ARTÍCULO DE INVESTIGACIÓN / RESEARCH ARTICLE

CyberDrone: una plataforma de ciberseguridad para detección de ataques a drones

CyberDrone: a cybersecurity platform for drone attack detection

Germán D. Zapata-Madrigal*
Rodolfo García Sierra**

* Profesor Asociado - Departamento de Energía Eléctrica y Automática, Facultad de Minas, Universidad Nacional. Medellín, Colombia. Ingeniero electricista, especialista en Alta Gerencia con énfasis en calidad, magister en Automática, doctor en Ciencias Aplicadas. gdzapata@unal.edu.co. Orcid: https://orcid.org/0000-0002-7739-1578. Teléfono: (+4) 4225266. Dirección: Carrera 80 #65-223, Oficina: M8-204

**Lead Auditor ISO55001, Asset Management Office, Infrastructure & Network Colombia, Enel – Codensa. Bogotá, Colombia. Ingeniero electricista, magister en Economía, doctor en Ingeniería – Industria y Organizaciones. rodolfo.garcia@enel.com. Orcid: https://orcid.org/0000-0002-3892-6189

INGENIERÍA y DESARROLLO | Vol. 39 n.° 1, 2021
2145-9371 (*on line*)
Universidad del Norte

Resumen

Se presentó el desarrollo de una plataforma de ciberseguridad para vehículos aéreos no tripulados (UAV, por sus siglas en inglés) o drones según la tecnología *cyber-deception*. Esta tecnología tiene como fundamento la creación deliberada de señuelos (*honeypots*) de fácil acceso y detección para detectar potenciales intrusos en el perímetro de una infraestructura crítica. Se explicó el modelo conceptual de la solución propuesta y la descripción detallada de cada uno de los procedimientos desarrollados, se implementó una metodología de desarrollo tecnológico, se llevaron a cabo procedimientos para la creación de señuelos en redes inalámbricas wifi y en bandas de radiofrecuencia (RF), y se incluyó la aproximación al desarrollo de un procedimiento de GPS Spoofing. Este último fue explorado usando un equipo de radio definido por software (SDR, por sus siglas en inglés) para la suplantación de señales GPS que permite la implementación de estrategias de defensa contra drones atacantes. Finalmente, se describe la plataforma web para monitorear los señuelos activos y para registrar los intentos de penetración. Estos registros de intento de penetración se almacenan en una *blockchain* desarrollada según la tecnología Ethereum. Se encontró que las redes inalámbricas wifi y de RF poseen vulnerabilidades que pueden ser explotadas por potenciales atacantes. También que el procedimiento GPS Spoofing es mucho más complejo que los procedimientos por redes inalámbricas, pero que permitiría tomar acción sobre drones atacantes.

Palabras clave: ciberseguridad, *cyber-deception*, dron; GPS Spoofing, radiofrecuencia, señuelo.

Abstract

This document presents the development of a cybersecurity platform for unmanned aerial vehicles (UAV), or drones, based on cyber-deception technology. This technology is based on the deliberate creation of easily accessible and detectable decoys (or honeypots) to detect potential intruders at the perimeter of a critical infrastructure. This document contains an explanation of the conceptual model of the proposed solution, and a detailed description of each of the developed procedures. A technological development methodology was implemented in this paper. Also, procedures were developed for the creation of honeypots in Wi-Fi wireless networks and in radio frequency bands, and the approach to the development of a GPS spoofing procedure was included. The latter was explored using software defined radio equipment (SDR) for the impersonation of GPS signals, which allows for the implementation of defense strategies against attacking drones. Finally, a web platform to monitor active decoys, and to register penetration attempts, is described. These penetration attempt records are stored in a blockchain, developed with basis on Ethereum technology. It was found that Wi-Fi and radio frequency wireless networks have vulnerabilities that can be exploited by potential attackers. Also, that the GPS spoofing procedure is much more complex than procedures by wireless networks, but it would allow to take action on attacking drones.

Keywords: cyber-deception, cybersecurity; drone, GPS Spoofing, honeypot, radiofrequency.

