

Diseño e implementación de un prototipo inhibidor de un vehículo aéreo no tripulado (UAV)*

| Fecha de recibido: 28 de mayo del 2020 | Fecha de aprobación: 19 de septiembre del 2020 |

Jhon Jairo Cárdenas Triana

Magíster en Radar

Corporación de Alta Tecnología
para la Defensa (CODALTEC)
Grupo de Investigación y
Desarrollo de Sensores (GIDS)

Rol de investigador: teórico, experimental y escritura
<https://orcid.org/0000-0003-3997-899X>
✉ jjcardenas@codaltec.com

Andrés Felipe Jaramillo Álvarez

Magíster en Radar

Corporación de Alta Tecnología
para la Defensa (CODALTEC)
Grupo de Investigación y
Desarrollo de Sensores (GIDS)

Rol de investigador: experimental y escritura
<https://orcid.org/0000-0002-6885-5596>
✉ ajaramillo@codaltec.com

Darwin Leonardo Gómez Pinzón

Magíster en Radar

Corporación de Alta Tecnología
para la Defensa (CODALTEC)
Grupo de Investigación y
Desarrollo de Sensores (GIDS)

Rol de investigador: experimental y escritura
<https://orcid.org/0000-0003-4988-1948>
✉ dgomez@codaltec.com

Iván Darío Duarte Brito

Magíster en Radar

Corporación de Alta Tecnología
para la Defensa (CODALTEC)
Grupo de Investigación y
Desarrollo de Sensores (GIDS)

Rol de investigador: experimental y escritura
<https://orcid.org/0000-0002-5136-8337>
✉ iduarte@codaltec.com

* Artículo de investigación derivado del proyecto "Diseño e implementación de un sistema de inhibición de UAV para las bandas GPS (L1 y L2), WiFi 2,4 GHz, y WiFi 5,8 GHz", adscrito al Grupo de Investigación y Desarrollo de Sensores (GIDS) de la Corporación de Alta Tecnología para la Defensa (CODALTEC).

Cómo citar este artículo: Cárdenas Triana, J. J., Jaramillo Álvarez, A. F. Gómez Pinzón, D. L., & Duarte Brito, I. D. (2020).

Diseño e implementación de un prototipo inhibidor de un vehículo aéreo no tripulado (UAV). *Revista Ciencia y Poder Aéreo*, 15(2), 94-109.
<https://doi.org/10.18667/cienciaypoderaereo.663>



Diseño e implementación de un prototipo inhibidor de un vehículo aéreo no tripulado (UAV)

Resumen: en los últimos años, la proliferación y fácil acceso a los vehículos aéreos no tripulados (UAV), ha causado un gran número de incidentes en el mundo. Los gobiernos han aunado esfuerzos para regular y controlar la operación de estos sistemas, al impulsar la creación de soluciones que permitan detectar y mitigar posibles ataques mediante estas plataformas. En el presente artículo se describe el proceso de diseño e implementación de un prototipo de inhibición de UAV para las bandas GPS (L1 y L2), WiFi 2,4 GHz y WiFi 5,8 GHz. Los resultados de las pruebas realizadas mostraron un alcance de inhibición de 150m con una potencia de transmisión por banda menor a 25 dBm.

Palabras clave: defensa aérea; drones; guerra electrónica; inhibición UAV; mitigación; neutralización.

UAV Jammer Prototype Implementation and Design

Abstract: Unmanned aerial vehicles (UAVs) easy access and proliferation have caused many incidents around the world over the last years. Numerous governments have joined forces to control and regulate the operation of these devices, promoting the creation of solutions to allow detection and mitigation of potential attacks from these platforms. Therefore, this paper presents the implementation and design process of an UAV jamming prototype for GPS (L1, L2), Wi-Fi 2.4 GHz and Wi-Fi 5.8 GHz bands. After testing, the prototype achieved a 150m range with a band transmission power of less than 25 dBm.

Keywords: Air defense; drone; electronic warfare; UAV jamming; mitigation; neutralization.

Desenho e implementação de um protótipo de inibição de VANT

Resumo: A proliferação e o fácil acesso aos veículos aéreos não tripulados (VANT) causaram um grande número de incidentes no mundo todo nos últimos anos. Governos do mundo inteiro uniram forças para regular e controlar a operação desses sistemas, promovendo a criação de soluções que permitem detectar e mitigar possíveis ataques por meio dessas plataformas. Este artigo descreve o processo de criação e implementação de um protótipo de inibição de VANT para as bandas GPS (L1 e L2), Wifi 2.4 GHz e WiFi 5.8 GHz, nos testes realizados um alcance de 150 m foi obtido com uma potência de transmissão por banda inferior a 25 dBm.

Palavras-chave: Defesa aérea; Drones; Guerra eletrônica; Inibição de UAV; Mitigação; Neutralização.

Introducción

Los vehículos aéreos no tripulados, UAV (por sus siglas en inglés, *Unmanned Aerial Vehicles*), han sido utilizados por las fuerzas armadas de diferentes países desde hace más de 15 años, facilitando las operaciones militares y disminuyendo riesgos del personal involucrado. Con el pasar del tiempo su uso en la industria civil se ha incrementado, por lo cual estos sistemas se han convertido en un producto de consumo masivo presente en diversas aplicaciones (Barrientos, del Cerro & Gutiérrez, 2007). Mediante los UAV se han mejorado procesos de prevención y gestión de riesgos en la seguridad industrial (Raygoza, Toriz & Sánchez, 2016), se ha fortalecido la investigación medioambiental y forestal (Tang & Shao, 2015), han sido fundamentales para tecnificar la agricultura (Berrio, Mosquera & Alzate, 2015) y se proyectan como solución para la distribución de insumos de salud en regiones apartadas (Scott & Scott, 2017).

Sin embargo, dada su rápida proliferación y disminución en los costos de adquisición, se han convertido en un factor de riesgo importante para el sector aeronáutico y militar (Medina, 2018). Su uso se ha evidenciado para actividades de espionaje, narcotráfico (Niño, 2016), robo de información, atentados y actividades que afectan el normal funcionamiento de las operaciones aéreas (Ferreira, 2016). Incluso, su uso autorizado para empresas de seguridad privada genera riesgos potenciales como lesiones personales, violación de la intimidad, afectación a bienes públicos y privados, así como violaciones de perímetros de seguridad nacional (Mora, 2016), tanto así, que en Colombia se registraron más de 17 incursiones indebidas por estas plataformas y en la actualidad, son percibidos como una amenaza global, la cual requiere de medidas regulatorias adecuadas a nivel mundial y nacional (Stöcker et al., 2017; González, 2017).

En el estudio de North Atlantic Treaty Organization (NATO, 2013), se estableció como prioridad el desarrollo de soluciones para minimizar los riesgos operacionales que pueden producir las plataformas aéreas no tripuladas por medio de la aplicación de

tácticas y tecnologías innovadoras capaces de controlar estas amenazas. Así mismo, se sugiere que para un correcto control de los UAV se establezcan soluciones que combinen diferentes tipos de sensores, además de generar estudios que demuestren cuál es el tipo de tecnología ideal para su neutralización y mitigación. Esto reafirma y demuestra el compromiso mundial adquirido para el control y protección de tecnologías emergentes como los UAV.

