Estado del Arte de las Tecnologías Antidrón

Cátedra Isdefe-UPM

Junio 2018

Contenido

1 Introducción

En la actualidad, el uso de vehículos aéreos remotamente tripulados (RPAs) está en crecimiento explosivo, apareciendo cada día nuevas aplicaciones de esta tecnología en muy diferentes ámbitos. Dado que la accesibilidad a los RPAs ha aumentado de forma exponencial en los últimos años, así lo ha hecho también la probabilidad de que se produzcan usos negligentes, o directamente malintencionados, lo que se traduce en una amenaza a la seguridad de las personas. Hasta ahora, la inmensa mayoría de los incidentes que se han producido en el ámbito civil se han debido al uso negligente o descuidado de la plataforma (uso en cercanías de aeropuertos o centrales nucleares, por ejemplo), considerándose que la probabilidad de que se produzca un acto terrorista basado en RPAs es actualmente muy baja. Sin embargo no debe bajarse la guardia en este sentido, ya que evidentemente no tiene el mismo grado de dificultad tratar de neutralizar a un dron de juguete operado con descuido, quea una plataforma profesional que haya tomado medidas para su propia protección.

En este pequeño estudio se analizan las distintas tecnologías existentes, que en muchos casos deben colaborar de manera armónica, para garantizar una protección suficiente, y que se están convirtiendo en objeto de interés prioritario en las políticas de I+D europeas **[1]**. La razón principal es que esta amenaza conlleva retos no completamente resueltos por las tecnologías actuales, por lo que actualmente constituyen una importante área de investigación.

1.1 Fases del proceso

Se acostumbra a dividir el proceso de defensa anti-dron en tres fases [2], aunque según como se plantee la estrategia algunas de ellas pueden tener fronteras difusas, o también definir fases adicionales. La clasificación más utilizada es la siguiente:

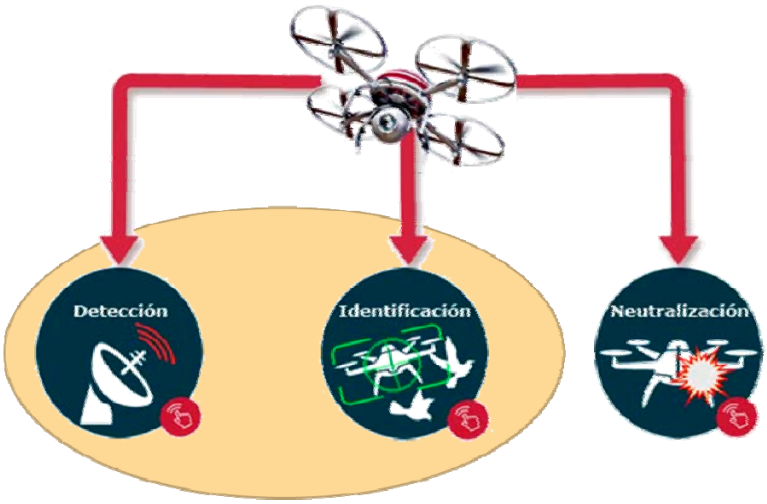

Figura 1. Fases de actuación en la defensa anti-dron

Detección. Permite levantar una alarma de que se ha producido una intromisión de un objeto no identificado en el volumen bajo vigilancia. En función del sensor empleado, esta etapa permite obtener distinto tipo de información de los blancos, tales como su posición angular, distancia al sensor, velocidad o tamaño. Además, es conveniente realizar un seguimiento de los blancos detectados para conocer su trayectoria y generar alarmas tempranas de posibles amenazas. Sin embargo, esta etapa no conlleva diferenciar las detecciones provocadas por RPAs de las de otros blancos que no son de interés como coches o aves.

Identificación. Consiste en la discriminación del blanco objetivo frente otros objetos o que no son de interés (por ejemplo aves) y que han sido detectados en la etapa anterior. De esta forma se reduce el número de las llamada "nuissance alarms" evitando una sobreactuación de los sistemas de neutralización. Con algunas tecnologías, esta fase y la anterior tienen fronteras difusas, haciéndose un proceso que en conjunto proporciona ambas funcionalidades, casi de manera simultánea.

Neutralización. En el caso de clasificar la detección como una amenaza, se tomará la decisión de actuar de forma que se garantice la protección del emplazamiento, bien o personas bajo amenaza. A menudo se define una intensidad de actuación distinta en función de la gravedad de la amenaza.

Debe tenerse en cuenta que actualmente las distancias típicas de detección de los drones son sólo de unos pocos Km, y que a sus velocidades de vuelo, esto implica una rápida secuenciación de las tres fases antes mencionadas (ver figura 2)

En los siguientes capítulos se presentan las tecnologías más destacadas para cada una de estas fases, junto a sus carencias y fortalezas.

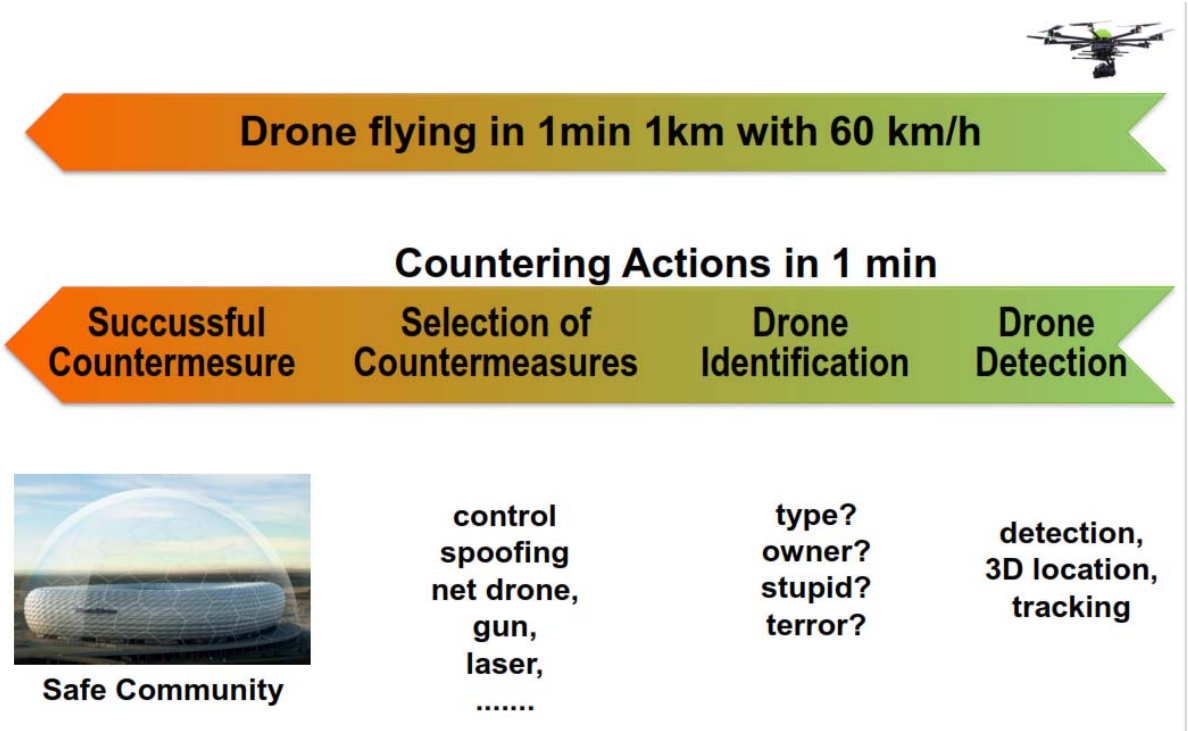

Figura 2. Las tres fases de la defensa antidrón en acción

2 Detección

En este primer paso el objetivo es conseguir detectar la posición de los blancos alcanzando un compromiso entre la dificultad intrínseca que supone detectar este tipo de blancosy el empleo de sensores de bajo coste y tamaño reducido. El entorno de aplicación para el que se enfoca cada despliegue tiene un papel decisivo en cuanto a las tecnologías que se utilizan, siendo unas más efectivas que otras.

