EFECTOS DE LA SUPLANTACIÓN DE SEÑALES GNSS SOBRE UNA FLOTA DE UAVS Y SU APLICACIÓN A LA DEFENSA DE ÁREAS RESTRINGIDAS

Autores:

PATRICIA LÓPEZ TORRES
ALEJANDRO MUÑOZ CUEVA
ALICIA ARCE
RICARDO GALÁN DE VEGA

Efectos de la suplantación de señales GNSS sobre una flota de UAVs y su aplicación a la defensa de áreas restringidas

Patricia López Torres, Alejandro Muñoz Cueva, Alicia Arce y Ricardo Galán de Vega

FUNDACIÓN AYESA

Área temática: Sistemas de control y comunicaciones.

El uso malintencionado o negligente de los vehículos aéreos no tripulados (UAV) pone de manifiesto la necesidad de desarrollar medidas de seguridad que neutralicen las amenazas aéreas.

Existen diferentes técnicas de seguridad empleadas contra aeronaves que vuelan de forma autónoma haciendo uso de los sistemas GNSS. Estas técnicas pretenden interferir en el receptor GNSS de la aeronave de forma que el posicionamiento obtenido no sea correcto. Uno de estos métodos se conoce como spoofing, técnica que consiste en suplantar las señales GNSS con las que la aeronave se posiciona mediante el envío de señales falsas. Esta técnica permite llevar a la amenaza hasta una zona de seguridad deseada o desviarla de su trayectoria original para que no sea capaz de acceder a una zona que se pretende proteger. Esta medida se ha estudiado previamente en situaciones en las que la amenaza aérea se trata de un solo UAV. El presente trabajo tiene como objetivo estudiar escenarios más complejos donde la amenaza está formada por una flota de aeronaves. Debido a que cada uno de los UAVs que pretende entrar en la zona restringida se encuentra en una posición distinta, la recepción de las mismas señales falsas GNSS afecta a cada uno de forma diferente. Por ello, se realiza un análisis del comportamiento que adopta cada una de las aeronaves amenaza al recibir las señales falsas. Además, se estudian las diferentes estrategias y configuraciones del spoofer (sistema HW and SW donde se implementa la técnica de spoofing) que se podrían adoptar para proteger una zona restringida en el caso en el que la amenaza aérea sea un conjunto de UAVs.

1. INTRODUCCIÓN

En los últimos años, la popularidad de los vehículos aéreos no tripulados UAVs (*Unmanned Aerial Vehicles*) ha experimentado un crecimiento exponencial. Esta irrupción se debe, en gran parte, al extenso campo de aplicación que se prevé que pueden alcanzar estas aeronaves, siendo posible emplearlas en tareas de ámbitos muy diversos, como pueden ser seguridad, vigilancia, fotografía, inspección de infraestructuras críticas, y un extenso etcétera.

Es tal la popularidad que están alcanzando los UAVs, que cada vez es más habitual encontrar firmas comerciales que ofrecen soluciones de bajo coste (multicópteros habitualmente) con unas funcionalidades considerables dado su bajo precio. De esta forma, queda lejos la idea de un UAV únicamente como una enorme aeronave de propósito puramente militar, englobándose en este término actualmente una gran cantidad de aeronaves de características y aplicaciones muy diversas.

Precisamente por esta creciente popularidad, cada vez son más las entidades y organismos que están dedicando esfuerzos a idear técnicas defensivas que sean capaces de neutralizar una posible amenaza con este tipo de aeronaves, ya que en la actualidad casi cualquier persona puede tener al alcance un UAV de unas características aceptables, y puede utilizarlo para comprometer la seguridad de alguna región.

Se están investigando en la actualidad múltiples técnicas para conseguir evitar la entrada de UAVs en áreas restringidas. Una de ellas, y la más relacionada con este artículo, se basa en el *spoofing* del sistema GNSS [1] de la amenaza.

Se conoce como *spoofing* a la generación de señales similares a las de un sistema de posicionamiento por satélite (GPS, GALILEO, GLONASS…), de forma que un receptor GNSS emplee estas señales falsas, en lugar de las señales reales enviadas por los satélites, y obtenga así un posicionamiento erróneo. Existen precedentes de que, manipulando la información que contienen estas señales y sus características, se puede conseguir que un receptor GNSS crea encontrarse en una posición falsa concreta, y definida a priori por el autor del *spoofing*.

Sin embargo, cuando la amenaza no se trata de un solo UAV, sino de una flota de aeronaves, esta estrategia se antoja mucho más compleja, ya que cada UAV de la flota se vería afectado por las señales de una forma diferente. Por ello, este artículo se centra en el estudio de los efectos que tiene un *spoofing* con una sola antena sobre una flota de UAVs, cuando todos los integrantes de la flota reciben las mismas señales, y se analiza el comportamiento de las aeronaves en distintas situaciones. Además, se estudian las diferentes estrategias y configuraciones del *spoofer* (sistema HW y SW que implementa el *spoofing*) que se podrían adoptar para proteger una zona restringida en el caso en el que la amenaza aérea sea un conjunto de multicópteros.

2. CASOS DE ESTUDIO

El objetivo de este trabajo es analizar cómo afecta la técnica *spoofing* a una flota de UAVs, y su aplicación a la defensa de un área restringida. En trabajos anteriores ([1]) se ha estudiado esta técnica aplicada a una sola aeronave. En ese caso, se observó cómo no sólo es posible evitar que el UAV entre en la zona protegida, sino que además se puede llevar a la amenaza hasta una zona de seguridad deseada, tal y como se muestra en la Figura 1. El UAV amenaza pretende acceder a la zona roja, pero gracias al *spoofing* se consigue desviar su trayectoria y llevarlo a la zona de seguridad que se desee, mientras su sistema de posicionamiento cree que se está dirigiendo hacia su objetivo.

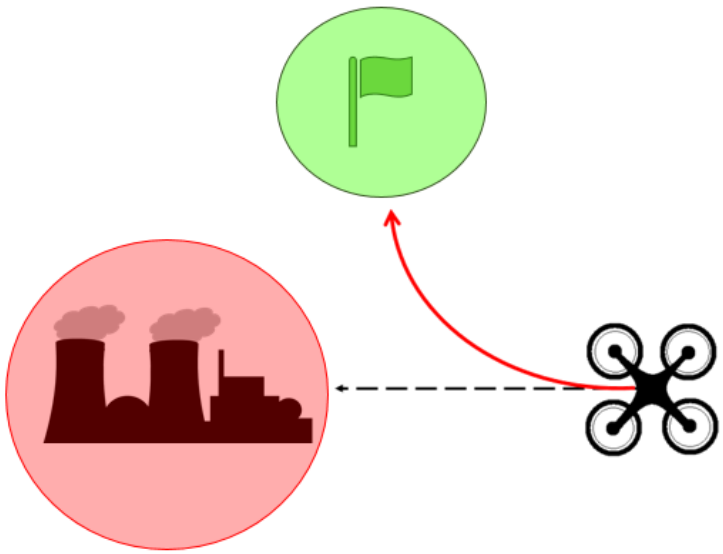

Figura 1: Representación del desvío de la trayectoria de un UAV.

Tras conseguir aplicar esta técnica de defensa con éxito en el caso de un UAV, se pretende estudiar como afectarían las señales GNSS emitidas si hubiese más de un UAV. Es decir, se desea analizar cuál sería el comportamiento de cada una de las aeronaves al recibir todas ellas las mismas señales falsas.