Fecha de recepción: 2 de agosto de 2020
Fecha de aceptación: 9 de junio de 2021

1. INTRODUCCIÓN

El uso de vehículos aéreos no tripulados (UAV, por sus siglas en inglés) o drones en la infraestructura eléctrica en Colombia y en el mundo ha incrementado [1] como una respuesta a las necesidades crecientes de inspección y mantenimiento de las redes aéreas y demás instalaciones críticas. Este incremento es esperado a medida que la demanda de energía y la escala del sistema aumentan, lo que genera nuevos retos tecnológicos en la supervisión, el control y el mantenimiento de los activos eléctricos. En sincronía con esta tendencia, y como parte de sus planes de mejora y desarrollo en su infraestructura eléctrica, Codensa ha implementado el uso de drones en tareas de inspección termográfica de conductores eléctricos y aisladores, mapeo de topografía, apoyo en casos de emergencia, desplazamiento de carga y tendido de conductores eléctricos. Estas tareas, que antes eran realizadas en su totalidad por operadores en campo que ponían en riesgo su integridad física al someterse a trabajos en altura y entornos de alto voltaje, han mejorado sustancialmente su eficiencia, reducido costos de operación y aumentado la productividad de la empresa. El segmento de mercado de UAV en la infraestructura eléctrica está en rápido crecimiento, con un futuro potencialmente brillante.

Según [2] la consultora de servicios profesionales PwC valoró el mercado de soluciones impulsadas por drones en el sector de energía y servicios públicos en US$9,46 mil millones. Se destacan aplicaciones relacionadas con inspecciones a instalaciones solares, turbinas eólicas y líneas de transmisión. Otras aplicaciones como la creación de gemelos digitales (*digital twins*) también son posibles gracias al uso de los drones. Otros trabajos se enfocan en aplicaciones para recolectar información que permita registrar el estado de los activos eléctricos.

Por ejemplo, [3] presenta una disertación sobre las tecnologías de vehículos aéreos no tripulados y un método a fin de controlar autónomamente un UAV para la inspección de líneas de transmisión, usando navegación visual y analizando en tiempo real las imágenes tomadas.

Por otra parte, en [4] se resalta la eficiencia de los UAV en diversas tareas, haciendo un recuento de la temporada de huracanes en 2017 en Estados Unidos. En esa época, se sacó provecho de la capacidad de los UAV de bajo costo para recorrer áreas que sufrieron daños graves en la infraestructura eléctrica o que se habían inundado, lo que ayudó a los esfuerzos de recuperación del servicio de energía en las áreas afectadas. En ese estudio, se evaluaron los beneficios monetarios y los desafíos institucionales de la introducción de UAV para la respuesta a desastres y las inspecciones programadas de la infraestructura eléctrica.

El potencial de los drones para ayudar a mantener el servicio de energía eléctrica y el buen estado de las redes de servicios públicos está aún por explotar. El mantenimiento

de los activos distribuidos en un área extensa, el acceso a la infraestructura de difícil acceso y la ejecución de procedimientos de inspección peligrosos normalmente realizados por humanos, o en helicópteros o aviones, pueden ser reemplazados por drones.

Los UAV superan a otras tecnologías al hacer que las inspecciones sean más baratas, más rápidas y más seguras. También permiten una mayor precisión y un mejor acceso a lugares difíciles de alcanzar.

El mantenimiento predictivo, enfocado en minimizar fallas y daños en la red, también es de gran valor. Lo más importante es que las inspecciones basadas en drones se pueden realizar sin tener que cortar el suministro de energía. Estas ventajas son cruciales, ya que cada vez más países implementan regulaciones que otorgan incentivos financieros a las empresas que mejoran la confiabilidad o imponen sanciones a aquellos que no logran los objetivos.

En [5] han calculado el valor global de los incentivos relacionados con la mejora de la confiabilidad de los sistemas de suministro de energía en US$609,3 millones, y se estima que globalmente las pérdidas del sector de energía y servicios relacionados con cortes de la red son cercanos a US$169 mil millones.

En los procesos que se llevan a cabo en el entorno de la infraestructura eléctrica mediante drones, existe un alto flujo de datos operativos y protocolos de comunicación para el control autónomo o remoto de los UAV. En estos se ha evidenciado vulnerabilidad a ciberataques dirigidos, pues los drones no poseen mecanismos de defensa cibernética eficientes, y en la mayoría de los casos no utilizan protocolos de comunicación seguros ni métodos de cifrado, lo cual afecta la integridad, disponibilidad y confidencialidad de los datos [6], [7].

Por ejemplo, en [6] se concluye que la investigación relacionada con UAV para contrarrestar las amenazas de ciberseguridad se centra en el bloqueo del GPS (por sus siglas en inglés) y la suplantación de identidad, pero ignora los ataques a los controles y al flujo de comunicaciones de datos.