2.1 Tecnología radar

2.1.1 Consideraciones de detección mediante radares convencionales

El radar es el detector más eficaz ante este tipo de amenaza. Las razones son varias:

- Es realmente el único sensor que trabaja en todo-tiempo, tanto de día como de noche, en presencia de lluvia o niebla, o de baja visibilidad en general. Esto es debido a que trabaja en el rango de las microondas que tienen alta capacidad de atravesar distintos medios de propagación.
- A diferencia de otros sensores, no se basa en la emisión de ningún tipo de señal (acústica o electromagnética) por parte del dron, por lo que puede detectar drones silenciosos.
- Es capaz de explorar alcances de varios kilómetros de distancia por varias decenas/centenas de metros de altura conn tiempos de hasta 1 segundo de refresco de la información
- Es capaz de indicar la posición del objetivo en distancia, acimut y opcionalmente altura

Sin embargo no puede ignorarse que la problemática de detección de drones mediante radares no está exenta de retos. Básicamente estos retos se concretan en tres características del blanco: son pequeños, vuelan lento y vuelan bajo. Las implicaciones de estas características se describen en la tabla de la figura 3.

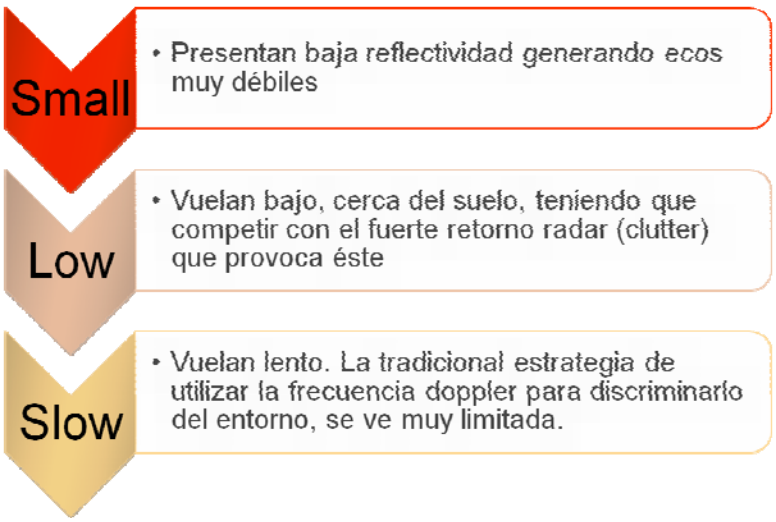

Figura 3. Problemática en la detección de drones mediante rádar

A estos condicionantes se une la necesidad de que el sensor sea de relativamente bajo coste, pequeño tamaño y no requiera una infraestructura de instalación excesiva. No tiene mucho sentido necesitar adquirir un sensor de 20 millones de euros para protegernos de una amenaza que cuesta 50€. Por otra parte, hay muchas instalaciones que requieren protección y que no pueden permitirse instalar una gran infraestructura radárica. Por lo que el foco se ha puesto en radares compactos y de coste moderado.

Afortunadamente, en los últimos años, habían aparecido en el mercado radares con estas características. Radares pensados principalmente para la vigilancia de fronteras terrestres y que se caracterizaban precisamente por ser compactos y económicos. Básicamente lo que ha ocurrido en los últimos años es que las empresas que tenían estos dispositivos los han adaptado de forma muy rápida a la nueva amenaza reconfigurando el diagrama de radiación de la antena y actualizando el firmware de detección y tracking. A nivel europeo estas empresas son las líderes en estos momentos del mercado: Blighter en el Reino Unido, Robin Radar en Holanda y Advanced Radar Technologies en España.

A pesar de todos los problemas mencionados, en aquellos emplazamientos donde la instalación de este tipo de radares ha sido viable, han demostrado ser el sensor más eficaz de los disponibles en la actualidad [3].

Figura 4. Drone-Sentinel de ART.S.A.

En muchas ocasiones, este tipo de radares utiliza onda continua, lo que permite grandes alcances sin necesidad de transmisores de alta potencia de pico, y muy alta resolución, lo que les da ventaja frente al clutter. A menudo es necesario alcanzar un compromiso entre tiempo de iluminación del objetivo (lo que mejora el alcance) y el tiempo de refresco de información, de modo que en algunos de estos equipos (por ejemplo los fabricados por Blighter) pueden configurarse bien para altas tasas de refresco, bien para largos alcances, pero no ambas cosas a la vez.

El reto más inminente de estos equipos es proporcionar información de altura. Por la necesidad de ser compactos y de bajo coste no es posible plantearse radares 3D (salvo en emplazamientos en que justifiquen instalar un radar de grandes dimensiones). Pero sí es posible introducir en el sensor elementos capaces de dar información de altura del blanco detectado. Esta resulta muy útil para por ejemplo enfocar posteriormente una cámara (fase de identificación) o dirigir mejor un ataque electromagnético (fase de neutralización).

2.1.2 Arquitecturas radar no convencionales

Dados los grandes problemas que representa la amenaza dron a los radares convencionales, se han planteado (y desarrollado) arquitecturas novedosas optimizadas para esta problemática. Entre ellas destacan los radares persistentes y los radares MIMO.

Los radares persistentes se basan en cubrir el volumen de vigilancia de manera permanente,

utilizando haces simultáneos en todas las direcciones, en lugar de un haz de antena que explora el espacio de manera secuencial. De esta forma, al no requerir la exploración mecánica o electrónica de los haces, se puede aumentar el tiempo de iluminación e integración sobre los blancos sin afectar al tiempo de refresco de la información por lo que se mejora la capacidad de detección de blancos de sección radar reducida.

Esta arquitectura es capaz de solucionar una parte de los problemas debidos a la baja sección radar de los RPAs y al ocultamiento por el clutter de tierra de los RPAs que vuelan a baja velocidad. Sin embargo, el principal problema que presenta este tipo de radares es el aumento de complejidad y tamaño al necesitar al menos tantos receptores y procesadores como distintos haces en acimut y elevación se requieran. Además, se debe evaluar si el aumento del tiempo de integración tiene efectos adversos en la capacidad de detección de RPAs de gran velocidad por la migración en distancia y Doppler que puede producirse. Para mitigar estos efectos, se han desarrollado técnicas de compensación de movimiento, necesarias para blancos veloces y en aceleración.

