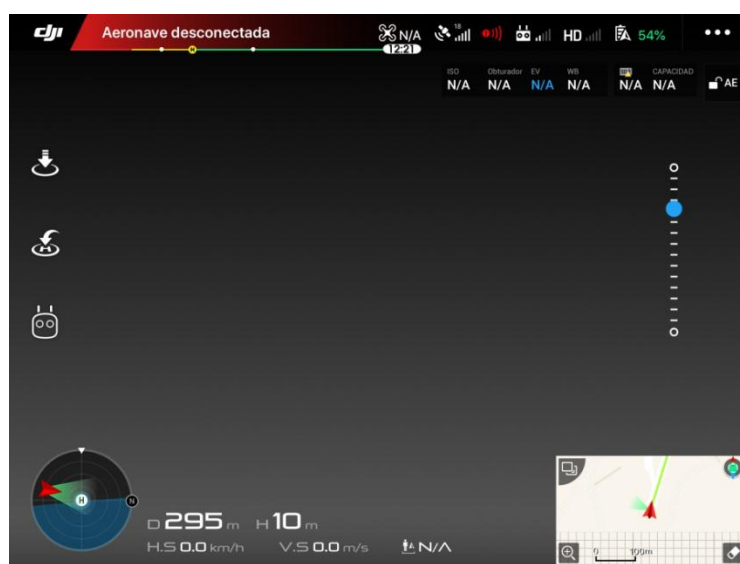


Figura 61. Prueba positiva ante *jamming*

En la figura 61 se observa que el drone se encuentra a 10 m de altura de la estación de interferencia. Podemos observar en la parte superior e inferior de la figura, que los parámetros de funcionamiento se encuentran obstruidos, lo que conlleva a degradar e interferir la comunicación entre el drone y el controlador remoto.

Para alturas menores a 10 m entre el drone y la estación de interferencia, los parámetros de funcionamiento se deshabilitan, ocasionando la pérdida de maniobrabilidad en intervalos de tiempo.

CAPITULO V

ANÁLISIS DE RESULTADOS

Este capítulo detalla el análisis de resultados obtenidos en las pruebas realizadas en el capítulo IV. Se analiza el funcionamiento del sistema inhibidor de drones, para cada técnica de *jamming* utilizadas en el proyecto, así como una comparación entre ellas y el alcance que el sistema presenta para cada escenario probado. Además, se analiza la efectividad del sistema diseñado, comparando las pruebas del mismo con las del sistema adicional de laboratorio para interferir las bandas de GPS y WIFI. En la figura 62 se representa un ejemplo de escenarios de prueba.



Figura 62. Escenario de Prueba

5.1 Sistema Inhibidor de Drones en las Bandas Comerciales WIFI

Todas las técnicas de *jamming* cumplen el objetivo de interferir el dron en los escenarios de 100 m y 200 m, con una altura de 80 m entre el dron y el controlador remoto. Se visualizó

en la pantalla de la tablet del controlador remoto la deshabilitación de los parámetros de funcionamiento, como se indica en la Tabla 15.

Tabla 15

Resultado de los parámetros de funcionamiento del drone

Parámetros de Funcionamiento	<i>Jamming</i> por Ruido generado en Arduino	<i>Jamming</i> por Ruido mediante circuito	<i>Jamming</i> por Barrido
Modo de vuelo.	deshabilitado	deshabilitado	deshabilitado
Intensidad de señal GPS.	deshabilitado	deshabilitado	deshabilitado
Sensor de detección de obstáculos.	deshabilitado	deshabilitado	deshabilitado
Intensidad de señal de transmisión de vídeo HD.	deshabilitado	deshabilitado	deshabilitado
Mapa.	deshabilitado	deshabilitado	deshabilitado
Posicionamiento visual.	deshabilitado	deshabilitado	deshabilitado
Telemetría de vuelo.	deshabilitado	deshabilitado	deshabilitado

Se verificó que en los momentos cuando el controlador puede maniobrar el drone, este puede desplazarlo tanto en altura como en distancia, sin embargo el detalle de la ubicación en el mapa, posicionamiento visual y telemetría de vuelo se mantienen bloqueados, y se visualiza solamente la ubicación en la que se había quedado antes de ser interferido.

A continuación se enlista los resultados obtenidos en referencia a los tiempos de deshabilitación del control remoto en la Tabla 16, ocasionado por las técnicas de *jamming* del sistema inhibitor, correspondientes a cada escenario de prueba.

Tabla 16*Tiempos de deshabilitación del control remoto*

Escenarios	Jamming por Ruido generado en Arduino	Jamming por Ruido mediante circuito	Jamming por Barrido
Escenario 1	5 segundos	15 segundos	10 segundos
Escenario 2	5 segundos	15 segundos	10 segundos

Si bien es cierto que en los dos escenarios de prueba se obtienen los mismos tiempos, se observó que en el escenario 2 al tener mayor distancia, la respuesta de deshabilitación tenía un retardo a comparación del escenario 1. El ancho de banda con el cual trabaja cada técnica de *jamming*, influye significativamente en la interferencia del vehículo no tripulado (drone).

La técnica de *Jamming por ruido mediante circuito* trabaja alrededor de los 80MHz, que es el ancho de banda WIFI, aquí el tiempo de pérdida del control remoto es mayor comparado con las otras técnicas de interferencia, siendo alrededor de 15 segundos.