La brecha en la investigación de ataques al flujo de comunicaciones de datos es preocupante, ya que un operador puede ver un UAV volando fuera de su trayectoria debido a un ataque de flujo de control, pero no tiene forma de detectar un ataque a la reproducción o grabación de video (sustitución de la señal de origen de un video).

También en [6] se hace un análisis de todos los ataques que han recibido los UAV en diferentes sectores, ya sean reportes de ataques reales, ya sean simulaciones en entornos controlados. Para el primer caso, se discriminaron los ataques por el tamaño del dron, pues en los entornos de la infraestructura eléctrica es más común el uso de UAV de pequeño tamaño. En estos, se ven ejemplos como el ataque de bloqueo de GPS

realizado en un S-100 Camcopter, un UAV basado en rotor de Schiebel, que provocó un accidente que mató a un ingeniero de Schiebel e hirió a dos pilotos remotos durante las pruebas. El ataque fue realizado por un actor desconocido el 10 de mayo de 2012 durante la prueba del UAV por parte del ingeniero, cerca de la ciudad portuaria occidental de Incheon (Corea del Sur). El ataque se detectó después del accidente y se sospecha que la interferencia del GPS comenzó el 28 de abril, que también interrumpió los vuelos de pasajeros en Kimpo e Incheon [6], [8].

Eventos como la pérdida de un Centinela RQ-170, interceptado por las fuerzas militares iraníes el 4 de diciembre de 2011 [9], o el virus Keylogging, que infectó una flota estadounidense de UAV en Creech Air Force Base en Nevada en septiembre de 2011, muestran que los esfuerzos del pasado para identificar riesgos y proteger los UAV son insuficientes.

No solo los equipos UAV son blanco de ataques cibernéticos. Las instalaciones de control de empresas de alto valor estratégico y de infraestructura crítica son blanco de atacantes que intentan introducir programas o rutinas que trunquen el funcionamiento normal de los equipos. Varios incidentes se han documentado en la literatura que dan cuenta de lo catastrófico que puede ser un ciberataque a una fábrica o una planta de generación eléctrica.

El incidente Stuxnet [10] es un claro ejemplo de ataques que resultaron en graves consecuencias físicas. Ocurrido en 2010, este ataque afectó la planta nuclear en Natanz (Irán), la cual fue víctima de un ciberataque. Este gusano se hizo con el control de 1.000 centrifugadoras utilizadas para enriquecer uranio y les dio la orden de autodestruirse. En este incidente, los atacantes indujeron exitosamente vibraciones o distorsiones excesivas para destruir las máquinas de centrifugado rápido. Este ataque fue un código sin precedentes que atacó, en primer lugar, a las máquinas y redes de equipos Windows, replicándose a sí mismo y actualizándose al encontrar conexiones a internet. El virus podría haber comprometido los controladores lógicos programables, enviar comandos en falso, intervenir en las señales del SCADA (por sus siglas en inglés) y hacerlo indetectable hasta ser catastrófico. Los autores del ataque podrían así espiar los sistemas industriales e, incluso, provocar que las centrifugadoras se desgarren, sin que los operadores humanos de la planta lo comprendan. Según estudios de Kaspersky Lab, este caso es considerado como la primera vez que un ataque cibernético logra dañar la infraestructura del mundo físico [10].

Otro ejemplo fue el *malware* Industroyer encontrado en Ucrania, el cual es fácilmente reproducible y modificable, por tanto, podría dirigirse a infraestructura local como proveedores de transporte, agua y gas [11]. Aunque el *malware* es capaz de causar interrupciones que duran hasta varios días en partes de la red de una nación, no es lo suficientemente potente como para apagar la totalidad de la red nacional. También

conocido como Crash Override, es solo la segunda pieza de *malware* descubierto hasta la fecha que es capaz de interrumpir procesos industriales sin la necesidad de que los *hackers* intervengan manualmente [11].

Es probable que continúen los ataques de *malware* en la red eléctrica y a otras infraestructuras clave que son administradas o mantenidas por sistemas informáticos. Los ciberataques en infraestructura crítica, específicamente en el sector de energía eléctrica, tienen la capacidad de afectar la integridad física y la estabilidad económica. Un ejemplo de esto fue el ataque ocurrido en Ucrania el 23 de diciembre de 2015, mediante el cual se logró tomar el control de los sistemas de control de tres de las principales distribuidoras regionales de electricidad. Este incidente provocó cortes de energía que afectaron a cerca de 225.000 usuarios [12].