Ya existen en el mercado radares con esta filosofía. En particular la empresa israelí IAI dispone del sistema EL2112 que ha vendido ampliamente en USA. En Europa existen varias iniciativas como por ejemplo el Radar Holográfico, desarrollado por Aveillant en el Reino Unido. En España existe en la actualidad en programa Coincidente financiado por el Ministerio de Defensa para el desarrollo de un radar de estas características [4]

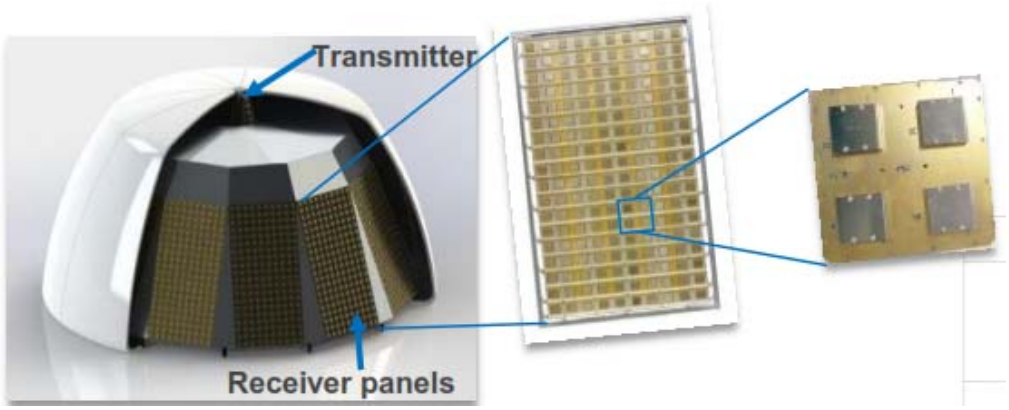

Figura 5. Sistema radiante de un moderno radar persistente

Otra tecnología con gran potencial son los radares MIMO (Multiple Input Multiple Output). En este planteamiento se utiliza la redundancia de receptores y transmisores para mejorar las características del sistema, utilizando sofisticados procesados de señal. Una de sus grandes ventajas es que relajan mucho los requisitos del hardware de cada nodo, substituyendo un único gran y complejo nodo central, por una red de sensores de bajo coste y procesado de señal intensivo. Todavía no son una realidad en el mercado, pero ya existen demostradores tecnológicos en universidades y centros deI+D.

2.2 Sonido

La detección de RPAs mediante técnicas acústicas se hace necesaria debido a las limitaciones en la aplicación de las tecnologías radar anteriores en ciertos entornos, como por ejemplo ciudades. El uso de estos radares es adecuado en entornos abiertos o en infraestructuras aisladas, pero poseen claras limitaciones en entornos urbanos debido al incremento excesivo de detecciones provocadas por otros elementos del entorno, que darían lugar a falsas alarmas, además de las implicaciones que tiene la radiación indiscriminada de potencia hacia las personas.

Algunas soluciones se basan en sensores sísmicos enterrados, creando un perímetro de seguridad en la zona que se desea proteger, con alcances de detección y seguimiento de centenares

de metros. Por otra parte existen sistemas que además son capaces de realizar una clasificación del tipo del RPA y que trabajan con dos tipos de sensores distintos, sensores acústicos omnidireccionales y sensores directivos de largo alcance

Otras técnicas tratan la huella digital acústica de los RPA, utilizada también en otros tipos de aplicaciones ya bastante maduras en otros campos, como en el reconocimiento de canciones o de personas por el habla. El objetivo es la identificación de patrones o firmas de una captura de audio, para que pueda ser reconocido contra una base de datos. En esta técnica así como en la del apartado siguiente, la detección y la identificación se realizan de manera simultánea.

La detección acústica mediante arrays de micrófonos es posiblemente la técnica más prometedora en este tipo de entornos donde los radares no son tan eficaces. El procesado en array permite realizar una estimación de la posición del RPA, aumentar el alcance de detección respecto al uso de un sólo micrófono, y realizar una clasificación basada en su huella sonora.

Sin embargo todavía sus prestaciones no son todo lo buenas que se requiere, en particular en lo que se refiere a la distancia de detección para que permita un tiempo de reacción suficiente.

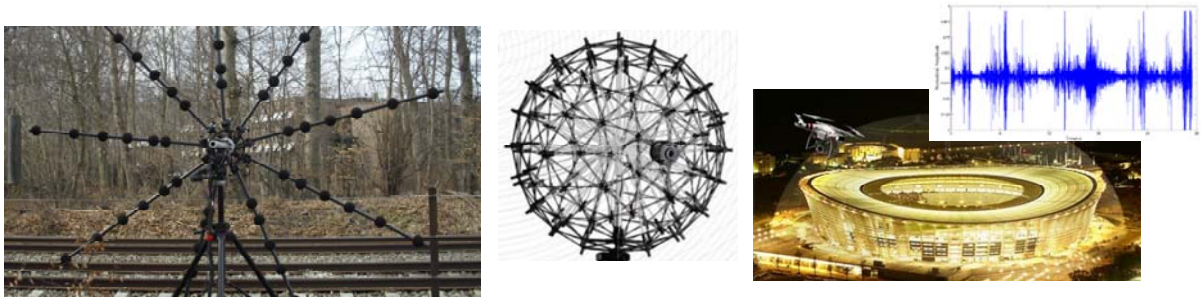

Figura 6. Utilización de arrays de micrófonos y detección de huella sonora para detección de UAVs en entornos donde no es viable la utilización de radares.

El problema que presenta este tipo de detección es la discriminación y reconocimiento satisfactorio en presencia de otras fuentes de ruido, frente al sonido del RPA. Múltiples investigaciones tratan de mejorar la capacidad de detección de las fuentes sonoras de interés en entornos ruidosos mediante el empleo de arrays de micrófonos y procesados de señal robustos de alta carga computacional.

Sin embargo, los arrays de micrófonos, al ser sensores pasivos, presentan generalmente un alcance reducido, aunque puede aumentarse o reducirse en función de la dirección del viento. Además, se debe tener en cuenta que los RPAs de ala fija (aeroplanos) no pueden ser detectados por esta tecnología al no emitir apenas sonido.

2.3 Vigilancia espectral de radiofrecuencia

Lo que se busca en este caso, es realizar la detección de las señales intercambiadas entre estación base y el RPA mediante equipos de vigilancia espectral. Pueden tratarse de comunicaciones UHF, WiFi o por satélite, aunque, en general, los RPAs emplean las bandas de frecuencia de 2,4 GHz, de 5 GHz o de 5,8 GHz**,** en ocasiones de forma simultánea. Una de las opciones para este tipo de detección es mediante la identificación de la modulación utilizada y de las características de los datos, ya que el problema principal es la gran cantidad de señales en estas bandas que pueden encontrarse, y la discriminación de cuáles de ellas implican a RPAs.

Una de las soluciones comerciales disponibles en el mercado es el sistema Aaronia Drone Detector, formado por un array de antenas y un analizador de espectros que cubren las frecuencias desde 9 kHz hasta 20 Ghz. El sistema trabaja en tiempo real, capturando y realizando el seguimiento de las emisiones de RF que se producen, activando una alarma automática en el caso de superar los valores máximos. Adicionalmente tiene la ventaja de ser compacto y flexible,

dando la opción de desplegarse en pocos minutos en la zona deseada. Gracias al software que incorpora trabajando en tiempo real, se estima la dirección en la que se encuentra el RPA, pudiendo identificar el tipo de RPA y rastrear el operador que lo controla.

Figura 7. Aaronia Drone Detector.

Sin embargo, este método no es capaz de detectar aquellos RPAs "silenciosos" que no mantienen un enlace de comunicaciones descendente con la estación base. En el caso de RPAs telecomnadados es a pesar de todo posible la detección de la señal de control, sin embargo la ubicación que entrega no es la del RPA sino la del piloto remoto. Por este motivo, en el ámbito de la defensa, o en sistemas que necesiten una actuación rápida contra la plataforma no es conveniente utilizar sistemas basados únicamente en este tipo de detección.

Una ventaja, para el caso de RPAs telecomandados, es que es la única técnica que permite también la localización del piloto remoto.

2.4 Detección con cámara

La cámara, ya sea de visible, IR o multiespectral, es sin duda un sensor de gran ayuda en el proceso de alerta dron. Sin embargo, se analizará como sensor de identificación, no de detección, ya que en general no resulta útil en este aspecto. Quizá habría que excluir aquí el caso de una cámara térmica, en el que se pueda detectar un dron más o menos caliente contra un fondo frío, pero es un caso demasiado concreto como para considerarse un sensor suficientemente versátil.

