Análisis de la seguridad del guiado por GPS en sistemas UAVs y Drones

Ciberseguridad en contornas industriales

Juan González Iglesias

29 de abril de 2022

Índice

1. Introducción

El objetivo de este documento es profundizar y analizar la utilización e importancia de *drones* y UAVs en el ámbito industrial, observando para ello las posibles vulnerabilidades y amenazas que pueden sufrir, así como el posible impacto de la seguridad que pueden tener en el ámbito industrial.

Para ello, como este es un campo muy amplio nos vamos a centrar en las vulnerabilidades y amenazas al sistema *gps* de estos dispositivos.

2. Definición de la tecnología

2.1. UAVs o drones

Vamos empezar hablando en lo referente a los *drones* o también conocidos como UAV (Unmanned Aerial Vehicles). Estos dispositivos o vehículos aéreos no tripulados ejercen su función remotamente.

Los UAV en un principio fueron diseñados para aplicaciones militares, como es el caso de los UCAV (Vehiculos Aéreos de Combate no tripulados), pero enseguida su uso se extendió, y en los últimos años el uso civil se popularizó, hasta tal punto que en la industria 4.0 empiezan a verse como una solución de mejora en algunos de los procesos industriales.

Existen diferentes abreviaturas y nombres para referirse a diferentes modelos y sistemas dentro de los UA (aeronaves no tripuladas). Estos son los siguientes:

- **UAV**: Son vehículos aéreos no tripulados y son el elemento principal de los UAVS. Normalmente se refieren aquellos vehículos que tienen un uso fundamentalmente militar. Muchas clasificaciones engloban dentro de este también los RPAS. Pero los UAV no siempre son RPA, pues no todos los *drones* se controlan por un piloto humano, algunas realizan tareas o vuelos automatizados (inteligencia artificial).
- **UAS**: *unmanned Aerial System*. Hace referencia al sistema conjunto, es decir al sistema formado por aeronave + estación en tierra + enlace de comunicaciones.
- **RPA**: *Remotely Piloted Aircraft*. Se trata de una aeronave tripulada de forma remota, es decir, dirigidas por un piloto de manera remota mediante un enlace de datos. Normalmente se refiere a aeronaves no tripuladas en el ámbito civil.
- **RPAS**: *Remotely Piloted Aircraft System*. Es el sistema en conjunto, formado por la aeronave + estación en tierra + enlace de comunicaciones.
- **Drone**: Es la denominación popular que realiza la gente, para referirse a esta clase de dispositivos.

Nosotros nos vamos a centrar en los *drones* de uso civil, pues normalmente son los más utilizados en el sector industrial. Por lo que según los modos de funcionamiento en el ámbito civil, podemos clasificarlos en

- **Modo manual**: Una persona, mediante un estación RC maneja la aeronave durante todo el transcurso del vuelo.
- **Modo asistido**: Similar al anterior, pero en este caso el piloto define las intenciones de vuelo y un autopiloto transforma esas accionas en la aeronave.
- **Modo automático**: El piloto establece un plan de vuelo y la aeronave vuela gracias a un autopiloto. El piloto mantiene el control del dispositivo en todo momento.
- **Modo autónomo**: Similar al automático pero en este caso el piloto no puede intervenir en el control de la aeronave.

Existen diferentes clasificaciones a la hora de organizar este tipo de *drones*, pero una de las mas extendidas, distingue tres tipos diferentes:

- **Multirrotor**: Este tipo de vehículos proporcionan una gran versatilidad y eficacia en las operaciones pues como los rotores están colocados a la misma distancia del centro de gravedad proporcionan una plataforma estable y de fácil pilotaje.

Según la cantidad de motores se distinguen: tricópteros (3 motores), cuadricópteros (4 motores), hexacópteros (6 motores) y octocópteros (8 motores). Hay que tener en cuenta, que a mayor número de brazos y motores se conseguirá una mayor estabilidad, seguridad y potencia pero al mismo tiempo el consumo crece. Otro tipo de multirrotores son los conocidos como *Coaxiales* los cuales su característica principal no es el número de brazos, sino la cantidad de motores por brazos, pudiendo incluir dos motores por brazo (mejor opción para trabajos profesionales).

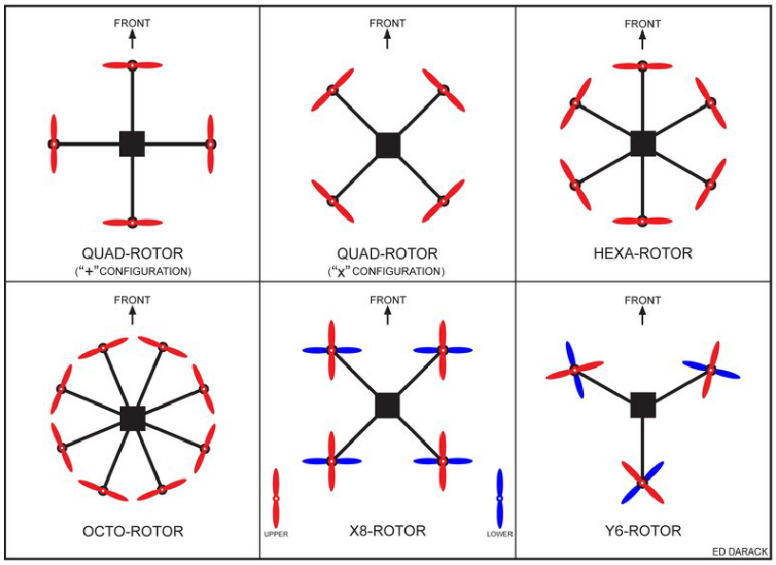

Figura 1: Multirotor drone

- **Helicoptero**: Son de las herramientas más polivalente a la hora de realizar todo tipo de operaciones. Funcionan del mismo modo que si de un helicóptero normal se tratase, por lo que consta de dos rotores, una de gran tamaño y un multirrotor que varía las revoluciones para mantenerse estable. Son más complicados de operar que los *drones* convencionales y tiene una complejidad mayor a nivel mecánico.

Figura 2: Helicopter drone

- **Ala fija**: Este tipo de *drones* tienen una alta autonomía, por lo que pueden permanecer en el aire varias horas, por lo que resultan idóneos para trabajos que abarquen una gran extensión de terreno. Por otro lado presenta algunas desventajas, pues este tipo de *drone* no permite el vuelo estacionario (permanecer estático en un punto determinado) y posee una reducida capacidad de carga.

Figura 3: Ala fija drone

Todos ellos utilizan diferentes protocolos y tecnologías para comunicarse y realizar sus funciones. En los últimos años esta tecnología aumentó a pasos agigantados, hasta tal punto que los últimos modelos son capaces de volar solos y hasta dirigirse a un lugar seguro cuando se produce algún error o perdida de conexión. No vamos entrar en detalle de todos los aspectos técnicos que los últimos modelos incorporan, pero si hacer referencia al tipo de tecnología y protocolos que utilizan para transmitir información entre la estación base y el dispositivo en si.