Al tratarse la amenaza de un conjunto de aeronaves, los posibles escenarios que se deben estudiar son mucho más complejos, ya que se pueden presentar situaciones diferentes en función del número de UAVs que conformen la amenaza, de la posición en la que se encuentran en el momento en el que son detectadas por el radar, de la referencia interna que pretende seguir cada una de ellas, etc. Por este motivo es necesario plantear una serie de casos de estudio que podrían darse y analizar el comportamiento que tendría cada aeronave al verse afectada por las señales procedentes del *spoofing*. En este apartado se presentan los diferentes escenarios que se van a analizar en este trabajo. Al igual que en el caso de una aeronave, las señales GNSS que pretenden confundir el sistema de posicionamiento del UAV serán emitidas por una sola antena. Como consecuencia todos los UAVs que forman la amenaza reciben la misma posición falsa.

Como se ha comentado anteriormente, para realizar el estudio de cómo afectaría el *spoofing* a una flota de UAVs se han realizado una serie de simulaciones en diferentes escenarios que podrían darse. Los casos estudiados en la sección 4 están formados por combinaciones de las siguientes configuraciones:

- Posición inicial de la flota: Al tratarse la amenaza de un conjunto de aeronaves y de realizar la emisión de señales desde una única antena, la posición inicial de cada UAV amenaza es un aspecto importante para tener en cuenta. Por ello, se han considerado situaciones en las que las aeronaves pretenden acceder al área restringida partiendo de puntos cercanos entre ellas, caso más favorable, y la situación opuesta, en la que cada UAV pretende acceder a la zona protegida desde direcciones diferentes, caso más desfavorable. Las dos configuraciones pueden observarse en la Figura 2.

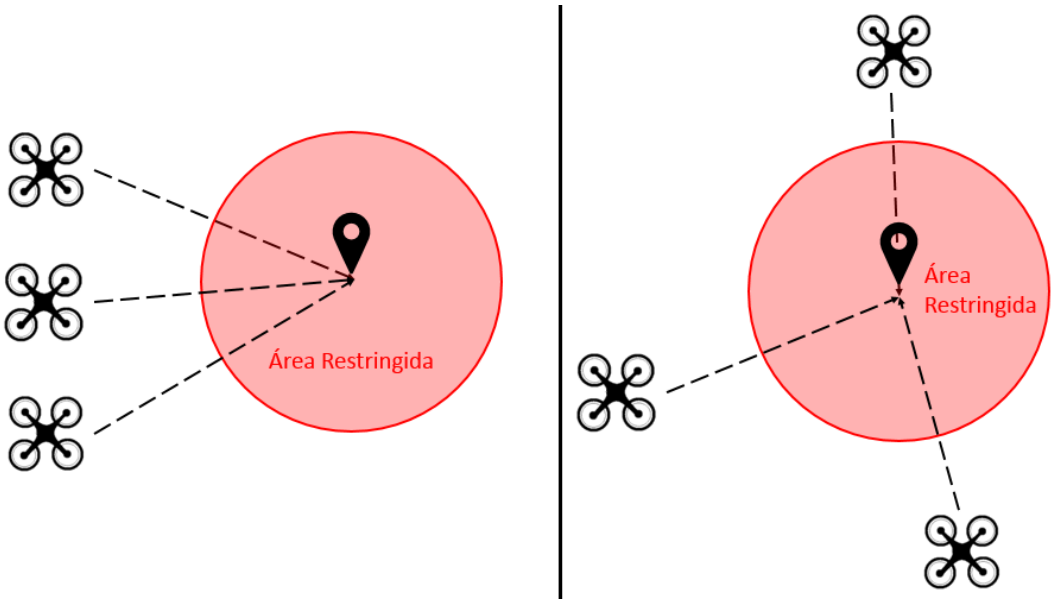

Figura 2: Distintas configuraciones de la flota de UAVs respecto al área restringida.

- Referencia interna de cada una de las aeronaves: Respecto a la referencia que pueden estar siguiendo cada UAV amenaza se han considerado dos alternativas. La primera de ellas contempla la posibilidad de que todas las aeronaves deseen ir al centro del área restringida. No obstante, existe la posibilidad de que no todas pretendan ir al mismo punto. Por este motivo, se analizarán también situaciones en las que cada UAV tenga una referencia distinta, contemplando la posibilidad de que el destino al que desee ir la aeronave no esté dentro del

área restringida, pero para llegar hasta él deba sobrevolar la zona a proteger. Estos escenarios aparecen reflejados en la Figura 3.

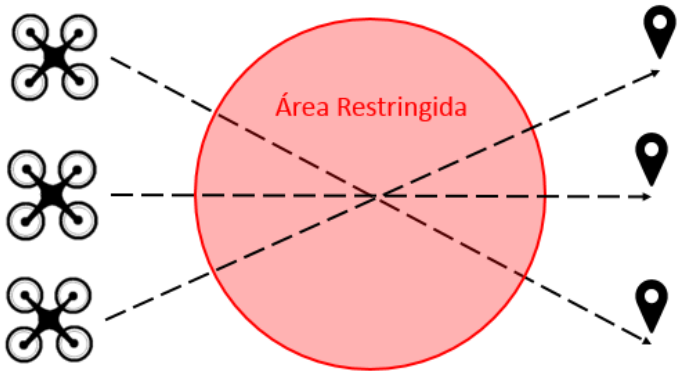

Figura 3: Representación de 3 UAVs que pretenden atravesar el área restringida.

3. ESTRATEGIAS DE SUPLANTACIÓN

Como ya se comentó anteriormente, el objetivo de este trabajo es analizar el comportamiento de una flota de UAVs cuando se ve afectada por la técnica *spoofing*, empleada como medida de defensa para proteger un área determinada. En esta sección se abordarán las diferentes estrategias que se pueden emplear para decidir en qué posición falsa deben creer las amenazas que se encuentran para conseguirlo, y estudiar el comportamiento que adoptaría cada una de ellas.

Es importante destacar que las estrategias analizadas se basan en que las señales GNSS falsas se emiten desde una sola antena. Por este motivo, es interesante estudiar en un primer momento cómo se aplicaría la técnica *spoofing* en el caso en que la amenaza sea un solo UAV.

Las aeronaves que vuelan de forma autónoma tratan de hacer coincidir la posición en la que creen que se encuentran con la referencia que pretenden alcanzar. Dicha estimación de la posición la realiza el módulo de navegación, apoyándose para ello principalmente en las señales GNSS. Tal y como se muestra en la Figura 4, la posición calculada por este módulo será una de las entradas del controlador del UAV, por lo que los cálculos realizados por este módulo afectan directamente a la acción de control calculada y enviada a los actuadores de la aeronave.

