# Técnicas de neutralización de amenazas aéreas basadas en el sistema de posicionamiento Galileo

**Alejandro Muñoz Cueva, Patricia López Torres, Alicia Arce, Santiago Blanco y Ricardo Galán**

Área temática: Sistemas de control y comunicaciones.

**Resumen:** El gran auge de vehículos aéreos no tripulados (UAVs) presenta grandes retos en el campo de la seguridad. En la actualidad diversos accidentes de UAVs han sido reportados en varios medios y existe una clara necesidad de desarrollar métodos de neutralización de amenazas aéreas.

En este contexto, este trabajo se centra en el estudio de técnicas de neutralización de amenazas de UAVs que vuelan con datos recopilados del sistema de posicionamiento Galileo. A pesar de que Galileo no esté operativo actualmente se prevé que muchos UAVs utilicen este servicio en un corto periodo de tiempo. Las técnicas que se presentan consisten en interferir en el sistema de navegación Galileo de los UAVs detectados como amenaza en las áreas a proteger, de manera que se suplante la señal de posicionamiento con una simulada, diseñada para dirigirlo a una zona segura para su regulación. Dentro de las técnicas de interferencia de los sistemas de navegación se han estudiado el denominado "*Jamming*" que pretende perturbar la calidad de la recepción de señales del sistema de posicionamiento y las técnicas de "*Spoofing*" que tienen como objeto suplantar las señales de posicionamiento para hacer creer a la aeronave que se encuentra en una posición distinta a la real. Para su implementación real es necesario una serie de dispositivos y otros diversos algoritmos que determinen las características de la suplantación para cada amenaza.

Estos trabajos se enmarcan en el proyecto DRONECAPTOR cofinanciado por el Ministerio de Economía y Competitividad, a través del CDTI, y por el Fondo Europeo de Desarrollo Regional (FEDER). Cuyo objetivo es el desarrollo de un sistema global de detección y neutralización de Amenazas con drones.

## 1. INTRODUCCIÓN

En los últimos años, el desarrollo de UAVs (unmanned aerial vehicles) ha crecido de forma exponencial y han empezado a emplearse en todo tipo de aplicaciones civiles. No obstante, un uso malintencionado o negligente de estas aeronaves puede suponer una gran amenaza para la seguridad, ya que pueden utilizarse, por citar algunos ejemplos, como medio de transporte para el tráfico de drogas, como herramienta de espionaje o incluso con fines terroristas.

Recientemente se han reportado numerosos casos de usos indebidos y accidentes con UAVs. En enero de 2015 un UAV comercial fue hallado en los jardines de la Casa Blanca, lo que deja entrever la facilidad de estos artefactos para acceder a zonas presuntamente protegidas. En abril de ese mismo año se detectó un UAV sobre la casa del primer ministro de Japón con tierra radioactiva de Fukushima, y en julio un UAV sobrevoló el Palacio de la Zarzuela. En marzo de 2016 un avión de pasajeros de la compañía Air France procedente de Barcelona estuvo a punto de colisionar contra un UAV cuando se aproximaba al aeropuerto Charles de Gaulle de París. No es el único incidente ocurrido en un aeropuerto, ya que en mayo de ese mismo año otro avión de pasajeros en el aeropuerto de Bilbao tuvo que esquivar a tres UAVs que volaban a una altura de 900 metros, cuando se encontraba dentro del espacio aéreo protegido y ya en descenso.


*Figura 1: Prohibición de volar drones que empieza a verse en algunas zonas restringidas*

La mayor parte de los incidentes mencionados responden a un uso indebido de los UAVs, más provocados por errores del usuario que los controlaba que por acciones malintencionadas. Sin embargo, es una posibilidad real la irrupción de usuarios que puedan intentar provocar incidentes con UAVs de forma deliberada, o simplemente que realicen cualquier actividad ilegal aprovechando las ventajas que ofrece esta tecnología. Por otro lado, debido a la popularización de estos dispositivos, los UAVs no sólo están al alcance de grandes compañías u organismos, sino que existen soluciones de bajo coste al alcance de cualquier persona.

Ante estos hechos, resulta evidente la necesidad del desarrollo de técnicas de neutralización de amenazas con UAVs. Por ello, diversos organismos han visto la necesidad de buscar soluciones y han surgido proyectos enfocados a solventar esta brecha en la seguridad de determinados recintos.

En este contexto surge el proyecto DRONECAPTOR, cofinanciado por el Ministerio de Economía y Competitividad, a través del CDTI, y por el Fondo Europeo de Desarrollo Regional (FEDER), que tiene como objetivo proteger un área determinada desarrollando un sistema para la detección y neutralización de amenazas con drones (término popular para referirse a UAVs). El núcleo del sistema está basado en inteligencia artificial y permitirá detectar las amenazas, analizar su peligrosidad y determinar un plan de actuación para interceptar la aeronave. El trabajo presentado, que forma parte del proyecto DRONECAPTOR, está centrado en técnicas de neutralización en las que se interfiere en el sistema de navegación del dron.