La técnica de *Jamming por barrido* también ocasiona la neutralización del control remoto, pero en un intervalo de 10 segundos. El ancho de banda es de 85MHz y debido al barrido muy rápido que hace esta técnica, logra que se solape la señal de interferencia con la frecuencia del drone, ocasionando que colapse el tiempo de respuesta entre el controlador remoto y el drone.

Y finalmente la técnica de *Jamming por ruido generado en el arduino* trabaja alrededor de los 100MHz de ancho de banda, en esta se pudo presenciar que la neutralización del control remoto duraba alrededor de 5 segundos, a pesar de que el Arduino estaba programado para dar valores entre 2 V y 3 V y sintonicen la frecuencia en los VCO's que se requería, daban valores fuera de este rango, generando así un ancho de banda más amplio.

Una vez analizados los resultados con las diferentes técnicas, se demostró que las tres técnicas interfieren al vehículo aéreo no tripulado (drone), sin embargo la técnica más eficiente es al de *jamming por ruido mediante circuito*, seguido del *jamming por barrido* y finalmente la de *jamming por ruido generado en arduino*.

5.2 Sistema adicional inhibidor de laboratorio de GPS y WIFI

Para estas pruebas se realizó la interferencia a la banda GPS ocasionada por la modulación FM de la señal del generador vectorial de señales RF para diferentes valores de potencia, 5 dBm 7dBm y 10dBm a la entrada del amplificador de potencia. Los resultados fueron exitosos, debido a que se perdieron las señales de GPS y al no disponer de ellas, la aeronave hace uso de su barómetro de posicionamiento para controlar la altitud, moviéndose a dirección del viento lo que se denomina en la aplicación DJI GO como ATTI. Cabe mencionar que la persona que poseía el controlador remoto perdió el dominio absoluto de movilización del drone durante todo el tiempo de prueba, tanto a los 100 m como a los 200 m de distancia y 80 m de altura entre el drone y el controlador remoto.

Para la interferencia en la banda de WIFI se consiguió la obstrucción de la comunicación del drone y el controlador remoto, en las cuales los componentes de funcionamiento como: modo de vuelo, intensidad de señal GPS, sensor de detección de obstáculos, intensidad de señal de transmisión de vídeo HD, mapa, posicionamiento visual y telemetría de vuelo se deshabilitaron por completo. La señal del controlador remoto se perdía en intervalos de tiempo y de duración reducida alrededor de 10 segundos, lo que llevó a no tener dominio para movilizar el drone. Cabe acotar que se presentó esta característica para todos los diversos valores de potencia entre 5 a 10 dBm de la señal modulada en FM del generador vectorial de señales RF. En la Tabla 17 se tabula los resultados obtenidos en referencia a los tiempos de

deshabilitación del control remoto, ocasionado por el sistema adicional inhibidor, considerando las distintas potencias emitidas por el generador, correspondientes a cada escenario de prueba.

Tabla 17

Tiempos de deshabilitación del control remoto

Escenarios	Potencia de la señal de salida del generador		
	5 dBm	7 dBm	10 dBm
Escenario 1	5 segundos	8 segundos	10 segundos
Escenario 2	5 segundos	8 segundos	10 segundos

Si bien es cierto que en los dos escenarios de prueba se obtienen los mismos tiempos, en el escenario 2 al tener mayor distancia, la respuesta de deshabilitación tenía un retardo a comparación del escenario 1.

Para el tercer escenario, el dron localizado a los 40m de altura de la estación de interferencia, presencia la interferencia puesto que le llega una alarma de aviso a la tablet del controlador remoto, pero no pierde los parámetros de funcionamiento. Pero, al ir variando la altura del dron, y acercándolo más a la estación de interferencia, con alturas inferiores a los 10m se consigue la obstrucción entre la comunicación del dron y el controlador remoto. A esta altura la señal del controlador remoto se pierde en intervalos de tiempo y de duración reducida alrededor de 10 segundos, lo que lleva a no tener dominio para movilizar el dron.

Los resultados de las pruebas con el sistema adicional inhibidor de GPS y WIFI descritas en la sección 4.5.3 y analizadas en este capítulo, fueron similares con los obtenidos con el sistema diseñado, tanto en tiempos de interferencia, como en la deshabilitación de los parámetros de funcionamiento. Por lo tanto, el prototipo diseñado cumple con todas las características de un sistema *jamming*, siendo viable y aplicable para su funcionamiento.

Las pruebas y mediciones realizadas confirman que la efectividad del prototipo depende de la disponibilidad de:

- Potencia de la interferencia.
- Directividad de la antena *jamming*, para que la relación Señal Drone/Señal Interferencia sea tan baja que el sistema de comunicación drone– controlador se vea afectado tanto en el downlink como en el uplink.

También se confirma que el uplink (dirección controlador –drone, en drones tipo Phantom) al trabajar con *hopping frequency* con anchos de banda de 2 MHz, presenta cierta inmunidad al *jamming* de banda ancha ya que la potencia del *jamming* (3W máximo en nuestro caso) se distribuye en un ancho de banda mucho mayor que 2 MHz.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

El sistema inhibidor de drones para las bandas comerciales WIFI fue desarrollado e implementado de forma efectiva, ya que se logró interferir al vehículo aéreo no tripulado (drone), neutralizando la comunicación controlador-drone, y bloqueando los parámetros de funcionamiento del vuelo del drone en diferentes escenarios.