En atención a todas las investigaciones sobre ciberseguridad en vehículos aéreos no tripulados y en los sistemas que componen la infraestructura eléctrica, es posible enfocar los estudios en busca de soluciones innovadoras que cumplan con los requisitos de seguridad y desempeño en la operación de los UAV para gestión de activos eléctricos. Para esto, existen diversos estudios en otros campos como el sector militar, donde tecnologías avanzadas como *cyber deception* están teniendo impactos positivos en cuanto a detección y neutralización de ataques cibernéticos.

Para [13], *cyber deception* se define como las acciones planeadas para confundir o desorientar a los atacantes y hacer que tomen o no medidas específicas que ayuden a las defensas de seguridad informática. Con esto, lo que se desea alcanzar utilizando *cyber deception* es crear un entorno dinámico que reaccione de manera diferente a cada ciberataque, mediante mecanismos que engañan a un atacante y le hacen creer que se encuentra frente a un sistema con información real y valiosa.

Según [14], después de que los intrusos ganan presencia en una red, en general realizan un reconocimiento para localizar activos valiosos en otras computadoras en la red e intentan comprometerlos para alcanzar sus objetivos. Los sistemas de detección de intrusiones (IDS, por sus siglas en inglés) de última generación no detectarán ataques de día cero, y también pueden generar muchas falsas alarmas que hacen que los defensores de la red pierdan tiempo identificando esos ataques.

Se cree que es fundamental aumentar el grado de complejidad y dificultad de los sistemas de protección de ciberataques para prevenir que cualquier intruso realice un reconocimiento de red y aumente la probabilidad y la precisión de detectar la presencia de intrusión. Sin embargo, el reconocimiento de la red puede no ser fácil de detectar, porque tales actividades pueden realizarse a un ritmo muy lento y, por tanto, ser sigilosas.

Además, las configuraciones de las redes empresariales suelen permanecer estáticas durante mucho tiempo, lo que permite a los intrusos recopilar inteligencia del entorno de red a lo largo del tiempo, como la topología de red, los *hosts* en la red, los servidores y los tipos de servidor. Como solución a este problema [14] propone un sistema de engaño cibernético adaptativo llamado ACyDS, que proporciona una vista de red virtual única para cada *host* en una red empresarial. En pocas palabras, el enfoque de engaño de ACyDS permite disuadir las actividades de reconocimiento, prevenir la suplantación si se han comprometido múltiples *hosts* y aumentar la probabilidad y la confianza de detectar la presencia de intrusos. Las técnicas basadas en el engaño proporcionan ventajas significativas sobre los controles de seguridad tradicionales.

Actualmente, la mayoría de las herramientas de seguridad son medidas receptivas para los ataques a vulnerabilidades previamente conocidas. Cuando surge un ataque, este es contrarrestado con todos los mecanismos preventivos a disposición del defensor. Eventualmente, los atacantes persistentes encuentran una vulnerabilidad que conduce a una infiltración exitosa, al evadir la forma en que las herramientas detectan las sondas o al encontrar nuevas vulnerabilidades desconocidas.

Según [13] existe una diferencia fundamental en cómo funcionan los mecanismos basados en el engaño, en contraste con los controles de seguridad tradicionales. Este último en general se enfoca en las acciones de los atacantes, las detecta o las previene, mientras que las primeras se enfocan en las percepciones de los atacantes, las multiplican y, por tanto, inducen a los adversarios a tomar acciones/inacciones de forma que sean ventajosas para los sistemas específicos. Los controles de seguridad tradicionales se posicionan en respuesta a las acciones de los atacantes mientras que las herramientas basadas en el engaño lo hacen ante la perspectiva de tales acciones.

Para [15] el engaño representa una forma de lograr una defensa activa. La defensa basada en el engaño permite agregar defensa adicional mediante la incorporación de información falsa que lleva a los atacantes a conclusiones imprecisas, y explotar el efecto sorpresa que resulta de la suposición de que los sistemas siempre responden con la verdad. Ofrece la posibilidad de comprender las estrategias del atacante al proporcionar medios para atraer a los adversarios y aumentar su percepción del riesgo de ser detectado. Esto hace que el adversario pierda tiempo y energía en obtener y analizar información falsa, así como que permite que la defensa detecte ataques desconocidos que otras herramientas de defensa pueden perder.

Asimismo [15] proponen un enfoque sistemático de modelado de múltiples paradigmas para incorporar tácticas de engaño en el diseño de *softwar*e. Con esto buscan mejorar el desarrollo de técnicas basadas en *cyber deception* para proteger los sistemas, ya que su uso se encuentra en un estado temprano de desarrollo y promete grades cambios a la forma en que se detectan y neutralizan los ciberataques.