Los receptores de señales GNSS funcionan con señales de potencia muy baja, lo cual provoca que las bandas en las que se trabaja se vean afectadas por ruido blanco gaussiano. Como consecuencia, las señales GNSS son muy susceptibles a las interferencias. Esta susceptibilidad da lugar a la técnica conocida como "*Jamming*" que consiste en interferir de forma intencionada en el sistema de posicionamiento de la amenaza. La idea es generar señales en las mismas bandas de frecuencias en las que emiten los satélites, pero con una mayor potencia, de forma que se evite la correcta adquisición de las señales reales por parte del receptor atacado. Es, a modo cualitativo, una forma de "ensuciar" el espectro para aislar al UAV.

Este trabajo se centra en una técnica de suplantación conocida como "*Spoofing*". El *spoofing* consiste en la generación de señales análogas a las de los satélites, de forma que se consiga suplantar a las mismas para que el receptor de la amenaza utilice estas señales falsas para calcular una posición distinta a la real. Para realizar un *spoofing* con éxito es necesario que la transmisión de la señal suplantada aumente la potencia de forma gradual, hasta ser más fuerte que las señales

GNSS auténtica. Mediante esta técnica se pueden interceptar drones que se acerquen al área que se desee proteger y redirigirlos fuera de la misma o a un punto determinado, consiguiendo eliminar la amenaza sin necesidad de destruir el UAV.

Durante los últimos años, se han publicado diversos casos de suplantación de señales de navegación mediante *spoofing*, todos ellos actuando sobre el sistema GPS. En enero de 2011 las fuerzas iraníes capturaron un UAV militar estadounidense que volaba cerca de la frontera entre Afganistán e Irán mediante la suplantación de la señal GPS, y consiguieron hacerse con el control de la aeronave. Un año más tarde, un grupo de jóvenes investigadores de la Universidad de Texas realizaron un experimento en la costa de Italia en el que pretendían hacerse con el control del sistema de navegación de un yate. Para conseguirlo emitieron señales de GPS hacia las dos antenas receptoras del barco; transcurridos unos minutos suplantaron por completo las auténticas señales GPS y lograron quedarse con el control del sistema GNSS del yate. El dispositivo diseñado por los estudiantes enviaba señales GPS con errores de posición cada vez mayores, consiguiendo así que el barco se alejara de su ruta programada. Como consecuencia, y pese a que en la carta de navegación la tripulación veía que el barco avanzaba en línea recta, éste se encontraba a cientos de metros del rumbo previsto.

En agosto de 2015, Huan Ling y Yang Quing, investigadores del grupo "Qihoo360's UnicornTeam", afirmaron en la conferencia de hacking DEF CON de las Vegas haber desarrollado una versión de bajo coste para realizar *spoofing* de la señal GPS. Al final de la presentación realizaron una demostración de su método en la que consiguen que un dron de la conocida marca DJI sobrevolara una zona restringida por el fabricante.

En algunos casos las señales GNSS están encriptadas, como el servicio militar de GPS, por lo que resulta imposible acceder a su contenido y modificarlo. A raíz de esto, surge una técnica conocida como "*meaconing*". En este caso, las señales de navegación son interceptadas y retransmitidas en la misma frecuencia, pero con un cierto retraso con el objetivo de conseguir confundir al dron y hacer que se desvíe de su ruta prevista.

La inmensa mayoría de los trabajos realizados hasta el momento están desarrollados para GPS, por lo que este trabajo se centra en el sistema de navegación GALILEO, ya que comenzará a operar en poco tiempo y se prevé que los UAVs comiencen a utilizar este sistema.

## 2. SISTEMA DE POSICIONAMIENTO GALILEO

Al hablar de sistemas de posicionamiento basados en satélites *(GNSS)*, es inmediato pensar en la tecnología GPS. Sin embargo, aunque es cierto que GPS es la tecnología más extendida en este contexto, no es la única. En el mismo ámbito se encuentran otros sistemas que utilizan los mismos principios, de los cuales el más conocido es el sistema de posicionamiento ruso *GLONASS*. En esta línea aparece el proyecto europeo conocido como Galileo, que pretende dotar a la Unión Europea de su propio sistema de posicionamiento GNSS. A diferencia de GPS, controlado por el Departamento de Defensa de los Estados Unidos, y de GLONASS, Galileo se convertirá en el primer sistema de navegación por satélite de uso civil. Sin embargo, Galileo no pretende competir con GPS y el resto de sistemas de navegación por satélite, sino que persigue la interoperabilidad que permita mejorar las prestaciones que ofrecen estos sistemas. Así, el objetivo a corto plazo es que los receptores de Galileo puedan utilizar satélites de GPS y GLONASS para mejorar la precisión en la estimación de su posición.


*Figura 2: Proyecto europeo Galileo.*

Este proyecto, llevado a cabo por la Unión Europea conjuntamente con la Agencia Espacial Europea, está en marcha desde 2003. A pesar de que aún no está disponible su funcionamiento definitivo, esta tecnología es toda una realidad, hasta el punto de que a finales de 2016 está previsto que comience a operar de forma normal. Inicialmente deberá apoyarse en el sistema GPS, debido a que aún no están en órbita todos los satélites que permitirán proporcionar cobertura global.