Normalmente los *drones* incluyen sistemas duales (o incluso tres) de frecuencia, generalmente siendo las bandas de 2.4GHz y 5.8GHz las más utilizadas. Disponen de varias bandas pues si el sistema detecta que una banda de frecuencia se ve comprometida, por ejemplo, mediante interferencia, el *drone* automáticamente puede operar en la otra, es decir, incluyen una redundancia para garantizar la conexión.

También es importante destacar que algunos modelos incluyen algún mecanismo de FPV, es decir, de vista en primera persona. Este tipo de tecnología permite al piloto ver los que el *drone* "ve.[en] tiempo real. Existen dos tipos, por un lado tenemos los FPV analógicos los cuales pueden transmitir por las bandas de 2.4 y 5.8 GHZ y por otro lado los FPV digitales que pueden transmitir a través de WiFi a 2.4 o 5G. La mejor opción es la banda analógica de 5.8Ghz pues permite transmitir calidad HD con una latencia ultra baja.

2.2. GPS

Por otro lado tenemos la tecnología *GPS* en la que se va a centrar este documento. El sistema de posicionamiento global nos permite determinar la posición de un objeto en casi cualquier lugar del mundo. Esto lo consigue gracias a un conjunto de 24 satélites los cuales transmiten señales unidireccionales. Proporcionan una precisión muy elevada, llegando incluso a ser inferior a centímetros utilizando GPS diferencial.

Este sistema de posicionamiento global basa su funcionamiento en señales unidireccionales, las cuales están compuestas principalmente por 3 partes:

- La primera parte contiene la hora GPS, la cual es determinada a partir de relojes atómicos.
- La segunda parte se conoce como *ephemeris* y contiene las coordenadas astronómicas del satélite.
- La tercera parte contiene información sobre la posición del satélite con respecto al resto de satélites y se conoce con el nombre de *almanac*.

El procedimiento para realizar el posicionamiento de un objeto, utilizando esta tecnología, es muy sencillo. El receptor GPS conoce la hora exacta a la que fue enviada la señal procedente de un satélite, por lo que puede utilizar ese dato para calcular la distancia a la que se encuentra el satélite, simplemente restando la hora en la que se transmitió el mensaje de la hora en la que se recibió.

A mayores, también conoce la posición exacta en el cielo de los satélites en el momento en que enviaron la señal, por lo que dado el tiempo de viaje de las señales de 3 satélites distintos y la posición exacta de cada uno, el receptor GPS puede determinar su posición en tres dimensiones: este, norte y altitud.

Al igual que sucedía con los *drones*, esta tecnología se utilizó en un principio para uso militar, concretamente para el ejercito de Estados Unidos. Fue ya a comienzos del año 2000 cuando el sistema fue liberado para uso civil, dando así la oportunidad de ser utilizado también en el ámbito industrial.

Los principales usos de los sistemas GPS son por ejemplo obtener la ubicación de una posición, navegación, seguimiento de objetos o movimientos de personas, mapeo o sincronización temporal de datos...

2.3. GPS en drones

La tecnología GPS a mejorado tanto en los últimos años, que ahora la mayoría de modelos de *drones* incluyen este tipo de tecnología, pues sea hecho los suficientemente asequible y ligera.

Tener un GPS en el *dron* marca una gran diferencia en su rendimiento y muchas veces desempeña un papel importante en muchas de las funciones que realiza, llegando incluso a solucionar o eliminar acciones que el piloto debía de realizar. Las más importantes son las siguientes:

- **Mantener la posición**: Cuando el *dron* consigue fijar la señal GPS, es capaz de identificar y mantener su posición en un lugar fijo (vuelo estacionario). Esto es tal, que incluso en condiciones con viento en las que el dispositivo se puede mover, es capaz de corregir su posición automáticamente y volver al mismo punto en el aire.

  Esto se puede aplicar al echo de conseguir un vuelo más estable. Un *dron* sin GPS se desvía mucho más de su rumbo por el viento, por lo que el piloto tiene que esforzarse en mantener una trayectoria de vuelo resta y suave.

- **Mantener la altitud**: Algunos *drones* utilizan el GPS para mantenerse una altitud constante durante el vuelo. Esto es importante pues la normativa FFA, la cual establece que las aeronaves no tripuladas deben operar por debajo de los 400 pies sobre el nivel del suelo. Por lo que muchos *drones* tienen este límite de altitud preprogramada en los controles de vuelo.

  Otros *drones* utilizan sensores para determinar la altitud o calculas la distancia con respecto a objetos que se encuentran directamente debajo, por lo que no siempre la altitud depende del sistema GPS.

- **Regreso a casa**: El *drone* será capaz de recordar la posición exacta en el momento del despegue, y volverá a dicha posición con una precisión bastante elevada.

  La vuelta a casa es importante si la batería se agota, si se está llegando al límite de la conexión con el controlador o si no das conseguido que el *drone* vuelva a la dirección correcta.

- **Generación de informes**: Algunos *drones* crean un registro de cada vuelo sobre cuanto tiempo ha volado, por dónde ha volado, etc. Esto puede ser especialmente útil por ejemplo en términos de mantenimiento de registros o también, por ejemplo, para localizar y recuperar un *drone* estrellado.

- **Waypoint navigation**: Un *drone* es capaz de navegar hacia unas coordenadas GPS específicas, previamente definidas. Por lo que un *drone* con GPS es capaz de recorrer una ruta que el piloto le haya preconfigurado.

  Esta es una función especial para sectores comerciales e industriales, pues dependen en gran medida de la navegación por puntos de referencia, como es el caso, por ejemplo, en cartografía, la inspección, construcción, agricultura...

- **Mapeo**: El GPS es esencial para el geoetiquetado de las imágenes, lo cual nos permite crear mapas mediante la utilización de cualquier software de mapeo.

La dependencia del *drone* con respecto al GPS está sujeta al nivel de autonomía, a la aplicación a la que se destina y al modo de vuelo. Estos modos de vuelo, que ya se comentaron en apartados anteriores, suponen exponer al *drone* a un nivel diferente de amenaza dependiendo del modo en el que se utilice. En la siguiente tabla se puede ver un ejemplo de esto:

Operational Mode	Range	Example Flight Modes	GNC Dependency	GPS Threats
Manual	VLOS	Manual	C2 Link	No
Semi-Autonomous Assisted	EVLOS	Stabilize, Alt Hold	C2 Link	Yes
		Circle, Drift, Follow, Loiter, Zig Zag, RTL	GPS	
Automatic	BVLOS	Auto, Guided, Smart RTL	GPS	Yes

Figura 4: Modos operacionales de los drones en base al GPS

En ella se puede observar como por ejemplo en el modo manual, como no se utiliza el sistema GPS, el *drone* no es vulnerable a amenazas basadas en este sistema, mientras que en los modos *semi-autónomo* y *autónomo* al utilizar este tipo de tecnología, si que se puede ver afectado por las vulnerabilidades que esta tiene.