Salvo en el caso anteriormente citado, en el que sí se puede basar la detección en la intensidad de la señal captada por la cámara, la alarma generada por este tipo de sensores está basada en hacer una identificación de la forma del dron (es por esto que se estudia en el apartado correspondiente). Pero tampoco resulta viable hacer una detección/identificación simultánea como se hace por ejemplo con la vigilancia espectral. La razón es el compromiso entre resolución y campo de visión (Fiel of View FOV). La figura 8 ilustra gráficamente este problema.

El ojo humano (y lo mismo le ocurre a un sistema de reconocimiento automático) necesita un número de pixels mínimo para poder reconocer una forma. Tal como se observa en la figura 8, la imagen del hombre puede ser "detectada" con sólo unos pocos pixels de definición, pero necesita un pixelado sensiblemente más fino para concluir que efectivamente es una persona. Si el objeto está lejos (y ese es el objetivo en esta fase, detectar la amenaza con suficiente tiempo para reaccionar), la única forma de conseguir que la imagen del dron ocupe un número de pixels suficiente sobre la matriz de captación de imagen, es utilizar un zoom alto, es decir un FoV de sólo unos pocos grados (unos pocos estéreoradianes para ser más precisos).

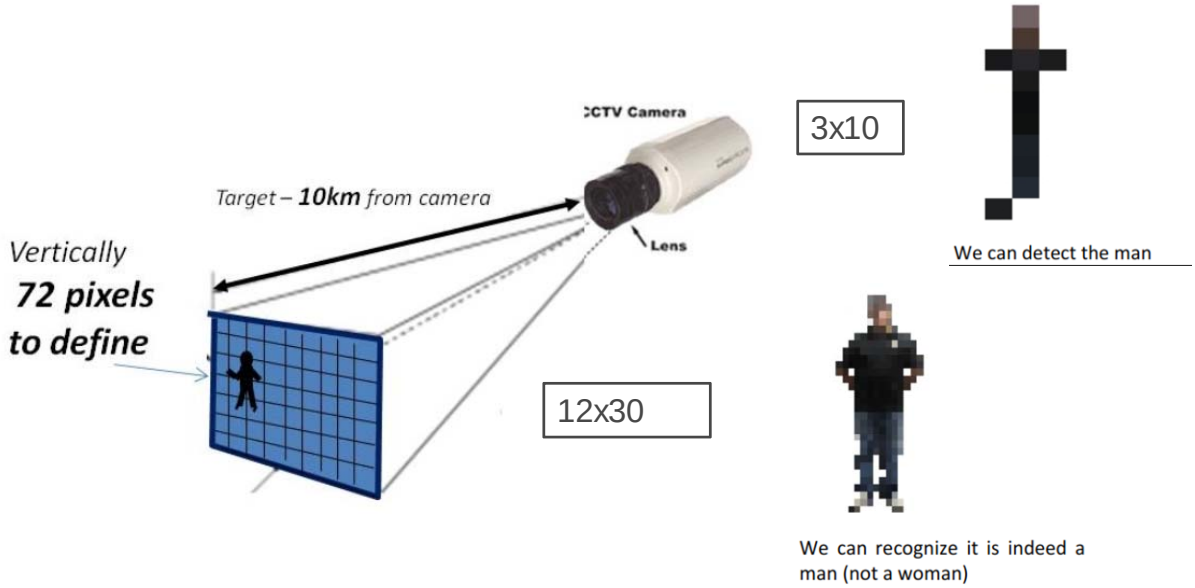

Figura 8. Compromiso entre resolución y FoV

La figura 9 presenta un estudio cuantitativo de este fenómeno (planteando el criterio de 40 pixels como requisito para que el objeto pueda ser identificado con seguridad) y analizando el alcance de detección de distintos RPAs existentes en el mercado en función de la distancia y del FoV de un pixel . Se presentan también algunas cámaras comerciales que pueden proporcionar esos valores de FoV.

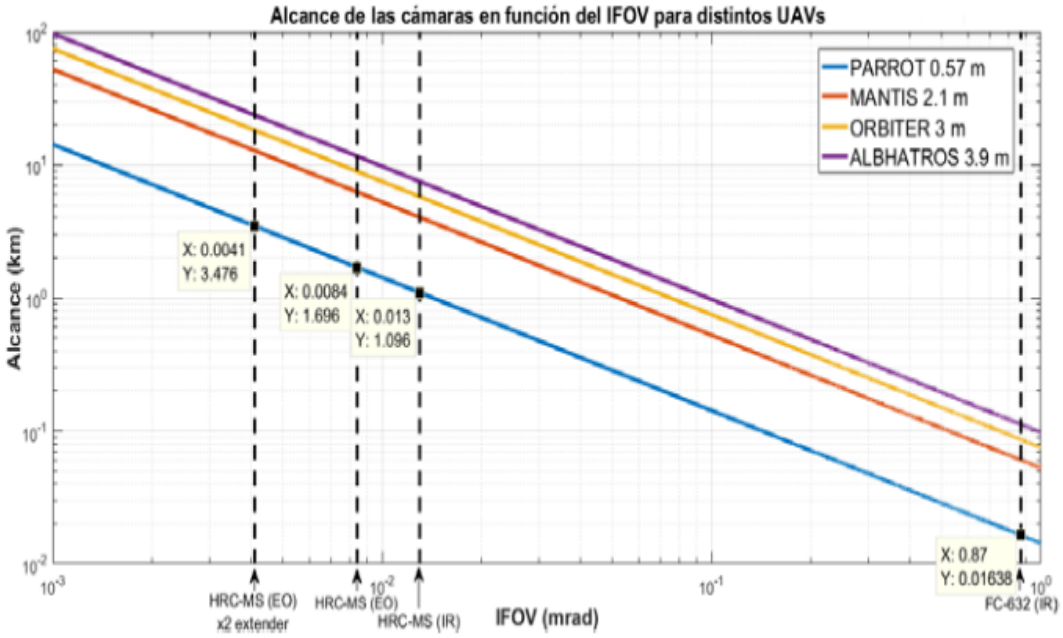

Figura 9. Compromiso entre alcance y FoV

En cada posición de apuntamiento de la cámara se deberá mantener unos segundos para que el sistema de reconocimiento (humano o automático) decida si la imagen contiene o no un dron, antes de moverse a un nuevo apuntamiento. En eso consiste la labor de vigilancia. Dado que el FoV

es muy bajo, el tiempo total necesario para explorar todo el espacio es prohibitivamente alto, dando unos tiempos de revisita inaceptables para una aplicación real, salvo que la dirección de la amenaza sea conocida.

Por ejemplo, si tenemos el objetivo de detectar un dron tipo Parrot a 3.5 Km de distancia (algo que hace actualmente un radar moderno de los existentes en el mercado), se precisa un FoV de unos 4 μrad, por pixel. Unos 11.6 mrad de FoV total si admitimos que la cámara tiene 8 Mpixels (2900x2900). Eso representa tan sólo una cienmilésima parte de todo el espacio a vigilar. Incluso pensando en que sólo es necesario vigilar el semi-espacio que está por encima del suelo, incluso aunque sea sólo un sector de 90º de ese semiespacio, e incluso admitiendo que con observar durante una décima de segundo la imagen se puede tomar una decisión sobre la presencia de una amenaza, serían necesarios veinte minutos de exploración de la cámara para cubrir todo el volumen objetivo.

Es cierto que se pueden tomar algunas medidas para mitigar estos efectos (por ejemplo explorar con un zoom más abierto y luego cerrarlo ante la presencia de una "sospecha de amenaza"), pero la realidad es que la cámara no es de manera nativa un sensor para detección y este problema siempre va a pesar mucho. El hecho de que no entreguen medida de distancia y que sean bastante sensibles al estado de la atmósfera (niebla, lluvia, baja visibilidad, etc) hacen que su uso se oriente mucho más hacia la fase de reconocimiento.