Galileo trabajará con distintas bandas de frecuencia para favorecer la robustez de su servicio, dificultar las interferencias y poder ofrecer distintos servicios a sus usuarios. Estas bandas son la E1 (1575.42 MHz), E5a (1176.45 MHz), E5b (1207.14 MHz) y E6 (1278.75 MHz). Además, el contenido de los mensajes de navegación será de distinto tipo según la banda de frecuencia. Estos mensajes serán de tipo I/NAV o F/NAV, además de los mensajes restringidos C/NAV.

Los principales campos que se envían en el mensaje de navegación son los datos de reloj y corrección del mismo, las efemérides y el almanaque. El almanaque contiene información que permite conocer la posición de los satélites. Sin embargo, esta información tiene una precisión limitada, ya que los datos del almanaque se actualizan con poca frecuencia. Sirve por tanto para conocer la posición de los satélites de forma orientativa. Las efemérides, en cambio, contienen información mucho más precisa para el cálculo de la posición, ya que está mucho más actualizada.

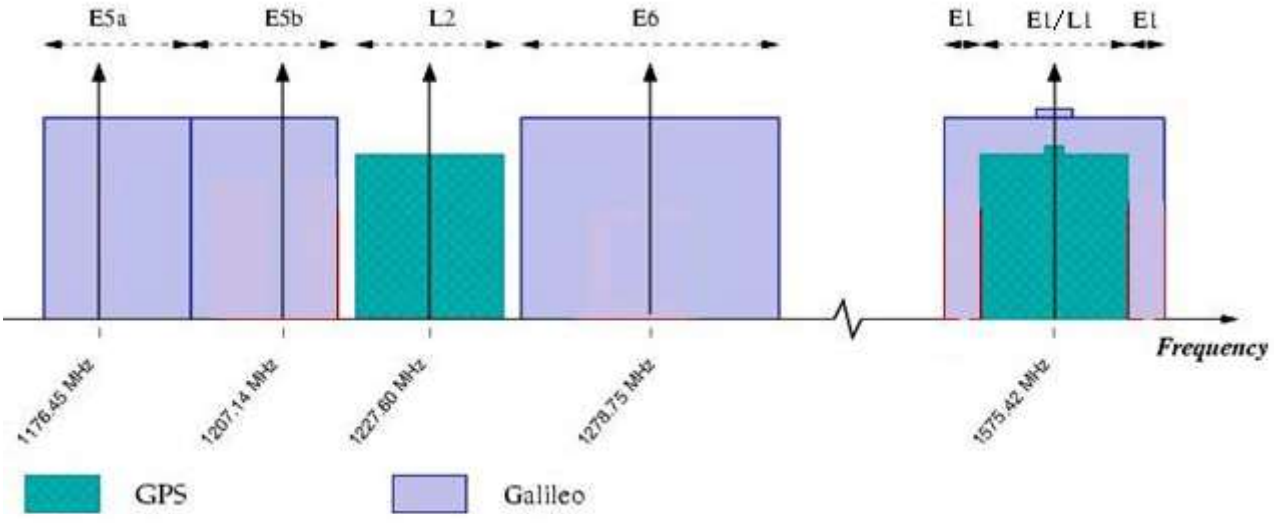


*Figura 3: Representación de las bandas de Galileo y GPS en el espectro de frecuencia.*

Los cinco tipos de servicios ofrecidos por Galileo, orientados a satisfacer las distintas necesidades de los usuarios, son los siguientes:

- *Open Service* (OS): Es el servicio básico de Galileo, que permite obtener estimaciones precisas de tiempo y posición de forma gratuita. A pesar de ser el servicio básico, su precisión y cobertura serán mayores que las del actual GPS. Este servicio operará en las bandas E5a, E5b y E1.
- *Public Regulated Service* (PRS): Este servicio está reservado para usuarios autorizados, como son la policía, la aduana o instituciones gubernamentales. La principal característica de este servicio es su robustez y seguridad, ya que las señales estarán protegidas por un fuerte cifrado, de forma que sólo los usuarios que conozcan esta codificación serán capaces de utilizar este servicio. Este servicio se podría entender como análogo al GPS militar, y se transmite en las bandas E1 y E6.
- *Safety of Life* (SoL): Se utilizará para aquellas aplicaciones críticas en las que alguna vida humana podría correr peligro si el sistema de radionavegación funcionara de forma deficiente. La precisión será la misma que en el OS, pero con una mayor integridad y robustez. Está orientado a sectores como la navegación aérea, y trabajará con las bandas E1, E5a y E5b.
- *Commercial Service* (CS): Su uso está orientado a aplicaciones comerciales que necesitan un nivel de prestaciones superior a las del OS. Mediante el pago de un canon se proporcionará acceso a dos señales adicionales, que serán emitidas en la banda E6.
- *Search and Rescue Service* (SAR): Está diseñado para aportar mejoras al servicio SoL, orientadas a facilitar las operaciones de rescate. Alguna de las funcionalidades que aportará son la recepción casi inmediata de mensajes de socorro, la localización precisa de alertas y la mayor cobertura en cualquier zona.

