

SISTEMA Y METODO PARA LA INTRUSIÓN DE SEÑALES DE COMUNICACIÓN Y GEOLOCALIZACIÓN DE DRONES

Campo de la invención

- 5 La presente invención está relacionada con la ingeniería electrónica y de sistemas, especialmente está relacionada con sistemas y métodos de detección, control y neutralización de UAVs (vehículos aéreos no tripulados).

Descripción del estado de la técnica

- 10 En el estado de la técnica se encuentran documentos que divulgan dispositivos relacionados con equipos y sistemas para la ubicación y neutralización de vehículos aéreos no tripulados como los enseñados en las siguientes publicaciones.

- El documento **US10103835** con título ***“PORTABLE COUNTERMEASURE DEVICE AGAINST UNMANNED SYSTEMS”*** divulga un dispositivo portátil de contramedidas que comprende una o más antenas direccionales, uno o más componentes de interrupción y al menos un activador. El dispositivo portátil de contramedidas comprende además un cuerpo, con las antenas direccionales fijadas a una parte frontal del cuerpo. El uno o más componentes de ruptura pueden estar montados externa o internamente al cuerpo del dispositivo. El dispositivo portátil de contramedidas está dirigido a un dron específico, el activador está activado y las señales perturbadoras se dirigen hacia el dron, interrumpiendo el control, la navegación y otras señales hacia y desde el dron.

A pesar de que la publicación citada involucra un conjunto de elementos para interrumpir en general el control sobre un dron, puntualmente dicha publicación no involucra como si lo hace nuestro sistema la posibilidad de atacar a más de un dron al tiempo, siempre y cuando estos se encuentren dentro del rango de la zona de ataque.

- 25 Además, encontramos el documento **US20210302533** titulado ***“DETERRENT FOR UNMANNED AERIAL SYSTEMS”*** que corresponde a un sistema para proporcionar detección integrada y disuasión contra un vehículo no tripulado que incluye, entre otros, sistemas no tripulados de tecnología aérea que utilizan un elemento de detección, un elemento de seguimiento, un elemento de identificación y un elemento de interdicción o disuasión. Los elementos contienen sensores que observan datos cuantificables en tiempo real sobre el objeto de interés para crear una evaluación de riesgo o amenaza para un área protegida de interés. Esta evaluación puede basarse, por ejemplo, en la extracción de datos de fuentes de datos internas y externas. El elemento disuasorio selecciona de un menú variable de posibles acciones disuasorias. Aunque está diseñado para una acción autónoma, un Human in the Loop puede anular las soluciones del sistema automatizado.

Aunque la mencionada solicitud se refiere como ya lo dijimos a un conjunto de equipos para la detección y disuasión de vehículos no tripulados esta presenta notables

diferencias con la materia reclamada en nuestra solicitud, por ejemplo, el sistema que hemos desarrollado utiliza antenas sintonizadas a distintas frecuencias para aumentar la probabilidad de éxito de un ataque que permita mitigar los UAV's y además nuestro sistema está programado para que trabaje de forma autónoma durante largos periodos de tiempo una vez es configurado por una persona, elementos y características no reveladas por la solicitud **US20210302533** y que permiten destacar la novedad y altura inventiva de nuestro producto frente al estado de la técnica.

Dentro de los sistemas ya conocidos también encontramos el divulgado en la solicitud de patente americana **US9524648** nombrado como "**COUNTERMEASURES FOR THREATS TO AN UNCREWED AUTONOMOUS VEHICLE**" allí se menciona que los vehículos autónomos sin tripulación "uav" pueden navegar de un lugar a otro, específicamente en este documento se describen sistemas, dispositivos y métodos que brindan contramedidas para amenazas que pueden comprometer los uav, una pluralidad de uav pueden establecer una red de malla para distribuir información entre sí, un primer uav puede recibir datos externos de un segundo uav utilizando la red de malla, los datos externos se pueden usar para confirmar o cotejar datos como la ubicación, el rumbo, la altitud, etc. El desacuerdo entre los datos generados por el primer uav con los datos externos del segundo uav puede resultar en la determinación de que el primer uav está comprometido. se pueden tomar medidas correctivas, como que el primer uav se pueda dirigir a un lugar seguro para aterrizar o estacionar, puede recibir comandos de otro uav, y así sucesivamente.