2.5 Sistemas combinados

En este apartado se trata la posibilidad de sistemas que se basan en la cooperación de las tecnologías, trabajando en conjunto para aumentar la efectividad de la detección de los RPAs. Un ejemplo podría ser la combinación de tecnología radar para realizar la detección de RPAs que se aproximen, estimando la posición del blanco. A continuación se proporciona esta información a un procesador que orienta a los arrays de micrófonos y las cámaras hacia el sector concreto, para realizar una clasificación del RPA o para eliminar falsas alarmas.

Sin embargo, en este tipo de soluciones se debe tener en cuenta la ganancia que realmente aporta añadir la cooperación de una tecnología adicional al sistema, frente al coste tanto económico como de manufactura que conlleva, pues podría no resultar rentable. Además, el uso de múltiples sensores conlleva aumentar el tamaño y los requisitos computacionales del sistema.

El cuadro siguiente, sin embargo, pone de manifiesto que todos los sensores existentes tienen debilidades, y que la fusión de sensores es sin duda el planteamiento más robusto para hacer frente a la situación. Esta fusión no está sin embargo exenta de retos tales como la heterogeneidad de los datos o la no-completitud de los mismos.

UAV Detection Summary

* Needs an active illuminator
** Only for close- and near-range radar

Sensor characteristics	Information value	Weather / night	Passive	Range	Mobile usage
EO	++	- -	++	+	++
IR	O	O	++	+	++
Audio	+	O	++	O	+
Passive Radar (GSM)*	O	++	+	+	-
Radar **	O	++	- -	+	+
Direction finder	O	++	++	++	+
Laser Range Finder	-	O	- -	++	++
Laser Scanner	O	O	- -	+	+

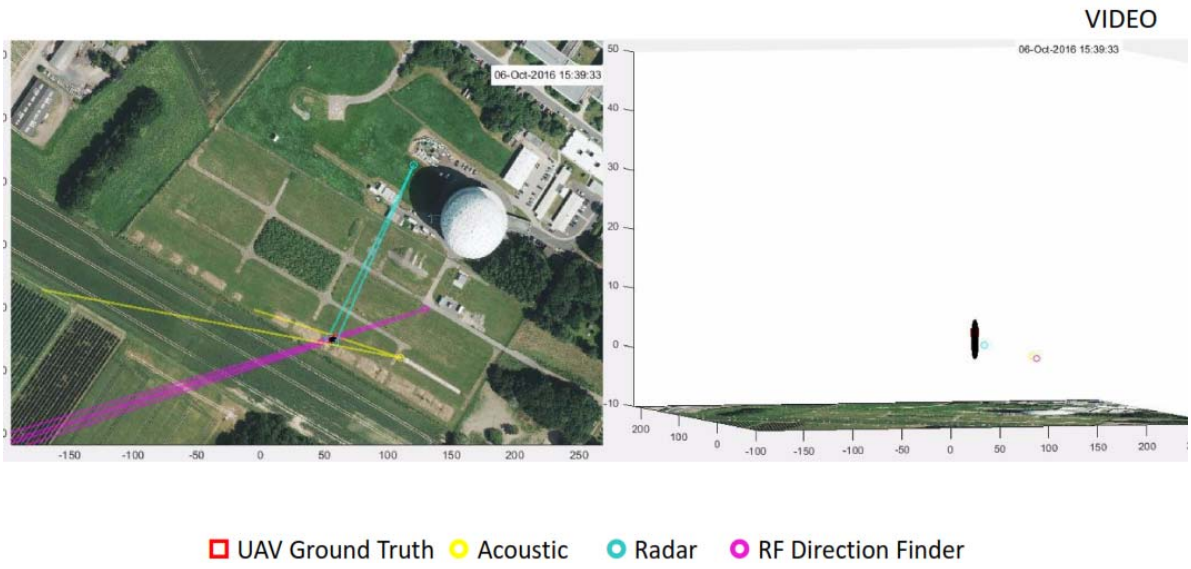

Figura 10. Simulación de un escenario multisensor con fusión de información de un radar un radiogoniómetro y un sensor acústico (GeoBasis-DE)

.

3 Identificación

La segunda tarea consiste en discriminar los RPA frente a otros objetos o aves con una probabilidad de falsa alarma baja (o mejor expresado probabilidad de “nuissance alarm” baja). Esta fase, en la que es necesario realizar de forma satisfactoria la identificación del RPA frente a otras posibilidades, juega un papel clave, ya que sobre ella recae la responsabilidad de determinar si el objeto que se aproxima representa una amenaza antes de pasar al siguiente paso de neutralización.

Para reducir el número de falsas alarmas se requiere una rápida clasificación del blanco, mediante reconocimiento automático o con un operador humano que revise la información, antes de realizar el seguimiento del mismo y, en caso de necesidad neutralizar al objetivo.

La posibilidad de la identificación automática, sin necesidad de un operador que revise la información recogida, es el principal reto tecnológico de esta fase. En la actualidad prácticamente todos los sistemas precisan de la intervención humana, aún así necesitan disponer de sensores adecuados que les proporcionen la información que necesitan.

3.1 Cámaras

La identificación de RPAs mediante técnicas de cámaras de espectro visible, de infrarrojos e hiperespectrales es un campo en el que se está trabajando activamente en la actualidad. De hecho, el sistema más utilizado en el presente es el uso de cámaras de espectro visible. Éstas técnicas abarcan desde sistemas que trabajan en el espectro visible, cámaras que trabajan en el infrarrojo hasta nuevos sistemas que buscan obtener la firma espectral mediante cámaras hiperespectrales. Esta tecnología se basa en realizar el procesado de las imágenes capturadas para identificar los RPAs y diferenciarlos de otros objetos automáticamente.

La ventaja de las cámaras, especialmente las visibles, es que dan la información al operador en el formato de una imagen que le es muy natural, y apenas necesita entrenamiento para poder distinguir un dron con alta fiabilidad. Como se puede observar en la 11, la identificación mediante cámaras que trabajan el infrarrojo consiste en detectar la huella de calor del RPA. Las imágenes aquí producidas no son tan familiares al operador como las de espectro visible, pero tienen la capacidad de trabajar en oscuridad. Aunque también pueden operar en condiciones meteorológicas adversas como niebla o lluvia, su correcto desempeño en estas circunstancias se ve más afectado que el de los sistemas radar.

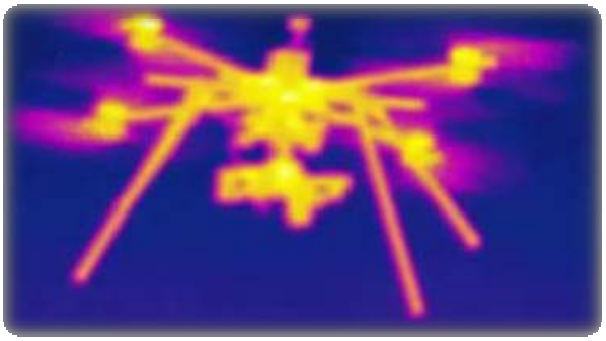

Figura 11. Imagen infrarroja de un RPA.

Por otra parte, la identificación mediante cámaras hiperespectrales es un planteamiento diferente. Estas cámaras cubren todo el espectro electromagnético con una buena resolución espectral. Esto hace que se disponga de una curva (huella espectral) para cada pixel individual de la imagen. De hecho una imagen hiperespectral es en realidad una matriz tridimensional (figura 12).