En su fase final Galileo contará con 30 satélites situados en 3 órbitas distintas, que permitirán alcanzar en cualquier punto del planeta una precisión del orden de 1 metro para el servicio normal, y de hasta 1 centímetro para el servicio de pago. Por todo lo expuesto hasta ahora resulta evidente que el sistema Galileo constituirá una valiosa herramienta para múltiples campos, y se espera que su implantación en la sociedad sea prácticamente inmediata una vez que comience a operar con normalidad.

A fecha de Septiembre de 2016 hay en órbita 10 de los 30 satélites de Galileo listos para funcionar con plena capacidad. En Octubre de este mismo año está previsto el lanzamiento de 4 satélites más que, unidos a los 10 anteriores, van a permitir comenzar con la plena operación del servicio OS para Diciembre. Como se ha comentado previamente, en un primer momento los dispositivos de Galileo se apoyarán en los satélites de GPS para mejorar la cobertura, aunque esta necesidad irá desapareciendo conforme vaya aumentando la flota de satélites, hasta los 30 finales.

En los últimos años el campo de aplicación de la tecnología GPS ha aumentado exponencialmente, y se prevé que Galileo tome el testigo de esta revolución, de forma que en un futuro cercano sea tan habitual encontrar dispositivos con receptores de Galileo como lo es en la actualidad encontrar dispositivos que funcionan con GPS. Sin ir más lejos, la conocida marca de teléfonos móviles BQ ha puesto a la venta el teléfono "*BQ Aquaris X5 Plus*", que es el primero en incluir un receptor de Galileo. Este hecho da una idea de la inminente entrada de Galileo en el panorama global.

En esta línea, se espera que los drones también acaben optando por las ventajas que aporta esta tecnología, y que gran parte de ellos confíen su sistema de posicionamiento al sistema Galileo. Resulta por tanto lógico pensar en la necesidad de desarrollar técnicas de defensa ante amenazas con drones cuyo posicionamiento dependa de Galileo, ya que será un escenario real en poco tiempo.

# 3. FUNCIONAMIENTO DE UN *SPOOFER*

## 3.1. Funcionamiento de los sistemas GNSS

Como se ha mencionado en apartados anteriores, el objetivo de este trabajo es el de presentar una técnica de defensa ante amenazas con drones cuyo sistema de posicionamiento dependa de Galileo. Al entrar un dron en una supuesta zona restringida, se comenzarían a enviar señales falsas para suplantar al sistema Galileo, de forma que el receptor calcule una posición errónea y pueda ser dirigido a alguna zona segura. Se trataría por tanto de dirigir el dron hacia una base, o simplemente alejarlo de la zona restringida, mediante técnicas de *spoofing*.

Inicialmente se expondrá el funcionamiento de los sistemas GNSS, para facilitar el entendimiento de la herramienta presentada. Los satélites de cualquier sistema GNSS envían periódicamente un mensaje de navegación, que a grandes rasgos contiene la posición del satélite y el instante exacto en el que se envió dicho mensaje. La señal enviada por los satélites contiene también un código, llamado PRN (*Pseudo-random Noise)* que permite identificar de qué satélite viene cada señal, ya que todos emiten en las mismas bandas de frecuencia.

Cuando la señal alcanza al dispositivo receptor, éste estima el tiempo de viaje de la onda desde que se envió, y teniendo en cuenta la velocidad de la luz obtiene una estimación de la distancia al satélite en cuestión, llamada pseudo-rango. El pseudo-rango, que posteriormente será corregido al decodificar el mensaje de navegación, tiene un papel fundamental en los sistemas GNSS, ya que permite saber la distancia entre el receptor y el satélite del que procede la señal. Así, conociendo la distancia a cuatro satélites y la posición de los mismos, obtenidas del mensaje de navegación, se puede calcular la posición del receptor mediante triangulación.

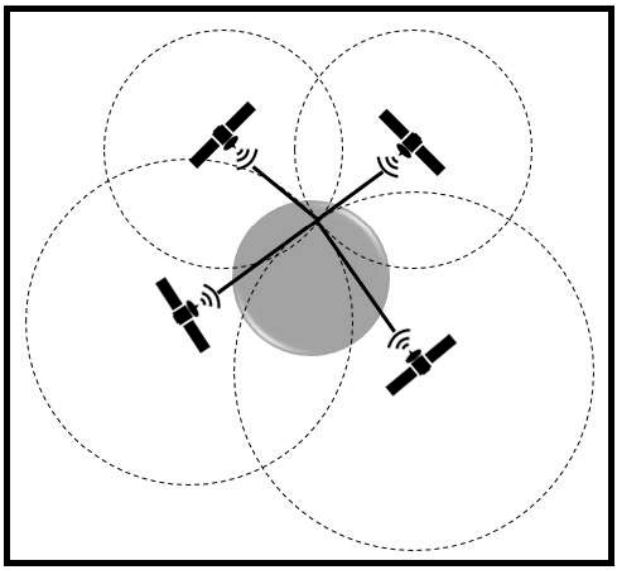

*Figura 4: Triangulación para calcular la posición.*

Aunque teóricamente debería ser suficiente con conocer la distancia a 3 satélites, en realidad el reloj del receptor no es perfecto, por lo que es necesario añadir una incógnita más a las ecuaciones, que es el error del reloj del receptor. Por ello, es necesario "ver" al menos cuatro satélites para poder calcular la posición y la hora del receptor, aunque cuanto mayor sea el número de satélites más precisa debería ser la estimación.