La mayoría de soluciones de neutralización o mitigación pueden ser agrupadas en las siguientes categorías:

- Captura física: incluye el lanzamiento de redes o mallas y la interceptación con aves o aeronaves.
- Técnicas de contramedidas electrónicas: incluye interferencia electromagnética y pulsos de alta potencia.
- Sistemas optrónicos: incluye láseres de baja y alta potencia.
- Munición: armas convencionales y misiles guiados (Birch, Griffin & Erdman, 2015).

De estas categorías, se destaca el método de interferencia electromagnética gracias a su óptima relación de efectividad versus precio (Farlik, Kratky & Casar, 2016). De la misma forma, este método reduce el riesgo para las personas y la infraestructura cercana, pues se evita que el UAV caiga de forma descontrolada, ya que mediante la inhibición de su sistema de control, comunicación y posición GPS (*Global Positioning System*), se logra hacer que la aeronave aterrice de inmediato, quede suspendida en el aire sin transmisión de video o, regrese a su punto de origen evitando así su cometido. En ese marco, también se han presentado soluciones novedosas como la integración de los sistemas de inhibición con sistemas radar (Multerer & Ganis, 2017), y el despliegue aéreo de módulos de inhibición en red de bajo costo y alcance (Tkachenko, 2015).

Teniendo en cuenta lo anterior, en el presente artículo se presenta el proceso de diseño e implementación de un prototipo de inhibición de UAV para las bandas GPS (L1 y L2), y las bandas WiFi 2,4 GHz y WiFi

5,8 GHz; con el objetivo de exponer los resultados obtenidos, el texto se organizó así: la sección de metodología en la cual se describen las técnicas generales usadas para la inhibición o interferencia electromagnética, selección y justificación de la técnica de barrido implementada. Otra sección sobre la arquitectura del diseño, en la que se presenta un diagrama de bloques sobre los principales subsistemas y elementos que lo componen. Luego, se describe la implementación del sistema para generar la forma de onda requerida y la forma de control e interfaz de usuario desarrollada.

Más adelante, en la sección de resultados se detallan las pruebas y mediciones realizadas en el laboratorio del Grupo de Investigación y Desarrollo de Sensores (GIDS), así como las pruebas de radiación en campo con los resultados del alcance evidenciado. Por último, se presentan las conclusiones obtenidas del trabajo y las propuestas para trabajos futuros.

Metodología

Técnicas de inhibición

Se conoce como inhibición al bloqueo o interferencia electromagnética intencional, a una comunicación inalámbrica buscando disminuir la relación señal a ruido (SNR). El transmisor genera una señal a la misma frecuencia del receptor a interferir con una intensidad de potencia adecuada para poder superponerse. En las tablas 1 y 2 se presenta la clasificación general y estrategias de inhibición:

Tabla 1. Clasificación general

Puntual	Barrera
Concentra la potencia transmitida en un solo canal o frecuencia.	Distribuye la potencia transmitida en un rango de frecuencias o canales.
Obvio	Sutil
Señal de inhibición fácil de detectar por el receptor.	Señal de inhibición difícil de detectar por el receptor.

Fuente: Priyanka, Rutvij & Shweta (2017).

Tabla 2. Estrategias de inhibición

Ruido	Portadora modulada por una señal aleatoria de ruido.	Ruido banda ancha (BBN). Ruido de banda ancha parcial (PBN). Ruido de banda angosta (NBN).
Tonos	Se ubican uno o varios tonos fijos a lo largo del ancho de banda de la señal.	Tono único (ST). Múltiples tonos (MT).
Pulsos	Generación de pulsos periódicos de corta duración y alta potencia.	El ciclo de trabajo dependerá de la aplicación específica y la naturaleza de la señal.
Barrido	Ruido de banda angosta o tonos que se desplazan por todo el ancho de banda requerido.	La velocidad del barrido dependerá de la aplicación específica y la tasa de transmisión de datos.
Seguimiento	Se identifica la frecuencia temporal de la señal objetivo y se genera ruido, tonos o pulsos a esa frecuencia.	Conocido también como inhibición de respuesta o repetición.
Inteligente	Estudio de la aplicación y señal objetivo para ahorrar recursos como potencia.	Ahorro de recursos suplantando identidades en la comunicación con el dispositivo.

Fuente: Nocedal de la Garza (2016).

En el artículo de Nocedal de la Garza (2016), se realizó el diseño e implementación de un inhibidor de telefonía celular en el cual se tuvieron en cuenta algunas consideraciones para seleccionar la estrategia de inhibición, consideraciones también aplicables para la inhibición de UAV, destacando que en este caso, las bandas de frecuencia a inhibir son las correspondientes a los servicios de GPS y WiFi.

Se descartó el inhibidor por ruido debido a que distribuir la potencia en el ancho de banda es complejo, se tendría que implementar una ganancia muy alta para la amplificación, y además, requerir un generador de ruido cuyo costo es elevado. De igual forma, se prescindió de la estrategia de tonos fijos, pues la mayoría de los sistemas y protocolos utilizan saltos de frecuencia entre subcanales. Y en este caso, el inhibidor por pulsos no sería efectivo, ya que para la presente aplicación se necesita inhibición continua, y por

último, el inhibidor por seguimiento y engaño no se consideró dada la complejidad de su implementación.

De modo que, se seleccionó el inhibidor por barrido debido a su relación eficiencia-complejidad, para aprovechar la máxima potencia disponible en cada frecuencia del espectro y fragmento del tiempo. La señal utilizada para el inhibidor de barrido se conoce como *Linear Chirp Swept*, es eficiente para la inhibición en servicios de navegación, celular, WiFi y Bluetooth (Priyanka, Rutvij & Shweta, 2017). Al enmascarar o superponer la señal original, se logra aumentar el BER (*Bit Error Rate*) lo que dificulta la correcta transferencia de datos (Fang et al., 2018). Los anchos de banda de la señal se establecieron a partir de los servicios que se desean inhibir, en el caso de los UAV, se utiliza GPS para la navegación y WiFi para el control y la transmisión de datos.

- Banda GPS L2: 1.210 - 1.254 MHz
- Banda GPS L1: 1.560 - 1.611 MHz
- Banda WiFi 2,4 GHz: 2.400 - 2.484 MHz
- Banda WiFi 5,8 GHz: 5.710 - 5.835 MHz

La señal GPS es más susceptible a la inhibición, pues su nivel de potencia en la tierra es de aproximadamente -120 dBm (Farlik, Kratky & Casar, 2016). Al implementar un tono desplazándose por saltos de frecuencia, este espaciado en frecuencia mínimo, se puede determinar a partir del número de canales del protocolo a inhibir, en este caso, con 1 MHz de espaciado fue suficiente para obtener resultados satisfactorios.