3. Aplicaciones de los drones

Hoy en día podemos encontrar todo tipo de *drones* capaces de realizar todo tipo de funciones. El ocio recreativo de estos, es una de las grandes bazas de los *drones* actuales, pues al proporcionar un vuelo estable y capacidad de grabación con una cámara de alta definición puede resultar muy atractivo para muchas personas.

Pero el ocio es solo una pequeña parte de las funciones o aplicaciones que puede cubrir un *drone*. Sus aplicaciones son de los mas variopintas, alguno ejemplos de ella son: fotografía aérea para periodismo o cine, recogida de información o suministro de elementos para la gestión de catástrofes, operaciones de búsqueda y rescate, vigilancia de las fuerzas del orden y del control de fronteras o seguimiento de tormentas o previsión de huracanes. Pero sin duda, donde destaca su uso y proporciona una gran cantidad de ventajas y mejoras en el sector industrial.

3.1. Aplicaciones en el ámbito industrial

Principalmente este tipo de vehículos, en el ámbito industrial, nos permiten tener una perspectiva aérea ilimitada, lo cual abren nuevas oportunidades y generan eficiencia en sectores como la minería, puertos marítimos, petróleo y gas, agricultura y muchos otros sectores industriales.

Principalmente, los *drones* son utilizados para las siguientes funciones:

- **Inspección**: Proporcionan un proceso de inspección más eficaz, rentable y seguro, eliminando así el riesgo que sufren los inspectores al realizar este tipo de tareas.
- **Topografía y mapeado**: Consiste en la recogida y análisis de distintos tipos de datos que permite una toma de decisiones informadas, una mejor gestión de riesgos y una mejora de la planificación.
- **Seguridad y respuesta a emergencias**: Permiten proporcionar una visión en tiempo real de las situaciones de seguridad y emergencia. A mayores de que permiten un recopilación precisa de la información.
- **Gestión de existencias**
- **Optimización de las vías de transporte**

El grupo de investigación sobre *drones* **Drone Industry Insights** (droneii) ha reunido información, durante el año 2021, acerca de las aplicaciones y sectores para tratar de averiguar como las distintas

industrias utilizan los *drones* y cuales son sus aplicaciones más populares. Esto se ve recopilado en el siguiente infograma:

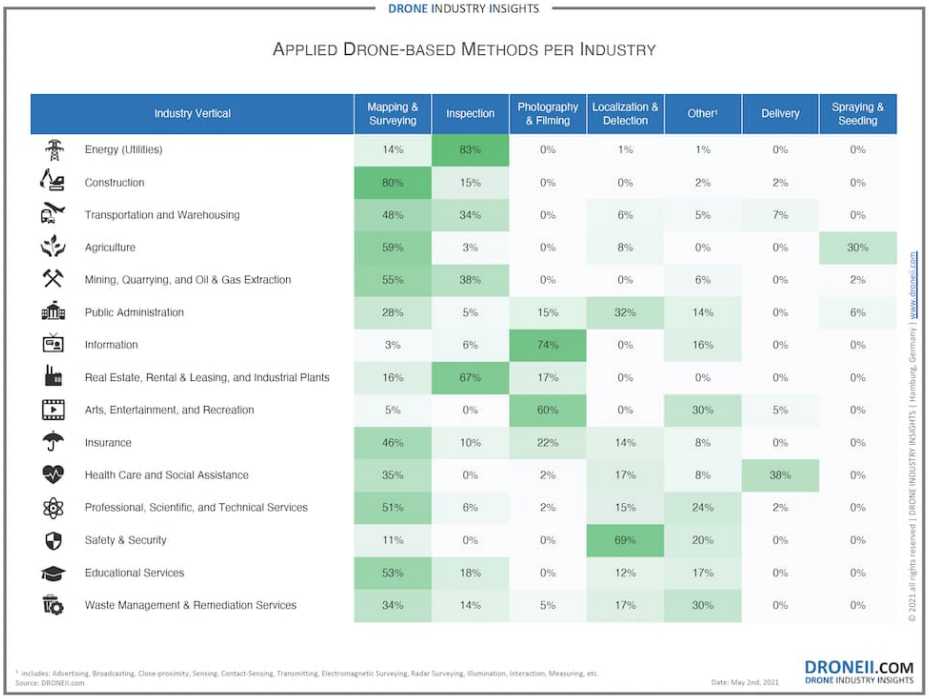

Figura 5: Infograma droneii

En el se puede observar como el principal uso de los *drones*, en el entorno industrial, es el mapeo o estudio de datos relativos a la organización, seguido de la aplicación de inspección y en un tercer puesto la fotografía o filmación.

Por último comentar que en los últimos años son más las empresas de logística que se suman al salto tecnológico que supone el uso de *drones*. Esto va desde la gestión de almacenes, hasta la realización de labores de transporte y entrega de paquetes. Recientemente **Google** ha conseguido la certificación de la *Administración Federal de Aviación*, la cual permite operar *drones* autónomos de reparto a domicilio en Estados unidos.

4. Impacto de la seguridad de los drones

Como pudimos ver en la sección anterior, los *drones* están teniendo una gran impacto dentro de la nueva Industria 4.0, es por ello que estos *drones* deben estar regulados por la Regulación general de *drones* que rige la Agencia Estatal de Seguridad Aérea (AESA).

A nivel industrial los riesgos que pueden suponer un mal uso del *drone* o que un atacante tome el control del *drone* son infinitos, pero quizás los riesgos más importantes son: poner en riesgo a terceros o trabajadores, interferir en el tráfico aéreo civil, dañar a material de la organización o acceder a infraestructuras críticas con zonas restringidas. Con todo los principales vectores de ataque identificados se dirigen o tienen como objetivo final a conseguir obtener el control sobre el *drone*, a conseguir su posicionamiento o alterarlo y el robo o suplantación de los datos transmitidos.

Esto se ve incrementado, pues la exposición es el principal problema de estos dispositivos, pues ninguno de los niveles de la red está aislado y cualquier atacante puede acceder a los sensores y actuadores. Las

comunicaciones industriales suelen producirse mediante cable, pero en este caso, todos los canales de comunicación son inalámbricos, por lo que el riesgo de que se vea afectada la seguridad aumenta.

Un ejemplo del impacto que puede suponer la vulnerabilidad de la seguridad de los *drones* en el ámbito industrial, es el producido recientemente en Aramco, en el cual, mediante una ataque con *drones*, se produjo un incendio en una planta de gas. Esto viene a manifestar los riesgos que este tipo de tecnología supone para el ámbito industrial y la necesidad de contar con medidas de seguridad para evitar este tipo de situaciones.