### 3.2. Sistema de navegación basado en GNSS

Uno de los módulos fundamentales en cualquier UAV que vuele de forma autónoma es el módulo de navegación, que es el encargado de estimar la posición en la que se encuentra la aeronave en cada momento. La estimación de la posición juega un papel fundamental en la navegación de cualquier aeronave, ya que constituirá una de las entradas del módulo de control y, por tanto, afectará directamente a la acción de control calculada y enviada a los actuadores del UAV.

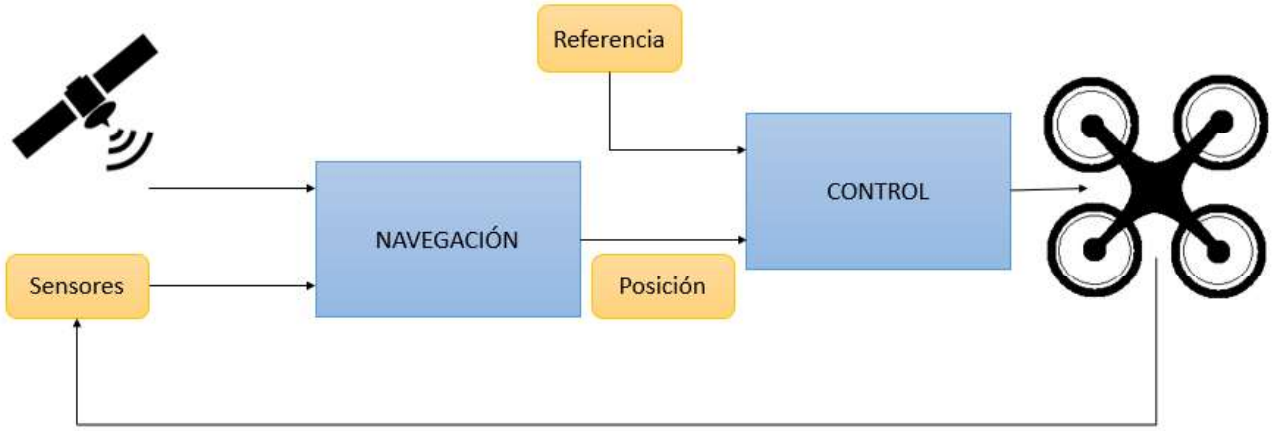


*Figura 5: Estructura del control de navegación de un UAV*

En la Figura 6 se muestra una visión general y simplificada de la estructura del control de navegación de un UAV que vuele de forma autónoma, y además haga uso de señales GNSS. En ella destacan los mencionados módulos de navegación y control, además de sus respectivas entradas y salidas.

Como se ha mencionado, el módulo de navegación se encarga de aportar una estimación de la posición del UAV, que será el dato fundamental utilizado por el sistema de control para calcular la acción que debe realizar la aeronave. En la mayor parte de UAVs que realizan vuelos en exteriores el posicionamiento depende fundamentalmente de la señal GPS, u otro sistema GNSS. Sin embargo, la frecuencia con la que un receptor de señales GNSS devuelve una estimación de la posición es habitualmente del orden de 1 Hz, llegando algunos receptores más sofisticados a los 5 o incluso 10 Hz. Resulta inmediato deducir que el lazo de control debe actuar a una frecuencia mayor, especialmente en el caso de un vehículo aéreo, ya que calculando una acción de control por segundo sería imposible controlar un UAV con buenas prestaciones.

Por ello, una estrategia muy habitual en los sistemas de control de navegación es la de integrar datos de los sensores, habitualmente menos precisos, con los datos de las señales GNSS. De esta forma, un UAV en vuelo estimaría su posición a una frecuencia relativamente alta mediante la integración de los datos de los sensores, por ejemplo de la IMU (*Inertial Measurement Unit*). Esta estimación tendría un error creciente a medida que avanza el tiempo, pero sería corregida por la señal de GNSS cada vez que ésta llegara. De esta forma se consigue una estimación de la posición a una frecuencia mayor que la que se consigue con el uso de señales GNSS, aunque éstas siguen siendo las principales responsables del resultado obtenido.

Una vez que se dispone de la estimación de la posición, el módulo de control se encarga de calcular la acción de control a realizar por el UAV, principalmente comparando dicha estimación con la referencia que se desea alcanzar. El estudio de distintas técnicas de control es un amplio campo por sí mismo, pero esencialmente todas las técnicas acaban comparando una medida más o menos precisa del estado con la referencia que se desea alcanzar. Por ello, resulta evidente que

modificando dicha estimación de la posición se puede afectar directamente a la salida calculada por el sistema de control de la aeronave, y eso es precisamente lo que pretenden explotar las técnicas de defensa ante amenazas con drones presentadas en este documento.

