PONTIFICIA UNIVERSIDAD CATOLICA DEL PERU

FACULTAD DE CIENCIA E INGENIERIA

ESTUDIO DEL GPS Y JAMMING PARA EL DISEÑO DE UN SISTEMA C-UAS DE USO CIVIL

Trabajo de investigación para obtener el grado académico de

BACHILLER EN CIENCIAS CON MENCIÓN EN INGENIERÍA DE LAS TELECOMUNICACIONES

AUTOR:

Daniel Paac Kaan Chú Santillán

ASESOR:

Manuel Augusto Yarlequé Medina

Lima, julio del 2020

Resumen

El presente trabajo tiene enfocado como problema el mal uso de los vehículos aéreos no tripulados (UAVs) en entorno civil. Debido a lo común que se han vuelto los UAVs en el entorno civil en conjunto con la falta de regulación para adquisición y especificaciones que ofrecen estos vehículos; existen usuarios maliciosos que los emplean para realizar actividades ilícitas tales como terrorismo, espionaje o transporte de drogas. Si se logra diseñar un dispositivo capaz de bloquear las señales GPS, siendo este el principal sistema de navegación empleado por los UAVs, este podría ser usado como medida contra el mal uso de estos vehículos. Por lo tanto, el presente trabajo, como una investigación bibliográfica, busca facilitar la realización de este tipo de sistemas, mediante la recopilación de la información acerca del GPS y del jamming. Por lo que los objetivos de este trabajo son: documentar acerca del Sistema de Navegación Global (GPS), identificar las diferentes técnicas empleadas para realizar jamming y definir criterios a tener a tener en cuenta en un sistema de este tipo.

Dedicatoria

A mi madre, por criarme para ser un hombre de bien y brindarme su apoyo incondicional, aún en los momentos más difíciles.

A mi padre, por sus grandes enseñanzas que me dio y por motivarme a seguir mis sueños en la gran cruzada que es la vida.

Agradecimientos

A mi asesor, el Dr. Manuel Augusto Yarlequé Medina, por su gran aporte a mis conocimientos que me permitieron comprender lo maravillosa que es la carrera que elegí.

A los miembros del grupo de tecnologías inalámbricas (GTI), por el apoyo brindado durante la realización de este trabajo.

Tabla de Contenidos

Índice de Figuras

Índice de Tablas

Introducción

Actualmente existe la problemática del mal uso de los UAVs civiles, los cuales gracias a una falta de regulación y sus características (cámaras, conexión con teléfonos inteligentes, etc.) son usado para cometer actos delictivos como espionaje, narcotráfico e incluso terrorismo. Por desgracia, si bien existen sistemas contra UAVs, estos están pensados, en su mayoría, para un entorno militar; por lo que el sector civil se encuentra en una situación vulnerable.

El presente trabajo busca facilitar el desarrollo de los sistemas contra UAVs de naturaleza civil, específicamente a aquellos que tengan como principal mecanismo de intercepción contra el UAV al jamming de GPS. Por ello, este trabajo de investigación bibliográfica tiene como objetivo principal recopilar de la mejor manera la información acerca del Sistema de Posicionamiento Global (GPS) y del mecanismo de jamming.

En el primer capítulo, se hablará acerca de la problemática y se justificará el porqué de esta investigación. En el segundo capítulo, se recopilará la información del GPS. En el tercer capítulo, se dará a conocer la teoría y criterios del jamming. Finalmente se dará una conclusión al trabajo y recomendaciones a aquellos que deseen usar este mismo como fuente para el diseño del jammer de señales GPS.

Capítulo 1 El Mal Uso de los Vehículos Aéreos No Tripulados en Entornos Civiles

1.1. Sistemas Aéreos No Tripulados

Un vehículo aéreo no tripulado, UAV por sus siglas en inglés, puede ser definido, tal como lo indica su nombre, como aquella aeronave que no cuenta con un piloto a bordo, sin embargo, es capaz de volar gracias a un control remoto o una programación de control [1]. En consecuencia, los sistemas aéreos no tripulados, también conocidos como UAS, son sistemas los cuales están compuestos por los UAVs y los elementos necesarios para permitir el vuelo de estos. Los componentes del UAS son [2]:

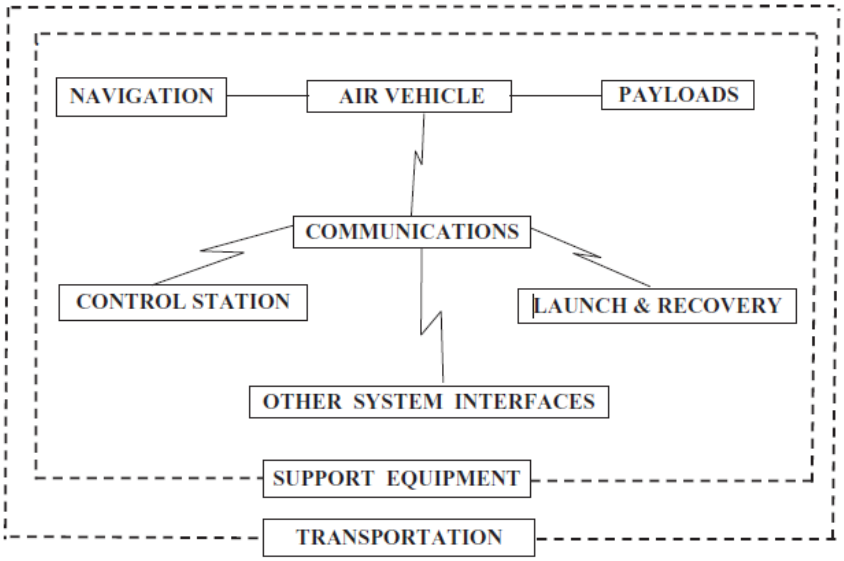


Figura 1.1 Diagrama de un UAS. Fuente: [2]

1.1.1. Estación de control (CS).

La estación de control es el centro de control de la operación y la interfaz hombre-máquina [2]. En este lugar el operador se comunica con el UAV mediante el sistema de comunicación, siendo así capaz de enviar ordenes tanto al UAV como a la cargar útil, y a su vez, de recibir información de estos mismos. También puede realizar la función adicional de planificación de vuelo del UAV, permitiendo que realice una misión de vuelo sin necesidad de un operador [3].

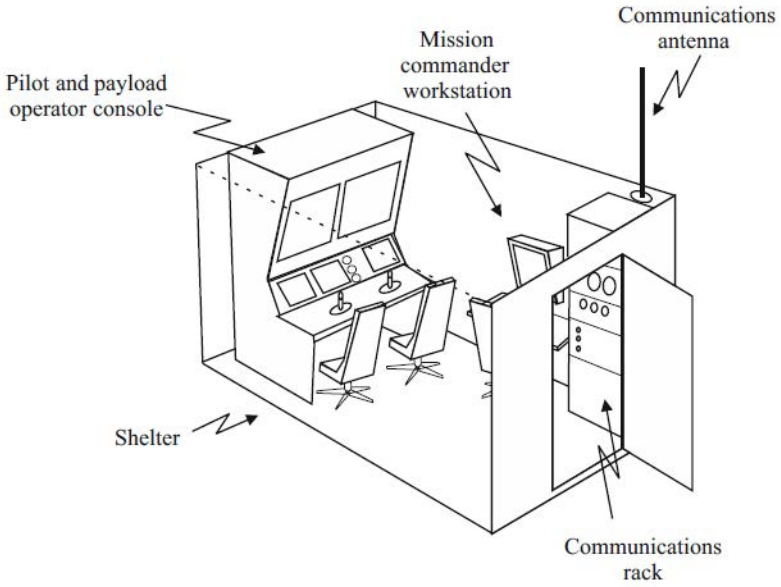


Figura 1.2 Ilustración de una CS. Fuente: [3]

1.1.2. Carga útil (Payload).

Tal como lo indica su nombre, la carga útil, es un peso adicional que carga el UAV con el fin de cumplir una tarea específica; las cuales son, por norma general, el motivo de la misión de vuelo del vehículo [2]. Estas cargas pueden ser destinadas a diferentes fines como: vigilancia y censado (cámaras electro-ópticas, cámaras infrarrojas o radares), transporte, comunicación o bélicos (armas de fuego) [4][3].

Figura 1.3 Ejemplo de un UAV equipado con un payload. Fuente: [4]

1.1.3. UAV.

Además de la definición dada anteriormente, los UAVs también pueden ser vistos como un sistema en sí mismo, los cuales están formados conformados por componentes como enlace de comunicación, equipamiento de control y estabilidad y equipamiento energético [2].

Figura 1.4 Ejemplificación de un UAV. Fuente:[5]

1.1.4. Sistemas de navegación.

Los sistemas de navegación son aquellos que indican su ubicación actual al UAV, normalmente en empleada en misiones programadas o cuando son manejados de manera remota. Actualmente la solución más eficiente es el sistema de posicionamiento global (GPS) [2]

1.1.5. Equipamiento de lanzamiento y recuperación.

Como su nombre indican, son los equipos que se encargan tanto de iniciar el vuelo de un UAV como finalizarlo [2]. Estos elementos pueden ser sumamente variable, pues mientras algunos vehículos requieren de equipos sumamente complejos, otro no requieren de prácticamente ninguno [4].