La invención mostrada en el anterior antecedente se enfoca en proteger a los drones de ataques como el generado por nuestra invención, lo que evidencia que es de un campo distinto, por lo que presenta muchas diferencias, entre ellas están, nuestro sistema utiliza el "firmware" del o los UAV's en su contra para neutralizar el vuelo. Esto se hace "engañando" al dron con datos de geolocalización que le indiquen que se encuentra en una zona de vuelo prohibida para forzar su aterrizaje y además el sistema bloquea la comunicación Wifi entre la aeronave y su mando, lo que evita cualquier contramedida.

Otra tecnología que se ubica dentro del campo de nuestra invención es la divulgada en la solicitud americana **US11280913** que lleva por título "**GLOBAL POSITIONING SYSTEM SPOOFING COUNTERMEASURES**" aquí se divulgan conceptos y tecnologías dirigidas a contramedidas de suplantación de identidad del sistema de posicionamiento global. Las realizaciones pueden incluir un sistema que comprende un procesador y una memoria que almacena instrucciones ejecutables por computadora que configuran un procesador para realizar operaciones que incluyen la identificación de un equipo de transporte móvil que incluye un dispositivo de registro electrónico y un dispositivo de área amplia de baja potencia. El dispositivo de registro obtiene datos de ubicación GPS de una unidad receptora GPS y el dispositivo de área amplia de baja potencia obtiene datos de ubicación independientes a través de una ruta de banda estrecha de una red de área amplia de baja potencia. Las operaciones pueden incluir determinar que existe una desalineación espacio-temporal entre los datos de ubicación

independientes y los datos de ubicación GPS para el equipo de transporte móvil, y proporcionar una alineación de datos espacio-temporales. Las operaciones pueden incluir la determinación de que se ha producido un ataque de suplantación de GPS y la creación de una alerta de suplantación de GPS para el equipo de transporte móvil.

- 5 La invención referida antes se enfoca en proteger a un dispositivo que usa datos de geolocalización, de ataques como el generado por nuestra invención, entonces es de un campo distinto, no obstante, destacamos que en nuestro sistema se delimita una zona de ataque, en la que no es posible que un dron circule con normalidad.

10 Por otra parte, de la información observada en la página web relacionada con la empresa **DRONE HUNTER** encontramos sistemas Anti-Dron para la protección del espacio aéreo para instituciones, empresas y particulares. Particularmente, los dispositivos detectan uno o varios drones simultáneamente a una distancia de hasta 450 metros, reconocen el tipo de dron, gestionan la alarma y neutralizan solo el dron que se desea intervenir. El equipo evita que señales de control o de orientación lleguen correctamente al dron y
15 dispone de capacidad para tomar el control de dicho dron.

Según lo anterior, los documentos **US10103835**, **US20210302533**, **US11280913** y los dispositivos enseñados por la empresa **DRONE HUNTER** divulgan tecnologías para interrumpir en general el control sobre un dron mediante la detección, seguimiento, identificación e interdicción o disuasión del dispositivo y en uno de los casos dicha
20 tecnología se enfoca en proteger a los drones de ataques como el generado por nuestra invención.

Sin embargo, ninguno de los anteriores dispositivos utiliza un sistema de bloqueo por GPS que mediante el software de control del sistema se le envía al UAV una ubicación en la que sea prohibido volar este tipo de aparatos, de tal manera que el dron “crea” que
25 se encuentra en dicha ubicación y se forcé así su aterrizaje. Los sistemas divulgados tampoco presentan un sistema de ataque Wifi que realiza ataques a través de las dos bandas de frecuencia que comúnmente utilizan los drones comerciales con su mando, estas son: 2,4 GHz y 5,8 GHz. Tampoco utilizan dos bloques de procesamiento independientes que permiten activar la intrusión de uno o de los dos medios de
30 comunicación (Wifi y GPS).