Sin embargo, también existen técnicas en la actualidad que persiguen detectar un posible ataque al sistema de posicionamiento. Una posible técnica de defensa ante un *spoofing* es la de detectar cambios bruscos en la estimación de la posición o de la hora calculada a partir de señales GNSS, razón por la cual la técnica de defensa propuesta debe generar una posición falsa que varíe gradualmente. De la misma forma, para una amenaza sería fácilmente detectable un cambio brusco en la potencia de las señales recibidas. Existen técnicas más sofisticadas, como la de analizar el ángulo de llegada de las señales, lo cual dificultaría la realización de un *spoofing* en el que todas las señales se enviaran desde el mismo punto.

Queda de manifiesto que se pueden realizar distintos tipos de *spoofing*, en función de la veracidad que se necesite que tenga las señales para que la técnica de defensa tenga éxito, o lo que es lo mismo, en función de las posibles técnicas de detección de las que disponga el UAV amenaza.

### 3.3. Posibles estrategias de *spoofing*

El objetivo del *spoofer* es generar señales análogas a las de los satélites, de forma que el receptor del UAV amenaza calcule una posición distinta a la real. Sin embargo, además de la complejidad que pueda entrañar la generación de estas señales, existen distintas posibles soluciones en función de la "veracidad" que se quiera dar a estas señales, entendida en términos de la sincronización con las señales enviadas por los satélites reales. Cuanto más ambicioso sea el *spoofer*, mayor será su complejidad y, habitualmente, mayor será también el coste del hardware necesario.

El escenario más simple es el de la generación de señales análogas a las de Galileo, sin preocuparse por la sincronización con las señales reales. En este caso se podría partir de los datos del almanaque, que se publican cada cierto tiempo. Con esta estrategia se puede llegar a conseguir un resultado exitoso, siempre y cuando el receptor se encuentre en modo de adquisición, es decir, que acabe de comenzar a buscar señales de satélites y directamente encuentre las señales falseadas. Por el contrario, si el receptor está calculando su posición en base a señales reales y comienzan a llegarle señales falseadas sin ninguna sincronización con las reales, es muy probable que estas señales falsas sean ignoradas.

Por el contrario, si las señales generadas por el *spoofer* están sincronizadas con las enviadas por los satélites, se podría conseguir que el receptor deje de seguir a las señales reales, para comenzar a seguir las falseadas. Para ello, la estrategia más habitual es la de alinear la señal falseada con la real, aumentar progresivamente su potencia hasta que sea algo mayor que la de la señal real, y posteriormente comenzar a diferenciarse progresivamente de ésta. Otra opción más ambiciosa es la de enviar las distintas señales falseadas desde distintos puntos, con el fin de dificultar las técnicas de detección que pudieran proteger al sistema de posicionamiento del UAV. Como resulta evidente, cuanto más difícil de detectar se pretenda que sea la suplantación, mayor será el coste necesario.

### 3.4. Esquema del *spoofer*

Para el estudio de las técnicas de suplantación con fines de seguridad en zonas restringidas, se presentará el caso general de un sistema de *spoofing* con una sola fuente de emisión de las señales. Al igual que en el caso de las distintas estrategias para realizar el *spoofing*, también existen distintas posibilidades en lo que al hardware se refiere. Así, existen generadores de señales GNSS comerciales, cuyo coste puede ser muy elevado. En este caso, los elementos hardware se presentan como SDRs (*Software Defined Radio*), que son elementos que permiten el trabajo con señales de radio de forma flexible.