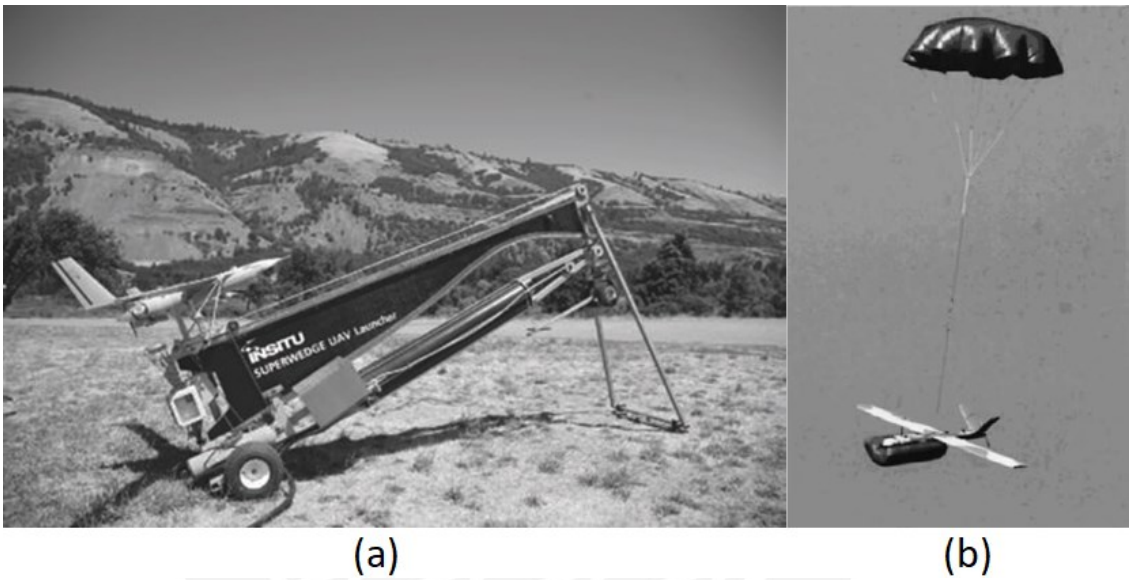


Figura 1.5 Ejemplo de equipamiento de lanzamiento (a) y equipamiento de recuperación (b). Fuente: (a) [4], (b) [2]

1.1.6. Sistema de Comunicaciones.

El sistema de comunicación es aquel que provee los radio enlaces entre el UAV y la estación de control. Estos radio enlaces son 2 [2]:

1.1.6.1. Uplink.

Este enlace lleva los mensajes desde la CS hasta la aeronave. Los datos que transporta pueden llegar a ser el plan de vuelo almacenado en la estación de control, las ordenes de

vuelo en tiempo real, comandos de control a la payload o información del posicionamiento de la estación actualizada [2].

1.1.6.2. Downlink.

Este enlace lleva los mensajes desde la aeronave hasta la CS. Los datos que transporta pueden llegar a ser la posición del UAV, información capturada por el payload o información del estado del vehículo (combustible, temperatura del motor, etc.) [2].

1.1.7. Interfaces.

Las interfaces son aquellos elementos que permiten la conexión entre los distintos elementos del sistema [2].

1.1.8. Interfaces con otros sistemas.

En entornos militares, el propio UAS es un elemento de un sistema más grande. Estas interfaces son aquellas que permiten la conexión de un UAS con uno de mayor jerarquía [2].

1.1.9. Equipos de soporte.

Son aquellos equipos que permiten alargar el tiempo de correcto funcionamiento del sistema. Estos equipos pueden ser herramientas de mantenimiento y pruebas, suministro de repuestos, suministro de combustible, entre otros [3].

1.1.10. Transportadores.

Debido a siempre se prefiere un UAS que sea móvil, se requiere un sistema de transporte capaz de movilizar a todos los elementos anteriormente mencionados [2].

Figura 1.6. Ejemplo de un transportador. Fuente: [2]

1.2. Sistemas Contra Sistemas Aéreos No Tripulados (C-UAS)

También conocidos como sistemas C-UAV, son aquellos sistemas que son diseñados para actuar en contra de los UAS, mediante la detección y/o intercepción de estos mismos [6].

Figura 1.7 Ilustración de un sistema C-UAS. Fuente: [6]

1.2.1. Técnicas de detección.

Como se mencionó anteriormente, un sistema C-UAS puede ser capaz de detectar UAS mediante el uso de diversas técnicas, siendo las más comunes las que se presentarán a continuación [6]:

1.2.1.1. Detección por radar.

Esta técnica consiste en un emitir una señal, la cual, al encontrarse con el objetivo a detectar, en este caso un UAV, ve una parte de su señal reflejada y es esta señal la cual finalmente llega a un receptor el cual con ayuda de un procesador puede llegar a determinar tanto la posición como la velocidad del objetivo [7]. Cabe resaltar, que este procesador debe contar con un algoritmo capaz de distinguir entre los UAVs objetivos y otros objetos voladores como los pájaros [6].

- **Ventaja:** Es capaz de detectar y seguir objetivos a varios kilómetros de distancia [8].
- **Desventaja:** Al desconocer las características del UAV, el detectarlo únicamente con este mecanismo es complicado [8].

1.2.1.2. Detección de emisión de radio-frecuencias.

Esta técnica consiste en escanear las frecuencias que se sabe son usadas por los UAVs a fin de poder detectar su presencia y usar algoritmos para determinar geográficamente un área en el que el dispositivo emisor de dichas frecuencias está ubicado, pues existe la posibilidad que sea un UAV [6].

- **Ventaja:** Es relativamente barato sumado al hecho que la mayoría de los UAVs comerciales emiten señales fáciles de detectar [6].

- **Desventaja:** No puede ubicar un objetivo en movimiento [8].

1.2.1.3. Detección electro-óptica.

Esta técnica consiste en detectar UAVs en función de las señales visuales percibidas por un equipo con sensores electro-ópticos [6].

- **Ventaja:** Numerosas opciones comerciales con diferentes precios y especificaciones [8].

- **Desventaja:** Bajo contraste entre el objetivo y otros elementos, por lo que es susceptible a confusión; requiere de iluminación para funcionar correctamente y puede verse afectado por fenómenos climáticos [8].

1.2.1.4. Detección infrarroja.

Esta técnica logra detectar a los UAVs midiendo las señales de calor emitidas por este mediante un sensor infrarrojo [6].

- **Ventajas:** Bajo índice de confusión con el fondo, debido a que únicamente ve las señales de calor; es capaz de trabajar en la noche y no es muy susceptible a fenómenos climáticos [8].

- **Desventaja:** La mayoría de los UAVs tienen una baja temperatura [8].

1.2.1.5. Detección acústica.

Esta técnica emplea una base de datos con los sonidos producidos por UAVs conocidos; por lo que, cuando se detecta un sonido, este es comparado esta base de datos para determinar si hay una presencia de UAV o no [6].

- **Ventajas:** Método de bajo costo y pasivo [8].
- **Desventajas:** Rango máximo de detección variable por fenómenos como el viento. No se pueden detectar UAVs no registrados en la base de datos. Posibilidad de error en entornos ruidosos como el urbano [8].

1.2.1.6. Detección por mecanismos combinados.

Esta técnica consiste en emplear múltiples sensores de detección en simultaneo, brindando así una detección más robusta, por lo que es usado en una gran variedad de soluciones en el mercado [6].

- **Ventaja:** Menos posibilidad de error [8].
- **Desventajas**: Mayor costo y complejidad [8].

1.2.2. Técnicas de intercepción.

Al igual que con las técnicas de detección, los sistemas C-UAS pueden emplear diversas técnicas de intercepción. De las cuales, las más comunes son [6]:

1.2.2.1. Jamming al operador.

Esta técnica, también conocida también como RF jamming, consiste en generar una señal de alta potencia en la frecuencia en la cual se encuentra el radio enlace entre el UAV y el

operador a fin de interrumpir la comunicación de estos dos. Una vez lograda la interferencia, el UAV puede llegar a aterrizar o regresar al punto de lanzamiento [6].

- **Ventaja:** Poca posibilidad de daños colaterales por caída repentina del UAV al ser interceptado [6].
- **Desventaja:** Puede llegar a interferir otros sistemas de comunicación [6]

1.2.2.2. Jamming al sistema de navegación.

Esta técnica, conocida también como GNSS jamming, al igual que el anterior, busca interrumpir una comunicación. Pero en este caso el objetivo es el radio enlace con el GNSS, el sistema de navegación por satélite, que el UAV usa como guía para su vuelo. Al generar satisfactoriamente la interferencia, el UAV puede flotar en su posición actual, aterrizar o regresar a su punto de lanzamiento [6].

- **Ventaja:** Poca posibilidad de daños colaterales por caída repentina del UAV al ser interceptado [6].
- **Desventaja:** El uso de esta técnica puede causar interferencia en el uso de GNSS de los dispositivos cercanos [6].

1.2.2.3. Spoofing.

Esta técnica, consiste en tomar el control del UAV al generar una señal que se hace pasar por el operador.[6]

- **Ventaja:** Es la técnica que brinda mayor efectividad [8].

- **Desventajas:** Es la técnica individual más difícil de implementar y puede no ser efectiva con todos los UAVs [6].

1.2.2.4. Intercepción por láser.

Esta técnica consiste en emitir un láser de alta potencia con el fin de afectar un área vital del UAV y lograr que este colisione contra el suelo [6].

- **Ventaja:** Cuenta con un alto grado de efectividad a la hora de neutralizar al UAV [8].
- **Desventajas:** Interrumpe físicamente el vuelo lo que puede desencadenar la caída brusca del UAV y daño colateral [6]. Costo elevado [8].

1.2.2.5. Intercepción por redes.

Esta técnica consiste en usar redes a fin de enredar al UAV y a sus rotores [6].

- **Ventaja:** Se puede usar una red usada para evitar la caída brusca del UAV atrapado [6].
- **Desventaja:** Interrumpe físicamente el vuelo lo que puede desencadenar la caída brusca del UAV y daño colateral [6].