Breve descripción de la invención

Por lo mencionado antes, existe la necesidad de un sistema para para la intrusión de señales de comunicación y geolocalización de drones comerciales ya que la utilización
35 de drones para atentar contra la seguridad de infraestructura crítica o para ejecutar acciones ilegales, ha hecho necesario recurrir a nuevas estrategias de detección, control y neutralización de UAVs (vehículos aéreos no tripulados) comerciales. Los sistemas convencionales de bloqueo de señales afectan a otros aparatos que se encuentren alrededor, lo cual limita su uso en zonas urbanas donde se encuentran edificaciones de

interés para terroristas, por ello se requiere de soluciones de contramedida que permitan mitigar los ataques con drones sin afectar los dispositivos electrónicos y comunicaciones circundantes a la zona que se desea proteger, igualmente el bloqueo repentino sobre drones destinados al terrorismo puede desencadenar un mayor problema, por ejemplo si se interviene un drone que contenga material explosivo lo más probable es que este pierda el control y caiga, acarreando consigo un mayor problema, por esto es necesario controlar también la aeronave después de ser bloqueada, garantizando la seguridad de terceros.

Nuestro sistema para la intrusión de señales de comunicación y geolocalización de drones se compone de dos conjuntos, con computadores de placa sencilla, un conjunto de módulo Wifi y un conjunto de módulo GPS o sistema de posicionamiento global, un sistema de radio definida por software (SDR) y un módulo de reloj TCXO externo, un computador portátil con conexión desde cualquier sistema operativo y switch de ethernet de varios puertos, interfaz de usuario: botones, entradas de texto y títulos, librerías y complementos del software, dos bloques de procesamiento independientes para activar la intrusión de uno o de los dos medios de comunicación (Wifi y GPS), un editor de código para poder realizar los códigos fuente de la interfaz, código de instrucciones en un lenguaje de programación para el ataque cibernético, encerramiento del sistema, que es una caja para equipos electrónicos resistente al agua.

Breve descripción de las figuras

La FIG.1 corresponde a un esquema del sistema para la intrusión de señales de comunicación y geolocalización de drones que de forma general se compone de un encerramiento, caja o carcasa (9), un computador portátil (10), un conjunto de modulo Wifi (11) y un conjunto de modulo sistema de posicionamiento global GPS (12).

La FIG. 2 corresponde a un diagrama de cómo están conectados los elementos que conforman el sistema para la intrusión de señales de comunicación y geolocalización de drones y que se encuentran ubicados en la caja o encerramiento (9).

Descripción detallada de la invención

La presente invención está relacionada a un nuevo sistema y método de detección, control y neutralización de UAVs (vehículos aéreos no tripulados).

SISTEMA PARA LA INTRUSIÓN DE SEÑALES DE COMUNICACIÓN Y GEOLOCALIZACIÓN DE DRONES COMERCIALES.

El sistema novedoso e inventivo de nuestra solicitud está destinado a la intrusión de señales de comunicación y geolocalización de drones comerciales, este sistema comprende los siguientes elementos y características:

Dos conjuntos, un conjunto de módulo Wifi (1) y un conjunto de módulo GPS (2) o sistema de posicionamiento global, más un SDR y un TCXO externo (módulo reloj). El conjunto de módulo Wifi se compone de un computador de placa sencilla, cable de alimentación, cable ethernet de módulo Wifi. El conjunto de módulo GPS se compone de un computador de placa sencilla, cable de alimentación, cable ethernet, módulo SDR y TCXO externo (módulo reloj).

Además, contiene un computador portátil, y la conexión de este se puede realizar desde Windows o Linux y un switch de ethernet. Una interfaz de usuario, para realizar esta interfaz se utilizó el software Glade GTK (herramienta de desarrollo visual de interfaces gráficas) el cual está diseñado para realizar aplicaciones en Linux desde distintos lenguajes de programación (Python, C, PHP, JS, etc.).

Para el funcionamiento del software se instalan las librerías y complementos del software en el PC

Se desarrolló en lenguaje C (un lenguaje de programación de propósito general para la implementación de sistemas operativos y aplicaciones) un código que tomara las instrucciones de la interfaz gráfica de usuario o frontend (menús desplegables, imágenes, íconos, colores, elementos gráficos, animaciones) y llevara a cabo el ataque deseado.