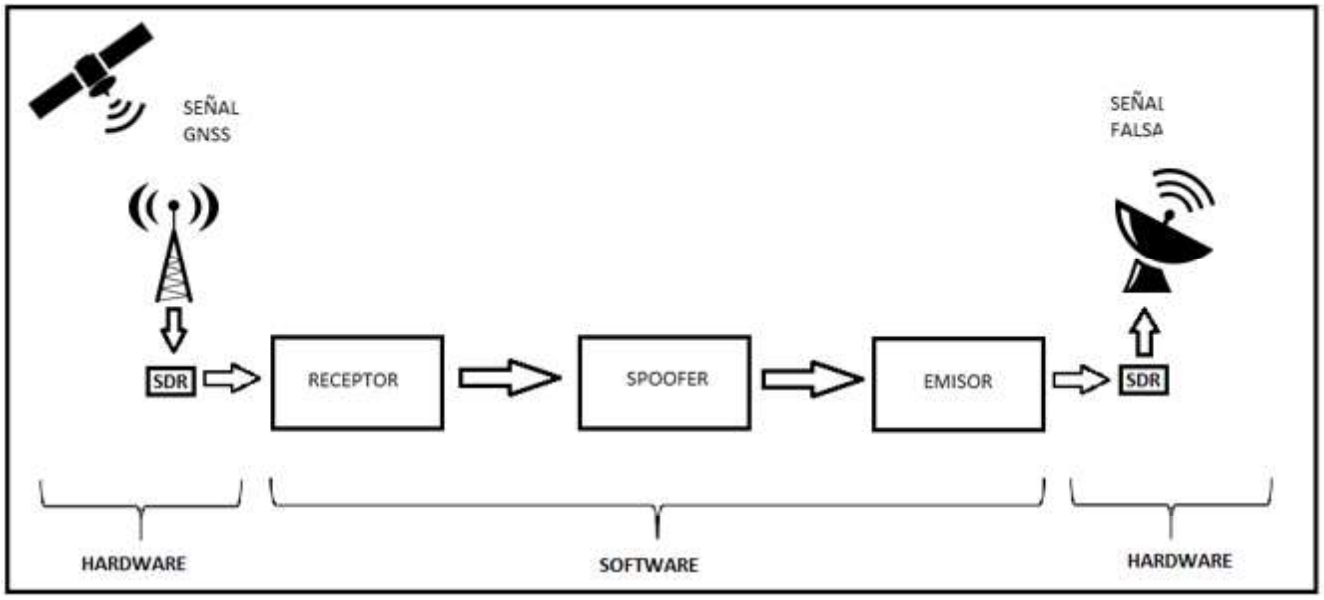


*Figura 6: Esquema de un módulo de suplantación de GNSS.*

En la Figura 7 se muestra el esquema de un sistema de suplantación de señales GNSS. Como se ha mencionado previamente, los elementos representados como SDRs podrían sustituirse por otros *front-ends*, que actúen como enlace hardware (convertidores, filtros, etc) entre las antenas emisora y receptora y los módulos de tratamiento software.

La idea fundamental sería la de recibir señales legítimas de los satélites, con el fin de extraer el mensaje de navegación de éstas y sus características principales, para posteriormente poder realizar la generación de las señales a enviar en distintos módulos software.

Una vez adquiridas las señales reales, los módulos software se encargarían en primera instancia de decodificar el mensaje de navegación y extraer las características de la onda, con el fin de conseguir generar una señal lo más parecida posible a la real. Posteriormente, el módulo llamado *Spoofer* se encargaría de calcular las características que debe tener la señal de salida, así como el mensaje de navegación a enviar, y el último módulo se encargaría de redefinir la señal para poder enviarla.

Como se ha mencionado, es importante para obtener un resultado exitoso el generar inicialmente una señal lo más parecida posible a la real, cuya potencia crecerá progresivamente, para evitar un cambio abrupto en las señales recibidas por el receptor que pueda provocar una detección por parte del mismo. De la misma forma, la posición falsa que se pretende que calcule el receptor de la amenaza debe ser inicialmente similar a la real e ir cambiando progresivamente, o de lo contrario la medida de defensa será fácilmente detectable por el UAV amenaza.

Un aspecto a tener en cuenta es la potencia de las señales generadas. Las señales GNSS llegan a la superficie terrestre con una potencia muy baja debido a la gran distancia que recorren. Esto relaja los requerimientos de potencia para las señales generadas, aunque también tiene el inconveniente de que es posible "afectar" a una amplia zona con un *spoofing* de baja potencia. Por ello, puede ser necesario el uso de atenuadores para controlar la zona de actuación de este mecanismo de defensa, con el fin de no afectar a los receptores de usuarios que se encuentren en zonas próximas a las áreas protegidas.

## 4. ESTRUCTURA DE UN *SPOOFER*

Dejando de lado las limitaciones físicas de un *spoofer*, que pueden ser subsanadas con una mayor inversión económica en la adquisición del hardware, se presenta a continuación la algoritmia que debe llevar a cabo esta herramienta de defensa.

Como se muestra en la Figura 7, los tres bloques principales que intervienen en el proceso son el módulo receptor, el módulo *Spoofer* y el módulo emisor. El módulo receptor es el encargado de extraer las características de las señales de Galileo recibidas y decodificar los mensajes de navegación. Posteriormente aparece el módulo llamado *Spoofer*, que decide el contenido de los mensajes de navegación a enviar, así como los retrasos que deben incluir las señales, con el fin de que el receptor de la amenaza calcule la posición deseada. Este módulo es el principal de todo el proceso, ya que calculará cómo deben ser las señales a enviar para que el receptor calcule los pseudo-rangos deseados. Para que esta técnica tenga éxito, debe conocerse la posición real de la amenaza, ya que el tiempo que tardará en llegar la señal falseada desde su envío puede influir considerablemente en el pseudo-rango calculado por el receptor.

Una vez que se conocen las características de las señales a enviar y el mensaje de navegación que deben contener, el bloque "Emisor" se encarga de generar dicha señal, de forma que pueda ser enviada por el hardware correspondiente. Para ello, este módulo puede dividirse en tres etapas, que se muestran en la Figura 8.