Partiendo del análisis de las técnicas de inhibición, se estableció que la técnica de *jamming* por ruido mediante circuito es la más eficiente para interferir el drone, con un tiempo de pérdida de control de alrededor de 15 segundos, debido a que se introduce el ruido en una parte específica del espectro, y al no desperdiciar potencia en otras frecuencias, que no trabaja el drone, la potencia se centra más en el ancho de banda necesario

La implementación y operación del sistema de inhibición de drones, presenta una eficacia favorable que llega a distancias de 200m, también se hizo pruebas que abordaban los 400m, donde se comprobó que se mantienen las mismas respuestas de interferencia que a 200m.

Los resultados de la interferencia hacia los drones con el sistema inhibidor desarrollado y el sistema adicional de laboratorio para la generación de la interferencia, fueron satisfactorios y representan las mismas características de respuesta. Por lo tanto, el sistema prototipo desarrollado cumple con todas las características de un sistema *jamming*, siendo viable y aplicable para su funcionamiento, debido a su reducido peso, volumen, costo computacional y precio en relación a los existentes en el mercado. Sin duda, el sistema de producción para

operación en escenarios reales, debe utilizar un amplificador de potencia mayor a los 3W que ha sido utilizado en este prototipo.

6.2 Recomendaciones

Se aconseja utilizar un amplificador RF con más ganancia, a fin de que la inhibición de señal provoque una pérdida total del control del drone (canal de transmisión de video, canal de control remoto), puesto que debe ser mayor la potencia del sistema de interferencia en comparación con la potencia del drone.

Para hacer más efectivo el *jamming* por ruido mediante una tarjeta electrónica de tipo arduino se recomienda utilizar una tarjeta controladora de mayor capacidad y superior desempeño que el arduino para cambiar la frecuencia de envío de datos de la salida analógica mediante el uso de los registros internos de los timers.

Para la elaboración de circuitos generadores de ruido se debe aislar todo ruido como son el ruido de la fuente con una puesta a tierra así como también colocar una bobina a la salida del voltaje para eliminar parte inductiva y contener al circuito en una caja aisladora de frecuencias o cargas. Sin embargo, para un sistema en producción se debe utilizar un generador integrado de ruido blanco disponible en el mercado, que por su costo fue prohibitivo para el desarrollo del presente prototipo.

Es obligatorio orientar la antena hacia el objetivo como si el sistema de *jamming* se tratase de un fusil, para que la relación Señal Drone/Señal Interferencia sea favorable para nuestros propósitos.

Manejar cada una de las secciones y etapas que constituyen el sistema de interferencia por separado en vista de que facilita la calibración y operatividad de las mismas.

BIBLIOGRAFÍA

- Analog Devices*. (s.f.). Obtenido de <https://www.analog.com/en/products/hmc321a.html>
- Arcangelis, M. (1983). *Historia de la Guerra Electronica*.
- Aviación, A. F. (2016). *FAA expande la Iniciativa Pathfinder de detección de drones*. Obtenido de <https://www.faa.gov/news/updates/?newsId=85532>
- Balanis, C. A. (2012). *Advanced Engineering Electromagnetics*. Arizona: Wiley.
- Battelle. (2018). *Battelle*. Obtenido de <https://www.battelle.org/government-offerings/national-security/aerospace-systems/counter-UAS-technologies>
- Carlson. (2002). *Communication Systems: An Introduction to Signals and Noise in Electrical Communication*. New York: McGraw Hill.
- Carrasco, J. (2015). *Integración de un UAV (vehículo aéreo no tripulado) en la plataforma robótica ARGOS*. Obtenido de <http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20150407JuanAlbertoBenitoCarrasco.pdf>
- Comunicaciones, E. d. (2016). Obtenido de <https://slideplayer.es/slide/11102363/>
- D. Lee, J. V. (2006). "A hardware Gaussian noise generator using the Box-Muller method and its error analysis". *IEEE*, vol. 55, 659-671.
- DGAC, D. G. (17 de Septiembre de 2015). *Aviación Civil*. Obtenido de <http://www.aviacioncivil.gob.ec/wp-content/uploads/downloads/2015/09/Resol.-251-2015-Normas-Operacion-Drones.pdf>
- Dieuleveult, F. (1999). *Electrónica aplicada a las altas frecuencias*. Madrid.
- Dji. (2016). *Dji*. Obtenido de <https://www.dji.com/phantom-4>
- Drones, C. d. (Mayo de 2018). *DRONES: Riesgos actuales de interferencia ilícita*. Obtenido de <http://www.ciber-drones.com/ciberseguridad/drones-riesgos-actuales-de-interferencia->