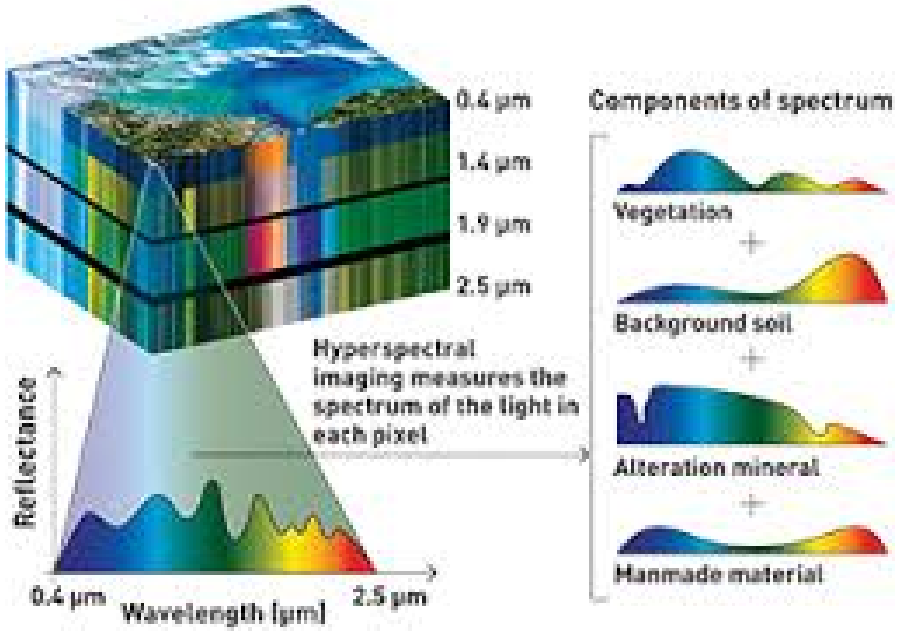

Figura 12. Imagen "cubo" hiperespectral

El punto clave de esta técnica es poder reconocer el material a que corresponde un pixel en base a su firma espectral, y no a su forma. Esto relaja enormemente el requisito del FoV de las cámaras ya que en teoría es posible la detección en base a un único pixel. Sin embargo el gran problema es la cantidad de información generada. Esta técnica requiere procesado automático y es este procesamiento y la potencia de cálculo requerida el actual cuello de botella para hacer la técnica realmente viable.

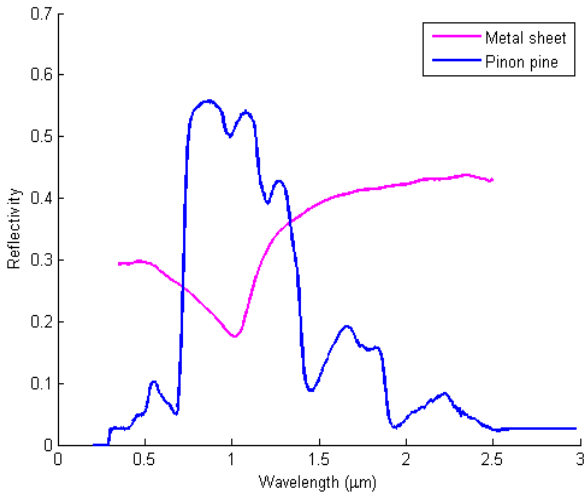

Figura 13. Diferente firma hiperespectral de distintos materiales

Sin embargo, pese a no ser actualmente una tecnología suficientemente madura, tiene muchas posibilidades de cara al futuro, en la identificación automática de blancos, sin necesidad de un operador humano que revise la información obtenida.

3.2 Microdoppler

Una de las técnicas que está en pleno desarrollo es la identificación mediante la firma microdoppler de los RPA, asociado a la detección mediante sensores radar. El crecimiento del uso de RPA de tamaño "mini" de características de baja altitud, sección radar pequeña y baja velocidad hacen que la clasificación y discriminación de aves frente a ellos presente un reto ya que presentan similitudes en su sección radar y en los patrones de vuelo.

El microdoppler es la desviación doppler que se produce en el eco radar de un objeto, no debido al movimiento de su centro de masas, sino a los movimientos de sus partes móvles como aspas, ruedas, alas, brazos, etc..La firma microdoppler de un objeto depende tanto del movimiento y rotación de las piezas, como del movimiento del cuerpo principal del mismo. Es una técnica que permite diferenciar RPAs de aves y da la posibilidad de realizar una clasificación de distintos tipos de RPA, estimando el tamaño y el número de rotores que posea

Se han realizado números experimentos trabajando con ésta técnica y muchos han demostrado ser capaces de realizar discriminaciones satisfactorias frente aves, además de ser capaces de clasificar el tipo de RPA, consiguiendo realizar un reconocimiento automático de los blancos. Al igual que en el caso de otras técnicas ya mencionadas, todavía es una tecnología poco madura. Aún así ya hay empresas que tienen productos comerciales, como es el caso de Robin Radar en Europa.

La implementación efectiva de esta técnica exige el uso de técnicas de reconocimiento de patrones, extensas bases de datos y posiblemente técnicas de machine learning.

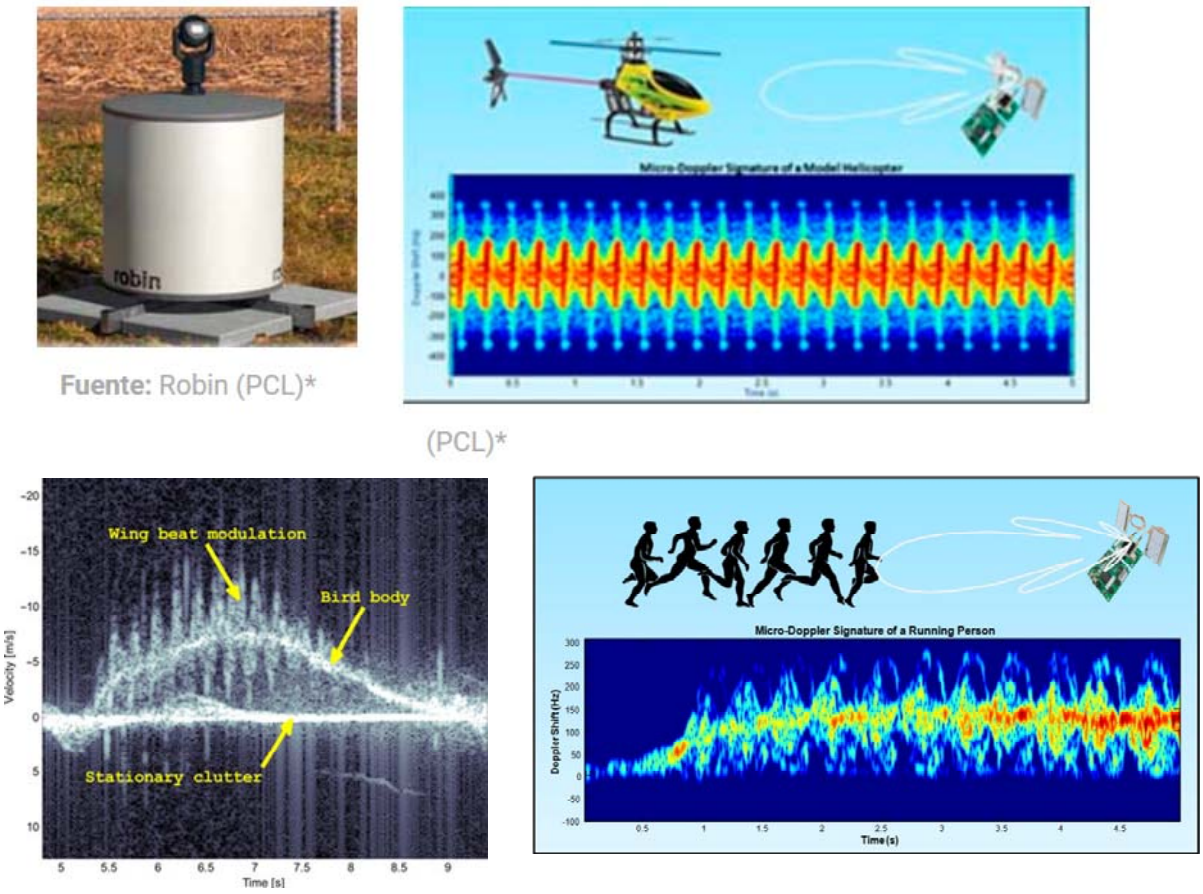

Figura 14. Sensor radar con capacidad de análisis micro-doppler y diferentes firmas micro-doppler.