Finalmente [16] hacen un estudio sobre el avance actual de la tecnología *cyber deception* y discuten la necesidad del engaño con respecto a las amenazas actuales y la noción de acercarse al engaño cibernético basado en la tecnología. Esto los condujo a examinar brevemente una gran cantidad de trabajo sobre las técnicas de engaño utilizadas en la actualidad. Las técnicas se categorizaron como basada en *host*, en red o híbrida. El engaño basado en *host* en general tiende a usar técnicas basadas en *honeypot*, al atraer a los adversarios a ambientes con capacidades de introspección. Los desarrollos modernos en el engaño basado en el *host* exploran entidades más nuevas que pueden ser falsificadas. Además, las técnicas recientes apuntan a mejorar el parcheo del *software* mediante la construcción de *honeypots* en parches de *software* y para ocultar las vulnerabilidades que corrigen los parches. Las técnicas de engaño basadas en la red tienen como objetivo ocultar los activos y aprovechar los avances en las redes dinámicas. Mediante el uso de redes definidas por *software*, las soluciones basadas en red dificultan a los adversarios ocultar sus ataques. Las soluciones híbridas combinan muchas de estas técnicas para crear amplias capacidades de engaño, como enrutar a los adversarios a redes clonadas creadas a pedido.

El engaño cibernético es una gran promesa en el ámbito de la ciberseguridad, ya que las tecnologías para respaldar el dinamismo de los servidores y las redes pueden utilizarse como recursos para manipular y engañar al adversario. Sin embargo, todavía hay mucha investigación que se puede hacer para tomar engaños desde simples técnicas de punto único hasta soluciones efectivas basadas en el sistema. Ante el problema descrito, y las oportunidades de las nuevas tecnologías, se propone implementar una plataforma de ciberseguridad que garantice todos los beneficios que prometen los UAV en las operaciones cerca de la infraestructura eléctrica, y preserve la integridad, disponibilidad y confidencialidad de los datos, mediante la integración con tecnologías de seguridad informática avanzadas como *cyber deception*. Esta tecnología ha tenido impactos muy positivos en el sector militar, donde la utilización de señuelos y el despliegue de trampas cibernéticas han reducido significativamente las alertas por falsos positivos en los sistemas y mejorado la detección y neutralización de ciberataques. *Cyber deception* utiliza técnicas de engaño mediante trampas o señuelos que consumen tiempo y recursos a los atacantes, y les hace creer que están frente a un sistema real con información valiosa. Este engaño otorga a los sistemas de defensa una ventaja para identificar el comportamiento del atacante y la información que desea obtener para neutralizarlo.

En atención a lo anterior, se ha desarrollado una serie de procedimientos de *cyber deception*, los cuales serán integrados en una plataforma de ciberseguridad para drones. Los procedimientos desarrollados van desde la creación de señuelos tipo *honeypots* en redes de comunicación TCP (por sus siglas en inglés), hasta el despliegue de señuelos con comunicación radiofrecuencia (RF).

2. METODOLOGÍA

El trabajo que se describe es una investigación tecnológica que busca proponer un sistema de ciberseguridad para drones según la tecnología *cyber deception*, a partir de la metodología de desarrollo tecnológico. La metodología de desarrollo del prototipo está definida en cuatro etapas, basada en el modelo general de desarrollo tecnológico que se encuentra en [17].

Las etapas de esta metodología son el estudio de necesidades, el diseño de la solución, su implementación y evaluación. Inicialmente, se debe definir el problema identificado en el uso de los drones para la evaluación de la infraestructura eléctrica. En el proceso de evolución tecnológica, las empresas del sector eléctrico implementan soluciones más eficientes en procesos de vigilancia, control y mantenimiento del sistema de transmisión y distribución de energía, donde tareas que antes eran ejecutadas por operarios, que se exponían a riesgos inherentes a trabajo en alturas y a entornos de alto voltaje, son ahora realizadas por nuevas plataformas autónomas o telecontroladas como los UAV o drones.

La ventaja de usar drones es que se reducen riesgos para los trabajadores y se evitan desconexiones indeseadas del sistema durante la revisión. También es una alternativa más económica a la tradicional inspección de las redes desde helicópteros. Los drones pueden ser utilizados en otras tareas como topografía, apoyo en casos de emergencia, transporte de carga y tendido de cables, lo que los hace una herramienta cada vez más utilizada por las empresas del sector eléctrico. Aunque el incremento en el uso de drones para tareas en diversas áreas de los sistemas de distribución de energía eléctrica ofrece beneficios asociados a la reducción de costos, menores riesgos para trabajadores y eficiencia en la supervisión y el control de la red, se tienen inconvenientes asociados a la seguridad de los datos y la integridad de la infraestructura física, debido a vulnerabilidades y riesgo a ciberataques en los UAV.