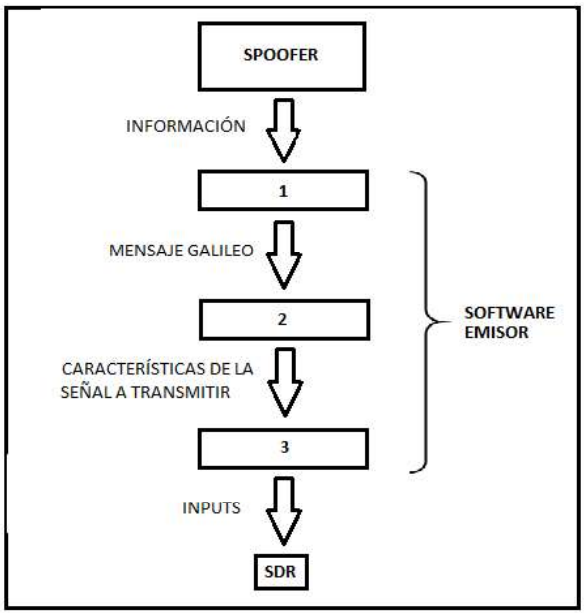


*Figura 7: Esquema del módulo emisor.*

El proceso a realizar es el siguiente:

- Una vez conocida la información que se desea enviar, codificación de la misma en un mensaje de navegación de tipo I/NAV, que es el formato que tienen los mensajes de Galileo OS.
- Al disponer de la cadena de bits que componen el mensaje de navegación, la segunda capa se encarga de combinarla con los códigos correspondientes y modularla para obtener la señal a enviar.
- Por último, se codifica dicha señal de la forma concreta que necesite el hardware de emisión, y ya podría enviarse correctamente.

## 5. CONCLUSIONES

Se ha analizado el funcionamiento del sistema de posicionamiento Galileo y las ventajas que éste ofrece, así como su previsible irrupción como una de las principales tecnologías de posicionamiento por satélite en los próximos tiempos. Por otro lado, el desarrollo de los vehículos aéreos no tripulados es una realidad en la actualidad, estando éstos cada vez más al alcance de cualquier usuario. Se han presentado algunos incidentes, la mayor parte de ellos afortunadamente sin consecuencias, que están empezando a hacerse habituales como resultado de esta creciente irrupción de los UAVs. Aunque hasta ahora no haya ocurrido ningún accidente de gravedad con esta tecnología, es innegable la necesidad del desarrollo de técnicas de neutralización y defensa ante posibles amenazas con UAVs.

En este documento se han propuesto técnicas de defensa de áreas restringidas, donde se pretende mantener la seguridad con actuaciones no destructivas. En concreto, se han propuesto técnicas que permitan actuar sobre el sistema de posicionamiento Galileo de las potenciales amenazas, actuando así sobre dos tecnologías en desarrollo cuyo punto de unión es muy previsible en los próximos tiempos.

Aunque se han analizado diversas técnicas en este ámbito, se ha entrado más en profundidad en el uso de la técnica conocida como *spoofing*. Esto es debido a que, como se ha mencionado a lo largo del artículo, es la técnica que nos permite controlar la posición en la que creerá la amenaza que se encuentra. De esta forma se puede redirigir la amenaza hacia un punto deseado sin necesidad de actuar sobre su sistema de control, lo cual supone una poderosa técnica de defensa. Así, observando la trayectoria que realiza un UAV que vuela autónomamente, se puede calcular una serie de posiciones falsas que el sistema de control del dron intentará corregir, de forma que finalmente éste siga una trayectoria predefinida por el centro de control.

Esta técnica se puede combinar con otras de las presentadas en el mismo ámbito, como por ejemplo el *jamming*, que podría facilitar la pérdida del seguimiento de las señales GNSS reales por parte del UAV amenaza, para facilitar la suplantación de las mismas mediante un *spoofing* posterior. También podría utilizarse el *meaconing*, para casos en los que el UAV amenaza no es susceptible al *spoofing*. Un escenario en el que pasaría esto sería aquel en el que amenaza utiliza un servicio encriptado como el PRS.

Estas técnicas presentadas permitirían evitar la incursión de amenazas en entornos críticos, como por ejemplo centrales nucleares, en recintos con personalidades importantes, como el mencionado caso de la Casa Blanca, y un sinfín de escenarios que pueden ser vulnerables a la entrada de pequeños vehículos volando de forma autónoma.

## 6. BIBLIOGRAFÍA

Agencia Espacial Europea. (2015). European GNSS (Galileo) Open Service.

Nighswander, T., Ledvina, B., Diamond, J., Brumley, R., & Brumley, D. (2012). GPS Software Attacks.

Plausinaitis, D. (2009). GPS And Other GNSS Signals.

RÜGAMER, A., & KOWALEWSKI, D. (2015). Jamming and Spoofing of GNSS Signals – An Underestimated Risk?!

Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B., & Capkun, S. (2011). On the Requirements for Succesful GPS Spoofing Attacks.

Wullems, C. (2011). A spoofing detection method for civilian L1 GPS and the E1-B Galileo Safety of Life service. *IEEE Transactions on Aerospace and Electronic Systems*.