1.2.2.6. Intercepción por proyectiles.

Esta técnica consiste en usar municiones para destruir el UAV [5]

- **Ventaja:** Facilidad a la hora de implementar, pues basta con tener acceso un arma de fuego [9].

- **Desventaja:** Interrumpe físicamente el vuelo lo que puede desencadenar la caída brusca del UAV y daño colateral [6].

1.2.2.7. Intercepción por métodos combinados.

De igual manera que la detección, existe la técnica que consiste simplemente en emplear múltiples técnicas de intercepción [6].

- **Ventaja:** Mayor la eficiencia [6].
- **Desventaja:** Implementación más costosa y compleja [6].

1.2.3. Clasificación.

De acuerdo a como se ha implementado el sistema C-UAS, se le puede categorizar en una de las siguientes categorías:

1.2.3.1. Implementadas en tierra.

Son aquellos sistemas que están diseñados para permanecer en el piso, ya sea de manera dinámica o estática [6]

1.2.3.2. Sostenida por mano.

Son aquellos sistemas diseñados para ser usados por un usuario mediante su mano, presentan una forma similar a un arma [6].

1.2.3.3. Implementadas en UAVs.

Son aquellos sistemas que están diseñados para estar montados encima de un UAV [6].

1.2.4. Retos.

Los sistemas C-UAS presentan los siguientes retos a superar para establecerse como una tecnología madura [6]:

1.2.4.1. Efectividad de la detección.

Este reto consiste en conseguir que el sistema tenga un grado alto de efectividad detectando UAVs. Pues como se mencionó anteriormente, existen múltiples métodos de detección; sin embargo, ninguno es perfecto, pues tienen desventajas. Sumado a esto, está el hecho que se están realizando estudios para desarrollar UAS capaces de burlar la detección de los mecanismos de detección actuales, por lo que las técnicas de detección también tiene que ir en constante mejora [6]

1.2.4.2. Falso positivos y falsos negativos.

Este reto consiste encontrar una correcta sensibilidad para el mecanismo de detección. Pues si el sistema es demasiado sensible podría comunicar alarmas para presencias inexistentes; pero si muy poco sensible, puede estar presente un UAV peligroso sin que el sistema comunique, que es lo menos deseable posible [6].

1.2.4.3. Distinción entre UAV maliciosos e inocente.

Este reto consiste en que el sistema sea capaz de saber diferenciar cuando un UAV está siendo usado de manera correcta y cuando está siendo usado de manera maliciosa, debido a que se estima que el uso de los UAVs va a ser común. Actualmente no hay ningún sistema C-UAS capaz de realizarlo [6].

1.2.4.4. Riesgos de la intercepción.

Este reto consiste en que el sistema reduzca los riesgos que presentan sus técnicas de intercepción, pues todos los mecanismos de interdicción presentan riesgos. Por ejemplo, hay técnicas que afecten físicamente el vuelo del UAV y pueden hacer que este caiga de manera abrupta lo cual es peligroso en ambientes con multitudes como el urbano; por otro lado, los mecanismos de interferencia presentan el riesgo de afectar comunicaciones legitimas en el área cercana al sistema [6].

1.2.4.5. Efectividad de la intercepción.

Al igual que con la detección, este reto consiste en conseguir que el sistema tenga un grado alto de efectividad interceptando UAVs. Pues los mecanismos de interdicción también tienen problemas que deben ser superados. Además se están realizando investigaciones para diseñar UAS que no se ven perjudicados por estas técnicas, por lo que las técnicas de intercepción también tiene que ir en constante mejora [6].

1.2.4.6. Legalidad de la Intercepción.

Este reto consiste en que el mecanismo de intercepción no vaya en contra de las leyes del lugar donde se va a implementar el sistema. Pues puede darse el caso, por diversos motivos, que un mecanismo de intercepción sea ilegal en el país; por ejemplo, en los países desarrollados, el jamming está prohibido.[6].

1.2.4.7. Falta de estándares.

El reto consiste en establecer un estándar, pues al ser una tecnología relativamente nueva, no existe un estándar el cual seguir, por lo que no se puede discriminar correctamente la calidad de un sistema frente a otro [6].

1.3. Análisis de la Problemática

1.3.1. Realidad problemática.

1.3.1.1. Mal uso de los UAS civiles.

Hoy en día, la proliferación del uso de los UAVs civiles, con herramientas como cámaras, compatibilidad con teléfonos inteligentes o la capacidad de transportar objetos, ha generado una gran vulnerabilidad en la seguridad ciudadana; pues estos pueden llegar a ser usados con fines malévolos tales como espionaje, contrabando e incluso terrorismo [10][11][12]. Sumado a esto, está la posibilidad de ser modificados, para realizar de mejor manera las actividades delictivas anteriormente mencionados de mejor manera, o llegar a ser una amenaza aún más peligrosa, convirtiéndose en misiles guiado o un sistema de ataque aéreo [13].

1.3.1.2. Accesibilidad a sistemas C-UAS.

Pese a existir soluciones para la problemática que representan el mal uso de los UAVs, los C-UAS. Estos no están muy presentes en un entorno civil debido a que, en su mayoría, están pensados para un mercado militar, por lo que son sumamente costosos [13]. Sumado al alto costo, están sus características adecuadas para entornos militares tales como mecanismos de detección altamente sensibles e interdicción de alta potencia, los cuales, en conjunto, hacen que estas soluciones sean inviables para un entorno civil [10].

1.3.2. Planteamiento del problema.

Se plantea como problema a solucionar la falta de sistemas C-UAS en el entorno civil.

1.3.3. Planteamiento de la solución.

Se plantea como solución, el diseño e implementación de un dispositivo jammer de señales GPS, el cual pueda ser usado como un C-UAS de naturaleza civil o como parte de uno.

1.3.4. Justificación de la solución.

Debido al entorno urbano, el cual es muy variable y complicado de parametrizar, los mecanismos de detección de los sistemas C-UAS deberían tener una alta complejidad y en consecuencia un alto costo. Pues de no ser así, la tasa de falsos negativos y falsos positivos sería sumamente alta. En consecuencia, se considera que un sistema C-UAS de naturaleza civil, el cual no debe tener un costo muy elevado, no debe contar con un mecanismo de detección.

Un sistema C-UAS de naturaleza civil no puede hacer uso de aquellos mecanismos de intercepción que puedan generar la caída abrupta del UAV, pues esto puede generar daños colaterales, tanto a personas como a objetos. Por lo que las estrategias como el uso de láseres, redes o proyectiles y sus combinaciones no pueden ser usados.

El mecanismo de intercepción de spoofing es un mecanismo que no genera la caída abrupta del UAV y presenta una alta eficacia. Sin embargo, su implementación es sumamente complicada y con un funcionamiento limitado a UAVs específicos. Por lo que, si quisiéramos que se desempeñe bien frente a toda la gama de UAVs civiles, el costo podría llegar a incrementarse, por lo que no se considera viable para un sistema C-UAS de entorno civil.

El mecanismo de intercepción de jamming al operador, también es un mecanismo que no genera como daño colateral la caída del UAV. Sin embargo, no todos los UAS operan de la misma manera, por lo que, si se quisiera que se eficaz con muchos UAVs civiles, al igual que con el spoofing, el costo de su diseño e implementación puede incrementarse, por lo que tampoco sería considerado viable para un sistema C-UAS de entorno civil.

El mecanismo de intercepción de jamming al GNSS sería el más adecuado para un sistema C-UAS de naturaleza civil. Debido a que el uso de GNSS es muy utilizado en los UAVs civiles; sumado a que las señales que usan estos sistemas son conocidas por lo que facilita desarrollar un jammer contra estas por un costo relativamente bajo. Al ser el sistema de navegación global (GPS) el GNSS más usado por los UAVs, y por todos los dispositivos en general, es adecuado para ser el GNSS a bloquear por el jamming. Cabe destacar, que, si bien el jammer es diseñado teniendo el GPS como GNSS objetivo, al usar todos los GNSS bandas cercanas, con los correctos cambios, este sistema puede ser escalable y ser capaz de bloquear todos los GNSS.

Pese a ser seleccionada como la estrategia de intercepción más adecuada para un sistema C-UAV de naturaleza civil, el sistema puede no llegar a ser efectivos con todos los UAVs civiles todo el tiempo. Debido a que estos pueden hacer uso de otro GNSS o ser controlado de manera que no necesite del GPS. Adicionalmente, el sistema tampoco tiene porque ser efectivo frente a UAVs militares, pues estos cuentan con características diferentes de los UAVs civiles.

1.3.5. Objetivos.

1.3.5.1. Objetivo general.

El presente trabajo de investigación busca recopilar y resumir la información acerca del GPS y de los jamming. Para que futuros trabajos que deseen desarrollar la solución propuesta anteriormente, tengan una fuente de información que facilite su realización.

1.3.5.2. Objetivos específicos.

Los objetivos específicos que se plantean para lograr el general son los siguientes:

- Documentar acerca del Sistema de Navegación Global (GPS)

- Identificar las diferentes técnicas empleadas para realizar jamming
- Definir criterios a tener a tener en cuenta en un sistema de jamming

Capítulo 2 Sistema de Posicionamiento Global (GPS)

Los sistemas de navegación global por satélite (GNSS) son aquellos sistemas que permiten determinar la posición de un punto en la superficie terrestre mediante el uso de satélites artificiales [14]. Siendo el primero y más usados de estos sistemas, el Sistema de Posicionamiento Global, también conocido como GPS por sus siglas en inglés [15].

2.1. Servicios

2.1.1. Servicio de posicionamiento estándar (SPS).

Este servicio está destinado para los usuarios civiles. Este es el servicio de navegación más usado en todo el mundo [16].