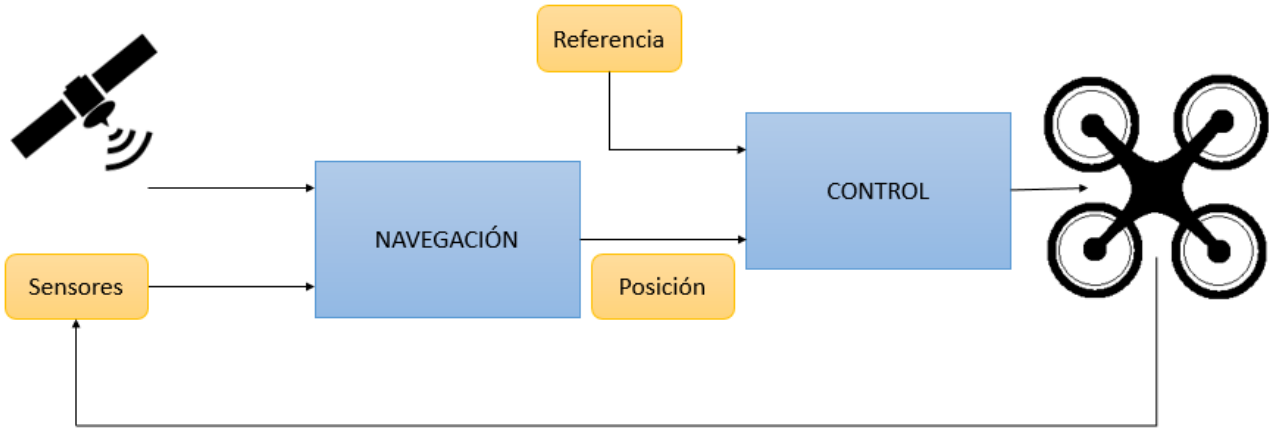

Figura 4: Estructura del control de navegación de un UAV.

La técnica *spoofing* pretende interferir directamente en una de las entradas del módulo de navegación, afectando de esta forma al sistema de control de la amenaza. La idea de emplear *spoofing* es generar señales falsas análogas a las de los satélites, de forma que el receptor del UAV amenaza crea que está en una posición distinta a la real para conseguir llevar a la aeronave a una zona de seguridad, evitando así que acceda a la zona restringida.

En el caso básico en el que sólo hay un UAV amenaza, la decisión de qué posición falsa enviar, es decir, en qué posición falsa debe creer la amenaza que se encuentra, se realiza en base a un algoritmo que tiene en cuenta su posición y la zona a la que se desea dirigirlo.

En el caso en el que la amenaza está formada por múltiples aeronaves es necesario decidir en base a qué UAV se van a generar las señales para proteger la zona restringida. A continuación, se describen las estrategias que se proponen y se estudian en este trabajo para generar las señales falsas, con la idea de que ninguna de las aeronaves amenaza sea capaz de acceder a la zona que se desea proteger.

3.1. Control en base al UAV que se encuentra más cercano a la zona protegida

Uno de los aspectos fundamentales para emplear el *spoofing* como técnica de defensa es que se debe conocer en todo momento la posición real de cada una de las amenazas. Por ello, se parte de la base de que se dispone de un radar o cualquier otro sistema que informe de las posiciones de las aeronaves.

Esta estrategia de control calcula en todo momento la distancia a la que se encuentra cada UAV del centro del área protegida y decide la posición falsa que debe enviar el *spoofer*, en base a la posición de la aeronave que se encuentre más cerca, tal y como se ilustra en la Figura 5. De esta forma se pretende que el vehículo más cercano se desvíe y no entre en la zona que se desea proteger. No obstante, como sólo se cuenta con una antena, la posición falsa que recibirán todas las amenazas será la misma, lo que puede provocar que al intentar alejar el UAV más próximo se consiga acercar a otro. Por este motivo, es necesario que continuamente se calculen las distancias entre las aeronaves y el centro del área restringida para, si en algún momento hay otra aeronave que esté más cerca de la zona a proteger, comenzar a controlar en base a ella.

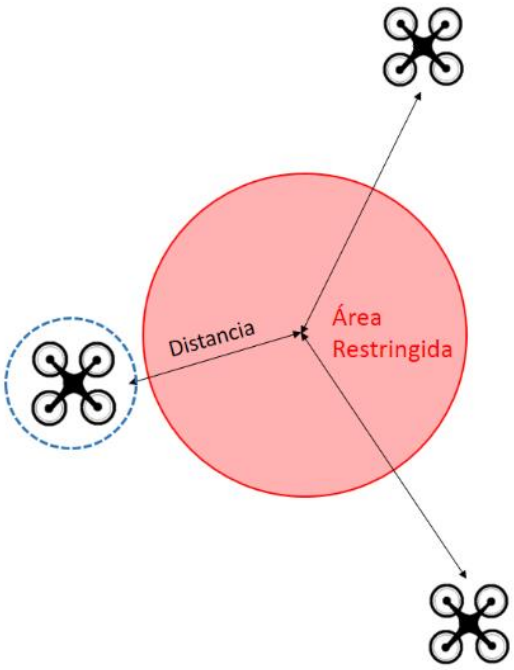

Figura 5: Representación del UAV más cercano como representativo de la flota.

3.2. Control en base a un UAV virtual

Al igual que en el apartado anterior, se parte de la premisa de que las posiciones de los UAV de la flota son conocidas en todo momento. Esta estrategia plantea la opción de controlar la posición falsa que se debe enviar en base a un UAV virtual que se encuentre en una posición intermedia, representando así a todas las amenazas. La posición de esta aeronave virtual se va actualizando en todo momento y depende de las posiciones actuales de las amenazas reales y de la distancia a la que se encuentren del área restringida. La Figura 6 representa la flota amenaza (cuadricópteros de color negro) y el UAV virtual (de color azul) en base al cual se realizaría el *spoofing*.

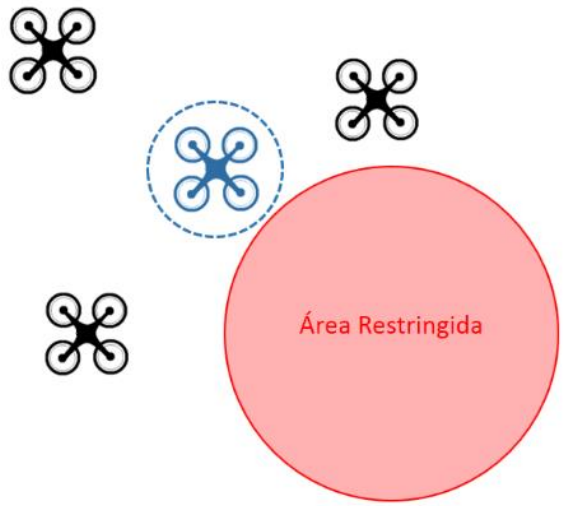

Figura 6: Representación del UAV virtual como representativo de la flota.

3.3. Selección de la zona a la que dirigir la amenaza

Otro parámetro que toma como entrada el algoritmo de *spoofing* que decide qué posición falsa enviar es la posición a la que se pretende llevar a la amenaza. En un caso general, esta posición puede ser prefijada. Sin embargo, como se muestra en la sección 4, una mala elección de la posición que se emplea como referencia en el algoritmo puede propiciar que las amenazas atraviesen el área restringida.

Por ello, se propone en este apartado una simple estrategia para la elección de la zona que el algoritmo tomará como referencia, en base a la posición del UAV amenaza, o representativo de la flota amenaza.

La estrategia se basa en la definición de un anillo de seguridad, de un determinado radio en torno a la zona a proteger, de forma que, cuando aparezca una amenaza dentro de este radio de seguridad, se tomará como posición segura de referencia a la intersección del anillo de seguridad con la línea perpendicular a aquella que conecta al UAV con el centro del área restringida. Esto se muestra gráficamente en la Figura 7, estando el anillo de seguridad representado en verde, y la referencia escogida finalmente resaltada sobre éste.