ilícita/

- Dynamics, C. (2018). *Chess Dynamics Anti-UAV*. Obtenido de <http://www.chess-dynamics.com/auds/>
- Fernández, E. (2016). *Evaluación en la Seguridad de las Comunicaciones de Drones e Implementación de nuevos Métodos de Seguridad*. Obtenido de https://www.researchgate.net/profile/Ernesto_Fernandez5/publication/314733146_Evaluacion_en_la_seguridad_de_las_comunicaciones_de_drones_e_implementacion_de_nuevos_metodos_de_seguridad/links/58c57ab645851538eb8afa67/Evaluacion-en-la-seguridad-de-las-comun
- G. Zhou, C. L. (2005). Unmanned aerial vehicle (UAV) real-time video registration for forest fire monitoring. En *Geosciencie and Remote Sensing Symposium*. IEEE International, vol 3.
- Haykin, S. (2001). *Communication Systems*. (4. edition, Ed.) New York: John Wiley & Sons.
- Hertz Systems . (2018). *Sistemas antidrones*. Obtenido de <https://www.hertzsystems.com/es/product/sistemas-antidrones/>
- Igor Bisio, Chiara Garibotto y otros. (2018). Unauthorized Amateur UAV Detection Based on WiFi Statistical Fingerprint Analysis. *IEEE Communications Magazine*.
- Instruments, N. (6 de Noviembre de 2014). *Understanding Spread Spectrum for Communications*. Obtenido de <http://www.ni.com/white-paper/4450/en/>
- Intrucción a la Guerra Electronica Aérea. (1983). *Revista de Aeronauticca y Astronautica*.
- Jaejoon Choi, J. J. (2016). *Area Efficient Approach for Generating Quantized Gaussian Noise*. Obtenido de IEEE Xplore: <https://ieeexplore.ieee.org/document/1628955>
- Kai, B. E. (2007). “A software-defined GPS and Galileo receiver: a single-frequency approach,” *Applied and numerical harmonic analysis*. Birkhäuser Boston.

León, M. C. (2010). *Redes convergentes*. Mexico: ; Instituto Politécnico Nacional.

López, F. (s.f.). *El estándar IEEE 802.11*. Obtenido de <http://web.dit.upm.es/~david/TAR/trabajos2002/08-802.11-Francisco-Lopez-Ortiz-res.pdf>

López, F. (s.f.). *El estándar IEEE 802.11*. Obtenido de <http://web.dit.upm.es/~david/TAR/trabajos2002/08-802.11-Francisco-Lopez-Ortiz-res.pdf>

López, H. (27 de Julio de 2018). Guacho utiliza drones para ubicar al Ejército. *Expreso*.

MiniCircuits. (s.f.). *Voltage Controlled Oscillator*.

Parkinson BW, S. J. (1996). *Global Positioning System: Theory and applications*, Vol. I, II. American Institute of Aeronautics and Astronautics, Progress in Astronautics and Aeronautics.

Parlin, K. (2017). Jamming of Spread Spectrum Communications used in UAV Remote Control Systems.

Phuan, Y. (2017). ¡Alarma, drones a la vista! *R&S@ARDRONIS* .

Poisel, R. (2004). *Modern Communication Jamming Principles and Techniques*. Norwood: Artech House.

Posiel, R. (2011). Spread Spectrum Technology. En *Modern Comumunication Jamming Principles and Techniques*. Estados Unidos : Artech HUse.

Prabakaran, P. (5 de Junio de 2003). *EE Times*. Obtenido de Tutorial on Spread Spectrum Technology: https://www.eetimes.com/document.asp?doc_id=1271899

Rodrigo Valim, André dos Anjos. (2017). Estudo e Simulação de Diferentes Tipos de. 14.

Rohde & Schwarz. (2018). *Rohde & Schwarz*. Obtenido de www.rohde-schwarz.com

S. D. Hanford, L. N. (2005). «A Small Semi-Autonomous Rotary-Wing Unmanned Air. En *Infotech Aerospace*. Virginia.

- Scherrer. (1985). *The WM GPS primer*. Switzerland: WM Satellite Survey Company.
- Scholtz, R. (1982). The Origins of Spread-Spectrum Communications. *IEEE Transactions on Communication, COM30(5)*, 822-854.
- Seide, N. R. (2005). 802.11 (Wi-Fi) Manual de Redes inalámbricas.
- Seybold, J. (2005). *Introduction to RF Propagation*. Estados Unidos: Wiley Interscience.
- Sklar, B. (2001). *Analog and Digital Communication Systems*. California: Prentice Hall.
- Thomas Multerer, Alexander Ganis y otros. (2017). Low-cost Jamming System Against Small Drones Using a 3D MIMO Radar Based Tracking.
- Tomasi., W. (2003). *Sistemas de comunicaciones electrónicas*. Mexico: Pearson Educación.
- UIT. (2016). *UIT*. Recuperado el 2019, de https://www.itu.int/dms_pubrec/itu-r/rec/v/r-rec-v.431-8-201508-i!!pdf-s.pdf
- Ureña, Á. G. (2009). *Investigación y Ciencia*. Obtenido de <https://www.investigacionyciencia.es/blogs/fisica-y-quimica/10/posts/descubrimiento-de-las-ondas-de-radio-la-confirmacin-de-la-teora-electromagntica-10186>
- Valderrama, C. (1980). Guerra Electrónica . *Revista de Marina*.
- Xu, W. y. (2005). *The Feasibility of Launching and Detecting Jamming Attacks in Wireless Network*. Obtenido de http://www.winlab.rutgers.edu/pub/docs/research/JamDetect_Mobihoc.pdf

ANEXOS

ANEXO 1. Especificaciones técnicas del VCO de 2.4 GHz

Coaxial

Voltage Controlled Oscillator

ZX95-2536C+

5V Tuning for PLL IC's 2315 to 2536 MHz

Features

- low phase noise
- low pulling
- low pushing
- protected by US patent 6,790,049

Applications

- r & d
- lab
- instrumentation
- industrial scientific and medical
- WIMAX
- TD-SCDMA / HSDPA



CASE STYLE: GB956

Connectors	Model
SMA	ZX95-2536C-S+

e-Noise Compliance
 The e-Noise Compliance Filter Component. See our web site for the e-Noise Compliance technology and guidelines.