5. Vectores de ataques en los drones

El organismo público **Incibe** identifica los siguientes vectores o tipos de ataques:

- **Man in the middle**: dirigido al intercambio de información entre el centro de control (transmisor de señales) y el control telemétrico (receptor de señales=. Normalmente para este tipo de comunicación se utiliza la tecnología *WiFi*.
- **Denial of Service**: dirigido a los canales o sensores del *drone*.
- **Communications sniffing and forwarding or injection**: se obtiene información sobre los protocolos utilizados e intenta inyectar datos y payloads en el canal observando el efecto que estos producen.
- **Impersonation of GPS or Denial of the GPS service**: Saturación del canal GPS con datos falsos para intentar afectar al vuelo del *drone*, o hacer que envíe una posición incorrecta al centro de control.

A mayores de los comentados anteriormente, existen otro tipo de ataques o vulnerabilidades que afectan a los *drones* como pueden ser ataques a los distintos sensores que esto incorporan o ataques dirigidos específicamente al *filmware o hardware*, introduciendo en estos errores intencionados o *payloads* maliciosos.

Existen ataques dirigidos a puertos de red vulnerables, como son el caso del puerto 21 (Ftp) y el puerto 23 (Telnet), los cuales pueden ser utilizados para obtener acceso a los directorios raíz del software. También existen ataques de desautentificación que tienen como objetivo desconectar el enlace establecido entre el controlador y el *drone*. Esto se realiza mediante la realización de técnicas de *snooping* en el enlace de comunicación y el posterior envío de múltiples paquetes de desautentificación. Por último comentar que también existen ataques dirigidos a la suplantación de direcciones IP y MAC para tratar de conseguir el control total del *drone*.

Esto todo se puede ver recogido o resumido en el esquema 6, el cual clasifica y enumera los distintos vectores de entrada así como los principales objetivos de los ataques hacia los *drones* o *UAVs*.

Como podemos observar existen multitud de vectores o formas de ataques a los *drones* pero en este documento nos vamos a centrar en los ataques dirigidos al sistema GPS que estos dispositivos incorporan. Existen dos ataques principales a este sistema de comunicación, por un lado el *jamming* y por otro el conocido como GPS *spoofing*.

El principal problema al que se enfrentan las comunicaciones GPS es la baja potencia de transmisión de las señales (alrededor de 130 dBm), es por ello que esta puede ser fácilmente interrumpida mediante la transmisión de señales de interferencia de alta potencia. Además, los servicios civiles de GPS no tienen mecanismos de encriptación o autenticación, por lo que este tipo de señales pueden ser fácilmente replicadas o creadas de cero, para realizar ataques de *spoofing*. A comentar vamos a profundizar un poco en ambos ataques.

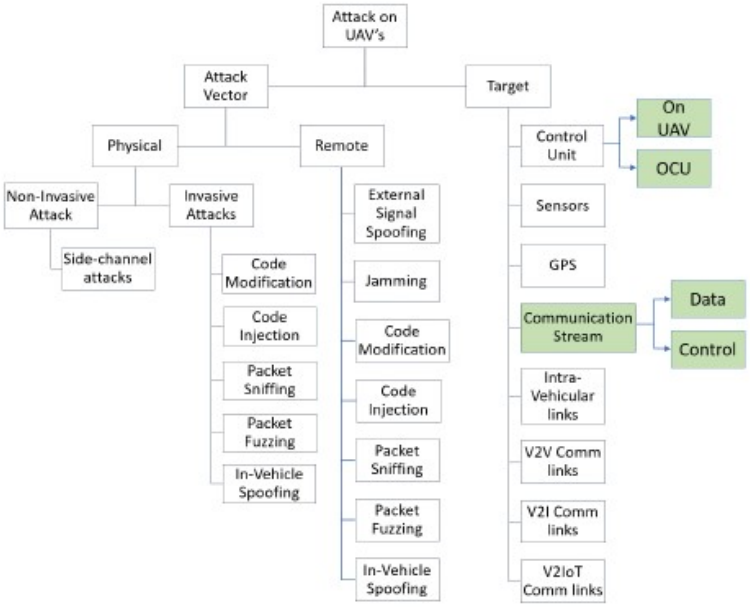

Figura 6: Clasificación ataques a UAVs

5.1. GPS Jamming

Se basa en la idea de generar y transmitir una señal de suficiente potencia en la dirección de un objetivo, la cual puede lograr que el receptor GPS no se capaz de recibir la señal del sistema de posicionamiento.

La baja potencia con la que llegan las señales GPS a los receptores, permite que la potencia necesaria para interferir la señal sea muy baja, lo que hace que dicha interferencia sea muy sencilla de realizar. Al evaluar la influencia de una señal interferente debemos utilizar la relación J/S (interferencia/señal). Cuando se expresa en dB, esta es la diferencia de potencia entre la señal interferente y la potencia recibida. Según distintos estudios, un nivel J/S de 27 dB es suficiente para prevenir o evitar la fase de adquisición de los receptores GPS.

La mayoría de ataques de *jamming* tienen la finalidad de que el atacante puede obligar a un *drone* a aterrizar, pues este, según un modo de seguridad, en cuanto detecta que no interferencias o no obtiene señal GPS aterriza automáticamente. Un ejemplo de esto sucedió con un *drone* estadounidense capturado por Irán (fig: 7).


Exclusive: Iran hijacked US drone, says Iranian engineer

In an exclusive interview, an engineer working to unlock the secrets of the captured RQ-170 Sentinel says they exploited a known vulnerability and tricked the US drone into landing in Iran.

Figura 7: Drone US capturado por Irán mediante jamming.

Esta interferencia GPS puede ser llevaba a cabo utilizando una diversa gama de hardware, el cual pueden emplear distintas antenas (omnidireccionales vs direccionales) y transmitir con distinta potencia. Dichos *jammer* se pueden encontrar fácilmente y varias su precio en función principalmente de la potencia de señal (8).

Figura 8: Jammers en el mercado.

A mayores este tipo de dispositivos pueden utilizar distintos tipos de tecnologías y técnicas de *jamming*. El *paper* Elezi et al. (2019) identifica 4 posibles modelos de señal para realizar *jamming* GPS, los cuales son *Pulse Jamming*. *Spot Jamming*, *Barrage Noise Jamming* y *Sweep Jamming*. Resultando el modelo **Spot Jamming** el más eficaz, causando una mayor tasa de error de bit (BER), debido a que concentra toda su potencia en una frecuencia concreta de señal.

Para mitigar este tipo de ataques existen varias soluciones. Una de ellas, llevada a cabo por Tedeschi, Oligeri & Di Pietro (2020), recoge la idea de aprovechar la señal de interferencia para localizar la fuente de la que proviene, utilizando para ello la intensidad de la señal recibida (*RSS*). Esto permitiría al *drone* o *UAV* salir de la zona de exposición del *jammer*.