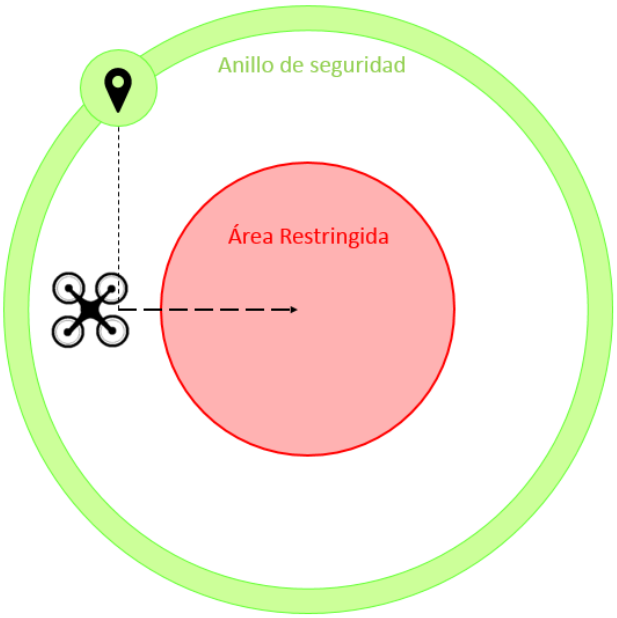

Figura 7: Representación de la selección del área segura a la que dirigir las amenazas.

4. SIMULACIONES Y EXPERIMENTOS

Esta sección presenta los resultados en simulación que ilustran cómo afecta los algoritmos de *spoofing* propuestos en este trabajo a una flota de UAVs que pretenden invadir un área restringida. Para ello, se presentan los resultados obtenidos en base a las distintas configuraciones de las amenazas relativas al área a proteger definidas en las Sección 2, así como distintas posibilidades en cuanto a las referencias que pretenden alcanzar dichas amenazas. Además, se estudia la influencia de la elección del área segura a la que se intentará dirigir a los UAVs en el éxito de la técnica defensiva.

Todas las simulaciones que se muestran en este apartado se han extraído de un escenario desarrollado en el entorno Matlab/Simulink. Se ha trabajado con un modelo matemático de un multicóptero, extraído de forma experimental. Mediante la repetición de modelos análogos a éste, ha sido posible simular una flota de tantos UAVs como se desee. Además, dicho escenario se ha implementado de forma que es posible seleccionar tanto las posiciones iniciales como las posiciones que pretenden alcanzar cada uno de los UAVs de forma independiente, de forma que el sistema de control de cada UAV intentará llevarlo hacia su objetivo. De esta manera, es posible simular el efecto que tendría en el comportamiento de cada aeronave el empleo de una posición falseada (*spoofing*).

Las simulaciones se han realizado en base a una serie de premisas:

- El *spoofing* se realiza con una sola antena, es decir, el artículo se centra en analizar cómo afecta el *spoofing* a una flota de UAVs cuando a todos ellos les llegan las mismas señales falsas.
- Las señales falsas llegan a todas las amenazas de la misma forma. Esto se traduce en la suposición de que todos los UAVs van a creer que están en la misma posición, que es la deseada al realizar el *spoofing*. Esto en la práctica puede no ser así, pero en las simulaciones realizadas se considera que los UAVs amenaza están a una distancia lo suficientemente similar de la antena como para poder despreciar la diferencia en el tiempo de viaje de cada señal.
- Se considera que el *spoofing* es efectivo. Es decir, se considera que los receptores GNSS de las amenazas son víctimas del *spoofing* en todo momento.

Como se comentó en la sección 3, el cálculo de la posición falsa a enviar se realiza tomando 1 de los UAVs (real o virtual) como el representativo de la flota. A continuación, se muestran las distintas simulaciones, agrupadas en función de qué UAV se toma como representativo de la flota, y el comportamiento de la misma ante el *spoofing*.

4.1. Control en base al UAV más cercano

Las simulaciones mostradas en esta subsección muestran cómo afecta el *spoofing* realizado sobre una flota de UAVs, cuando la posición falsa se calcula con el objetivo de dirigir al vehículo más cercano a un área restringida hacia un área de seguridad, intentando así evitar que alguna de las amenazas entre en el área a proteger.

La Figura 8 muestra un caso en el que aparecen tres UAVs, que se dirigen hacia el área restringida por el mismo lado, y que tienen como objetivo llegar al centro del área restringida. En todas las simulaciones mostradas el área restringida está representada por un círculo rojo, y las líneas de colores representan la trayectoria seguida por cada una de las amenazas, estando la posición inicial de los mismos cuando comienza a realizarse el *spoofing* representada por un rombo del color correspondiente. Además, la posición en la que aparece representado cada cuadricóptero es aquella en la que se encuentra al finalizar la simulación, y las líneas discontinuas representan la referencia que tratan de alcanzar los UAVs. Por otro lado, la circunferencia verde representa el área segura al que se pretende dirigir el UAV que se esté tomando como representativo de la flota.

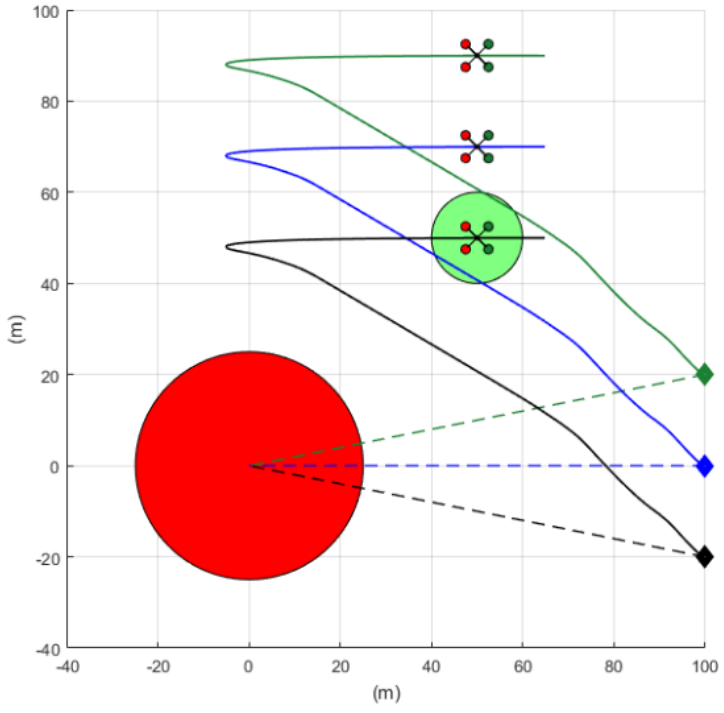

Figura 8: Trayectoria de 3 UAVs que quieren ir al centro del área restringida

En la Figura 8 se observa que el *spoofing* consigue sacar el cuadricóptero base de los cálculos (en este caso el más cercano) del área a proteger, mientras que los otros UAVs realizan una trayectoria similar pero desplazada, debido principalmente a que todos tienen como referencia el mismo punto. Cabe destacar que, falseando todas las amenazas con el punto, en la mayoría de casos será imposible dirigirlos a todos hacia la zona segura.