A causa de la adopción en el uso de drones para diferentes labores de montaje y mantenimiento de líneas de transmisión, estos se han convertido en un blanco de ataques cibernéticos, que representan un alto riesgo para la operación del sistema eléctrico. En entornos de operación cercanos a las líneas de transmisión o a las subestaciones de potencia, los riesgos son más evidentes, ya que la pérdida de control parcial o total puede ocasionar colisiones que generan en el mejor de los casos la desconexión del sistema o en escenarios más graves producir daños a la infraestructura o lesiones al personal en campo.

Es evidente que los drones son un blanco atractivo para los ciberataques, y se potencia aún más este interés al ser empleados en tareas asociadas a los sistemas de infraestructura crítica. Los sistemas de monitoreo de infraestructura crítica basados en modelos

de las tecnologías de la información y la comunicación (TIC) como las Smart Grid y los sistemas autónomos o telecontrolados como los drones son vulnerables a diversos ciberataques que pueden comprometer la privacidad de los datos y poner en riesgo la infraestructura de Enel-Codensa y el Sistema Interconectado Nacional (SIN).

El acceso no autorizado a la información operativa puede ocasionar problemas que van desde desconexiones en el servicio hasta afectación de la infraestructura física. En la mayoría de los casos, se ha detectado que estos inconvenientes están relacionados con vulnerabilidades en los mecanismos de seguridad del sistema. En este trabajo, se propone desarrollar estrategias de ciberseguridad adaptadas a los algoritmos y las tecnologías de comunicación utilizados en *cyber deception*, especialmente en la creación de objetivos falsos mediante señuelos y trampas cibernéticas, que sean aplicables a UAV mediante integración con algoritmos de control y mecanismos para intercambio de información en estos dispositivos.

El diseño y la implementación de un prototipo de plataforma de ciberseguridad para UAV representa un gran reto para Enel-Codensa al garantizar que la evolución tecnológica en la gestión de sus activos se encuentre alineada con los requerimientos de ciberseguridad establecidos para el sector de energía eléctrica, donde el crecimiento constante de la demanda aumentará la necesidad de contar con sistemas avanzados para vigilar, supervisar y controlar el estado de la infraestructura eléctrica. Además, la tecnología *cyber deception* se puede escalar a todos los sistemas que manejen intercambio masivo de datos y operen con tecnologías de la información, lo que representa una oportunidad no solo para Enel-Codensa, sino también para las demás empresas del sector.

Mediante una serie de procedimientos de *cyber deception* y su integración en una plataforma de ciberseguridad, será posible identificar ataques cibernéticos dirigidos a los drones y permitir tomar acciones de defensa oportunas. Los procedimientos van desde algoritmos y modelos de *software* que hacen posible desplegar señuelos y trampas cibernéticas, hasta la virtualización de drones que transmiten información falsa para desorientar al atacante.

La figura 1 muestra el modelo conceptual de la solución propuesta, donde se presentan las diferentes interacciones entre los tipos de comunicación considerados: wifi y RF. En este artículo, se describen los procedimientos de *cyber deception* que han sido desarrollados y probados a lo largo del proyecto, para identificar ataques informáticos dirigidos a los drones. Entre las señales que pueden utilizar diferentes tipos de drones en el mercado, existen las comunicaciones por wifi o las comunicaciones por RF.

Para brindar el mayor espectro de posibilidades a la plataforma de ciberseguridad, se ha desarrollado un procedimiento para cada una de estas comunicaciones. Los procedimientos efectuados utilizan tecnologías de *cyber deception* que permiten identi-

ficar atacantes cibernéticos a fin de prevenir incidentes de seguridad. Para el caso de los drones con comunicación wifi, se propone un procedimiento que permite crear un señuelo en la red, evitarle a un posible atacante acceder a la información y crear una señal de alerta para los administradores del sistema.