Encerramiento del sistema: para el encerramiento se seleccionó la caja 1550 del fabricante Pelican (caja convencional para equipos electrónicos resistente al agua) en la cual caben todos los componentes de forma correcta, sin presentar riesgos eléctricos o de índole similar. La caja cuenta con dos paneles, uno en su base para fijar los componentes y otro en la tapa que contiene las conexiones exteriores del equipo. Los elementos que componen la caja son: dos computadores de placa sencilla, un switch de Ethernet, tres preamplificadores y tres amplificadores, sistema SDR y módulo generador de señal Wifi.

También fue necesario incluir otros componentes, como, una multitoma, dos ventiladores, dos conectores SMA de chasis, un conector de corriente, un conector de ethernet y fuentes de alimentación.

Otro aspecto que se tuvo en cuenta fue el consumo de energía de cada uno de los componentes de la caja, con el fin de energizar la misma de forma correcta, teniendo en cuenta esto, es necesario tener una fuente de al menos 12 A de corriente y 180 W.

Para la amplificación y radiación del sistema se utilizaron preamplificadores de cerca de los 20db de ganancia, los cuales a su vez van conectados a amplificadores de alta ganancia. La señal se irradia de forma independiente para los tres canales de frecuencia

utilizados, dos de Wifi (2.4GHz y 5.8 GHz) y uno de GPS (1.6GHz) a través de antenas direccionales.

Para mayor claridad, de acuerdo a las figuras 1 y 2 el sistema para la intrusión de señales de comunicación y geolocalización de drones se compone de un encerramiento, caja o carcasa (9), un computador portátil (10), un conjunto de módulo Wifi (11) y un conjunto de módulo sistema de posicionamiento global GPS (12). Instalados en el encerramiento o caja (9) se ubica el switch ethernet (1), que permite la conexión entre el pc que realiza el ataque y los dos computadores de placa sencilla, uno para el control del ataque Wifi (2w) y una para el control del ataque GPS (2G) las cuales contienen el software y la configuración de cada ataque, un dispositivo SDR (3) que permite el ataque GPS, dispositivo de monitoreo Wifi (4) que permite el ataque Wifi, pre-amplificador de señal (5), esta etapa se compone de tres preamplificadores de señal de acuerdo a cada frecuencia, GPS (1.5MHz) Wifi (2.4MHz y 5.8MHz), se ajusta la señal para que pueda ser amplificada a mayor potencia, amplificadores de señal (6), esta etapa amplifica la señal de forma que sea posible obtener un mayor alcance, fuentes y alimentación (7) el sistema requiere de una conexión a 110V, antenas (8) el dispositivo cuenta con 5 puertos, 1 puerto ethernet para el pc que opera el sistema, 1 puerto de conexión a 110V y 3 puertos de antenas de acuerdo a cada ataque (1 para GPS y 2 para Wifi), encerramiento, caja o carcasa (9) y computador portátil (10).

METODO DE INTRUSIÓN DE SEÑALES DE COMUNICACIÓN Y GEOLOCALIZACIÓN DE DRONES

El método de intrusión de señales de comunicación y geolocalización de drones se compone de las siguientes etapas:

Etapa a. Ciberataque Wifi. Las tareas para llevar a cabo el ciberataque Wifi (red inalámbrica de banda ancha) son: conectar el cable de red al equipo y alimentarlo con 110 VAC. Realizar la conexión de escritorio remoto con el computador de placa sencilla asociado al ataque Wifi (2w). Abrir el software para realizar el ataque y bloquear todos los dispositivos que estén conectados a un canal específico de Wifi.

Etapa b. Ciberataque GPS. Las tareas para llevar a cabo el ciberataque son: conectar el cable de red al equipo y alimentarlo con 110 V. Realizar la conexión de escritorio remoto con el computador de placa sencilla asociado al ataque de geolocalización (2G). Abrir una terminal de comandos en la carpeta que contiene el software para el ataque y cargar las coordenadas falsas en un nuevo archivo. Abrir el software para realizar el ataque mediante el envío de las coordenadas falsas. Conexión de Dispositivos.