La Figura 9 muestra una situación similar, pero más compleja de controlar. En este caso, los 3 UAVs parten de las mismas posiciones que en la Figura 8, pero en este caso la referencia que desean alcanzar no es el centro de la zona restringida. En este caso, el punto de referencia final que tiene cada uno de los UAVs se encuentra en la línea que une el punto inicial con el centro del área restringida, pero al otro lado de la misma.

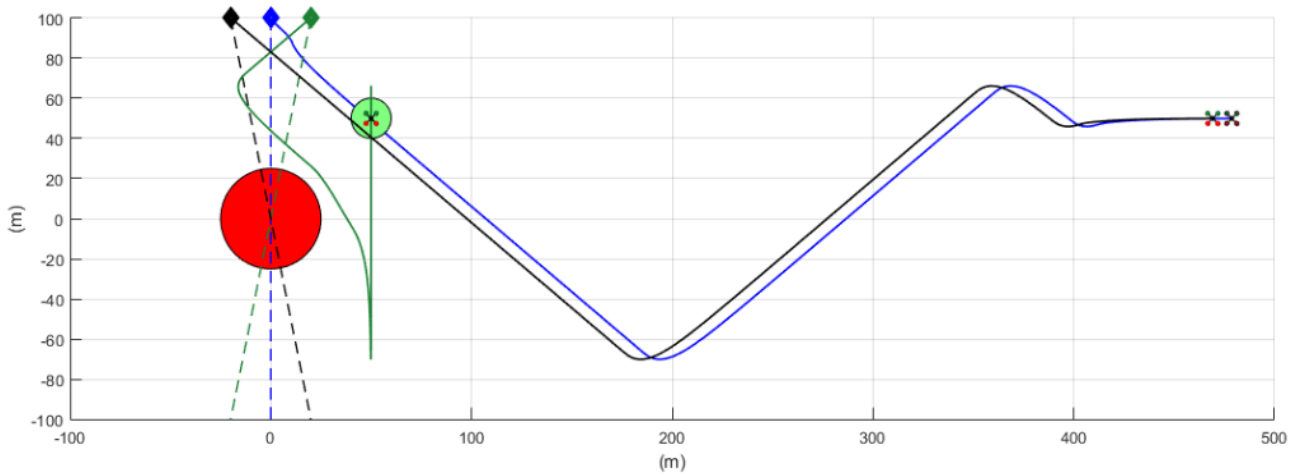

Figura 9: Trayectoria de 3 UAVs que pretenden atravesar el área prohibida

Dado que cada aeronave tiene una referencia distinta, se observa que se consigue dirigir a la aeronave más cercana a la zona de seguridad deseada, mientras que el resto de los UAVs se desvían indefinidamente fuera de la zona a proteger.

Otro aspecto que influye en las probabilidades de éxito a la hora de tratar de impedir a una flota de UAVs la entrada en un área restringida es la elección de la zona segura a la que se desea dirigir al vehículo representativo de la flota. Para ilustrar esto, la Figura 10 muestra una situación similar a la mostrada en la Figura 8, pero en este caso la flota se aproxima a la zona prohibida por el lado opuesto.

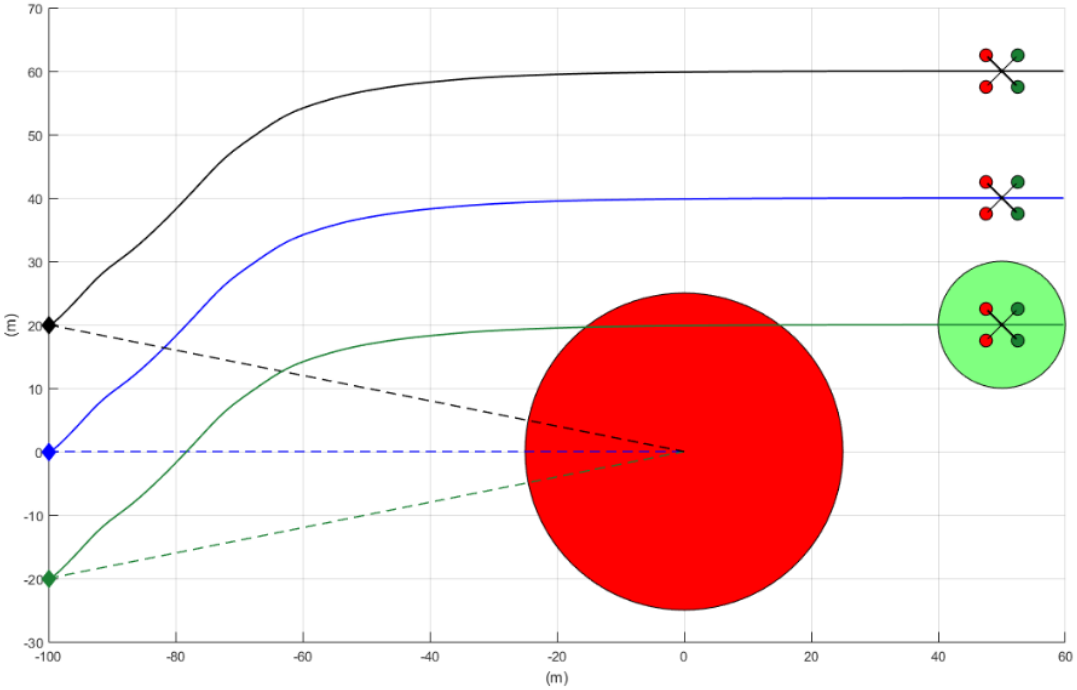

Figura 10: Situación similar a la Figura 8, pero con la flota aproximándose por el lado opuesto.

En la Figura 10 se observa que, ante una situación a priori sencilla en la disposición de los UAVs, una mala elección de la zona de seguridad hace que uno de los vehículos entre en la zona restringida. Una posibilidad es la elección automática del área de seguridad en base a la posición del UAV más cercano. Utilizando la estrategia presentada en la subsección 3.3, se obtiene el resultado mostrado en la Figura 11. Como se observa, se vuelve a evitar que todos los vehículos pasen por la zona restringida.

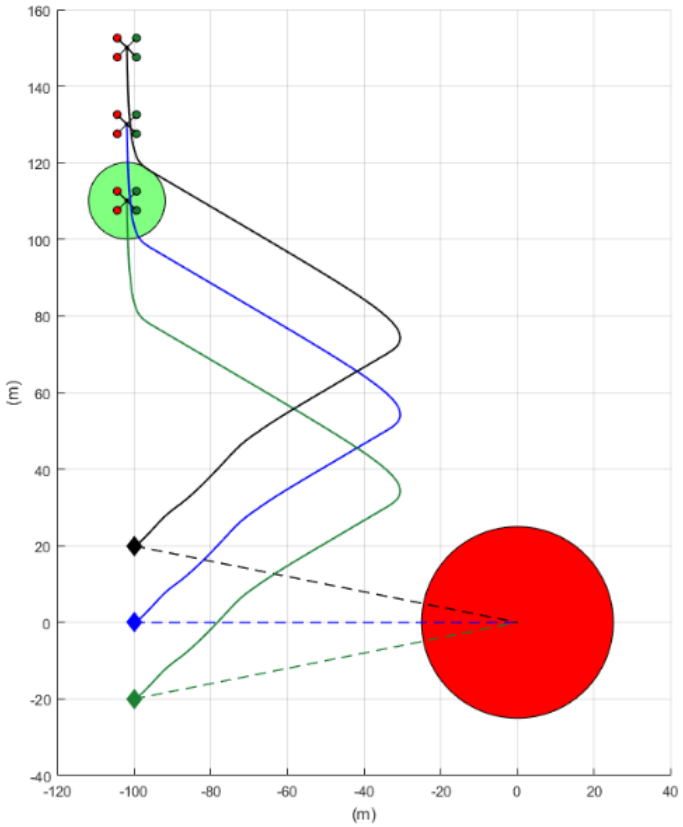

Figura 11: Comportamiento de 3 UAVs que se dirigen al centro de la zona restringida, con selección automática de zona segura

Sin embargo, es posible que las flotas de UAVs no se acerquen a la zona restringida por el mismo lado, sino de forma distribuida. La Figura 12 muestra una situación en la que cada vehículo se aproxima por un sitio distinto, y todos ellos tienen como objetivo alcanzar el centro de la zona restringida.