Electrical Specifications

MODEL NO.	FREQ. (MHz)		POWER OUTPUT (dBm)	PHASE NOISE dBc/Hz SSB at offset frequencies, kHz				TUNING					NON HARMONIC SPURIOUS (dBc)	HARMONICS (dBc)			PULLING pk-pk @ 12 dB (MHz)	PUSHING (MHz/V)	DC OPERATING POWER	
	Min.	Max.		Typ.	1	10	100	1000	VOLTAGE RANGE (V)	SENSITIVITY (MHz/V)	PORT CAP (pF)	3 dB MODULATION BANDWIDTH (MHz)		Typ.	Typ.	Max.			Typ.	Max.
ZX95-2536C+	2315	2536	+6	-75	-105	-128	-148	0.5	5	57-77	13.6	70	-90	-18	-10	2.5	2.5	5	45	

Maximum Ratings

Operating Temperature	-55°C to 85°C
Storage Temperature	-55°C to 100°C
Absolute Max. Supply Voltage (Vcc)	5.6V
Absolute Max. Tuning Voltage (Vtune)	7.0V
All specifications	50 ohm system

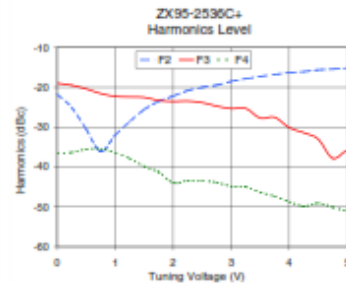
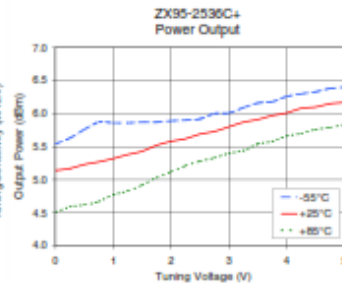
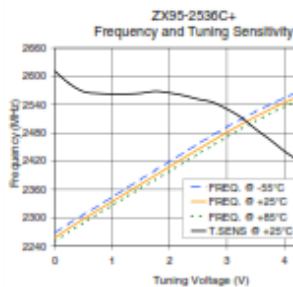
Permanent damage may occur if any of these limits are exceeded.



NOTE: When soldering the DC connections, caution must be used to avoid overheating the DC terminals. See Application Note AN-40-10.

V TUNE	TUNE SENS (MHz/V)	FREQUENCY (MHz)			POWER OUTPUT (dBm)			Icc (mA)	HARMONICS (dBc)			FREQ. PUSH (MHz/V)	FREQ. PULL (MHz)	PHASE NOISE (dBc/Hz) at offsets				FREQ. OFFSET (KHz)	PHASE NOISE at 2432 MHz (dBc/Hz)
		-55°C	+25°C	+85°C	-55°C	+25°C	+85°C		F2	F3	F4			1kHz	10kHz	100kHz	1MHz		
0.00	81.90	2267.6	2257.4	2249.2	5.54	5.14	4.51	36.63	-21.7	-19.0	-36.6	2.44	3.28	-77.7	-104.8	-127.5	-147.0	1.0	-75.73
0.50	74.61	2306.7	2297.3	2289.5	5.76	5.23	4.62	37.11	-30.5	-20.4	-35.5	1.96	0.44	-76.2	-105.1	-128.0	-147.9	2.0	-84.74
0.75	73.96	2325.2	2315.9	2308.2	5.87	5.27	4.67	37.29	-36.1	-21.6	-35.4	1.65	1.90	-76.2	-105.7	-128.6	-148.2	3.5	-93.54
1.00	73.76	2344.0	2334.4	2326.4	5.86	5.32	4.77	37.45	-32.0	-22.3	-36.4	1.49	2.67	-75.5	-105.6	-128.2	-147.6	6.0	-99.82
1.25	73.75	2362.7	2352.9	2344.6	5.86	5.38	4.83	37.57	-28.6	-22.4	-37.9	1.42	2.27	-77.8	-105.5	-128.7	-148.3	8.5	-103.77
1.50	74.01	2381.6	2371.3	2362.6	5.87	5.43	4.92	37.67	-25.6	-22.5	-39.9	1.37	1.25	-77.6	-105.5	-128.7	-148.4	10.0	-105.41
1.75	74.71	2400.7	2389.8	2380.6	5.87	5.52	5.03	37.73	-23.5	-23.3	-41.2	1.38	1.27	-76.5	-105.6	-128.9	-148.5	20.8	-113.60
2.00	74.15	2419.7	2408.5	2398.2	5.89	5.58	5.12	37.80	-22.2	-23.5	-44.0	1.41	2.83	-77.1	-105.6	-128.9	-148.4	35.5	-118.96
2.25	73.21	2438.5	2427.0	2417.2	5.90	5.62	5.21	37.87	-20.8	-23.5	-43.4	1.51	2.86	-76.1	-105.9	-128.8	-148.6	60.7	-124.10
2.50	71.91	2456.9	2445.3	2435.4	5.92	5.69	5.28	37.92	-20.0	-23.9	-43.5	1.75	1.53	-76.5	-105.6	-128.7	-148.8	85.2	-127.31
2.75	70.82	2475.0	2463.3	2453.3	6.00	5.73	5.33	37.95	-19.5	-24.7	-43.9	2.12	1.51	-75.3	-104.9	-128.6	-148.1	100.0	-128.68
3.00	68.45	2492.6	2481.0	2471.1	6.01	5.80	5.40	37.97	-18.5	-25.3	-44.9	2.58	3.12	-76.0	-104.4	-128.3	-148.6	142.9	-131.46
3.25	65.44	2509.4	2498.1	2488.3	6.09	5.87	5.44	37.99	-17.9	-25.3	-45.0	3.09	2.95	-74.7	-104.6	-128.1	-148.7	167.8	-133.29
3.50	61.36	2525.2	2514.5	2504.9	6.16	5.91	5.54	38.02	-17.3	-27.7	-46.3	3.65	1.69	-76.0	-104.2	-128.2	-148.0	200.6	-134.52
3.75	57.60	2540.3	2529.8	2520.7	6.18	5.97	5.58	38.06	-16.8	-27.5	-47.3	4.08	1.15	-75.5	-103.9	-128.4	-147.5	281.6	-137.84
4.00	53.56	2554.4	2544.2	2535.4	6.26	6.01	5.66	38.06	-16.3	-30.1	-48.7	4.52	2.96	-77.2	-103.4	-128.0	-147.9	330.7	-138.85
4.25	50.01	2567.6	2557.6	2549.0	6.30	6.08	5.70	38.06	-16.1	-31.4	-49.8	4.84	3.53	-77.3	-103.2	-127.7	-147.8	464.2	-141.63
4.50	45.62	2579.9	2570.1	2561.7	6.33	6.10	5.76	38.05	-15.6	-33.0	-49.1	5.01	3.11	-77.3	-103.3	-127.8	-148.3	554.9	-143.78
4.75	41.10	2591.0	2581.5	2573.3	6.38	6.15	5.79	38.05	-15.5	-37.8	-50.1	5.07	2.11	-76.0	-103.0	-127.6	-148.2	914.6	-147.64
5.00	36.26	2601.0	2591.8	2583.8	6.40	6.17	5.83	38.06	-15.2	-35.9	-51.1	4.89	0.87	-75.8	-103.4	-128.1	-148.4	1000.0	-148.33