3.3 Otras técnicas

Existen otras posibilidades, asociadas por ejemplo al objetivo operativo no ya de decidir si un objeto es un dron, sino de analizar si el mismo transporta algún tipo de carga peligrosa, por ejemplo explosivos y armas químicas o bacteriológicas.

Para realizar este cometido, son muchas veces los operadores humanos los que se encargan de revisar en la medida de lo posible la carga que portan éstos vehículos a partir de las imágenes obtenidas. Sin embargo también se han realizado avances recientes en los que se emplea otro RPA, como el SpectroDrone, que podemos observar en la Figura 15, encargado de la misión de analizar la carga del RPA detectado utilizando para ello un sensor láser, embarcado en un segundo RPA

Figura 15. SpectoDrone.

Por otra parte, la detección de emisiones de RF, ya mencionada para la detección, es por supuesto también un método de identificación. La mayoria de los RPAS profesionales poseen múltiples sistemas de comunicaciones. Dichos sistemas al operar dejan una huella en el espectro radioeléctrico que puede ser detectada. Estos detectores barren el espectro con una o varias antenas buscando sistemas de comunicaciones que utilizan los drones habitualmente. Dependiendo de la complejidad del sistema, este puede permitir localizar la ubicación desde la que se originan las comunicaciones, pero también, con la correspondiente base de datos y sistemas de reconocimiento de patrones, llegar a identificar la plataforma. Un ejemplo de este tipo de sistemas es Drone Alert (Rohde & Schwartz) que se puede ver en la figura 16.

Figura 16. Drone Alert de Rohde & Schwartz

4 Neutralización

[Una vez realizados los procesos de detección e identificación, si consideramos que el RPA representa una amenaza, debemos llevar a cabo alguna técnica de anulación. A medida que la industria de los RPA evoluciona, también lo hacen las prestaciones de los mismos en lo referente a sus capacidades de defensa propias, por lo tanto, el sector de tecnologías asociadas a la neutralización debe estar preparado para las novedades de los RPA más modernos.

El tipo de tecnologías de neutralización a emplear tiene una alta dependencia con el entorno en el que se desee instalar el sistema, siendo unas técnicas más apropiadas que otras. La presencia o ausencia de población civil representa uno de los parámetros a tener en cuenta en la elección del sistema adecuado, evitando poner en riesgo la seguridad de las personas.

4.1 Métodos basados en interferencias

4.1.1 Jamming

Las tecnologías de jamming buscan crear interferencias para que los sistemas de telecontrol, radionavegación y comunicaciones del RPA no funcionen correctamente, cortando los enlaces de comunicaciones que necesite para operar.

El uso de ésta técnica debe ser controlado, ya que no se sabe con certeza cómo reaccionará el RPA, pudiendo provocar amenazas si lleva cargas peligrosas como explosivos o químicas o si hay presencia de población civil en sus alrededores, por tanto su uso no es conveniente en cualquier tipo de entorno. Si bien. Debe decirse que en la mayoría de los casos los drones atacados de esta manera tienden a descender hasta colisionar con el suelo.

Se han desarrollado sistemas tanto fijos como desplegables, como las “pistolas jammer”, tal y como se observa en la Figura 17, utilizadas por un operario que la apunta hacia el RPA que representa una amenaza**.** Este es por ejemplo el ámbito de tecnologías más afín al programa Condor lanzado recientemente en nuestro país. Otros sistemas más sofisticados van asociados a un radar u otro sensor y se apuntan automáticamente (figura 18). Obsérvese la profusión de diferentes antenas (y diferentes transmisores) en distintas bandas de frecuencia, para poder inutilizar todas las señales de interés (señales de telecomando, GPS, señal de vídeo, etc..)

Figura 17. Batelle DroneDefender.

Figura 18. Sistema de jamming guiado por radar: Blighter AUDS.

El punto principal de estas técnicas es conseguir suficiente interferencia, lo que obliga a menudo a radiar potencias muy importantes. Son muy eficaces para el caso de uso negligente, y son uno de los sistemas más potentes para la amenaza actual, que es predominantemente de este tipo. Sin embargo, posiblemente en un futuro de medio plazo pueden resultar insuficientes para atacar drones intencionadamente maliciosos, que incorporen rechazo de interferencias, o antenas con haz conformado, o incluso sistemas de navegación inercial sin necesidad de telecomando o GPS.

Otro aspecto positivo de esta técnica es su utilidad para neutralizar enjambres de UAVs, una amenaza que se vislumbra como preocupante para el medio plazo, y que normalmente sí que requerirá el uso de sistemas de comunicaciones entre plataformas para su coordinación.

Figura 19. Hipotético ataque con un enjambre de drones

4.1.2 GPS spoofing

La mayoría de los RPAs están equipados de receptores GPS para realizar distintas misiones de navegación y guiado. El GPS spoofing consiste en intentar "engañar" al RPA, es decir, transmitirle señales GPS falsas para que el vehículo crea que está en otro lugar distinto del que realmente está, apoderándose del control del mismo.

Se han realizado numerosos estudios sobre las vulnerabilidades del GPS, y en consecuencia se han desarrollado algunos (todavía pocos) sistemas comerciales basados en ésta técnica, tanto dispositivos fijos como desplegables, ejemplos de ello se muestran en la Figura 2 0.

Figura 20. Sistema de GPS spoofing ClearSky

Las limitaciones de los spoofer son similares a las de los jammers. Adicionalmente, el uso de la técnica GPS spoofing no está permitido en todos los países como EE. UU., por lo que se deben valorar también otras alternativas.

4.1.3 Hacking de las comunicaciones WiFi

Uno de los tipos de comunicaciones que pueden establecerse entre estación base y el RPA es mediante una conexión WiFi. De esta forma, se pueden realizar varios tipos de ataques sobre esta conexión para interrumpir las comunicaciones, utilizando técnicas típicas de hackeo informático

Los sistemas transmisores y receptores tienen que saber a quién deben transmitir y escuchar, por tanto se produce un intercambio de tramas al comienzo de la comunicación para asociar los dispositivos. En muchas ocasiones esta parte del proceso no está protegida, lo que causa vulnerabilidades a la hora de recibir un posible ataque.

4.2 Métodos de anulación física

La próxima generación de drones para uso hostil, muy probablemente no va a utilizar ondas electromagnéticas para la realización de su misión, por lo que será necesario proceder a ataques físicos, más letales. El uso de ráfagas de disparos de alta cadencia queda prácticamente descartado en la mayoría de los casos por la gran cantidad de daños que podrían ocasionar tantas balas perdidas, por lo que se exploran otras alternativas.

4.2.1 Láser

Se han desarrollado armas de neutralización basadas en tecnología láser de alta potencia que consiguen derribar a los RPA a una distancia de hasta 1 km enfocando de forma precisa el haz láser hacia la posición del drone. Estos sistemas requieren el empleo de sensores, como radares o cámaras, o al menos miras telescópicas que permitan identificar la amenaza y localizarla de forma muy precisa realizando un seguimiento de precisión de la misma antes de derribarla.