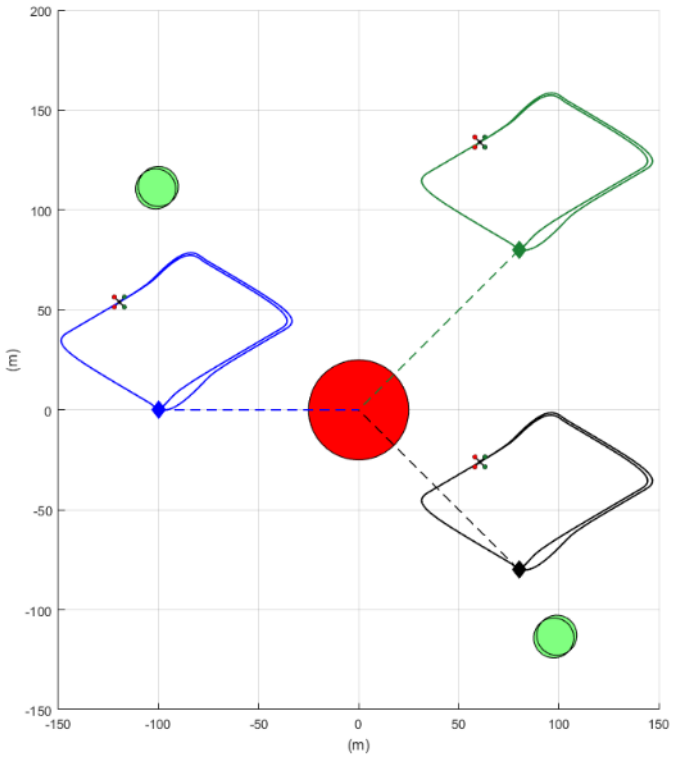

Figura 12: Situación en la que 3 amenazas pretenden alcanzar el centro del área protegida, cada una por un lado distinto.

Como se ilustró en la Figura 11, situar la zona segura a la que se pretende que se dirija la amenaza más cercana en un punto fijo puede ser perjudicial según la dirección por la que se acerque dicha amenaza. Esto se acentúa en el caso de amenazas que se acercan por distintas direcciones, ya que es probable que alguna de ellas se introduzca en la zona restringida al intentar ser llevada al área segura. Por ello, en la Figura 12 se muestran distintas zonas seguras, correspondientes a las que se han ido calculando automáticamente cada vez que cambiaba el UAV que se encontraba más cerca del área a proteger. De esta forma, se observa que las amenazas realizan un circuito cerrado, fruto de estar intentando ser dirigidas a una zona segura distinta en cada momento. De la misma forma que en el caso de la Figura 8, las trayectorias de las aeronaves tienen formas muy similares debido a que todas pretenden alcanzar la misma referencia.

Por otro lado, cabe destacar que la probabilidad de que en esta trayectoria cerrada algún UAV entre en algún momento en la zona restringida o no depende en gran medida de la velocidad que lleve cada aeronave, así como de la distancia respecto a esta zona a la que se comienza a realizar el *spoofing*.

A continuación, la Figura 13 muestra una situación muy desfavorable a la hora de intentar evitar que una flota de UAVs entre en un área restringida. Esta situación es aquella en la que las aeronaves que conforman la flota se aproximan de forma distribuida al área protegida, y su objetivo es sobrepasar esta zona, es decir, pasar por ella, pero no quedarse en el centro, lo que se traduce en que cada aeronave tiene una referencia distinta. Aplicando la estrategia comentada, se obtiene el siguiente resultado:

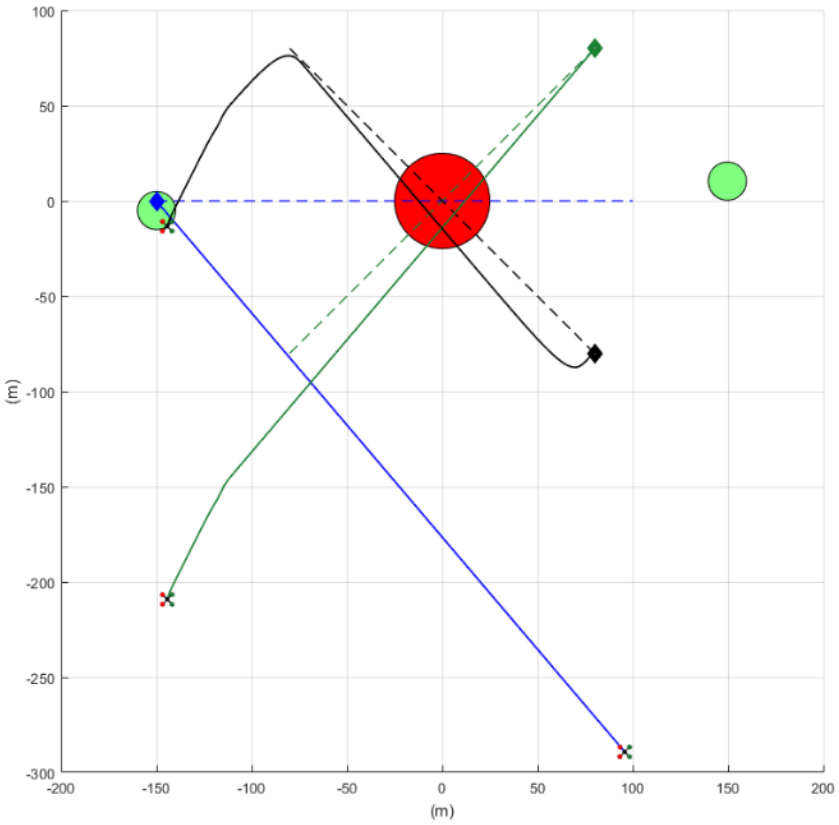

Figura 13: Situación en la que 3 amenazas pretenden sobrepasar el área protegida, cada una por un lado distinto.

Como se observa en la Figura 13, en esta disposición no ha sido posible evitar que dos de las amenazas atraviesen el área restringida. De hecho, independientemente de la estrategia empleada, para el caso en el que una flota de UAVs se acerque a una zona protegida por distintas direcciones, y tengan el objetivo de sobrevolarla, puede resultar imposible evitar que alguno de los vehículos sobrepase el área a proteger, ya que puede no existir ninguna posición falsa que, siendo la misma para toda la flota, haga retroceder a todas las aeronaves.