*at 25°C unless mentioned otherwise



ANEXO 2. Especificaciones técnicas del VCO de 5.8 GHz

2X Fundamental

Voltage Controlled Oscillator

ZX95-5776+

Frequency Doubling 5726 to 5826 MHz

Features

- frequency based on multiplication of carrier frequency
- low phase noise
- low pushing & pulling
- 5V Tuning voltage range
- protected by US patent 6,790,049

Applications

- r & d
- lab
- instrumentation
- wireless communications
- uniband cable program



CASE STYLE: GB956

Connectors	Model
SMA	ZX95-5776-S+

e-Parts Compliance
The e-Parts Identifier (EPI) Compliance file on our website for EPI Compliance, authenticity and quality.

Electrical Specifications

MODEL NO.	FREQ. (MHz)		POWER OUTPUT (dBm)	PHASE NOISE dBc/Hz SSB at offset frequencies, kHz				TUNING				NON HARMONIC SPURIOUS (dBc)	HARMONICS (dBc)			PULLING pk-pk @ 12 dB (MHz)	PUSHING (MHz/V)	DC OPERATING POWER		
	F	2X(1/2F)		Typ.	1	10	100	1000	VOLTAGE RANGE (V)	SENSITIVITY (MHz/V)	PORT CAP (pF)		3 dB MODULATION BANDWIDTH (MHz)	F0.5	F1.5			F2	Vcc (volts)	Current (mA)
ZX95-5776+	5726	5826	+1.5	-75	-102	-122	-142	0.5	5	50-78	18	130	-90	-19	-21	-16	0.5	3	5	33

Maximum Ratings

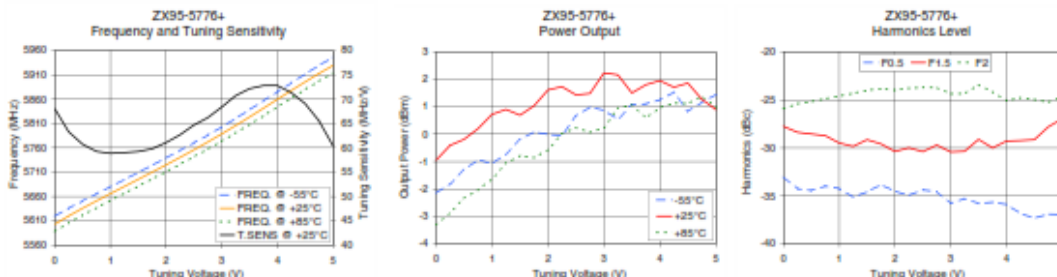
Operating Temperature -55°C to 85°C
 Storage Temperature -55°C to 100°C
 Absolute Max. Supply Voltage (Vcc) 7V
 Absolute Max. Tuning Voltage (Vtune) 7V
 All specifications 50 ohm system
 Permanent damage may occur if any of these limits are exceeded.



NOTE: When soldering the DC connections, caution must be used to avoid overheating the DC terminals. See Application Note AN-40-10.