Figura 21. Sistemas antidrone basados en laser para aplicaciones terrestre y marina

Las principales desventajas de estos sistemas son su elevado coste y peso, aunque actualmente se están desarrollando sistemas más compactos. Además, se deben tener en cuenta los aspectos de seguridad y los permisos necesarios para el empleo de este tipo de armas además de las limitaciones impuestas por la convención de Ginebra en su protocolo IV que limita el uso de armas láser. Sin embargo, dada la elevada precisión y enfoque de energía en estos sistemas, se ha demostrado que el empleo de armas láser permite neutralizar los drones con menores daños colaterales e impacto en el entorno que utilizando otros tipos de armas como proyectiles o armas de fuego. Su capacidad de ataque incremental y el uso de munición no explosiva son otras de sus ventajas.

Existen varios tipos de sistemas láser en función de las técnicas que se utilizan para generar el haz. Estas categorías son:

- High-power diode laser arrays: Estos sistemas están formados por pilas de diodos laser individuales o multistripe. Su gran ventaja es su gran eficiencia electro-óptica, aunque presentan una baja calidad de haz. Su máxima eficiencia se alcanza en longitudes de onda comprendidas entre 880nm y 980nm, aunque pueden funcionar entre 400nm y 2200nm. Alcanzan potencias de hasta 1kW utilizando refrigeración activa.

- High-power solid-state lasers: Un láser de estado sólido es un láser que utiliza un medio de ganancia que es un sólido. Generalmente consiste en un material de vidrio al que se añade un "dopante"(neodimio, cromo, erbio, tulio o iterbio). Mediante esta técnica se pueden conseguir eficiencias de hasta 60% y potencias de salida de hasta 30kW.

- Optical fiber lasers: Estos sistemas generan el haz utilizando fibra óptica de núcleo dopado. Utilizando esta técnica se pueden alcanzar eficiencias de hasta 46% y potencias inferiores a 1kW.

- Beam combining: El beam combining no es una técnica de generación en sí, sino que es una forma de superar las limitaciones de potencia de los diferentes sistemas mediante combinaciones de haz. Hay 3 modos de combinación:

- Combinación coherente. Utilización de interferencia constructiva.
- Wavelength combining. Combinación de varias longitudes de onda en un solo haz mediante redes de difracción o espejos dicroicos.
- Hibrida. Consiste en la utilización de las dos técnicas anteriores de manera simultánea.
- Heat-capacity lasers. Son sistemas de estado sólido que utilizan diferentes técnicas para aumentar la potencia de salida. Alcanzan hasta los 67kW. Esto se consigue agregando rápidamente disparos individuales haciendo que el calor residual se almacene en el medio. La no utilización de medios de refrigeración permite menos distorsiones ópticas en el sistema y por tanto mayor potencia de salida del láser.
- Chemical lasers. La energía y el haz se obtienen mediante reacciones químicas, y el sistema se refrigera mediante el flujo de gases. Se pueden alcanzar potencias del orden de 100kW en frecuencias cercanas a los infrarrojos.

Estas técnicas se han implementado en diferentes sistemas de defensa que ya están en el mercado o que se espera que estén disponibles en los próximos años. Algunos ejemplos de estos sistemas se recogen en la tabla siguiente.

Nombre del sistema	Fabricante	Tipo	Características	Estado de desarrollo
LaWS	Kratos	Solid State	30kW. Embarcado.	En uso. USS Ponce
Oerlikon	Rheinmetall	Fibra & Beam Combining	10kW. Ground based.	En el mercado.
Silent strike	Boeing		10kW. 22 millas de alcanza. Desmontable y ligero	En el mercado.
Iron Beam	Rafael		Sin información publica	En el mercado.
Lockheed Martin Laser System	Lockheed Martin	Solid state & Beam Combining	60kW	En desarrollo.
Hellads	Darpa & Weaponer Textron	Combinación de láseres químicos y de estado sólido.	150kW. Pequeño tamaño	En desarrollo. 2020
Excalibur	Darpa	Beam combining	Orden de kW para cada laser.	En desarrollo. 2020.

Tabla. Algunos sistemas de neutralización radar actuales o en desarrollo

Debido a que el desarrollo de los sistemas láser está en auge, están surgiendo a su vez sistemas de defensa contra ellos. A continuación, listamos algunos de ellos:

- Sistemas basados en "espejos”
- Materiales ablativos: Absorben la energía del láser y generan gas.

- Thermal transport delay. Ralentización de la propagación del calor mediante capas de materiales aislantes.

- Obscurants and atmospheric degradation. Generar polvo o humo para reducir la efectividad.

- Meta materiales. Ttodavía en etapas tempranas de desarrollo.

- Proyecto Helios. Sistema de senseres para descubrir el laser y laser propio para apuntar al laser atacante y confundirlo haciéndole creer que no está enfocado.

4.2.2 Redes

Existen métodos comerciales desarrollados mediante los cuales un único operador con un sistema transportable dispara un proyectil que es capaz de alcanzar al RPA, atrapándolo con una red o derribándolo. En algunos sistemas en los que se lanza una red, el RPA cae de forma segura gracias a un paracaídas sin ocasionar daños a terceros.

En el siguiente caso, un RPA (dron anti-dron) vigila el perímetro mediante una cámara de alta resolución. En el caso de que un RPA sea detectado e identificado como amenaza por parte de los sistemas anteriormente expuestos o por el propio dron anti-dron, éste lanzará una red para inmovilizar a la amenaza, como se muestra en la Figura 22, dejándolo caer mediante un paracaídas o llevándolo a un lugar seguro**.**

Figura 22. Anti-dron Excipio.

Éstas técnicas, que están en desarrollo, podrían ser útiles en entornos donde no conviene utilizar contramedidas electrónicas y en los que se debe controlar el punto de caída del RPA que representa una amenaza. Actualmente todavía adolecen de una tasa de fallos excesivamente elevada.

4.2.3 Águilas

El entrenamiento de águilas para la caza de RPAs es una práctica que se está dando en varios países, principalmente para proteger aeropuertos, que son los primeros emplazamientos que se han encontrado con la amenaza del uso negligente. Los RPAs son identificados como una presa para las águilas, para después dejarlos en un lugar seguro**.** Evidentemente tienen importantes limitaciones y no son útiles para drones a partir de un cierto tamaño. Pero la realidad es que es una solución ya disponible, muy segura, y bastante eficaz para la amenaza actual.

Figura 23. Águila entrenada para la neutralización de drones pequeños

5 Conclusiones

Quizá lo más llamativo de este estudio es la gran variedad de tecnologías y soluciones diferentes que se están planteando y utilizando. Normalmente eso es un síntoma de que ninguna de ellas por sí sola da una solución totalmente satisfactoria. En este sentido, el uso combinado de varias alternativas es una buena estrategia.

Creo que puede concluirse que para el estado actual de la amenaza, los sistemas de protección existentes permiten un grado de seguridad alto. Pero sin duda quedan escenarios y situaciones que previsiblemente se pueden producir en un futuro no demasiado lejano y para los que queda camino por recorrer en las soluciones de detección y neutralización necesarias para abordarlos.

Como última conclusión es interesante resaltar que la industria nacional ha producido soluciones altamente competitivas algunas de las cuales están obteniendo gran éxito en el contexto internacional. Sin duda esto es síntoma de una buena orientación de las políticas de incentivación de la I+D nacional, que debe potenciarse en los próximos años para no perder la buena posición de la que se goza en la actualidad.

6 Referencias

[1] Horizon 2020, Work Programme 2016-2017. Secure societies - Protecting freedom and security of Europe and its citizens [online]. http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-security_en.pdf [Accessed on: 23/11/2016]

[2] Birch, G. C., Griffin, J. C. and Erdman, M. K. Erdman, "UAS Detection, Classification, and Neutralization. Market Survey 2015," Sandia Report, 2015.

[3] Resultados del C-UAS Challenge, organizado por MITRE en 2015. [online] https://www.mitre.org/news/press-releases/mitre-names-c-uas-challenge-winners

[4] Programa coincidente 2018. [online] https://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Presentacion/ImasD/Paginas/Coincidente.aspx