La banda WiFi 2,4 GHz posee 14 canales separados cada 5 MHz, en el que cada canal consta de 22 MHz. La banda WiFi 5,8 GHz cuenta con 8 canales separados cada 10 MHz, cada canal consta de 20 MHz. En este caso, la tasa de barrido de la señal transmitida es crítica, ya que depende directamente de la tasa de transmisión de datos. En el artículo *Jamming of UAV Remote Control Systems using software defined radio*, Seebeck & Alam (2018) sugieren que la frecuencia de barrido debe ser mayor a 1,6 kHz para poder inhibir adecuadamente el servicio de WiFi, para este respecto, dada la capacidad del *hardware* implementado se estableció

una frecuencia de barrido de 100 kHz para asegurar la inhibición del servicio.

Arquitectura de diseño

A continuación, se presenta el diagrama de bloques por banda en la figura 1, así como una descripción general de los principales elementos y subsistemas necesarios para la implementación del prototipo de inhibición por barrido.

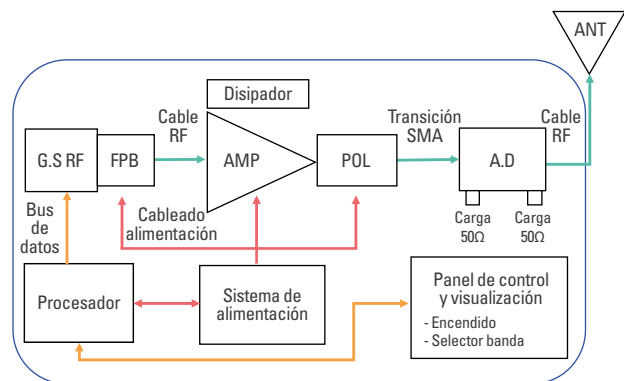


Figura 1. Diagrama de bloques implementado por banda

Fuente: elaboración propia.

Generador de señal (GS) RF: es el subsistema encargado de generar la señal RF de barrido dentro del ancho de banda deseado. Puede implementarse mediante un sintetizador programable, o un vco con su respectiva señal de control. En el prototipo implementado se utilizó un sintetizador programable de dos salidas para las bandas GPS, y dos vco para las bandas WiFi. En la siguiente sección se describirá con mayor detalle el hardware implementado para la generación de la señal de barrido.

Filtro pasa banda (FPB): este filtro se utiliza a la salida del generador de señal RF para evitar que armónicos o señales espurias ingresen al amplificador y sean radiadas posteriormente. En el prototipo implementado se utilizaron filtros coaxiales con conectores SMA, según cada banda.

Amplificador de potencia (AMP) + disipador: es el elemento encargado de aumentar la potencia de la

señal RF para lograr el alcance de inhibición deseado. En el prototipo implementado se utilizaron dos modelos de amplificadores: el modelo A, con 15dB de ganancia y un ancho de banda desde DC hasta 28 GHz; y el modelo B, con 30dB de ganancia y un ancho de banda desde 1,8 GHz hasta 2,7 GHz, en ambos casos la potencia de salida máxima especificada es de 30 dBm (1W).

Polarizador: es el elemento que permite energizar correctamente el amplificador de RF. Para el amplificador modelo A se requiere un *Bias Tee* que permite generar un voltaje DC a la salida del amplificador, y para el amplificador modelo B, se requiere un *DC-Block* que filtra el voltaje DC a la salida de este. En el prototipo implementado se utilizaron *Bias Tee* y *DC-Block* SMA para cada banda de frecuencia.

Acoplador direccional (AD): protege el amplificador RF de señales que puedan entrar por la antena de transmisión y adicionalmente permite tomar muestras de la señal RF de inhibición sin interrumpir su operación. En el prototipo implementado se utilizaron acopladores bidireccionales SMA cuyo ancho de banda soporta hasta 6 GHz.

Procesador: es el subsistema encargado de la programación para generar la señal de RF y la comunicación con el panel de control y visualización. En el prototipo implementado se utilizó una tarjeta de desarrollo LattePanda, la cual cuenta con puertos USB, Ethernet y un sistema operativo embebido Windows 10.

Sistema de alimentación: su función es generar los niveles de voltaje y corriente adecuados para energizar los diferentes elementos y subsistemas del prototipo de inhibición.

Panel de control y visualización: interfaz que permite activar y configurar los parámetros de cada banda de inhibición. Se describirá con mayor detalle en secciones posteriores.

Antena: encargada de radiar la señal RF hacia el objetivo deseado. Para obtener un alcance destacado se usan generalmente antenas directivas. En el prototipo implementado se utilizaron antenas Vivaldi de banda ancha directivas, las cuales poseen una ganancia de 11 dBi y soportan un ancho de banda desde 675 MHz hasta 12 GHz.

Por último, se replicaron y combinaron estos elementos en las 4 bandas necesarias, GPS L1, GPS L2, WiFi 2,4 GHz y WiFi 5,8 GHz para obtener el diseño implementado del prototipo inhibidor de UAV.

Señal de barrido

El sintetizador de RF empleado para generar el barrido de frecuencia para las bandas GPS L1 y GPS L2 es programable y posee dos canales de salida, tiene la capacidad de generar señales en el rango de frecuencia de 54 MHz a 13,6 GHz con niveles de potencia de hasta 18 dBm.

Los barridos de frecuencia se programaron para que se efectuaran en periodos de 5 ms, mediante saltos de 1 MHz en el ancho de banda correspondiente para cada una de las bandas de inhibición. La programación del sintetizador se realizó por medio de la tarjeta de desarrollo LattePanda desde la cual se envían comandos para su control.

La generación de la señal RF en las bandas de WiFi 2,4 GHz y 5,8 GHz, se implementó mediante osciladores controlados por voltaje (vco) debido a que pueden generar frecuencias de barrido mayores a las producidas por el sintetizador de RF, estas altas frecuencias son necesarias para afectar la transferencia de datos de los protocolos de comunicación WiFi. Su funcionamiento requiere un voltaje de sintonización a la entrada, para generar un tono a determinada frecuencia en RF a la salida. Teniendo en cuenta que se debe recorrer de forma lineal el ancho de banda asociado al espectro de frecuencias que se usa para los controles remotos de los UAV, es necesario generar una señal triangular periódica a la entrada del vco (figura 2) con las especificaciones mencionadas en la tabla 3.



Figura 2. Barrido de frecuencia lineal (LFM)

Fuente: elaboración propia.

Tabla 3.
Señal de sintonización de los VCO implementada

	WiFi 2.4 GHz	WiFi 5.8 GHz
Frecuencia de barrido	100 kHz	
Forma de la señal	Triangular	
Voltajes de sintonización	1.882 – 3.042V	1.882 – 3.641v
Frecuencias interferidas	2.400 – 2.484 MHz	5.710 – 5.835 MHz

Fuente: elaboración propia.