Etapa c. Configuración simultanea del conjunto Wifi y del conjunto GPS: realizar la conexión desde Linux, en caso de utilizar Windows se descarga la aplicación de Ubuntu

directamente desde Microsoft store o una similar que permita ejecutar una máquina virtual de Linux. Para realizar la conexión por Ethernet se fijó la dirección IP de los dos computadores de placa sencilla (2w, 2G) que controlan cada etapa, cada uno con una dirección IP diferente, después se configura. Se realiza una conexión remota entre el PC
5 y los dos computadores de placa sencilla (2w, 2G), mediante un servicio de tipo escritorio remoto, el cual permite el acceso gráfico al sistema de estos. Se realiza la conexión por escritorio remoto, teniendo en cuenta la IP asignada a cada computador de placa sencilla.

Estas tareas se implementaron simultáneamente para los dos sistemas.

- 10 Etapa d. Ciberataque Simultaneo Wifi-GPS. Estas tareas se llevan a cabo con el fin de realizar los dos ataques simultáneamente, operando los diferentes dispositivos desde un solo computador (10), mediante conexión Ethernet.

Los elementos necesarios para realizar esta conexión son los siguientes:

- 15 Computador portátil (10), la conexión se puede realizar desde un sistema operativo (Windows o Linux), switch de ethernet (mínimo 3 puertos), conjunto de ataque Wifi y conjunto de ataque GPS.

Otros elementos y características novedosas del sistema y método de intrusión de señales de comunicación y geolocalización de drones son:

- 20 El conjunto de bloqueo por GPS (12) utiliza las características de seguridad del firmware del dron (software que controla el computador que hace volar el dron) en su contra, ya que mediante el software de control del sistema se le envía al UAV (Unmanned Aerial Vehicle, que se vierten en español como el vehículo aéreo que no lleva tripulantes) una ubicación en la que sea prohibido volar este tipo de aparatos, por ejemplo un aeropuerto, de tal manera que el dron “crea” que se encuentra en dicha ubicación y se force su
25 aterrizaje.

- El conjunto de ataque Wifi (11) realiza ataques a través de las dos bandas de frecuencia que comúnmente utilizan los drones comerciales con su mando, estas son: 2,4 GHz y 5,8 GHz. Adicionalmente, mediante el uso de antenas direccionales se mitiga la afectación a aparatos y comunicaciones circundantes, lo cual permite que se pueda usar
30 el equipo para la protección de edificaciones que se encuentren en entornos urbanos.

Se utilizan dos bloques de procesamiento independientes que permiten activar la intrusión de uno o de los dos medios de comunicación (Wifi y GPS).

- Para controlar la activación y desactivación del sistema, se accede mediante un computador externo con conexión ethernet, lo cual permite que el usuario pueda ubicar
35 el sistema en una zona y manejarlo desde otra zona como un cuarto de control o de seguridad.

Se desarrolló una interfaz gráfica en software por cada ataque que permite controlar el inicio o la detención del mismo, así como un entorno gráfico amigable con el usuario que evite que este tenga que memorizar y ejecutar comandos complejos para el uso del sistema.

5

Algunas ventajas de nuestro sistema y método para la intrusión de señales de comunicación y geolocalización de drones son:

Con diferencia al estado del arte mencionado, el dispositivo implementado genera una señal con tecnología SDR, no solo para generar un error sino también para cambiar por completo la ubicación de la aeronave y forzar su aterrizaje de la forma más segura posible, inhibiendo también su comunicación con el mando mediante protocolos de aircracking en la comunicación Wifi.

10

El dispositivo implementado usa la seguridad del dron en su contra para obligarlo a aterrizar o moverse de la zona sin necesidad de tener que tomar el control de su movimiento.

15

Finalmente, el dispositivo implementado bloquea la señal del control remoto del dron y lo engaña con una posición falsa, para que este regrese automáticamente a su origen o aterrice, según su configuración de seguridad de fábrica.

20