V TUNE	TUNE SENS (MHz/V)	FREQUENCY (MHz)			POWER OUTPUT (dBm)			Icc (mA)	HARMONICS (dBc)			FREQ. PUSH (MHz/V)	FREQ. PULL (MHz)	PHASE NOISE (dBc/Hz) at offsets				FREQ. OFFSET (KHz)	PHASE NOISE at 5776 MHz (dBc/Hz)
		-55°C	+25°C	+85°C	-55°C	+25°C	+85°C		F0.5	F1.5	F2			1kHz	10kHz	100kHz	1MHz		
0.00	68.04	5619.2	5602.8	5587.7	-2.15	-0.95	-3.32	21.27	-33.0	-27.8	-25.9	2.19	0.38	-76.4	-100.6	-120.6	-141.9	1.0	-72.27
0.25	63.29	5635.4	5619.8	5605.4	-1.81	-0.41	-2.86	21.42	-34.2	-28.4	-25.4	2.29	0.39	-74.3	-102.2	-120.9	-141.0	2.0	-82.58
0.50	60.74	5650.7	5635.6	5621.5	-1.30	-0.19	-2.34	21.56	-34.4	-28.6	-25.2	2.39	0.42	-76.6	-101.4	-121.2	-141.5	3.5	-90.80
0.75	59.26	5665.4	5650.8	5636.9	-0.93	0.20	-2.03	21.70	-34.0	-28.7	-24.9	2.46	0.43	-74.9	-101.4	-120.3	-140.8	6.0	-96.72
1.00	58.86	5680.0	5665.6	5651.8	-1.08	0.72	-1.63	21.83	-34.2	-29.5	-24.6	2.54	0.40	-76.3	-102.5	-122.1	-141.3	8.5	-99.09
1.25	59.01	5694.6	5680.3	5666.4	-0.72	0.90	-1.07	21.97	-35.1	-29.8	-24.3	2.63	0.47	-77.9	-102.3	-122.1	-141.3	10.0	-101.83
1.50	59.23	5709.2	5695.1	5681.0	-0.20	0.69	-0.78	22.12	-34.6	-29.1	-24.0	2.70	0.30	-76.8	-101.9	-121.6	-141.2	20.8	-108.40
1.75	59.79	5723.9	5709.9	5695.7	0.08	1.03	-0.86	22.28	-33.8	-29.6	-23.8	2.75	0.27	-78.4	-102.6	-121.5	-141.8	35.5	-111.49
2.00	61.06	5738.9	5724.8	5710.7	-0.01	1.61	-0.57	22.43	-34.5	-30.4	-24.0	2.82	0.42	-76.5	-102.9	-121.6	-142.3	60.7	-116.09
2.25	62.66	5754.3	5740.1	5725.9	-0.05	1.73	0.01	22.59	-34.9	-30.0	-23.8	2.90	0.48	-76.4	-102.5	-121.8	-141.6	86.7	-121.21
2.50	64.67	5770.0	5755.7	5741.3	0.66	1.43	0.23	22.74	-34.4	-30.4	-23.7	2.99	0.35	-74.7	-103.2	-121.5	-142.1	100.0	-121.84
2.75	66.19	5786.1	5771.9	5757.2	0.99	1.48	0.06	22.90	-34.5	-29.7	-23.7	3.07	0.27	-76.5	-103.1	-122.8	-142.2	148.1	-124.53
3.00	68.36	5802.9	5788.5	5773.7	0.87	2.23	0.23	23.05	-35.8	-30.4	-24.4	3.13	0.30	-76.2	-103.5	-121.9	-142.5	177.0	-126.12
3.25	70.71	5820.2	5805.6	5790.5	0.54	2.16	0.95	23.20	-35.3	-30.4	-24.4	3.19	0.42	-75.8	-102.3	-121.5	-141.4	211.6	-128.69
3.50	72.15	5838.1	5823.2	5807.9	1.07	1.50	1.07	23.35	-35.8	-29.1	-23.4	3.23	0.37	-77.1	-103.1	-122.0	-142.9	302.4	-131.59
3.75	72.81	5856.3	5841.3	5825.7	1.10	1.80	0.59	23.51	-35.7	-30.0	-24.2	3.15	0.35	-75.4	-102.7	-121.8	-142.4	361.5	-133.77
4.00	72.81	5874.0	5859.5	5843.9	1.25	1.95	0.96	23.65	-35.9	-29.3	-25.1	2.96	0.22	-75.8	-102.7	-123.4	-142.4	507.5	-136.78
4.50	69.08	5911.7	5895.5	5879.9	0.83	1.86	1.11	23.89	-37.3	-29.1	-25.0	2.19	0.38	-74.6	-102.6	-123.3	-142.1	606.7	-138.86
4.75	65.55	5929.3	5912.8	5897.2	1.16	1.27	1.38	23.98	-36.9	-27.8	-25.3	1.70	0.26	-75.2	-102.1	-122.4	-142.3	851.6	-140.91
5.00	60.47	5945.8	5929.2	5913.7	1.44	0.90	1.00	24.07	-36.9	-27.0	-24.7	1.22	0.22	-74.5	-101.6	-120.9	-143.1	1000.0	-142.38

*at 25°C unless mentioned otherwise



ANEXO 3. Especificaciones técnicas del amplificador RF

Coaxial High Power Amplifier

ZVE-3W-83+

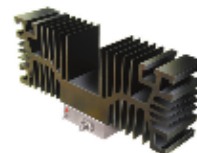
50Ω 3W 2000 to 8000 MHz

Features

- High power, 3 Watt
- Wideband, 2000 to 8000 MHz
- Low noise figure, 5.8 dB typ.
- High IP3, +42 dBm typ.
- High dynamic range
- High gain, 35 dB typ. and good directivity, 35 dB typ.
- Internal voltage regulated for 13 to 18 VDC

Applications

- Satellite communications
- Line-of-sight transmitters
- Signal generators
- Spread-spectrum communication