La señal de sintonización de los vco se generó mediante un sintetizador en forma de onda digital DDS, el cual puede producir señales triangulares, sinusoidales y rectangulares de hasta 12,5 MHz. Este circuito integrado dispone para su funcionamiento de un puerto de comunicaciones SPI mediante el cual se pueden controlar diferentes parámetros de la señal generada. Sin embargo, las características de tensión de salida del DDS no son adecuadas para cubrir las necesidades de los rangos de voltaje de sintonización, razón por la cual se implementó una etapa de acondicionamiento de la señal. La etapa de acondicionamiento está basada en un amplificador de señal no inversor (figura 3) y un fijador de nivel DC, de esta forma, se le da la ganancia en voltaje necesaria a la señal del DDS y el nivel DC requerido según la excursión de frecuencia requerida.

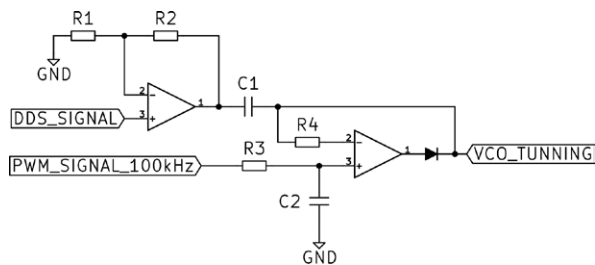


Figura 3. Esquema de amplificador de señal no inversor implementado
Fuente: elaboración propia.

El fijador de nivel DC se implementó mediante un generador de señal PWM a 100 kHz, un filtro pasa bajos de primer orden y un fijador de precisión con diodo obteniendo un rizado menor a 1,25 mVpp (figura 4 y 5).

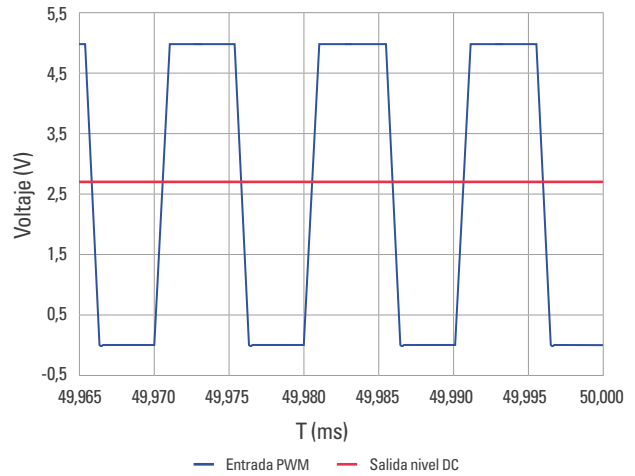


Figura 4. Simulación señal DC mediante PWM
Fuente: elaboración propia.

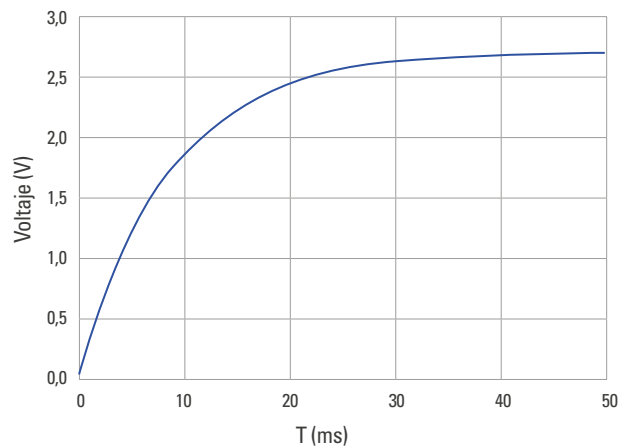


Figura 5. Simulación curva de respuesta fijador de nivel
Fuente: elaboración propia.

Esta implementación presenta la ventaja que el ancho de banda del barrido generado puede ser reprogramado o ajustado, facilitando su calibración y futuras actividades de mantenimiento.

El sistema de control para la generación del barrido se implementó mediante una tarjeta Arduino, cuya función es comunicarse con el software de la tarjeta de desarrollo LattePanda, y de esta manera recibir los comandos y parámetros de configuración del sintetizador DDS, así como los ajustes de nivel DC de la señal. Dicha comunicación se realiza por medio de una

conexión serial a 115kbps 8N1 con la tarjeta LattePanda y mediante protocolo SPI con el sintetizador DDS.

Control e interfaz de usuario

Se implementó una interfaz física y *software* que en ambos casos permite activar la radiación de la señal de inhibición y seleccionar la banda deseada GPS L2, GPS L1, WiFi 2,4 GHz y WiFi 5,8 GHz. La tarjeta LattePanda utilizada para su desarrollo cuenta con un sistema operativo Windows 10 y un microcontrolador Arduino embebido, el cual permite acceder a puertos analógicos y digitales.

Sobre el sistema operativo Windows 10 se implementó la interfaz *software* de control (HMI), para el control del inhibidor y mediante el microcontrolador Arduino embebido se implementó la interfaz física (Leds + Botones). El usuario tiene la capacidad de usar simultáneamente ambas interfaces, *hardware* y *software*, ya que se encuentran comunicadas entre sí. En la figura 6 se presenta la arquitectura general del sistema de control desarrollado y los principales puertos utilizados.

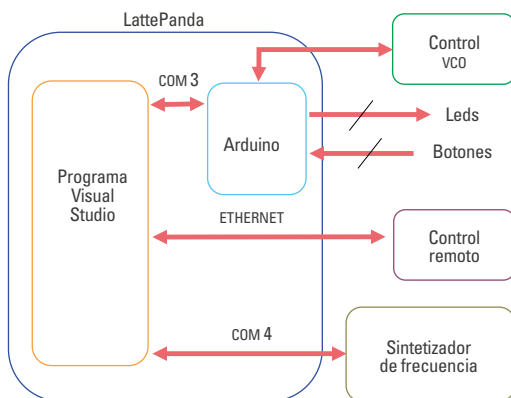


Figura 6. Arquitectura del sistema de control implementado
Fuente: elaboración propia.

La interfaz *software* HMI puede utilizarse cuando se conecta una pantalla a la plataforma, en la figura 7 se presenta la disposición final de botones y seleccionables de la interfaz *software* desarrollada.

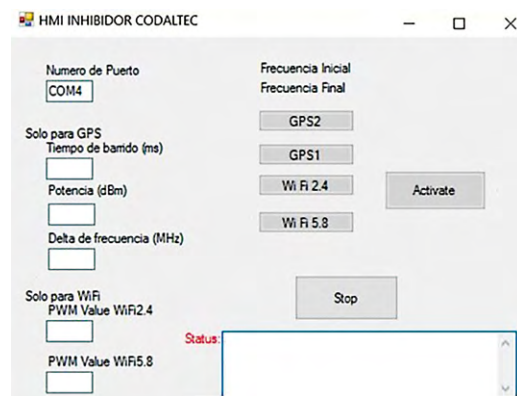


Figura 7. Interfaz *software* de control (HMI) implementada
Fuente: elaboración propia.