Otros estudios recogen una clasificación general de técnicas *Anti-Jamming*, las cuales son:

- **Pre-correlation techniques**: Suelen implementarse en el hardware externo, antes del procesamiento del GPS. Siguen una estructura sencilla, la cual puede aplicarse a cualquier receptor GPS sin necesidad de modificaciones. Principalmente este tipo de técnicas incluyen uso de distintos tipos de filtros, como son el uso de filtros temporales adaptativos, espacio-temporales, espacio-frecuencia...
- **Post-correlation techniques**: Una ventaja importante frente a las anteriores, es que son eficaces contra todas las formas de onda de interferencias. Algunas de las técnicas utilizadas son por ejemplo la utilización de un *Adaptive Loop Bandwidth* o la utilización de la técnica *Data Wiping*.

5.2. GPS Spoofing

Si se produce una ataque exitoso de falsificación del GPS, este puede tener graves consecuencias, pues se puede llegar a conseguir desviar el curso del vuelo o hacer que un *drone* se estrelle. A mayores, gracias a este proceso, también se puede eludir la función de seguridad *Geofencing*, la cual impide que los *drones* vuelen sobre zonas prohibidas de vuelo (**DJI**), poniendo en riesgo a personas o instalaciones.

Dentro de esta categoría de ataques, existen distintos tipos y variantes. Un ejemplo de ello son los ataques llamados **Meaconing**, en los cuales, a groso modo, el atacante simplemente captura las señales GPS auténticas y las retransmite hacia el objetivo. Pudiendo así realizar un ataque más avanzado construyendo una señal falsa que contenga información maliciosa.

Para empeorar las cosas, la falta de cualquier tipo de mecanismo de autentificación hace que el receptor GPS no tenga forma de distinguir mensajes auténticos de los que no lo son. Además como el estándar GPS, es un estándar abierto y se conocen de antemano todos los parámetros técnicos, el GPS civil puede ser fácilmente imitado y replicado.

Otro tipo de ataque de suplantación, son aquellos que tienen como objetivo manipular el mensaje GPS, ya sea causando perturbaciones o desviaciones en el cálculo del tiempo o induciendo errores en las mediciones de ubicación.

- *Suplantación de la hora*: La señal GPS suplantada transmitida por un atacante puede provocar una desviación temporal y cambios bruscos en el reloj de la víctima, por lo que la hora percibida de estos dispositivo se ve modificada, lo que puede dar lugar a una planificación errónea de la ruta e incluso a la posible colisión.
- *Falsificación de la localización*: Este tipo de ataques tiene como finalidad la manipulación de los cálculos de localización basado en el GPS, introduciendo así una posición fija que no es la real, tal y como muestra el esquema de la figura 9. Este tipo de falsificación puede dar lugar a un desvío del rumbo real, a un choque, a un secuestro o incluso llegar a conseguir el control total del dispositivo, obligándolo a aterrizar en un lugar de elección del atacante.

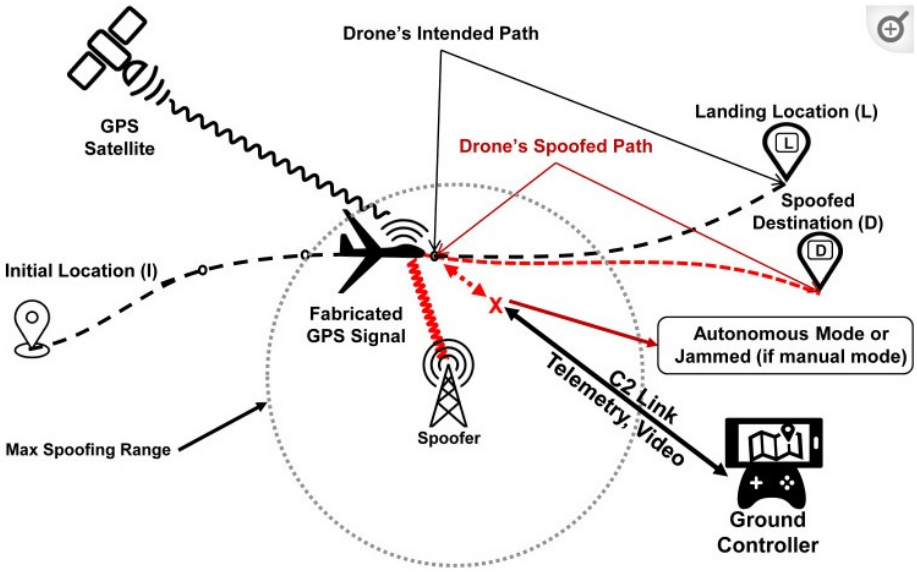

Figura 9: Falsificación de la localización

El siguiente esquema (fig: 10) categoriza los distintos tipos de ataque *spoofing* en función de diferentes parámetros como son la localización, el carácter sigiloso del ataque, el objetivo final del atacante...

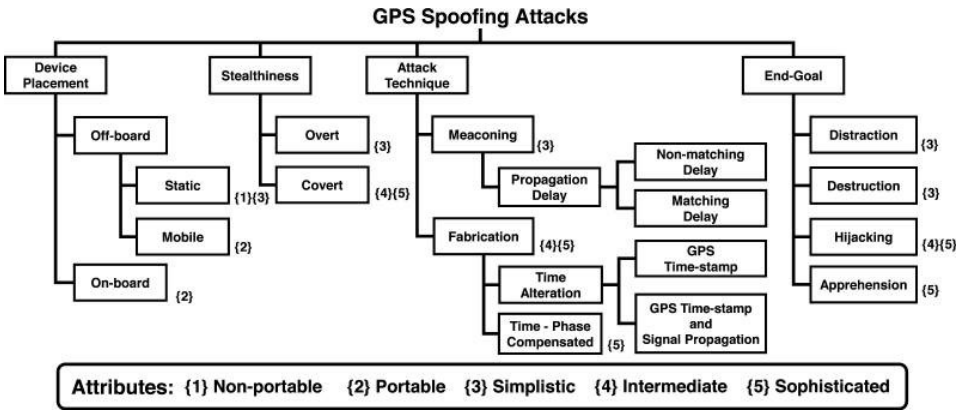

Figura 10: Clasificación de ataques GPS Spoofing

A continuación vamos a comentar los aspectos más importantes:

- **Ubicación del *spoofer***: Se pueden dar dos situaciones, dispositivos que se mantienen a distancia del objetivo (*Off-board*) y dispositivos que se incluyen y ocultan en un lugar sobre el objetivo (*On-Board*). Este último tipo de dispositivos normalmente requiere de una comunicación inalámbrica para recibir los comandos de suplantación e enviar al mismo tiempo una correcta retroalimentación, aunque también puede ser configurar para realizar tareas autónomas.
- **Grado de ocultación o *stealthiness***: Los ataques pueden ser divididos en dos grandes grupos atendiendo a este criterio: *abiertos*, es decir, el *spoofer* no intenta ocultar el ataque y *encubierto*, el *spoofer* intenta evadir la detección transmitiendo señales de *spoofing* elaboradas de tal manera que son casi idénticas a las originales, por lo que se evita que la víctima active posibles alarmas de detección de *spoofing*.