2.1.2. Servicio de posicionamiento preciso (SPP).

Este servicio está destinado a usuarios autorizados de agencias gubernamentales militares y seleccionadas de EE. UU. Cuenta con mecanismos que lo hacen más resistente al jamming y al spoofing que el SPS [16].

2.2. Segmentos

2.2.1. Segmento espacial.

Este consiste en una constelación de satélites conformada nominalmente por 24 satélites de órbita terrestre media (MEO). Estas orbitas son circulares y están inclinadas 55° grados respecto al plano ecuatorial, tienen un radio de 26 559 Km y un periodo orbital de 11 horas con 58 minutos. Actualmente, hay 31 satélites en operación, por lo que se ha tenido que hacer modificaciones en la constelación nominal a fin de poder introducir a los satélites excedentes [15].

Cada satélite GPS cuenta con un reloj atómico abordo, el cual esta sincronizado a una escala de tiempo del sistema interno, denominado tiempo del sistema GPS. Además, estos transmiten las señales que permiten determinar la ubicación de los receptores, denominados señales de navegación [16].

A lo largo de los años, la constelación ha sido formada por diferentes satélites; los cuales se agrupan en los siguientes bloques [15]:

- Bloque I: Conformado por los satélites de prueba, actualmente ninguno se encuentra en operación [15][17].
- Bloque II/IIA: Conformado por los satélites lanzados entre el 1900 y el 1997, transmiten las señales de código C/A en la frecuencia L1 y las señales de código P(Y) en las frecuencias L1 y L2. Actualmente se encuentra no se encuentra ninguno en operación [17]
- Bloque IIR: Conformado por los satélites lanzados entre el 1997 y el 2004, destinados a reemplazar a los satélites del bloque IIA. Estos transmiten todas las señales de los satélites anteriores; además, de contar con ciertas variaciones en sus especificaciones, como una antena con un haz más angosto en comparación a sus predecesores. Actualmente se encuentra 10 satélites en operación [15][17].
- Bloque IIR-M: Conformado por los satélites lanzados entre el 2005 y el 2009. Estos transmiten todas las señales que transmite el bloque IIR; además, de las segundas señales civiles, L2C y las nuevas señales militares de código M. Actualmente se encuentra 7 satélites en operación [17].

- Bloque IIF: Es aquel bloque conformado por los satélites lanzados entre el 2010 y el 2016. Estos transmiten las mismas señales que el bloque IIR-M; además, de las terceras señales civiles, L5C. Actualmente se encuentran 12 satélites en operación [17].

- Bloque III/IIIF: Es el bloque todavía no ha sido completado. Los satélites que la conforman están pensados para transmitir las mismas señales que el bloque IIF; además, de las cuartas señales civiles, L1C. Actualmente se encuentran solamente dos satélites en operación [17].

2.2.2. Segmento de control.

El segmento de control es el responsable del monitorear, comandar y controlar la constelación de satélites del GPS. Este monitorea las señales que transmite los satélites y la salud de los mismos, actualiza los mensajes de navegación y resuelve las anomalías que presenten los equipos [15].

2.2.3. Segmento de usuario.

El segmento de usuario es el equipo de recepción GPS del usuario, al que anteriormente se ha referido como receptor GPS. Actualmente los receptores se encuentran dentro de muchos dispositivos de uso diario como celulares, automóviles, etc. Los componentes de un equipo de recepción está compuesto por 5 elementos: la antena, el receptor, el procesador, el dispositivo I/O y la fuente de poder [16].

2.3. Señales de Navegación

Los satélites que conforman la constelación del GPS transmiten diversas señales de manera simultánea. Todas estas señales, denominadas señales de navegación, presentan una polarización circular derecha (RHCP) y hacen uso de las siguientes frecuencias portadoras [14]:

- 1575.42 MHz, denominada Link 1 o L1.
- 1227.60 MHz, denominada Link 2 o L2.
- 1176.45 MHz, denominada Link5 o L5.

Los datos que son enviados en esta señal, son denominados datos de navegación. Dentro de estos datos, se encuentran los datos de efemérides, los cuales permiten determinar con precisión la ubicación del satélite que envió los datos [15].

Estas señales cuentan con una modulación por desplazamiento de fase, principalmente la modulación por desplazamiento de fase binario en conjunto con la técnica de espectro ensanchado por secuencia directa (BPSK-DSSS) y derivadas de esta, tales como la modulación BOC [16].

2.3.1. Espectro ensanchado por secuencia directa.

Las comunicaciones de espectro ensanchado son aquellas que utilizan un ancho debanda mucho mayor al mínimo que necesitan. Una de las técnicas que se usan para esto es denominado espectro ensanchado por secuencia directa (DSSS) [18].

El espectro ensanchado por secuencia directa utiliza una secuencia especifica de ceros y unos, denominados códigos pseudoaleatorios (PRN), para aumentar el ancho de banda de la señal. La tasa con la que estos son generados es denominada tasa de chips, R_c, el cual es mucho más alta que la tasa de datos, R_b. Por lo que, al multiplicarse, la señal resultante presenta un

ancho de banda mucho más alto que la señal de datos original. Esta señal codificada es la señal que finalmente es modulada en la portadora [18].

El receptor para poder desmodular la señal tiene que ser capaz de generar el mismo código PRN utilizado para codificar los datos de manera sincronizada al receptor. Tras ser pasada a banda base, la señal recibida es correlacionada con el código PRN en el receptor; lo cual permite que potencia se concentre en un ancho de banda más angosto, el de la señal de datos. Por lo que la hace que la relación señal a ruido, SNR, aumente. A este aumento de SNR se le denomina ganancia de procesamiento, G_P. Y permite que la señal, al emplear DSSS, sea más resistente al ruido. Para calcular la G_P se calcula mediante la siguiente formula [18].:

$$G_P = \frac{R_c}{R_b} \qquad (2.1)$$

G_P: Ganancia de procesamiento (adimensional)

R_c: Tasa de chips (en bps)

R_b: Tasa de datos (en bps)

Un grupo de códigos PRN es una agrupación de códigos PRN los cuales son generados de manera similar y tienen la misma longitud; sin embargo, tienen una correlación muy baja entre sí mismos, casi ortogonal. Esto permite que diferentes comunicaciones que emplean diferentes códigos PRN puedan usar un mismo espectro, sin interferencia los unos a los otros. Esto es denominado acceso múltiple mediante división de código (CDMA) [18].

Los códigos PRN se clasifican de acuerdo a la relación entre la longitud de secuencia, L, y la ganancia de procesamiento, G_P. Los códigos cortos, son aquellos que tienen una longitud menor o igual a la ganancia de procesamiento, $L \leq G_P$; y en consecuencia toda la secuencia del código es transmitida al menos una vez en cada bit de datos. Por el otro lado, los códigos largos son aquellos que tienen una longitud mucho mayor a la ganancia de procesamiento, $L >> G_P$, en

consecuencia, se requieren muchos bits para que el código sea transmitido completamente. Cabe mencionar que el código largo es más resistente a los ataques de jamming que los códigos cortos [18].

2.3.2. Tipos de señales de navegación.

Las señales de navegación que se transmiten por los diferentes satélites del GPS, se pueden agrupar en los siguientes grupos:

2.3.2.1. Señales legacy.

Este grupo está formado por aquellas señales que empezaron a ser transmitidas desde antes que se añadieran satélites del bloque IIR-M a la constelación GPS. Estas señales modulan directamente la información de navegación, sin ninguna codificación o mecanismo de detección y corrección de errores [16].

2.3.2.1.1. Señales de código C/A.

Estas señales son denominadas así debido a que los códigos que usan pertenecen al grupo de los códigos C/A (Coarse/Adquisition). Emplean una modulación BPSK-DSSS y usan como portadora a L1. Estas fueron las primeras señales en ser usadas para SPS. Los parámetros principales de esta señales se pueden observar en la Tabla 2.1 [14].

2.3.2.1.2. Señales de código P(Y).

Estas señales son denominadas así debido a que usa los códigos PRN que utilizan pertenece al grupo de los códigos P, los cuales al ser encriptados son denominados códigos Y. Emplean una modulación BPSK-DSSS. Estas fueron las primeras señales en ser usadas para el PPS [14]. Cada satélite transmite dos de estas señales, ambas con los mismos datos

y el mismo código PRN, pero, una usando como portadora L1 y la otra L2. Los parámetros principales de esta señales se pueden observar en la Tabla 2.1 [16].

2.3.2.2. Señales modernizadas.

Este grupo está formado por aquellas señales que fueron añadidas al GPS durante y después del bloque IIM [16]. Todas las señales civiles de este grupo cuentan con códigos PRN más largos, mejoras en la codificación de datos y una componente sin datos que permite un mejor seguimiento de la señal por parte del receptor, denominado piloto [15]

2.3.2.2.1. Señales L2C.

Estas señales son las primeras señales para SPS que utiliza como portadora a L2; siendo creadas para satisfacer necesidades comerciales. Emplean modulación BPSK-DSSS. La componente con datos de este tipo de señales usa un código PRN del grupo de los códigos L2CM. Mientras que la componente piloto usa un código PRN del grupo de los códigos L2CL. La multiplicación de estas dos componentes chip por chip da lugar a una señal L2C propiamente dicha. Los datos de este tipo de señales son transmitidos a 25 bps, lo cual es bajo en comparación a las demás señales que tienen una tasa de 50 bps, y cuentan con un FEC 1/2 como mecanismo de corrección de errores. Los demás parámetros de la señal se presentan en la Tabla 2.1 [16].