4.2. Control en base a un UAV virtual que representa a la flota

En este apartado se muestran una serie de simulaciones que reflejan situaciones similares a las de la sección anterior, pero empleando la estrategia presentada en el apartado 3.2, que consiste en tomar como vehículo representativo de la flota a un UAV virtual, situado en una posición calculada en base a las posiciones de cada uno de los vehículos de la flota, así como la distancia de cada uno de ellos respecto al área protegida.

La Figura 14 representa una situación idéntica a la mostrada en la Figura 8 (toda la flota se aproxima por el mismo lado, y pretende alcanzar el centro del área protegida), con la única diferencia de la mencionada determinación del UAV representativo de la flota. En esta figura se muestran tanto la representación de las trayectorias de las 3 aeronaves, como la posición del vehículo ficticio que se toma como referencia en todo momento (representado por una estela de círculos negros en todas las simulaciones).

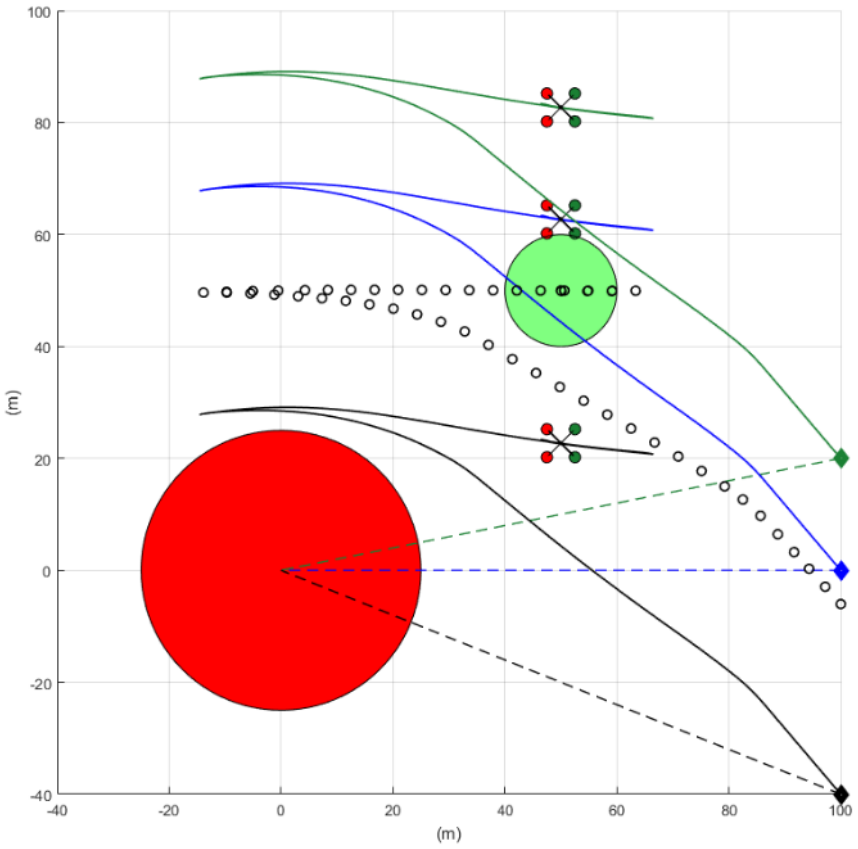

Figura 14: Trayectoria de 3 UAVs que quieren ir al centro del área restringida, y UAV virtual.

Al controlar en base a un UAV virtual, es éste el que acaba situándose en la zona segura a la que se pretende llevar la flota. Ésta es una diferencia fundamental con respecto al método del apartado anterior, ya que en este caso no se pretende que ninguno de los vehículos individuales se dirija a la zona segura, sino el UAV virtual representativo de la flota.

El hecho de centrarse en la posición del UAV virtual hace que el algoritmo tenga en cuenta la posición de toda la flota, y no sólo del vehículo más cercano, lo cual puede ser perjudicial en algunas ocasiones, ya que puede ocurrir que el UAV virtual no pase por el área restringida, pero alguno de las aeronaves que conforman la flota sí que lo haga. Un ejemplo de esto se muestra en la Figura 15(izquierda), en la que aparecen 3 UAVs por el mismo lado, y que pretenden llegar al lado opuesto de la zona prohibida, atravesando a ésta (en esta figura no se representan las referencias de las amenazas para evitar confusión). En ella, se observa que el UAV ficticio acaba en la zona segura y no llega a entrar en el área restringida, mientras que uno de los UAVs de la flota sí que entra en la misma. Un caso más claro se muestra en la Figura 15(derecha). En ella, tres aeronaves se acercan desde distintos lados, aproximadamente en una disposición regular en torno a la zona restringida, y tienen el objetivo de alcanzar el centro de la misma. Se trata de una situación idéntica a la mostrada en la Figura 12, en la que se conseguía evitar que alguno de los integrantes de la flota invadiera la zona restringida. Sin embargo, en este caso se controla en base a un UAV virtual, que en el instante inicial se encuentra dentro del área restringida. El algoritmo es capaz de expulsar este UAV virtual de la zona restringida y de conducirlo a la zona segura, pero para conseguirlo se observa que uno de los vehículos de la flota ha atravesado la zona prohibida.

Se infiere de esta última simulación que esta estrategia puede ser menos adecuada para casos en los que las amenazas se aproximan a la zona restringida desde distintas direcciones, ya que la

aproximación del UAV virtual puede conllevar una pérdida de información importante en estos casos concretos.