  A mayores comentar que en los ataques de *spoofing abiertos* se suele adoptar la estrategia **jam-then-spoof**, es decir, el receptor GPS de la víctima pierde la señal GPS auténtica antes de cambiar a la señal de *spoofing*.
- **Técnicas de ataque**: Principalmente existen dos tipos principales de técnicas de ataques, por un lado tenemos el **meaconing** o ataque de repetición, que viene a ser la reproducción o re-radiación de las señales GPS originales, interceptándolas y volviéndolas a emitir con el propósito malicioso de confundir al receptor GPS. Y por otro lado tenemos los ataques de *fabricación*, que son más avanzados y elaborados que los anteriores y tienen como objetivo forzar al receptor GPS a ejecutar comandos maliciosos con el fin de obtener el control completo del sistema.
- **Objetivos principales del *GPS spoofing***: Principalmente son 4 los objetivos principales que persigue un *spoofer*:
  - Con el objetivo de distraer, con el fin de impedir o retrasar de que llegue a su destino.
  - Con el fin de conseguir la destrucción del dispositivo.
  - Para obtener el control temporal del objetivo.
  - Con el objetivo de dirigir a la víctima a un destino predefinido para obligarla a aterrizar y así capturar el *drone* o su carga útil.

Este tipo de ataques también presenta una serie de limitaciones o consideraciones a tener en cuenta, así como herramientas *anti-spoofing* a la hora de realizarlos:

- **Posición relativa del spoofer**. La eficacia de este tipo de ataques, entre otros aspectos, depende de la posición relativa del suplantador con respecto a la víctima objetivo. Se requiere establecer una línea de visión clara y consistente con la víctima, lo que en algunos casos puede resultar complicado, pues dicha víctima está en constante movimiento.

  Por otra parte cabe mencionar, que cuando se trata por ejemplo de un enjambre de *drones* y solo se quiere atacar a uno en concreto, es muy difícil dirigir el directo a ese *drone* sin afectar a los demás de su alrededor.
- **Variaciones de distancia**. Las distancias cambiantes entre el atacante y la víctima pueden provocar un fluctuación brusca en la intensidad de la señal. Esto es porque, en este caso, la potencia recibida por el *drone* viene dada por la fórmula de **Free-space path loss** ($Pr = Pt/4\pi^2$), la cual nos viene a decir, que la potencia recibida varía inversamente con el cuadrado de la distancia entre el emisor y el receptor.
- **Receptores *anti-spoofing***: Principalmente funcionan identificando cualquier pico o intento de conexión GPS, es decir, detectando valores o cambios inusuales de los parámetros relacionados con la potencia. Se realiza un control de los parámetros relacionados con el tiempo por ejemplo la duración del intervalos entre las transiciones de fase o el retardo entre las señales transmitidas en diferentes frecuencias.

  Otros conceptos importantes, a la hora de utilizar técnicas *anti-spoofing* son, el procesamiento espacial, que viene a ser la detección de múltiples señales con la misma dirección de llegada

o también la protección criptográfica de los mensajes GPS. También se utiliza la inteligencia artificial para la detección de señales GPS falsificadas.

- **Receptores *multi-gnss***: Vienen a ser aquellos receptores que son capaces de utilizar simultáneamente dos os mas sistemas GNSS, es decir, por ejemplo pueden recibir señales GPS, Galileo y GLONASS, por lo que en caso de un intento de interferencia o ataque pueden migrar a otro sistema GNSS para conseguir la posición de su ubicación.
- **Angulo de llegado (AoA) de la señal**: Las antena GPS suele montarse en la parte superior de los *drones* o UAV, para así tener una línea de visión directa con los satélites GPS. Un spoofer o atacante que tenga su base en tierra, va a tener difucultades para entablar comunicación con el objetivo. A mayores, esto sirve como herramienta *anti-spoofing* pues se pueden filtrar o rechazar señales recibidas desde una única ubicación.

6. Caso práctico 1. GPS Jamming

Al no disponer de un *drone* o UAV que dispusiese de GPS, se decidió comentar alguna publicación publicada por terceros.

En este primer caso, el cual fue extraido del siguiente enlace vamos a ver una demostración de un ataque *jamming* a un drone, en concreto al modelo *DJI Phantom 4 Pro* (fig: 11). Este tipo de *drone* incorpora una antena GPS en la parte superior bajo la cubierto de ABS. Entre dicha antena y el propio dispositivo se incorpora una cinta de cobre que actúa como una capa de protección contra una posible señal maliciosa la cual provenga del suelo.

Figura 11: DJI Phantom 4 Pro

Para producir una señal capaz de interferir en el receptor GPS, la señal se construye utilizando el *software* **GNU Radio**, el cual, entre otras cosas nos permite crear bloques de procesamiento de señal para implementar radios definidas por software y sistemas de procesamiento de señales. Es entonces, cuando se genera un bloque *Nopise Source* con ruido blanco *gaussiano*, como se muestra en la figura 12, produciendo una señal de espectro amplio.

Esta señal se procesa y transmite mediante un SDR. Un SDR o radio definida por software es un sistema de comunicación por radio donde los componentes, que tradicionalmente se implantaban mediante hardware ahora, se implementan mediante software en un ordenador personal o sistema integrado. En este caso se utilizó el dispositivo SDR hackrf, conectado este a un amplificador y a una antena direccional, siguiente el esquema de la figura 13.