Para su utilización primero se deben configurar los parámetros de inhibición ubicados al costado izquierdo, luego se deben seleccionar las bandas de inhibición deseadas y por último, se activa la radiación.

La interfaz física compuesta de botones y leds, se diseñó para un ambiente de operación donde no se tenga acceso a una pantalla para visualizar la interfaz *software* HMI. Los botones incorporados permiten seleccionar cada una de las bandas de inhibición, también, permiten activar y detener la radiación. En este caso, los parámetros de configuración como el número de puerto, la velocidad de barrido y el delta de frecuencia serán los establecidos previamente por defecto, en la figura 8 se presenta la interfaz física implementada.

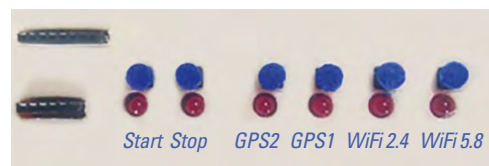


Figura 8. Interfaz física de control implementada
Fuente: elaboración propia.

Los botones y los leds son gestionados directamente por el microcontrolador Arduino, el que a la vez, se comunica con el *software* HMI implementado en la plataforma LattePanda, y es esta, quien realiza la comunicación con el sintetizador de RF y demás componentes del sistema para controlar la inhibición.

Resultados

Pruebas de laboratorio

En el laboratorio del Grupo de Investigación y Desarrollo de Sensores (GIDS), se realizaron pruebas de polarización y de excursión de señal, con potencias de entrada entre -10 dBm y 12 dBm para el amplificador modelo A. De la misma forma, se probó con potencias de entrada entre -20 dBm y 0 dBm para el amplificador modelo B. Adicionalmente, se realizó un monitoreo de temperatura en los disipadores, los cuales nunca superaron los 40 °C, los resultados obtenidos se presentan en la tabla 4.

Tabla 4. Resultados medición de amplificadores

Amplificador	Banda	Ganancia promedio
A	GPS L2	15,8 dB
A	GPS L1	15,1 dB
B	WiFi 2,4 GHz	28,2 dB
A	WiFi 5,8 GHz	12,8 dB

Fuente: elaboración propia.

Una vez se verificó el correcto funcionamiento de los amplificadores, se procedió a implementar cada cadena por banda de frecuencia, se generó la señal de entrada con el sintetizador o vco respectivo y se verificó la potencia de la señal de salida con un analizador de espectro. En las figuras 9, 10, 11 y 12 se presentan los resultados obtenidos.

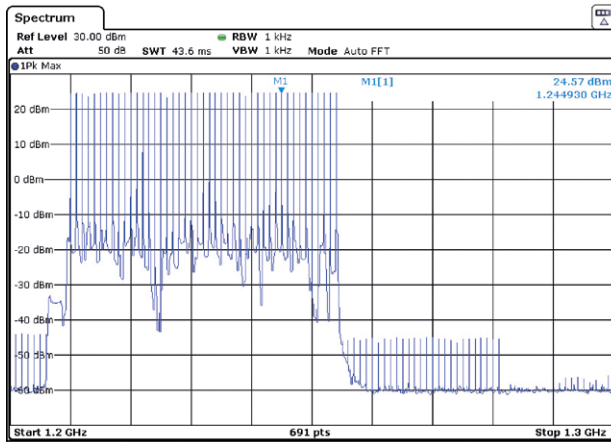


Figura 9. Medición barrido banda GPS L2

Fuente: elaboración propia.

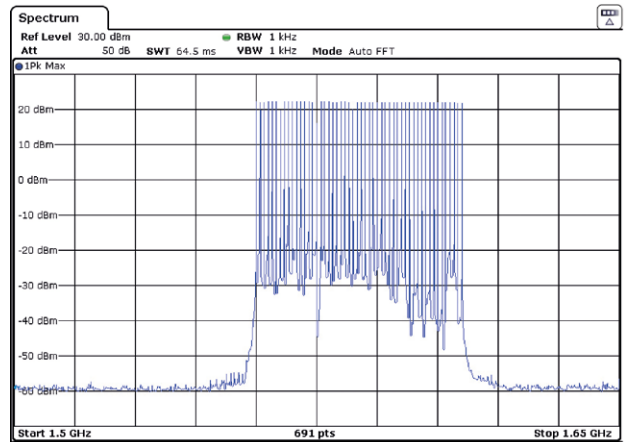


Figura 10. Medición barrido banda GPS L1

Fuente: elaboración propia.

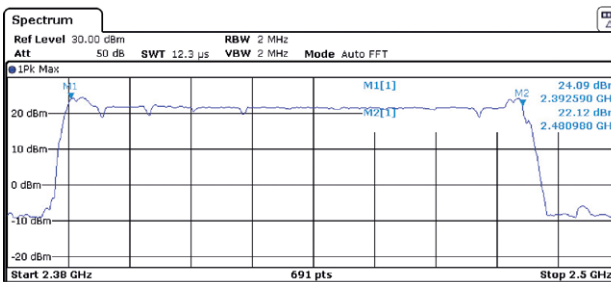


Figura 11. Medición barrido banda 2,4 GHz

Fuente: elaboración propia.

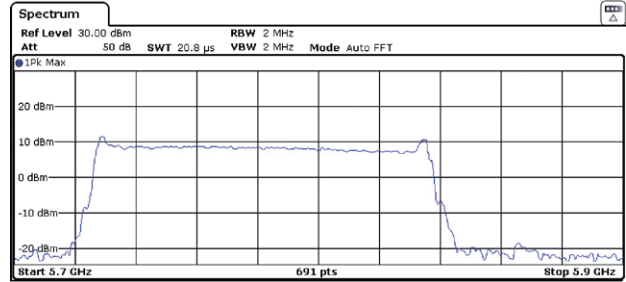


Figura 12. Medición barrido banda 5,8 GHz

Fuente: elaboración propia.

Se evidenció que las señales de barrido corresponden con las bandas de frecuencia deseadas y el rizado de la señal de salida no supera los 2 dB. En la tabla 5 se presenta el consolidado de las potencias de salida por cada banda.

Tabla 5.
Mediciones potencias de salida por banda

Banda	Pin (dBm)	Pout media (dBm)
GPS L2	12	24,5
GPS L1	12	22,4
WiFi 2,4 GHz	6	22,6
WiFi 5,8 GHz	1,5	9,3

Fuente: elaboración propia.

Es importante destacar que para la bandas WiFi se utilizaron osciladores controlados por voltaje (vco), cuya potencia de salida es fija, contrario al sintetizador de RF usado para generar el barrido en las bandas GPS que tiene potencia de salida ajustable. Para las bandas GPS y WiFi 2,4 GHz se obtuvieron potencias de salida mayores a 20 dBm, para el caso de la banda WiFi 5,8 GHz se obtuvo una potencia de salida de 9,3 dBm, dado a que la potencia generada por el vco usado es menor, además, al ser la banda de frecuencia más alta, la ganancia del amplificador disminuye y las pérdidas en el cableado y acoplador direccional aumentan, por lo cual, la banda WiFi 5,8 GHz se convierte en un desafío en el que se recomienda usar elementos y cableado de bajas pérdidas, siempre y cuando el costo económico lo permita.