2.3.2.2.2. Señales de código M.

Estas señales obtienen su nombre porque los códigos PRN que utilizan pertenece al grupo de los códigos M, con un uso exclusivamente para militares; por lo que estas señales son para PPS. Se espera que estas señales eventualmente reemplacen a las señales de código P(Y), dado que cuentan con mayor seguridad, aislamiento de las señales civiles,

mejoras para detectar, seguir y desmodular la señal. Al igual que sus predecesoras, cada satélite transmite dos de estas señales, ambas con los mismos datos y el mismo código PRN, pero, una usando como portadora L1 y la otra L2. Estas señales fueron las primeras en emplear una modulación diferente de una BPSK-DSSS, la modulación BOC. Los parámetros principales de esta señales se pueden observar en la Tabla 2.1 [16].

2.3.2.2.3. Señales L5C.

Estas señales son las primeras que utilizan como portadora a L5, usadas para SPS, específicamente para aplicaciones de seguridad. La componente con datos de este tipo de señales usa un código PRN del grupo de los códigos I5. Mientras que, la componente piloto usa un código PRN del grupo de los códigos Q5. Estas dos componentes son transmitidas en cuadratura en simultaneo, por lo que se podría decir que son dos modulaciones BPSK-DSSS en cuadratura o una modulación QPSK-DSSS. Los datos de esta señal cuentan con el mismo FEC que usa L2C, además de con un codificación mediante los códigos de sincronización de Neuman-Hofman. Los parámetros principales de esta señales se pueden observar en la Tabla 2.1 [16].

2.3.2.2.4. Señal L1C.

Estas señales usan como portadora L1, para SPS. La componente de datos de este tipo de señales usa un código PRN del grupo de los códigos $L1C_D$. Mientras que, la componente piloto usa un código PRN del grupo de los códigos $L1C_P$ [14]. Los datos de la señal cuentan con una codificación adicional, generado por un código secundario. Su modulación es una modulación BOC modificada. Los parámetros principales de esta señales se pueden observar en la Tabla 2.1 [15].

Tabla 2.1. Parámetros de las señales GPS. Fuente: Elaboración propia

Señales	Portadoras	Longitud del código PRN (chips)	Tasa de código PRN (Mcps)	Tasa de datos (bps)	Modulación	Ancho de banda entre nulos (MHz)
Señales de código C/A	L1	1023	1.023	50	BPSK-DSSS	2.046
Señales de código P(Y)	L1, L2	P: 6187104000000 Y: Generado criptográficamente	10.23	50	BPSK-DSSS	20.46
Señales L2C	L2	CM: 10,230 CL: 767 250	CM: 0.5115 CL: 0.5115	25	BPSK-DSSS	2.046
Señales de código M	L1, L2	Generado criptográficamente	5115	50	BOC	30.69
Señales L5C	L5	I5: 10 230 Q5: 10 230	10.23	50	QPSK-DSSS	20.46
Señales L1C	L1	$L1C_D$: 10 230 $L1C_P$: 10 230	1.023	50	BOC	4.092

2.4. Funcionamiento del Sistema

Dado que todas las señales de navegación usan una modulación BPSK-DSSS o derivada, se puede hacer uso del CDMA. Por lo que todos los satélites pueden transmitir sus señales en el mismo espectro sin interferirse mutuamente. Adicionalmente, los códigos PRN brindan otro beneficio, el de la identificación; pues el código PRN que utiliza un satélite para cualquier tipo de señal es único en la constelación. Por lo que si se obtiene el código PRN de una señal, se sabe el satélite del que proviene [15]

Como se mencionó anteriormente, para que el receptor pueda recuperar la información de una señal que emplea DSSS, este tiene que ser capaz de generar el código PRN con el que se codifico y estar sincronizado al transmisor. En el caso del receptor GPS, este es capaz de replicar todos los códigos PRN utilizados en un tipo de señal. Por lo que, en el caso ideal en el que el receptor este sincronizado al tiempo del sistema GPS, cuando una señal de este tipo llega al receptor, la cual está desfasada respecto al tiempo del sistema GPS debido al tiempo que le tomo llegar a ese punto, y se compara el código PRN de esta señal con su réplica generada en el receptor se puede determinar su desfase. Con este desfase se estima una distancia entre la ubicación del

receptor y del satélite, que puede ser calculada por los datos de efemérides que se obtienen al desmodular la señal recibida. Repitiendo este proceso dos veces más, el receptor puede tener una mejor aproximación acerca de su ubicación, la que estaría en la intersección entre tres esferas centradas en los tres satélites localizados y con radios iguales a las distancias de estos al receptor [16].

Por desgracia, los receptores GPS no sueles estar sincronizados con el tiempo del sistema GPS, pues cuentan con un reloj de menor calidad a los presentes en los satélites, sumado a que presentan un desfase cada vez que son prendidos. Por lo que, para poder sincronizarse con el tiempo del sistema GPS, y poder determinar su ubicación como se explicó anteriormente, el receptor necesita 4 señales de diferentes satélites, siendo la cuarta con la cual determinar el desfase de su reloj respecto al tiempo del sistema GPS. Es oportuno mencionar que la recepción de más señales de diferentes satélites puede aumentar la precisión del receptor, sin embargo, el mínimo necesario es cuatro [16].

Capítulo 3 Teoría de Jamming

El termino jamming hace referencia a las acciones que buscan interferir la transferencia de información de una comunicación electrónica. Se le denomina jammer aquel dispositivo que genera estas acciones [19].

En las comunicaciones inalámbricas, el jamming a una comunicación ocurre cuando en el receptor que recibe la señal transmitida en el transmisor, a la cual se le denomina como señal objetivo, se genera una interferencia debido a la inserción una señal no deseada, denominada señal de jamming [18].

3.1. Relación Jamming a Señal (JSR)

Un parámetro importante cuando se habla de jamming es la relación jamming a señal, denominada como JSR por sus siglas en ingles. Este se obtiene mediante el cociente entre la potencia de la señal de jamming y la de la señal objetivo en el receptor. Esta se puede calcular mediante la siguiente expresión [19]:

$$JSR = ERP_J - ERP_S - L_J + L_S + G_{RJ} - G_R \quad (3.1)$$

JRS: Relación jamming a señal (en dB)

$EIRP_J$: Potencia isotrópica radiada equivalente por el jammer (en dBm)

$EIRP_S$: Potencia isotrópica radiada equivalente por el transmisor (en dBm)

L_J: Perdidas por propagación desde el jammer hasta el receptor (dB)

L_S: Perdidas por propagación desde el transmisor hasta el receptor (dB)

G_{RJ}: Ganancia de la antena receptora en dirección al jammer (dBi)

G_R: Ganancia de la antena receptora en dirección al receptor (dBi)

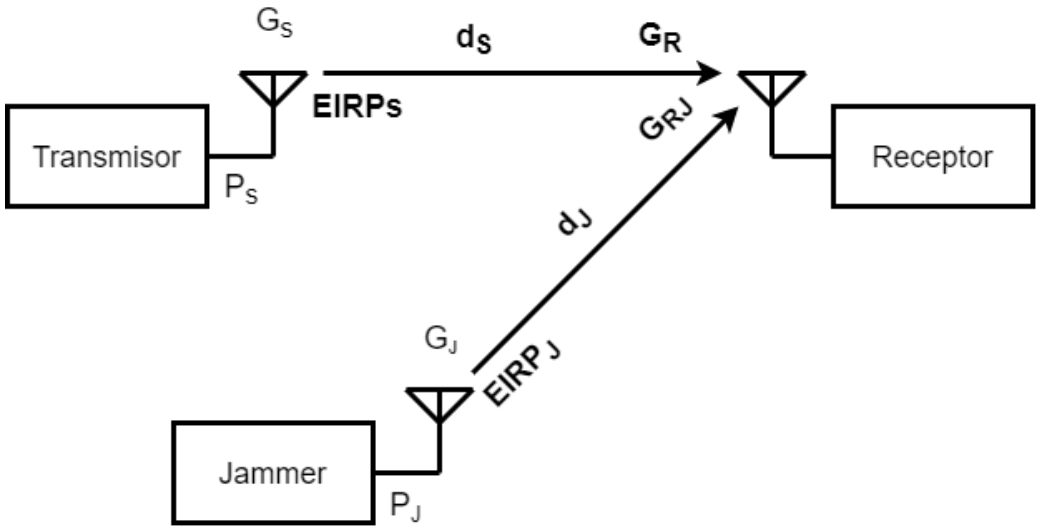


Figura 3.1. Diagrama de Jamming. Fuente [19]

3.1.1. Modelos de pérdidas por propagación.

Los cálculos de las pérdidas por propagación varían de acuerdo a la frecuencia de la señal y la geometría del camino. Por lo que para poder estimar un valor de perdidas, se puede hacer uso de los siguientes modelos de propagación [19]:

3.1.1.1. Propagación de línea de vista (LOS).

Este modelo considera que no hay reflectores significativos entre el transmisor y el receptor y que las antenas de estos se encuentran ubicado a una altura mucho mayor en comparación a la longitud de onda. Las pérdidas para este modelo se calculan con la siguiente formula [19]:

$$\mathrm{L} = 32.44 + 20\log_{10} d + 20\log_{10} F \qquad (3.2)$$

L: Perdidas (en dB)

d: Distancia entre transmisor y receptor (en Km)

F: Frecuencia de la señal (en MHz)

Cabe añadir, que el terreno obstruye el camino de la señal, se suele usar el modelo de línea de vista, pero considerando perdidas adicionales. Estas son denominadas perdidas por difracción de filo de cuchillo [19].