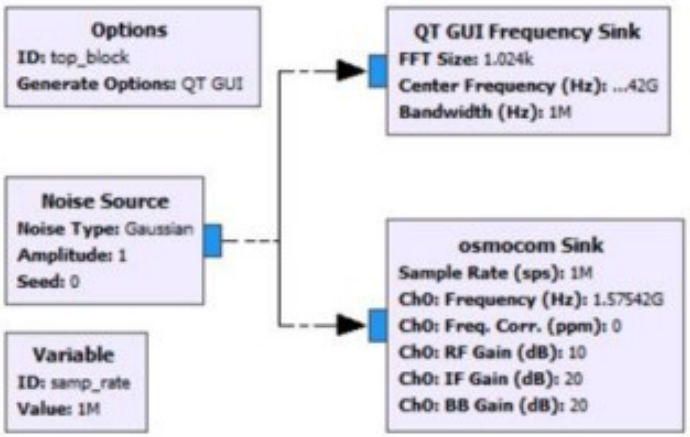

Figura 12: Jamming Signal block

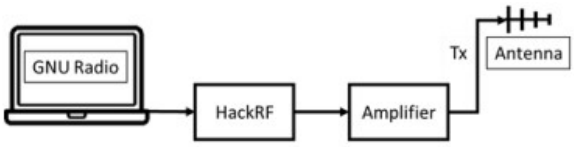

Figura 13: Esquema configuración del hardware

Esta señal de interferencia se va a transmitir a la frecuencia central de 1575.42 MHz, que es la frecuencia del GPS y con una amplitud de más de 10 MHz, suficiente para cubrir todo el código del GPS. A la hora de realizar las pruebas la antena que radia la señal *jamming* se coloca en una posición a 1.5 metros elevada del suelo. El *drone* se vuela a 4 alturas diferentes, 1.5 metros, 2.5 metros, 50 metros y 100 metros. En cada altura, el *drone* es probado a 50 metros, 100 metros y 150 metros de distancia de la antena *jammer*, empleando diferentes ángulos de inclinación de la antena que radia. Se puede ver un ejemplo de este entorno en la siguiente imagen (fig 14).

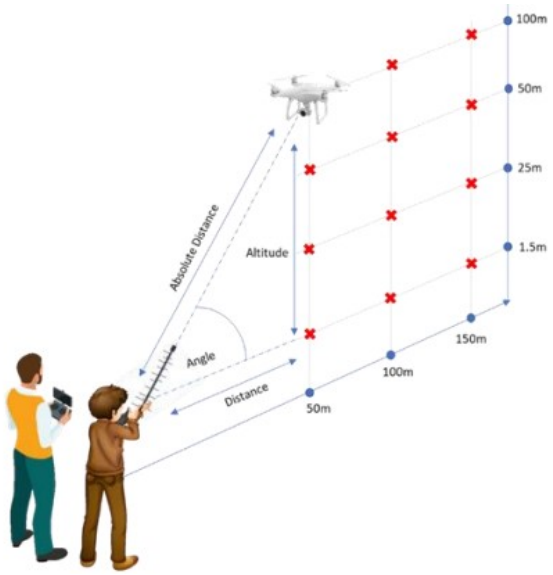

Figura 14: Entorno de pruebas

Si los resultados son satisfactorios esto se ve directamente reflejado en la aplicación DJI a la hora de volar el *drone*. Se considera que la prueba *jamming* tiene éxito cuando el recuento de satélites es de 0 a 3, lo que provoca que el GPS quede inutilizado y sin conexión, como se muestra en la figura 15.

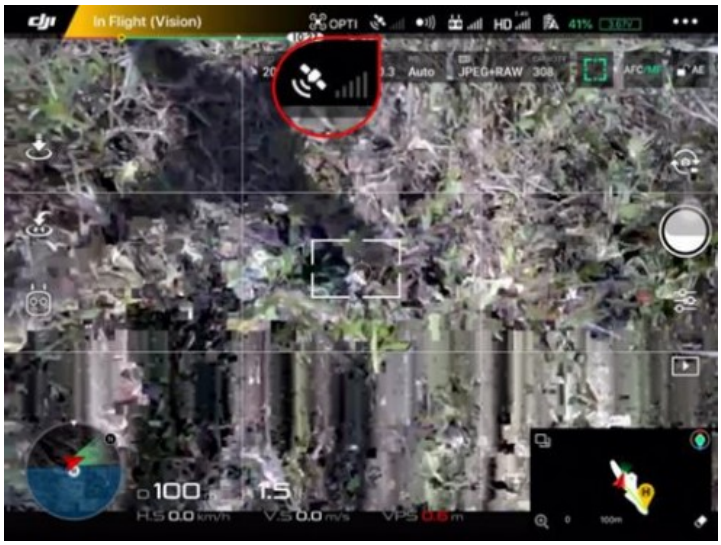

Figura 15: DJI GO 4 app - fallo de conexión

A continuación se muestran los resultados del estudio para las distintas situaciones:

Altitud 15 metros			
Distancia	50	100	150
Ángulo de elevación	0	0	0
Distancia absoluta	50	100	150
Resultado	Satisfactorio	Satisfactorio	Satisfactorio

Cuadro 1: Altitud 15 metros

Altitud 25 metros			
Distancia	50	100	150
Ángulo de elevación	26.57	14.04	9.46
Distancia absoluta	55.90	103.08	152.10
Resultado	Satisfactorio	Satisfactorio	Erróneo

Cuadro 2: Altitud 25 metros

Altitud 50 metros			
Distancia	50	100	150
Ángulo de elevación	45	26.57	18.44
Distancia absoluta	70.71	111.80	158.11
Resultado	Satisfactorio	Satisfactorio	Erróneo

Cuadro 3: Altitud 50 metros

Altitud 100 metros			
Distancia	50	100	150
Ángulo de elevación	63.44	45	33.69
Distancia absoluta	111.80	141.42	180.28
Resultado	Erróneo	Erróneo	Erróneo

Cuadro 4: Altitud 100 metros

Podemos observar como la capacidad de interferencia disminuye con el aumento del ángulo de elevación y la distancia. Por lo que cuando tenemos un ángulo de elevación de 0 grados se consigue el mejor rendimiento de la señal de interferencia. Es por eso que se puede observar la eficacia de la capa protectora bajo la antena GPS, pues cuando nos situamos en una posición inferior al *drone*, es decir, con un ángulo de elevación elevado, no somos capaces de realizar *jamming* al dispositivo.

7. Caso práctico 2. GPS Spoofing

Este caso práctico se detalla en el siguiente paper, en el cual para la prueba va a utilizar el *drone* **DJI Matrice 100**. Como equipamiento *hardware* se va a utilizar un ordenador portátil, una radio definida por *software* (SDR), una antena que opere en la frecuencia del GPS (1575,42 MHz) y un atenuador adecuadamente seleccionado para garantizar que las señales falsas no se desplacen más allá del radio de pruebas. El funcionamiento que va seguir este equipamiento se representa mediante el siguiente esquema 16.

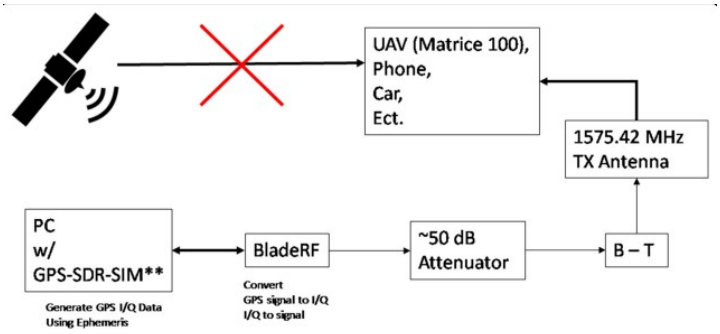

Figura 16: Esquema hardware ataque GPS Spoofing

Es decir, este ataque va a seguir cuatro fases:

1. Entrenar o crear coordenadas GPS falsas con la ayuda de nuestro ordenador.
2. Dichas coordenadas son enviadas utilizando para ello *BladeRF*.
3. El *drone* reconoce dichas señales como si fuesen transmitidas por el satélite.
4. Se puede llevar el secuestro o realización de diversos ataques al *drone*.