Durante las pruebas de medición en el laboratorio, se pudo evidenciar la importancia de realizar un adecuado procedimiento de polarización secuencial de los amplificadores RF haciendo uso de los *Bias Tee* y los *DC-Blocks*. Es recomendable limitar la corriente de las fuentes de voltaje de acuerdo con los máximos soportados por el amplificador, y evitar así, su daño.

Dado el reducido tamaño de los amplificadores implementados, menor a 25 cm², y su eficiente disipación de calor, se convierten en candidatos adecuados para su implementación en inhibidores de rápido despliegue, bajo consumo y operación portable, características altamente valoradas por las fuerzas armadas.

B. Pruebas de inhibición en campo

Las pruebas de inhibición en campo se realizaron utilizando un UAV Phantom 4 Pro ubicado a 100m del prototipo desarrollado, se probaron las bandas GPS L1 (1.560 MHz – 1.611 MHz) y WiFi 2,4 GHz secuencialmente. En la figura 13 se presenta el escenario y montaje implementado para la realización de las pruebas:



Figura 13. Montaje implementado pruebas de inhibición en campo
Fuente: los autores.

En la figura 14 se presenta su manera de operación, apuntando de forma manual con la antena direccional hacia el objetivo deseado.



Figura 14. Operación prototipo de inhibición
Fuente: los autores.

En la figura 15 se presenta el escenario empleado para la prueba de inhibición en la banda GPS L1 a 100m, por seguridad, la prueba se realizó con el UAV en posición de despegue.

En la figura 16 se evidencia que el UAV antes de ser inhibido está conectado a 15 satélites, luego, durante la inhibición en la figura 17 se evidencia que el UAV se desconecta de todos los satélites, por lo cual se concluye que la prueba de inhibición GPS L1 fue satisfactoria.



Figura 15. Escenario de prueba GPS L1-100m
Fuente: elaborado a partir de imagen de Google Maps (2020).

Más adelante, se realizó una prueba de inhibición para la banda WiFi 2,4 GHz a 100m de distancia. Se ubicó el control del UAV a 25m de este, como se muestra en la figura 18 y se obtuvieron resultados satisfactorios durante la inhibición del control y la transmisión de video como se muestra en las figuras 19 y 20.

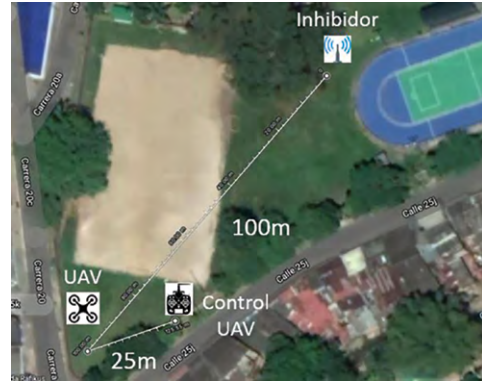


Figura 18. Escenario de prueba WiFi 2,4 GHz -100m
Fuente: elaborado a partir de imagen de Google Maps (2020).



Figura 16. Estado GPS antes de la inhibición - 100m
Fuente: elaboración propia.



Figura 19. Estado control y video antes de la inhibición - 100m
Fuente: elaboración propia.

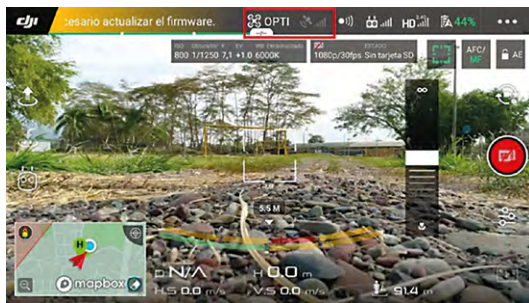


Figura 17. Estado GPS durante la inhibición - 100m
Fuente: elaboración propia.



Figura 20. Estado control y video durante la inhibición -100m
Fuente: elaboración propia.

Las distancias probadas fueron validadas a partir del cálculo de la relación de interferencia a señal como se muestra en la tabla 6.

Tabla 6.
Cálculos alcance de inhibición 100m

	GPS L1	WiFi 2,4 GHz
Potencia del transmisor (dBm)	43	26
Ganancia de la antena transmisora (dBi)	36	3
Distancia entre transmisor y receptor (km)	20.000	0,025
Pérdidas de transmisión en espacio libre (dB)	182,56	68,26
Ganancia antena receptora (dBi)	3	3
Potencia de recepción (dBm)	-100,56	-36,26
Ancho de banda señal recibida (MHz)	51	84
Ruido de fondo (dBm)	-96,92	-94,76
Potencia de salida del inhibidor (dBm)	24	23
Ganancia de la antena de inhibición (dBi)	11	11
Distancia de inhibición (km)	1	0,1
Pérdidas por polarización (dB)	3	3
Pérdidas propagación del inhibidor (dB)	94,06	80,3
Potencia de inhibición en el receptor (dBm)	-59,0557	-46,3030
Potencia de inhibición + ruido (dBm)	-59,0550	-46,3030
Relación interferencia a señal (I/S)	41,51	-10,04
(I/S) Límite	10	-10

Fuente: elaboración propia.

Finalmente se realizó una prueba adicional de inhibición en la banda WiFi 2,4 GHz, ubicando el UAV a 150m del inhibidor y el control a 100m del UAV como se muestra en la figura 21.



Figura 21. Escenario de prueba WiFi 2,4 GHz-150m
Fuente: elaborado a partir de imagen de Google Maps (2020).

Se obtuvo un resultado satisfactorio durante la inhibición del control y transmisión de video, como se presenta en la figura 22.

La prueba de inhibición de control y video fue satisfactoria a 150m, ya que se encontraba dentro del margen adecuado de relación interferencia a señal como se muestra en la tabla 7.



Figura 22. Estado del control y video durante la inhibición-150m
Fuente: elaboración propia.

Tabla 7.
Cálculos del alcance de inhibición 150m

	WiFi 2.4 GHz
Potencia del transmisor (dBm)	26
Ganancia de la antena transmisora (dBi)	3
Distancia entre transmisor y receptor (km)	0,1
Pérdidas de transmisión en espacio libre (dB)	80,3
Ganancia antena receptora (dBi)	3
Potencia de recepción (dBm)	-48,3
Ancho de banda señal recibida (MHz)	84
Ruido de fondo (dBm)	-94,76
Potencia de salida del inhibidor (dBm)	23
Ganancia de la antena de inhibición (dBi)	11
Distancia de inhibición (km)	0,15
Pérdidas por polarización (dB)	3
Pérdidas propagación del inhibidor (dB)	83,82
Potencia de inhibición en el receptor (dBm)	-49,8249
Potencia de inhibición + ruido (dBm)	-49,8247
Relación interferencia a señal (I/S)	-1,52
(I/S) Límite	-10

Fuente: elaboración propia.