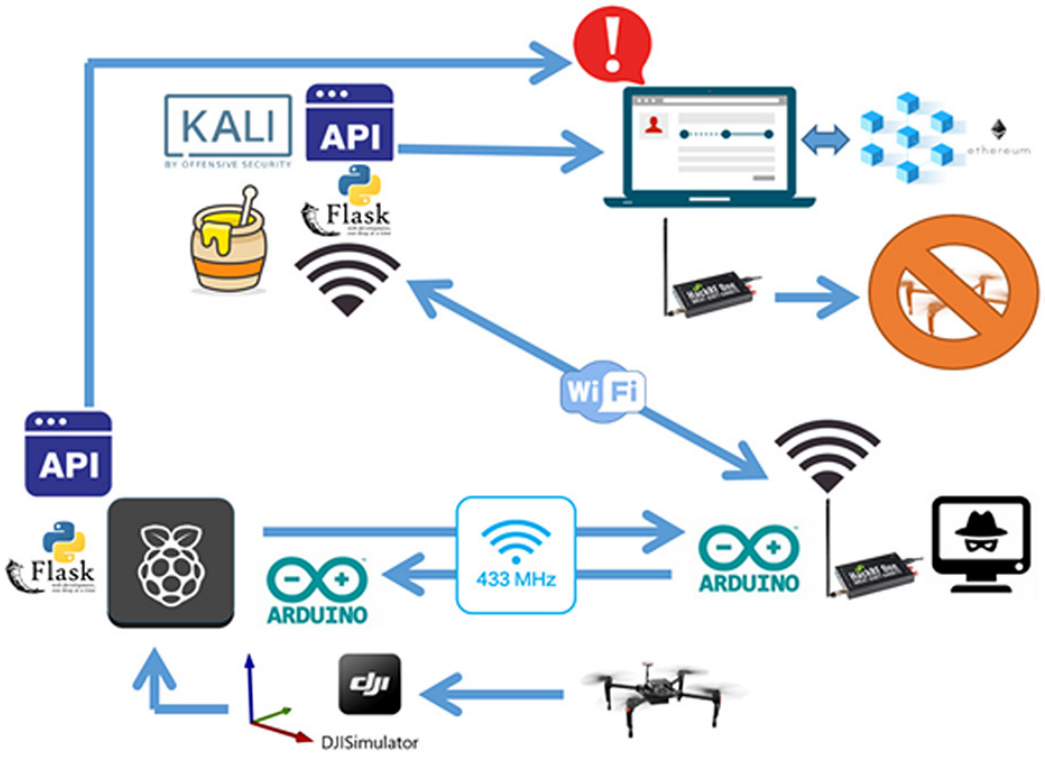

Figura 1. Modelo conceptual del prototipo para la plataforma CyberDrone según cyber deception. Se detallan las interacciones para cada tipo de comunicación: wifi y RF

Por otro lado, en cuanto a la comunicación RF, se desarrollaron los procedimientos realizados con diferentes frecuencias de comunicación. Se utilizan dispositivos de transmisión de RF que simulan el comportamiento de las señales de comunicación real de un dron. Todas estas señales se ubican en diferentes rangos de frecuencia y en un bajo nivel de seguridad de manera intencional, a modo de *honeypots* o señuelos, para identificar intrusos en la red y tomar acciones correctivas en los equipos reales para prevenir incidentes.

A continuación, se detallan los diferentes procedimientos diseñados, se explica el objetivo de cada uno y se presentan las salidas que obtienen los usuarios de la plataforma.

3. RESULTADOS Y DISCUSIÓN

Existe una gran cantidad de drones en el mercado que se comunican utilizando señales wifi en la banda de frecuencias de 2.4 GHz. A través de estos canales, se transmite información como video, señales de posicionamiento, entre otros. Las señales wifi pueden ser interceptadas y suplantadas fácilmente por un atacante, y brindar acceso a información y señales del dron e, incluso, el control del equipo mismo [18].

Este tipo de ataques se ha realizado con éxito en los drones Parrot Bebop y en el Parrot AR.Drone 2.0 y el 3DR Solo [9]. A pesar de que existen drones que encriptan la comunicación y otros que se comunican por medios de mayor seguridad como la comunicación RF, un atacante busca siempre las superficies de ataque que conlleven menor esfuerzo. Por tanto, entre los procedimientos de *cyber deception* se ha incluido el de despliegue de un *honeypot* como mecanismo de detección de intrusos en redes TCP. El *honeypot* permite engañar a un atacante al escanear el espectro de 2.4 GHz, específicamente las señales wifi, para hacerlo creer que existe un dron en esta red. En el momento en el que el atacante intenta interceptar las comunicaciones, el sistema bloquea automáticamente el acceso y genera una alerta para tomar acciones correctivas de seguridad en el perímetro.