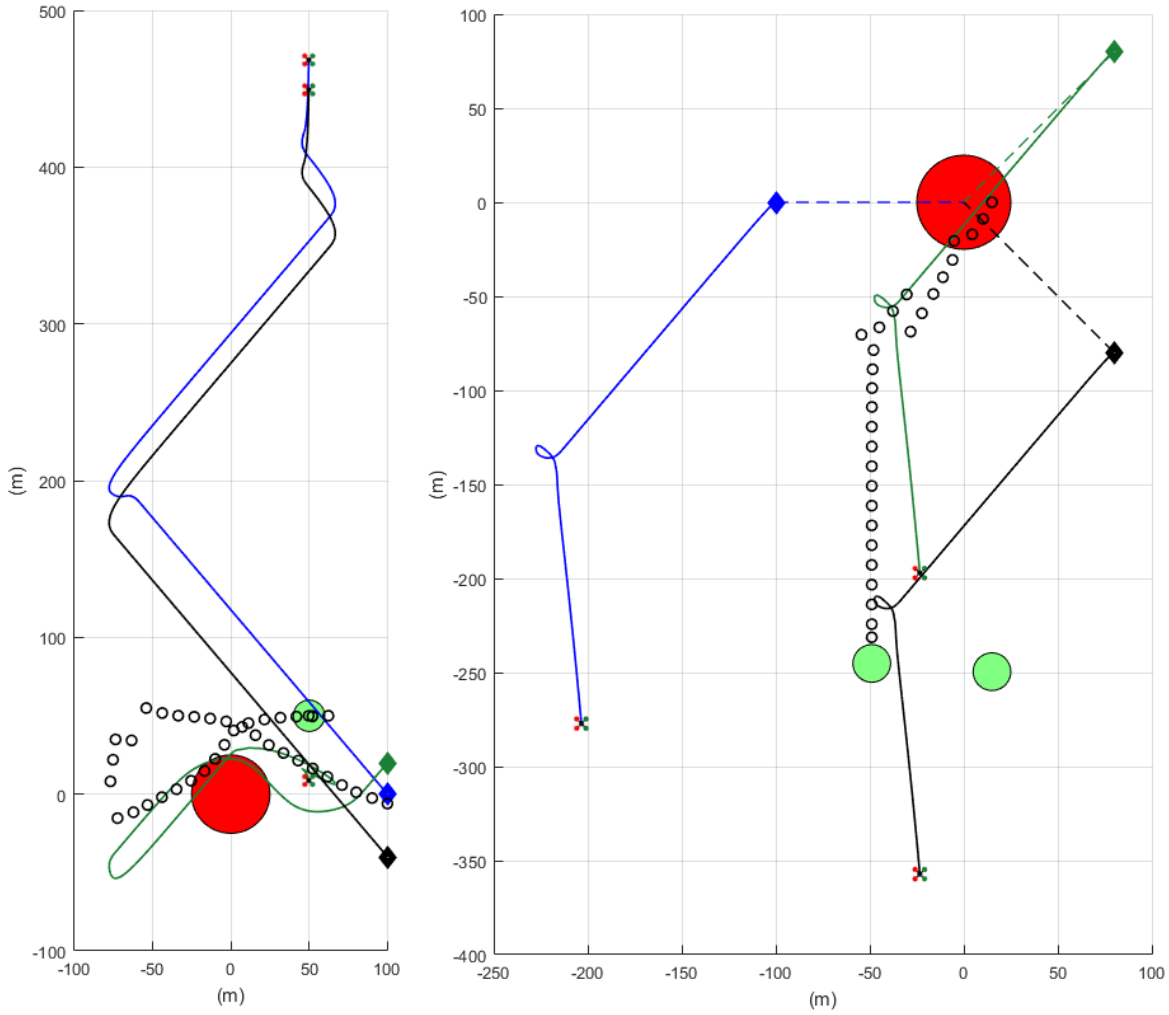

Figura 15: Representación de 3 UAVs y el ficticio cuando: Parten del mismo lado y pretenden sobrevolar el área restringida (izquierda); Parten de distintos lados del área restringida y pretenden ir al centro de la misma (derecha).

Una vez analizadas las simulaciones mostradas en esta sección, queda patente que el comportamiento de una flota de UAVs cuando se realiza un *spoofing* con una sola antena depende fuertemente de la disposición de las aeronaves que la conforman, así como de la referencia que tenga programado alcanzar cada una de las aeronaves, existiendo situaciones en las que no es posible proteger una zona restringida con garantías antes determinadas disposiciones de la amenaza.

5. CONCLUSIONES

Se ha analizado la influencia de un *spoofing* realizado con una única antena sobre una flota de UAVs, y se ha estudiado la posibilidad de emplear esta técnica en la defensa de un área restringida. Para ello, se han mostrado una serie de simulaciones suponiendo distintas configuraciones de la flota y distintas referencias para cada una de las aeronaves que la conforman. Apoyándose en las simulaciones realizadas, se han extraído una serie de conclusiones:

La forma en que un *spoofing* afecta a cada aeronave de la flota, así como la probabilidad de que se consiga evitar que las aeronaves entren en un área restringida empleando las técnicas mencionadas, depende en gran medida tanto de la disposición de cada uno de los UAVs de la flota como de la

referencia que internamente pretenden alcanzar. Así, se ha observado que, cuando todas las aeronaves pretenden alcanzar una referencia común (el centro del área a proteger en las simulaciones de la sección anterior), las trayectorias resultantes del *spoofing* sobre cada aeronave tienden a ser bastante similares entre sí. En cambio, cuando cada UAV de la flota pretende alcanzar una referencia distinta, el *spoofing* afecta de manera distinta a cada integrante de la flota, por lo que resulta más complicado evitar que alguna de las aeronaves entre en el área restringida. Además, la distancia a la que es necesario comenzar a realizar el *spoofing* para aumentar las probabilidades de éxito al intentar proteger un área restringida depende también de la velocidad con la que se acercan los UAVs.

Cuando los UAVs de la flota se aproximan desde distintas direcciones, se considera más adecuada la estrategia de controlar la flota en base al vehículo más cercano, en lugar de respecto a un UAV ficticio, como se ilustró en las simulaciones de la sección anterior.

Por otra parte, hay situaciones en las que evitar que alguno de los UAVs de una flota entre en el área restringida resulta imposible, al menos con una sola antena que falsee la misma posición para todas las aeronaves. Un ejemplo de estas situaciones es aquella en la que un gran número de UAVs se aproximan a la zona restringida, cada una desde una dirección distinta y en disposición radial, y con el objetivo de sobrevolar el centro de dicha zona. En este caso, no existe una posición falsa que haga que todos los UAVs se desvíen y no entren en la zona restringida, ya que siempre existirá algún UAV cuya referencia apunte hacia la posición falsa elegida, manteniéndose por tanto en su trayectoria original. En este caso, sería necesario realizar distintos *spoofing* desde distintas antenas, enviando señales falsas distintas a distintos sectores del espacio. Esta situación más desfavorable se hace más realista a medida que incrementa el número de amenazas de la flota, al ser posible cubrir un mayor rango de direcciones de aproximación, por lo que este incremento del número de integrantes es un factor muy a tener en cuenta a la hora de seleccionar la estrategia de defensa más efectiva.

Pueden existir también otras limitaciones, en función de las herramientas *anti-spoofing* con las que puedan contar las amenazas, ya que al actuar con una sola antena es inevitable que aparezcan saltos repentinos en la posición aparente de alguno de los UAVs, por lo que es más fácilmente detectable.

Como conclusión, se demuestra que el problema estudiado es un problema de gran complejidad, y que a menudo será necesario el uso de más de una antena, que permitan enviar distintas posiciones falsas en función de la disposición de la flota, para así conseguir una mayor probabilidad de éxito en la protección de un área restringida. En esta línea surgen distintas posibilidades como trabajo futuro. Es posible estudiar el mencionado *spoofing* con más de una antena, para aquellas situaciones más desfavorables, o introducir técnicas de inteligencia artificial, tales como redes neurales, para seleccionar la técnica defensiva más adecuada en función de la tipología y configuración de la amenaza que se necesite neutralizar.

6. BIBLIOGRAFÍA

[1] A. Muñoz Cueva, P. López Torres, A. Arce, S. Blanco y R. Galán, «Técnicas de neutralización de amenazas aéreas basadas en el sistema de posicionamiento Galileo,» de *CIVILDRON'17*, Madrid, 2017.

[2] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen y S. Capkun, «On the Requirements for Succesful GPS Spoofing Attacks,» 2011.

[3] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley y D. Brumley, «GPS Software Attacks,» 2012.

[4] A. RÜGAMER y D. KOWALEWSKI, «Jamming and Spoofing of GNSS Signals – An Underestimated Risk?!,» 2015.

[5] D. Plausinaitis, «GPS And Other GNSS Signals,» 2009.

[6] D. A. G. Álvarez, «Sistema GNSS,» Madrid, 2008.

[7] S. A. S. Bernal, «Detection solution analysis for simplistic spoofing attacks in commercial mini and micro UAVs,» 2008.

[8] Y. Q. Huang Lin, «GPS Spoofing, Low cost GPS simulator,» 2015.