3.1.1.2. Propagación de dos rayos.

Este modelo considera que las antenas están cerca de una única superficie reflectora y que el patrón de la antena es lo suficientemente ancho como para irradiar en dirección a esta. Las pérdidas para este modelo se calculan con la siguiente formula [19]:

$$L = 120 + 40\log_{10} d + \log_{10} h_T + \log_{10} h_R \quad (3.3)$$

L: Perdidas en (en dB)

d: Distancia entre transmisor y receptor (en Km)

h_T: Altura del transmisor (en m)

h_R: Altura del transmisor (en m)

Para determinar el modelo de propagación adecuado se utiliza la siguiente tabla [19]:

Tabla 3.1. Modelo de propagación adecuado. Fuente [19]

Frecuencia y entorno	Modelo de propagación	
Alta frecuencia y/o lejos del suelo y/o antenas de haz angosto	**Línea de vista**	
Señal cerca al suelo o agua y frecuencia menor a las de microondas	Longitud del enlace menor a la zona de Fresnel	**Línea de vista**
	Longitud del enlace mayor a la zona de Fresnel	**Dos rayos**
El camino de la señal es obstruido por el terreno	**Línea de vista** con pérdidas adicionales por difracción de filo de cuchillo	

3.2. Jamming en Señales Analógicas y Digitales

3.2.1. Jamming en señales analógicas.

Cuando se realiza un jamming a señales analógicas, es necesario tener un JSR relativamente alto, normalmente de 10dB, además de estar operando el 100% del tiempo.

Pues si la señal deseada no es totalmente opacada por la señal de jamming, los operadores de los receptores pueden llegar a ser capaces entender el mensaje, que normalmente es un audio, pese a la interferencia generada [19].

3.2.2. Jamming en señales digitales.

Cuando se realiza un jamming a señales digitales, se busca atacar la señal con el fin de hacerla ilegible para el demodulador digital, lo cual se puede lograr mediante la interferencia de la sincronización o aumentar la tasa de bits errados, también denominada como BER. Siendo principalmente el método común el aumento de la tasa del BER, ya que actualmente la sincronización suele ser bastante robusta [19].

Normalmente, cuando el JSR llega a un valor de 0 dB, el BER llega a un valor bastante cercano al máximo posible, 50%. Cabe aclarar que en sistemas que emplean algún tipo de ensanchamiento del espectro, como el GPS que emplea DSSS, la eficiencia del JSR en el receptor se ve atenuado por la ganancia de procesamiento [19].

Otro tema a considerar en el jamming a señales digitales es ciclo de operación. Pues en las comunicaciones digitales, si una señal es ilegible un tercio del tiempo, esta es considerada inútil. Esto permite a que el dispositivo jammer pueda llegar a necesitar operar solamente un tercio del tiempo; sin embargo los códigos de corrección de errores puede incrementar el ciclo de trabajo necesario [19].

3.3. Estrategias de Jamming

Existen diferentes técnicas que se pueden emplear para realizar jamming. La efectividad de cada una depende principalmente de las características de la señal a la que se planea interferir [18].

3.3.1. Jamming por ruido.

Esta estrategia consiste en modular la portadora de la señal de jamming con ruido aleatorio, comúnmente gaussiano. La señal de jamming resultante ocupa una parte del espectro usado por la señal objetivo, esto con el fin del reducir el SNR de la señal objetivo. Existen diferentes tipos de jamming por ruido de acuerdo a la porción de ancho de banda del objetivo que ocupa [18]:

3.3.1.1. Jamming por ruido de banda completa (BBN jamming).

Esta estrategia como indica su nombre, consiste en insertar el ruido en la totalidad de la banda que utiliza la señal objetivo. Este método es útil frente a cualquier tipo de señal, sin embargo, puede llegar a consumir mucha energía e interferir en comunicaciones aliadas que ocupen la misma banda [18].

3.3.1.2. Jamming por ruido de banda parcial (PBN jamming).

Esta estrategia como indica su nombre, consiste en insertar el ruido en múltiples canales del espectro no necesariamente continuos, de la banda que utiliza el objetivo. Este método suele ser más eficiente que el BBN jamming debido a que no emplea tanta energía [18].

3.3.1.3. Jamming por ruido de banda angosta (NBN jamming).

Esta estrategia consiste en insertar el ruido en únicamente un canal del espectro que utiliza el objetivo, ya sea el canal completo o solamente una parte de él [18].

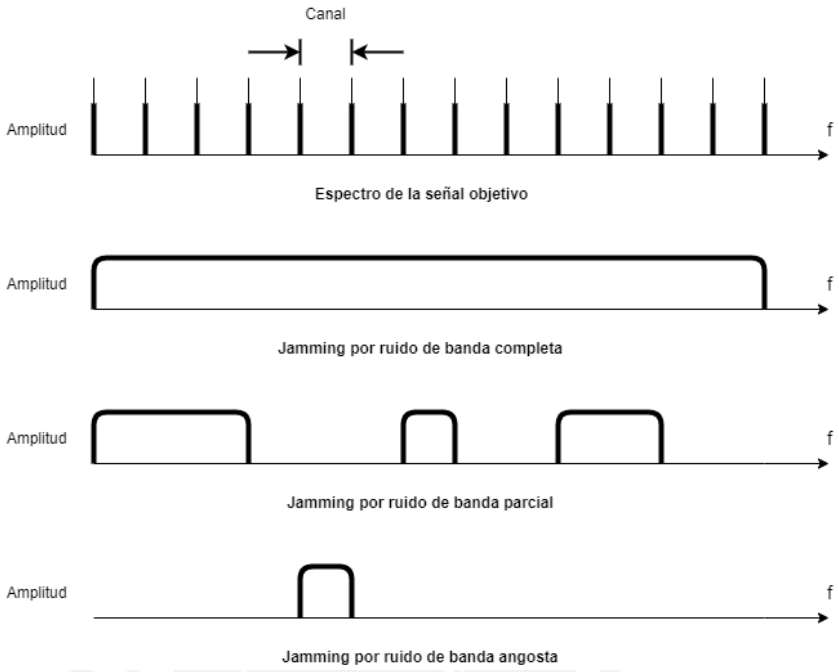


Figura 3.2. Ilustración de los diferentes tipos de jamming por ruido. Fuente [18]

3.3.2. Jamming por tonos.

Esta estrategia consiste en poner tonos en lugares estratégicos en el espectro que utiliza el objetivo con el fin de interferir en la comunicación. Tanto la ubicación del tono, como la fase relativa respecto a la señal objetivo pueden llegar a afectar el desempeño de esta estrategia. Este se puede dividir de acuerdo al número de tonos que inserta en el espectro:

3.3.2.1. Jamming por tono único.

Esta estrategia, tal como lo indica su nombre, inserta únicamente un tono [18].

3.3.2.2. Jamming por tonos múltiples.

Esta estrategia, tal como indica su nombre, inserta más de un tono [18].

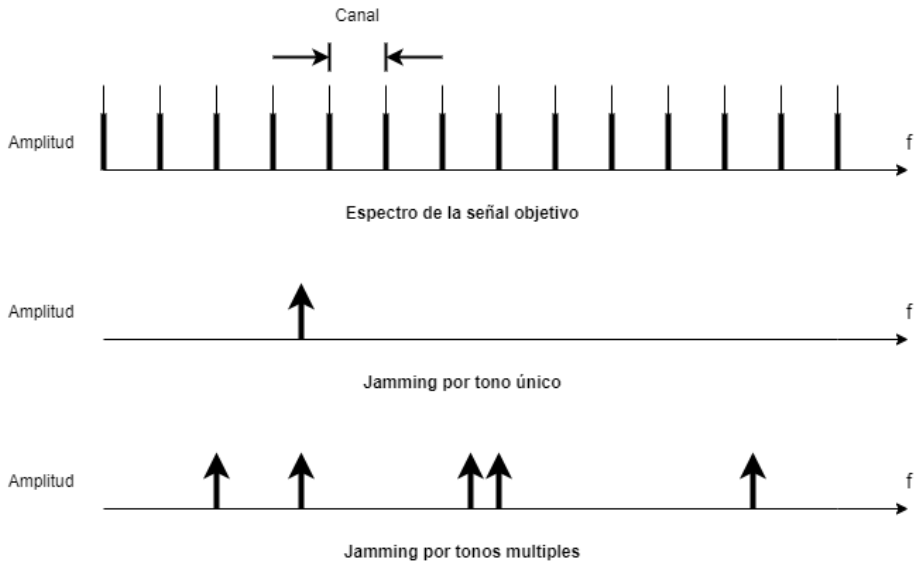


Figura 3.3. Ilustración de diferentes tipos de jamming por tonos. Fuente: [18]

3.3.3. Jamming por barrido.

Esta estrategia consiste en tener una señal de jamming de banda angosta o de tonos y desplazarlo a lo largo del espectro de la banda de interés, que podría ser todo el espectro que utiliza el objetivo o solamente una parte. Esta estrategia es útil frente a objetivos que realizan saltos en frecuencia. Uno de los parámetros a tener en cuenta es la sincronización, pues de ser el barrido muy lento no va a poder seguir los saltos del objetivo y de ser muy rápido su presencia en la frecuencia correcta va a ser muy corta por lo que no generara interferencia alguna [18].