Por lo tanto, el primer paso será generar el flujo de datos que será enviada al nuestro dispositivo objetivo. Para ello se utiliza el *software* **GPS-SDR-SIM**, el cual es de código abierto, y se encuentra en el siguiente repositorio. Esta herramienta, para generar la *IQ data* hace uso de un fichero de navegación **RINEX**, el cual puede ser encontrado en el mismo repositorio, y sirve para generar el *stream* de datos justamente para el momento exacto, respetando la hora *ephemerides*. Un ejemplo de comando sería el siguiente:

```
# gps-sdr-sim -e brdc1010.13n -l 47.9253, 97.0329, 0 -d 300
```

Comentar que el archivop RINEX se corresponde con la fecha 11 de Abril de 2013 y las coordenadas se sitúan en Australia. Dichos datos generados, pueden ser enviados a nuestro SDR (BladeRF) con la configuración predeterminada del *GPS-SDR-SIM* utilizando para ello el siguiente comando:

```
# bladeRF-cli -s bladerf.script
```

Este script se corresponde con una configuración de la frecuencia en 1575.42 MHz, una frecuencia de muestro a 2.6 MHz, un ancho de banda de 2.5 MHz y una ganancia de transmisión a -25dB.

Se demostró que dicho ataque tuvo éxito sobre el *drone* **M100** pues la aplicación DJI Go mostraba la ubicación como en Australia (fig: 18), tal y como se había configurado en los mensajes de suplantación de identidad.

ç

Figura 17: M100 DJI GO app Location - Spoofing attack

A mayores se llevó otro ataque, en le que se fue introducido un perfil de ubicación dinámico predefinido, incluido en el repositorio oficial. Para ello, el *drone* fue colocado sobre un banco de pruebas con las hélices retiradas, y cuando se introdujeron los mensaje ilegítimos se pudo observar como la aplicación *DJI GO* (18) informaba de que el *drone* se movía en una gran trayectoria circular y los motores del *Matrice 100* funcionaban a plena potencia para contrarrestar el movimiento falsificado. Si en ese momento el *drone* estuviese volando seguramente se habría estrellado al intentar su localización contra el perfil de movimiento falsificado.

Figura 18: M100 ubicación dinámica GPS Spoofing

8. Conclusiones

Cada vez más, en múltiples sectores e industrias, se están utilizando *drones*, UAVs y en general dispositivos y robótica inteligente para realizar múltiples funciones y tareas. Algunas de estas funciones vienen a intentar evitar o reducir riesgos para trabajadores u operarios, así como reducir costes y automatizar procesos para las distintas empresas que los utilicen.

La gran mayoría de esto dispositivos, utilizan aplicaciones basadas o que necesitan el uso de sistemas como el GPS, por lo que las vulnerabilidades inherentes a este tipo de servicios presentan unas graves amenazas, y pueden provocar consecuencias desastrosas para la compañía u organización.

Se puede observar como un atacante, sin necesidad de tener mucho conocimiento previo, puede poner en una situación de aprieto aquellas personas o industrias que utilicen este tipo de tecnologías. Las medidas mitigadoras y de defensa que existen muchas veces no están de manera correcta llevadas a cabo o incluso mediante ataques más elaborados, dichas medidas no tendrían ningún efecto. A mayores la gran mayoría de *drones* de uso civil no incluyen este tipo de tecnología para así poder reducir costes o *hardware* adicional.

Referencias

[1] Los drones aportan nuevas soluciones a la Industria 4.0. DYNATEC enlace.

[2] Analysis of the GPS Spoofing Vulnerability in the Drone 3DR Solo. Sandra Pérez Arteaga; Luis Alberto Martínez Hernández; Gabriel Sánchez Pérez; Ana Lucila Sandoval Orozco; Luis Javier García Villalba enlace.

[3] Global Positioning Systems Market Size, Share & Trends Analysis Report By Deployment, By Application (Aviation, Marine, Surveying, Location-Based Services, Road), And Segment Forecasts, 2018 - 2025. enlace.

[4] What Are GPS Drones, and Why Does It Matter. droneblog enlace.

[5] Bandas de frecuencia en drones. Vekigo enlace.

[6] On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. Shah Zahid Khan, Mujahid Mohsin and Waseem Iqbal enlace.

[7] Unmanned Aerial Vehicle (UAV) GPS Jamming Test by using Software Defined Radio (SDR) platform. Ahmad Danial Bin Abdul Rahman, Kamaruddin Abdul Ghani, Nor Hisham H Khamis, Abd Rahim Mat Sidek enlace.

[8] 237 WAYS DRONE APPLICATIONS REVOLUTIONIZE BUSINESS. Drone Industry Insights enlace.

[9] Robots and drones in the Industry 4.0. Incibe-cert enlace.

[10] What is spoofing and how to ensure GPS security?. Septentrio enlace.

[11] Houthi drone attack on Saudi oilfield causes gas fire, output unaffected. Reuters enlace.

[12] GPS Jamming Signals Propagation in Free-Space, Urban and Suburban Environments. Lester de A. Faria1, Caio A. de Melo Silvestre1, Marcelino A. Feitosa Correia1, Nelson A. Roso1 enlace.

[13] A review on cybersecurity vulnerabilities for unmanned aerial vehicles. C. G. Leela Krishna; Robin R. Murphy enlace.

[14] Using GPS Spoofing to Control Time - Def con 25. Dave/Karit enlace.

[15] The effect of Electronic Jammers on GPS Signals. Esat Elezi; Göksel Çankaya; Ali Boyaci; Serhan Yarkan enlace.

[16] GPS Interference Mitigation for Small UAV Applications. Joy Li enlace.

[17] Leveraging Jamming to Help Drones Complete Their Mission. Pietro Tedeschi; Gabriele Oligeri; Roberto Di Pietro enlace.

[18] Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing. J. Magiera, R. Katulski enlace.

[19] Unmanned Aerial Vehicle (UAV) GPS Jamming Test by using Software Defined Radio (SDR) platform. Ahmad Danial Bin Abdul Rahman, Kamaruddin Abdul Ghani, Nor Hisham H Khamis2, Abd Rahim Mat Sidek enlace.

[20] Github GPS-SDR-SIM. Takuji Ebinuma enlace.

[21] Development of a GPS spoofing apparatus to attack a DJI Matrice 100 Quadcopter. Eric Horton and Prakash Ranganathan enlace.

[22] DEF CON Safe Mode Aerospace Village. Harshad Sathaye enlace.