De acuerdo a los resultados obtenidos, se validó que la técnica seleccionada de inhibición por barrido es eficaz operativamente y las frecuencias de barrido implementadas, 0,2 kHz para las bandas GPS y 100 kHz para las bandas WiFi, permiten interrumpir la comunicación y posicionamiento del UAV impidiendo que cumpla su objetivo.

Como se pudo evidenciar, el alcance de inhibición depende de varios parámetros entre los cuales se destaca la distancia existente entre el sistema de inhibición, el sistema de control del UAV, la plataforma UAV, la potencia de transmisión del control, la potencia de inhibición, la ganancia de las antenas y las pérdidas asociadas a la propagación. En conjunto, todos estos parámetros convergen en una relación interferencia a señal (I/S), la cual se convierte en un indicativo de la eficacia de la inhibición, durante las pruebas realizadas se obtuvieron alcances de inhibición de 100m y 150m para relaciones de interferencia a señal (I/S) superiores a -10dB. Es importante destacar, que al utilizar esta técnica de inhibición se logra aprovechar la potencia transmitida para inhabilitar los servicios GPS y WiFi sin llegar a dañar la plataforma UAV, minimizando riesgos y daños por precipitaciones a tierra.

Al utilizar antenas directivas se obtiene una mayor ganancia que con las antenas omnidireccionales, dicha ganancia está relacionada con la concentración de energía en un sector angular del espacio, que permite aumentar el alcance con la misma potencia de inhibición. Adicionalmente, al cubrir un sector angular específico se logra direccionar la mayor cantidad de energía hacia el objetivo, para evitar interferir en zonas que no sean de interés y minimizar riesgos por afectación a dispositivos no deseados. La antena directiva puede ser apuntada de forma manual hacia el objetivo simplificando la operación y rápido despliegue del sistema. Al ser una antena de banda ancha, posee la ventaja de soportar las 4 bandas de frecuencia de interés, sin embargo, también es posible utilizar una antena con un ancho de banda específico para cada servicio. Las antenas omnidireccionales pueden ser útiles para aplicaciones de sistemas de inhibición fijos, que requieran cubrir sectores angulares amplios como por

ejemplo 360°, no obstante, se debe tener en cuenta la respectiva reducción en el alcance.

Por otra parte, es de especial cuidado el diseño de la banda WiFi 5,8 GHz, pues al ser de mayor frecuencia se presenta un incremento tanto en las pérdidas de inserción de los elementos de la cadena, como en las pérdidas por propagación, se debe procurar buscar un equilibrio entre costo económico y prestaciones técnicas.

Teniendo en cuenta todo lo anterior, se demostró el correcto desempeño del prototipo implementado, el cual podría convertirse en un sistema de inhibición portable y de rápido despliegue que permita dar solución a las necesidades de seguridad y preocupaciones expresadas por diferentes organismos alrededor del mundo.

Conclusiones

En el artículo se presentó el diseño e implementación de un prototipo de inhibición de UAV para las bandas GPS (L1 y L2) y las bandas WiFi 2,4 GHz y WiFi 5,8 GHz. Se implementó la técnica de inhibición por barrido para la generación de la señal, mediante el uso de sintetizadores para las bandas GPS con una frecuencia de barrido de 0,2 kHz y dispositivos vco para las bandas WiFi con una frecuencia de barrido de 100 kHz, que permitió un adecuado costo beneficio. Así mismo, se desarrolló una interfaz HMI software que permite configurar los parámetros de inhibición vía remota y una interfaz HMI hardware, que posibilita seleccionar las bandas a inhibir y controlar la radiación de señal, esta última, es útil para escenarios en los cuales no se cuenta con disponibilidad de una pantalla.

De igual manera, se midieron características como ancho de banda y potencia de las señales de inhibición en el laboratorio del Grupo de Investigación y Desarrollo de Sensores (GIDS), mediante el uso de un analizador de espectro. De esto se concluyó que la banda de WiFi 5,8 GHz presenta mayores pérdidas de inserción en el cableado y elementos RF, por lo cual se debe procurar buscar una adecuada relación costo

beneficio de acuerdo al alcance de inhibición deseado y el presupuesto disponible. Adicionalmente, se debe ser muy riguroso con el procedimiento de polarización de los amplificadores RF, usar la secuencia sugerida por el fabricante y emplear elementos como *Bias Tee* y *DC-Blocks* según se requiera, así como limitar la corriente suministrada para proteger los amplificadores de daños no deseados. Dado el tamaño reducido de los amplificadores implementados, menor a 25cm², bajo consumo, menor a 800mA, y eficiente disipación de calor, permitió proyectar su utilización para aplicaciones portables y de rápido despliegue.

Más adelante se realizaron pruebas de radiación en campo para las bandas GPS L1 y WiFi 2,4 GHz con un UAV Phantom 4 Pro, ubicado a 100m del prototipo desarrollado, se obtuvo como resultado la afectación de los servicios de posicionamiento, control y transmisión de video del UAV. Además, se realizó una prueba de inhibición en la banda WiFi 2,4 GHz, con una potencia de inhibición de 23 dBm, ubicando el UAV a 150m del inhibidor y a 100m del control, se obtuvo nuevamente como resultado la afectación de los servicios de control y transmisión de video del UAV. Dichos resultados permitieron validar la selección de la técnica de inhibición, con frecuencias de barrido de 0,2 kHz para las bandas GPS y de 100 kHz para las bandas WiFi. Los alcances obtenidos dependen de parámetros técnicos como la distancia entre el inhibidor, el control del UAV y la plataforma UAV, la potencia de inhibición, la potencia de control del UAV, las ganancias de las antenas involucradas y las pérdidas por propagación, los cuales, en conjunto constituyen una relación interferencia a señal (I/S) que repercute finalmente en la eficacia de la inhibición.

Por otro lado, las antenas directivas presentan mayor ganancia que las antenas omnidireccionales, lo cual permite concentrar la energía en un sector angular específico logrando extender el alcance con la misma potencia de inhibición, y así, se evita interferir con dispositivos no deseados. Al usar una antena tipo Vivaldi se aprovechó la ventaja de que posee un bajo perfil y peso menor a 0,3 kg, lo cual facilita su almacenamiento, operación y futuro montaje sobre plataformas de apuntamiento mecánico si así se diseñará.

En suma, se demostró la efectividad del prototipo diseñado para interferir los servicios de posicionamiento y comunicación de la plataforma UAV, con potencias de transmisión por banda menores a 25 dBm (0,32W) que evitan su daño físico y precipitación a tierra, lo cual podría generar daños materiales y riesgos al personal circundante. Finalmente, mediante el trabajo realizado se establece una arquitectura de diseño viable para producir sistemas de neutralización y mitigación de UAV tácticos, portables y de rápido despliegue que permitan dar solución a las necesidades de seguridad actuales.