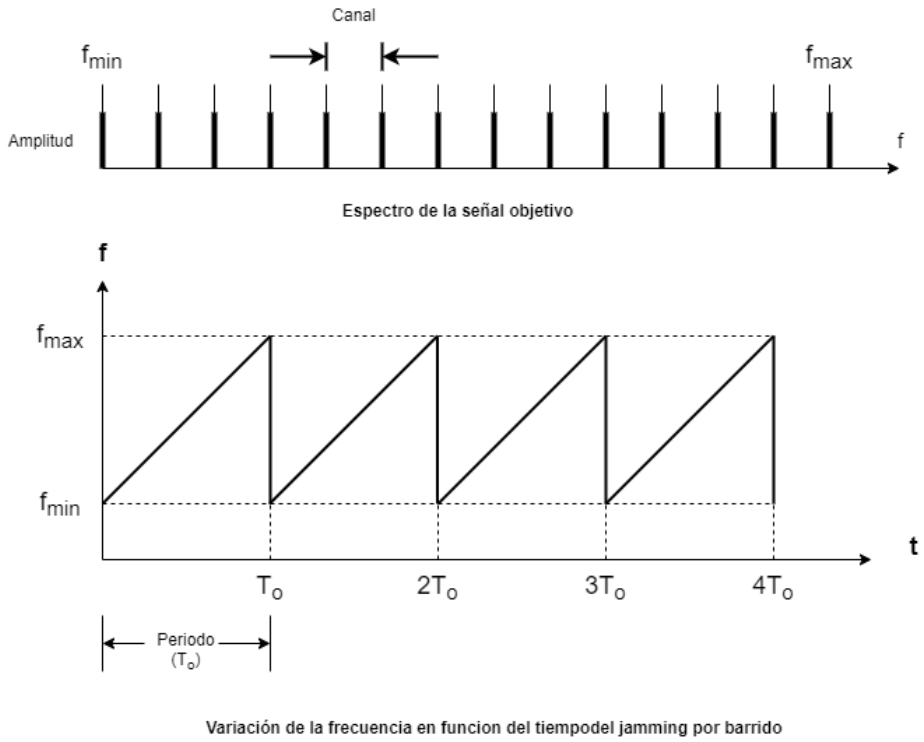


Figura 3.4. Ilustración del funcionamiento un jamming por barrido. Fuente: Elaboración propia

3.3.4. Jamming por pulso.

Esta estrategia consiste en utilizar una señal de jamming BBN durante un periodo de tiempo τ, cada periodo T_o. La relación entre τ, y T_o permite es denominado como ciclo de trabajo, el cual determina la relación entre la potencia máxima y la promedio. Si bien esta estrategia consume menor energía que otras, puede llegar a ser igual de efectiva o incluso mejor que otras dependiendo de la señal objetivo [18].

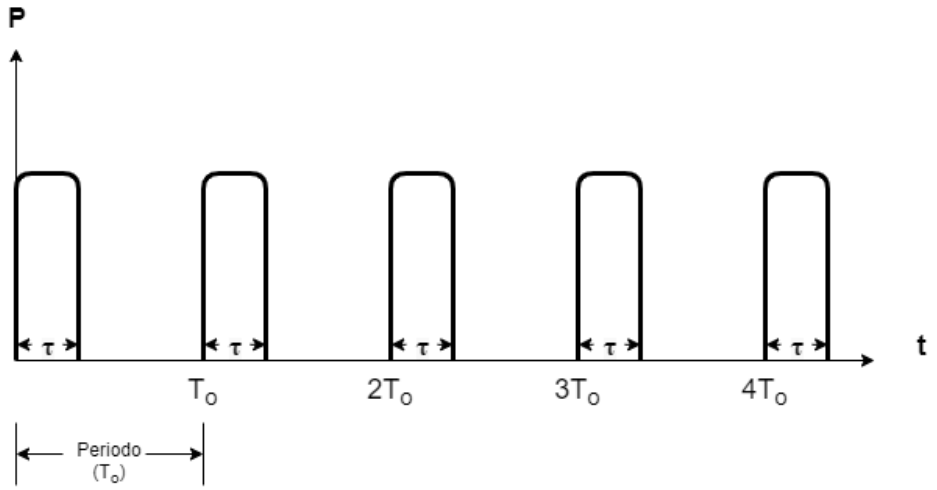


Figura 3.5. Ilustración del funcionamiento de un jamming por pulsos. Fuente: Elaboración propia

3.3.5. Jamming por seguimiento.

Esta estrategia se utiliza contra objetivos que realizan saltos en frecuencia, y consiste en localizar la frecuencia en la que se encuentra e introducir una señal de jamming, ya sea de ruido o de tono. Y cuando el objetivo salte en frecuencia, detectar el salto y mueve la señal de jamming a la nueva frecuencia a la que se ha movido. Cabe mencionar que el seguimiento presenta un retraso debido a que hay un tiempo de procesamiento en el jammer para determinar si la señal objetivo ha realizado un salto [18].

3.3.6. Jamming inteligente.

Esta estrategia consiste en generar disrupción en solamente una porción de la señal digital y siendo esto suficiente para denegar la comunicación. Este método es sumamente eficiente en términos de potencia, pero requiere de un gran conocimiento del objetivo, además de una sincronización precisa, por lo que suele ser complicado de implementar [18].

3.4. Técnicas de Optimización

Existen diferentes técnicas para optimizar el uso de los jammers, estos van desde afectar a la mayoría de objetivos afectados en simultaneo hasta de reducir su tiempo de funcionamiento al óptimo para no desperdiciar recursos. Estos son [18]:

3.4.1. Look-Through.

Esta técnica está hecha con el fin de poder reducir el consumo de recursos e incrementar la eficiencia del jammer. Esta técnica consiste en apagar el jammer durante un pequeño periodo de tiempo y analizar el espectro con el fin de determinar si la señal objetivo ha dejado de transmitir o ha realizado un salto en frecuencia [18].

3.4.2. Potencia compartida.

Esta técnica consiste en dividir la potencia en diferentes señales de jamming para afectar a varios objetivos en simultáneos [18].

3.4.3. Tiempo compartido.

Esta técnica consiste tener múltiples señales de jamming que afectan a diferentes señales objetivos y asignar la máxima potencia a cada una, pero en diferentes tiempos [18]

3.5. Jamming a Señales BPSK-DSSS

Dado que las señales L1C todavía no son usadas, dada la falta de satélites que la transmitan; todas las señales de uso civil funcionales del sistema GPS hacen uso de una modulación BPSK-DSSS. Por lo que se considera oportuno hablar acerca del comportamiento de la comunicación BPSK-DSSS frente al jamming, la cual, pese a contar con la ganancia de procesamiento que incrementa su resistencia frente a la interferencia, no la hace inmune al jamming. A continuación

se presentan modelos matemáticos para estimar el BER en estas comunicaciones frente a diferentes técnicas de jamming [18]:

3.5.1. Jamming por ruido de banda completa.

Como se mencionó anteriormente, el jamming BBN inserta un ruido aleatorio, normalmente gaussiano, en todo el espectro de la señal objetivo. Esto implica que sus efectos son muy parecidos al AWGN, por lo que se puede considerar que el ruido del jamming se puede sumar al ruido térmico ya existente en el sistema. Por ello, la probabilidad de un bit errado se puede expresar de la siguiente manera [18]:

$$BER = Q\left(\sqrt{\frac{2G_P}{\frac{1}{SNR} + JSR}}\right) \quad (3.4)$$

BER: Tasa de bits errados (adimensional)

G_P: Ganancia de procesamiento (adimensional)

SNR: Relación señal a ruido (adimensional)

JSR: Relación jamming a señal (adimensional)

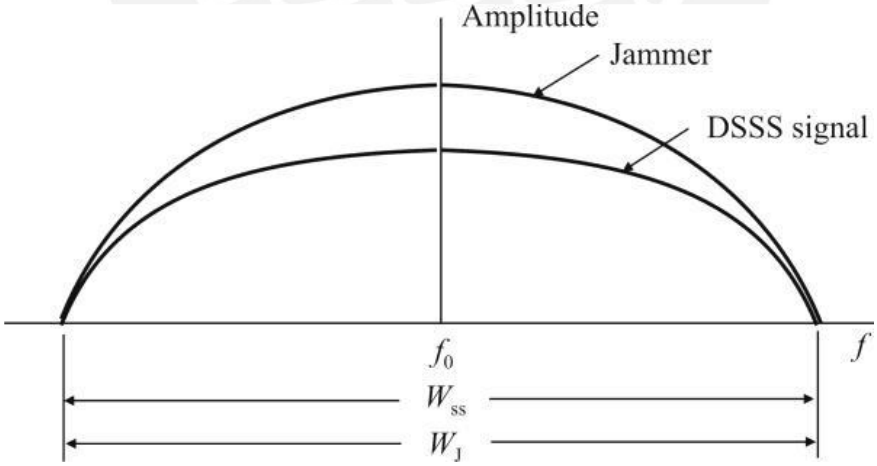


Figura 3.6. Jamming BBN en DSSS. Fuente: [18]

3.5.2. Jamming por ruido de banda parcial.

Como se mencionó anteriormente, el jamming PBN inserta un ruido aleatorio, normalmente gaussiano, en una parte del espectro de la señal objetivo. El espectro ocupado por la señal de jamming no necesariamente debe estar centrado a la frecuencia de la portadora de la señal objetivo [18].