CASE STYLE: BN1327

Connectors Model
SMA ZVE-3W-83+

RF Compliance
The +Radio Identifier (P/N) Compliance. See our web site for P/N Compliance information and qualifications

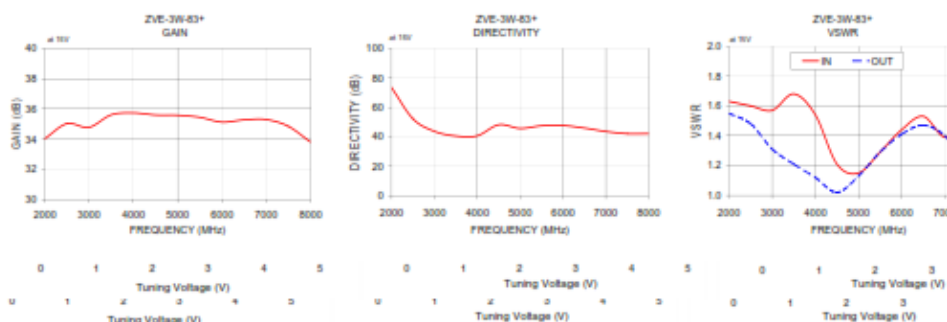
Electrical Specifications

Parameter	Min.	Typ.	Max.	Units
Frequency Range	2000		8000	MHz
Gain	30		40	dB
Gain Flatness		±1.15	±2.0	dB
Output Power at 1dB compression ¹	+31.5	+33		dBm
Saturated Output Power at 3dB compression ¹	+33.5	+35		dBm
Noise Figure		5.8		dB
Output third order intercept point		+42		dBm
Input VSWR		1.5		:1
Output VSWR		1.4		:1
DC Supply Voltage		15		V
Supply Current ²			1.5	A

1. At 25°C operating temperature
2. If Voltage set below 15 VDC, current may go up to 2A/ma.

Permanent damage may occur if any of these limits are exceeded.

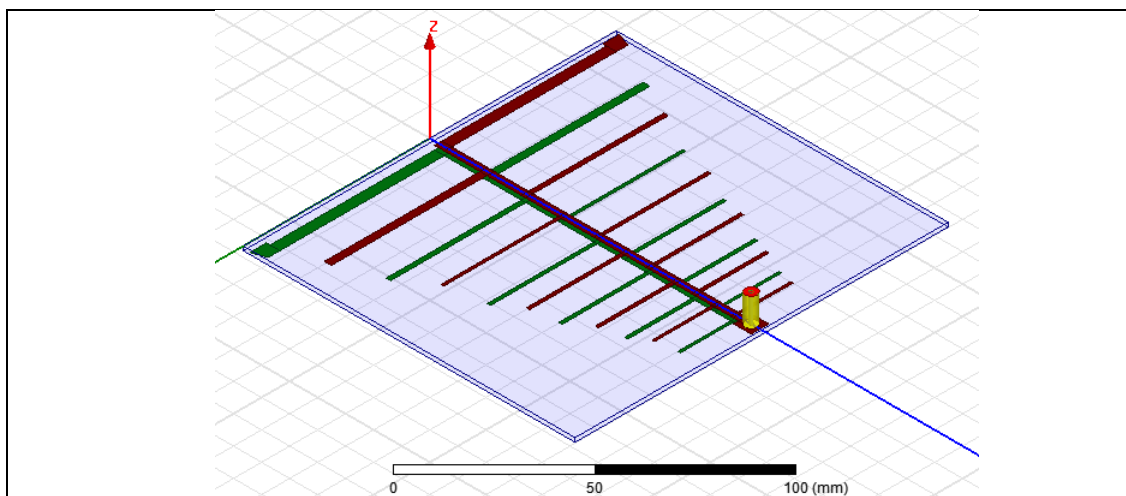
FREQUENCY (MHz)	GAIN (dB)		DIRECTIVITY (dB)		VSWR (:1)		NOISE FIGURE (dB)		POUT (dBm) at 15V		OUTPUT IP3 (dBm)
	15V	15V	IN	OUT	IN	OUT	15V	1 dB Compr.	3 dB Compr.	15V	
2000.00	34.01	73.37	1.63	1.55	5.69	33.42	34.53	42.30			
2500.00	35.02	52.19	1.60	1.48	5.61	34.44	35.37	44.04			
3000.00	34.77	43.74	1.57	1.31	5.97	33.67	35.26	44.17			
3500.00	35.60	40.56	1.68	1.21	5.78	33.91	35.28	44.00			
4000.00	35.73	40.67	1.54	1.12	5.70	33.75	35.22	43.39			
4500.00	35.59	48.18	1.21	1.02	5.61	34.84	36.05	43.44			
5000.00	35.57	45.70	1.15	1.13	5.92	34.65	36.12	43.19			
5500.00	35.44	47.51	1.29	1.29	6.04	34.32	35.63	42.65			
6000.00	35.12	47.69	1.44	1.41	6.16	34.24	35.67	42.50			
6500.00	35.27	45.25	1.53	1.47	6.64	35.51	36.11	42.32			
7000.00	35.29	43.62	1.39	1.40	6.96	36.25	36.37	43.84			
7500.00	34.84	42.16	1.48	1.21	6.87	34.82	35.85	45.57			
8000.00	33.80	42.17	1.44	1.07	6.24	33.57	34.75	44.16			



ANEXO 4. Especificaciones de la antena log periódica.

Antena tipo: Log periódica

Banda de operación: 900 MHz a 2,3 GHz



Curvas de desempeño