Trabajos futuros

Con el propósito de mejorar el desempeño del prototipo desarrollado, para trabajos futuros se plantea implementar amplificadores RF de mayor potencia con el objetivo de aumentar la distancia de inhibición. A su vez, se propone complementar el diseño de alimentación eléctrica incorporando un convertidor AC-DC y una batería recargable que conmuten automáticamente de acuerdo al uso requerido, así como la implementación de circuitos de protección de corriente para evitar daños en los componentes. También se recomienda el diseño mecánico de una carcasa para el prototipo, con el objetivo de hacerlo robusto durante la operación en intemperie. Y por último, se propone el diseño de una plataforma mecánica que permita controlar el apuntamiento de la antena al objetivo deseado.

Agradecimientos

Los autores desean agradecer especialmente a la Corporación de Alta Tecnología para la Defensa (CODALTEC) por el apoyo y financiación del presente proyecto. De igual forma, al Ministerio de Defensa Nacional de Colombia (MDN) por el acompañamiento y financiación del proyecto radar, mediante el cual se creó el Grupo

de Investigación y Desarrollo de Sensores (GIDS), y se dotó el laboratorio con equipos que permitieron la realización de las pruebas y mediciones requeridas.

Referencias bibliográficas

- Barrientos, A., del Cerro, J., Gutiérrez, P., San Martín, R., Martínez, A., & Rossi, C. (2007). *Vehículos aéreos no tripulados para uso civil. Tecnología y aplicaciones*. Universidad Politécnica de Madrid. <http://webdiis.unizar.es/~neira/docs/ABarrientos-CEDI2007.pdf>
- Berrío, M., Viviana, A., Mosquera, T., & Alzate, V. (2015). Uso de drones para el análisis de imágenes multiespectrales en agricultura de precisión. @Limentech, *Ciencia y Tecnología Alimentaria*, 13(1), 28-40. <https://doi.org/10.24054/16927125.v1.n1.2015.1647>
- Fang, L., Wang, X., Zhou, H., & Zhang, K. (2018). Design of Portable Jammer for UAV Based on SDR [conferencia]. *International Conference on Microwave and Millimeter Wave Technology (ICMMT)*. <https://doi.org/10.1109/ICMMT.2018.8563735>
- Farlik, J., Kratky, M., & Casar, J. (2016). Detectability and Jamming of Small UAVs by Commercially Available Low-cost Means [conferencia]. *International Conference of Communications (COMM)*. <https://doi.org/10.1109/ICComm.2016.7528287>
- Ferreira, I. (2016). *Los riesgos que representa el uso no autorizado de drones en el espacio aéreo Colombiano*. Universidad Militar Nueva Granada. <http://hdl.handle.net/10654/14244>
- González, A. (2017). *Propuesta de marco normativo para el uso deportivo de drones en Colombia de hasta 25kg* [Tesis de maestría]. Universidad Santo Tomás. <http://hdl.handle.net/11634/4130>
- Medina, L. (2018). *Drones un nuevo factor de riesgo para la seguridad del componente físico de la Fuerza Aérea Colombiana*. Universidad Militar Nueva Granada. <http://hdl.handle.net/10654/18010>
- Mora, L. (2016). *Análisis de riesgos asociados a la operación de drones ante un posible uso en la vigilancia privada*. Universidad Militar Nueva Granada. <http://hdl.handle.net/10654/18010>
- Multerer, T., Ganis, A., Prechtel, U., Miralles, E., Meusling, A., Mietzner, J., Vossiek, M., Loghi, M., & Ziegler, V. (2017, October). Low-cost Jamming System against Small Drones Using a 3D MIMO Radar Based Tracking [conferencia]. *2017 European Radar Conference (EURAD)*. <https://doi.org/10.23919/EURAD.2017.8249206>
- North Atlantic Treaty Organization [NATO]. (2013, July). *Final Report of NIAG SG170 on engagements of Low, Slow and Small aerial targets*. Industrial Advisory Group (NIAG). <https://slideplayer.com/slide/14574568/>
- NATO Army Armaments Group (NAAG). (2019, 11 de septiembre). *Joint Capability Group on Ground Based Air Defence (GBAD)*. https://www.dsei.co.uk/___media/libraries/east-theatre/Alan-Moore---NATO-GBAD-in-Transition---A-high-priority-complex-capability.pdf
- Niño, C. (2016). El narcotráfico mutante: nueva perspectiva de análisis del fenómeno en Colombia. *Revista Científica General José María Córdova*, 14(18), 113-124. <http://dx.doi.org/10.2139/ssrn.3159511>
- Nocedal, J. (2006). *Rf Jamming* [tesis de pregrado]. Universidad de las Américas. http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/nocedal_d_jm/indice.html
- Lineswala, P., Shah, S., & Shah, R. (2017). Different Categorization for Jammer: The Enemy of Satellite Navigation [conferencia]. *2017 2nd International Conference for Convergence in Technology (I2CT)*. <https://doi.org/10.1109/I2CT.2017.8226136>
- Raygoza, M., Toriz, A., & Sánchez, M. (2016). Prospectiva de gestión de riesgos industriales en México con el uso de drones. *RICEA Revista Iberoamericana de Contaduría, Economía y Administración*, 5(9), 37-55. <https://www.ricea.org.mx/index.php/ricea/article/view/51>
- Birch, G., Griffin, J., & Erdman, M. (2015). *UAS Detection, Classification and Neutralization: Market Survey Report*. Sandia National Laboratories. <https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/2015/156365.pdf>
- Scott, J., & Scott C. (2017). Drone Delivery Models for Healthcare [conferencia]. *Proceedings of the 50th Hawaii International Conference on System Sciences*. <http://128.171.57.22/handle/10125/41557>
- Seebeck, T., & Alam, M. (2018). Jamming of UAV Remote Control Systems using software defined radio [conferencia]. *2018 International Conference on Military Communications and Information Systems (ICMCIS)*. <https://doi.org/10.1109/ICMCIS.2018.8398711>
- Pärllin, K., Alam, M., & Le Moullec, Y. (2018). Jamming of UAV Remote Control Systems Using Software Defined Radio [conferencia]. *2018 International Conference on Military Communications and Information Systems (ICMCIS)*. <https://doi.org/10.1109/ICMCIS.2018.8398711>

- Stöcker, C., Bennett, R., Nex, F., Gerke, M., & Zevenbergen, J. (2017). Review of the Current State of UAV Regulations. *Remote Sensing*, 9(5), 459. <https://doi.org/10.3390/rs9050459>
- Tang, L., & Shao, G. (2015). Drone Remote Sensing for Forestry Research and Practices. *Journal of Forestry Research*, 26(4), 791–797. <https://doi.org/10.1007/s11676-015-0088-y>
- Tkachenko, O. (2015). System of electronic warfare with uavs [conferencia]. *2015 IEEE International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD)*. <https://doi.org/10.1109/APUAVD.2015.7346632>