En el caso de que la señal de jamming está centrado a la frecuencia de la portadora de la señal objetivo y su espectro solo ocupa una pequeña parte del espectro que utiliza la señal objetivo, la probabilidad de un bit errado se puede expresar de la siguiente manera [18]:

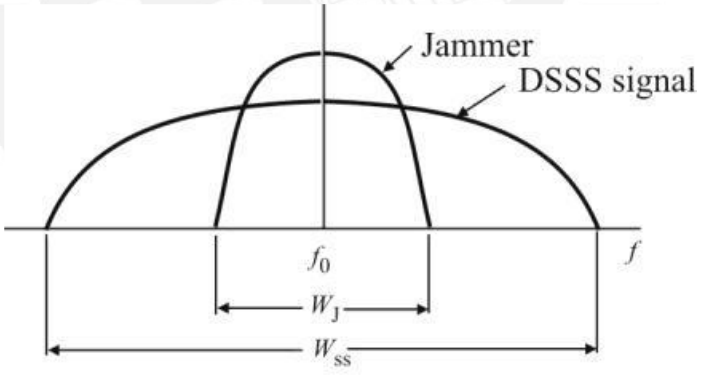
$$\text{BER} = Q\left(\sqrt{\frac{2G_P}{\frac{1}{SNR} + 2\text{JSR}}}\right) \quad (3.5)$$

BER: Tasa de bits errados (adimensional)

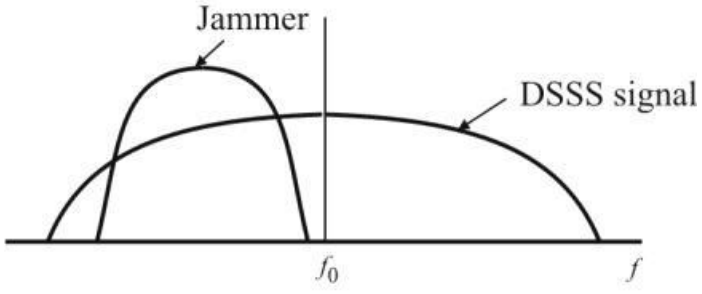
G_P: Ganancia de procesamiento (adimensional)

SNR: Relación señal a ruido (adimensional)

JSR: Relación jamming a señal (adimensional)



(a)



(b)

Figura 3.7. Jamming PBN en DSSS. Fuente:

3.5.3. Jamming por pulso.

Para el modelo se define el parámetro γ que representa el tiempo que el jammer está activo, también denominado ciclo de trabajo, y siendo 1-γ el tiempo que no estará ocupado; se considera que la señal de jamming es del tipo BBN. Siendo el BER para este caso el siguiente [18]:

$$\text{BER} = (1-\gamma)Q(\sqrt{2G_P.SNR}) + \gamma Q\left(\sqrt{\frac{2G_P}{\frac{1}{SNR}+JSR}}\right) \quad (3.6)$$

BER: Tasa de bits errados (adimensional)

γ: Ciclo de trabajo (adimensional)

G_P: Ganancia de procesamiento (adimensional)

SNR: Relación señal a ruido (adimensional)

JSR: Relación jamming a señal (adimensional)

3.5.4. Jamming por tono único.

Los modelos para estimar la tasa de bits errados de una señal BSPK-DSSS bajo un jamming por tono único se define en función a sus códigos [18]:

3.5.4.1. Para códigos largos.

En estos casos, el BER depende en gran medida de la fase relativa de la señal de jamming respecto a la señal objetivo, al que se denomina θ. Siendo el modelo el siguiente [18]:

$$BER(\theta) = Q\left(\frac{1-g_1(\theta)\cos\theta}{\left[\frac{1}{2G_P.SNR}+\frac{1}{2G_P}.JSR.sinc^2\left(\frac{\pi(\Delta f)}{G_P.R_b}\right)\left(1+\frac{1}{L}\right)\left(1+g_2(\theta)\right)\right]^{\frac{1}{2}}}\right) \quad (3.7)$$

Siendo $g_1(\theta)$ [18]:

$$g_1(\theta) = \sqrt{JSR}\frac{1}{L}sinc\left(\frac{\pi(\Delta f)}{G_P.R_b}\right)\frac{sinc\left(\frac{\pi(\Delta f)}{R_b}\right)}{sinc\left(\frac{\pi(\Delta f)}{G_P.R_b}\right)} \quad (3.8)$$

Y $g_2(\theta)$ [18]:

$$g_2(\theta) = \frac{sinc\left(\frac{2\pi(\Delta f)}{R_b}\right)}{sinc\left(\frac{2\pi(\Delta f)}{G_P.R_b}\right)}cos(2\theta) - \frac{2G_P}{L}\frac{sinc^2\left(\frac{\pi(\Delta f)}{R_b}\right)}{sinc^2\left(\frac{\pi(\Delta f)}{G_P.R_b}\right)}cos^2(\theta) \quad (3.9)$$

BER: Tasa de bits errados (adimensional)

θ: Diferencia de fase entre la señal objetivo y la del jammer (radianes)

G_P: Ganancia de procesamiento (adimensional)

SNR: Relación señal a ruido (adimensional)

JSR: Relación jamming a señal (adimensional)

Δf: Diferencia entre la frecuencia de la señal de jamming y la portadora de la señal objetivo (Hz)

R_b: Tasa de datos (bps)

L: Longitud del código (adimensional)

3.5.4.2. Para códigos cortos.

En estos casos, a diferencia del caso de los códigos largos, el BER no depende de la fase relativa de la señal de jamming respecto a la señal objetivo. Considerando que la diferencia entre el tono de la señal de jamming y la frecuencia de la portadora de la señal objetivo es diferente de cero, se puede estimar el BER mediante la siguiente formula [18]:

$$\text{BER} = Q\left(\sqrt{\frac{2G_P}{2JSR\left(\frac{\sin\left(\frac{\pi(\Delta f)}{R_b}\right)}{\frac{\pi(\Delta f)}{R_b}}\right)^2\left(1+\frac{\cos\left(2\phi+\left(\frac{G_P.2\pi(\Delta f)}{R_b}\right)\right)+\sin\left(\frac{G_P.2\pi(\Delta f)}{R_b}\right)}{G_P\sin\left(\frac{2\pi(\Delta f)}{R_b}\right)}\right)}}\right) \quad (3.10)$$

BER: Tasa de bits errados (adimensional)

G_P: Ganancia de procesamiento (adimensional)

JSR: Relación jamming a señal (adimensional)

Δf: Diferencia entre la frecuencia de la señal de jamming y la portadora de la señal objetivo (Hz)

R_b: Tasa de datos (bps)

φ=Diferencia entre la fase de la señal y la fase del tono de jamming (radianes)

CONCLUSIONES Y RECOMENDACIONES

El presente trabajo de investigación se ha dedicado a la revisión bibliográfica acerca de los tema del sistema de posicionamiento global (GPS) y de la teoría detrás de los dispositivos de jamming. Por lo que en el desarrollo de este se han alcanzado los objetivos inicialmente planteados en cuanto a:

- Documentar acerca del Sistema de Navegación Global (GPS)
- Identificar las diferentes técnicas empleadas para realizar jamming
- Definir criterios a tener a tener en cuenta en un sistema de jamming

Se recomienda que para aquellos futuros trabajos que deseen diseñar el sistema propuesto en esta investigación, utilicen como señales objetivos a las señales de código C/A; dada que es la única señal civil que es transmitida por todos los satélites del GPS, por lo que es la más utilizada. Adicionalmente, se recomienda realizar una comparación de las señales GPS objetivos frente a las diversas estrategias de jamming, haciendo uso de los modelos matemáticos brindados.

BIBLIOGRAFIA

[1] Y. B. Sebbane, *Smart autonomous aircraft: Flight control and planning for UAV*. 2015.

[2] R. Austin, *Unmanned Aircraft Systems: UAVS Design, Development and Deployment*. Chichester: John Wiley and Sons, 2010.

[3] P. G. Fahlstrom and T. J. Gleason, *Introduction to UAV Systems: Fourth Edition*. John Wiley and Sons, 2012.

[4] R. K. Barnhart, S. B. Hottman, D. M. Marshall, and E. Shappee, *Introduction to Unmanned Aircraft System*. Boca Raton: CRC Press, 2012.

[5] K. Dalamagkidis, K. P. Valavanis, and L. A. Piegl, *On integrating unmanned aircraft systems into the national airspace system: Issues, challenges, operational restrictions, certification, and recommendations*. Berlin: Springer Science+Business Media, 2012.

[6] A. H. Michel, "Counter-Drone Systems," *Cent. study drone*, no. February, p. 23, 2018.

[7] D. M. Pozar, *Microwave Engineering, 4th Edition*. Hoboken: John Wiley and Sons, Inc, 2012.

[8] G. C. ; Birch, J. C. ; Griffin, and M. K. Erdman, "UAS Detection Classification and Neutralization: Market Survey 2015," *Sandia Rep.*, p. 74, 2015.

[9] B. Manz, "Dethroning the drone," *J. Electron. Def.*, vol. 41, no. 4, pp. 24–33, 2013.

[10] J. M. Navarro García, "Sistemas contra UAVs," *Tecnol. Mil.*, vol. 39, no. 3, pp. 64–68, 2017.

[11] A. Sims, "The Rising Drone Threat from Terrorists," *Georg. J. Int. Aff.*, vol. 19, no. Fall

2018, pp. 97–108, 2018.

[12] A. Holland Michel and D. Gettinger, “Drones At Home Drone Incidents: A Survey of Legal Cases,” *Cent. Study Drone Bard Coll.*, 2017.

[13] A. H. Michel, “COUNTER-DRONE SYSTEMS 2nd Edition,” no. December, 2019.

[14] B. Hofmann-Wellenhof, H. Lichtenegger, and E. Wasle, *GNSS – Global Navigation Satellite Systems GPS, GLONASS, Galileo, and more*. Springer-Verlag Wien, 2008.

[15] P. Teunissen and O. Montenbruck, *Springer Handbook of Global Navigation Satellite Systems*. Cham: Springer International Publishing AG, 2017.

[16] E. Kaplan and C. Hegarty, *Understanding GPS. Principles and applications*, 2nd ed. Norwood: Artech House, 2006.

[17] GPS, “Space Segment.” [Online]. Available: https://www.gps.gov/systems/gps/space/. [Accessed: 26-Jun-2020].

[18] R. Poisel, *Modern Communications Jamming Principles and Techniques*, 2nd Editio. Norwood, 2011.

[19] D. Adamy, *EW 103 : tactical battlefield communications electronic warfare*. 2009.