En la figura 2, se describe el procedimiento de cyber deception en las redes wifi. En esta se muestran dos recursos seguros; en este caso, son dos drones que se comunican por wifi, pero las comunicaciones han sido debidamente encriptadas. El honeypot es un dron virtual, cuyos puertos de comunicación se encuentran abiertos a propósito para tentar al atacante a intentar vulnerarlo a modo de señuelo. Una vez que el atacante intenta acceder a las señales del CyberDrone, el sistema genera una alerta y recolecta toda la información posible del atacante.

Para desplegar este mecanismo de seguridad, se utiliza una distribución de Linux especializada en temas de seguridad informática llama Kali Linux. Entre los procedimientos, se incluye la instalación del sistema operativo en una USB booteable, lo cual permite correr el *honeypot* desde cualquier computador. En primer lugar, se ingresa en la sección de descargas de la página oficial de Kali Linux (https://www.kali.org/downloads/). Se descarga el archivo ISO correspondiente al equipo (32 bits o 64 bits).

Una vez se tenga corriendo y funcionando el sistema operativo Kali Linux, se descarga dentro de este la herramienta PenTbox por medio del comando Wget. PenTBox permite configurar y desplegar diferentes tipos de *honeypots* en la red. Luego de ejecutar la herramienta PenTBox, se despliega un menú en la consola, donde se muestran numeradas las opciones disponibles que permite la herramienta.

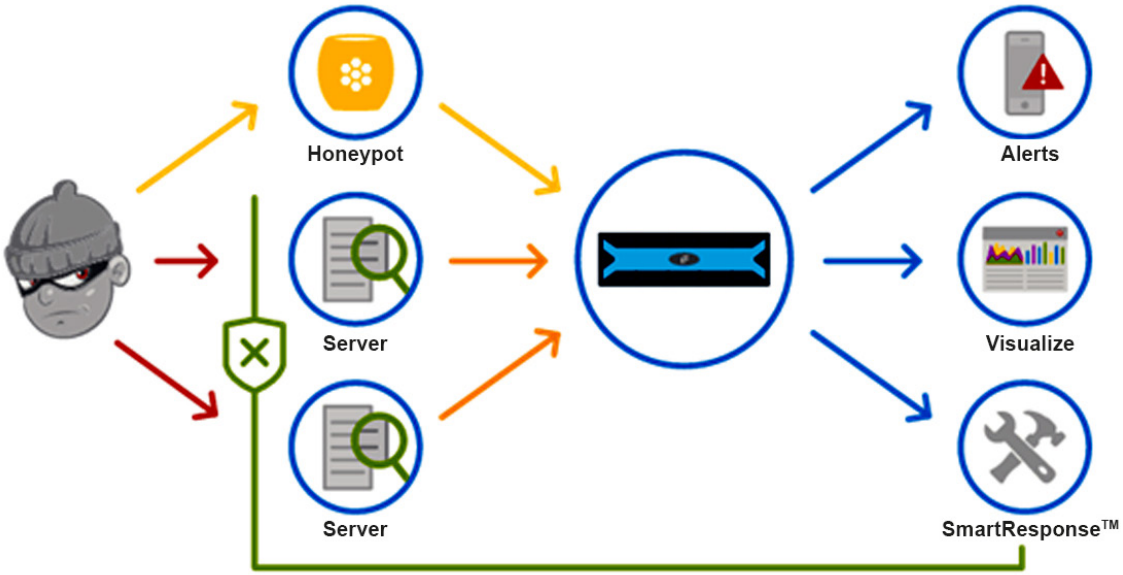

Figura 2. Modelo conceptual del señuelo o honeypot para redes wifi. En esta estrategia, se crea deliberadamente un acceso vulnerable para detectar la procedencia de los ataques

Se selecciona la opción 2-Network Tools (figura 3). Entre las herramientas de red de PenTBox, se elige la opción tres, correspondiente a la funcionalidad de *honeypot* (figura 4). Al ingresar en la opción *honeypot* en PenTBox, se muestran dos opciones. La primera es una configuración automática en que se selecciona por defecto el puerto 80 y se crea un mensaje falso predeterminado. Para comprobar el *honeypot* desplegado, se realiza una prueba de penetración y se ingresa desde un navegador a la dirección IP del *honeypot* desde otro computador que esté en la misma red.

En la figura 5, se puede ver que el *honeypot* le muestra un mensaje al atacante. Este mensaje es personalizable en la herramienta PenTBox. Para agregar una segunda capa de seguridad, se desarrolla un segundo procedimiento de *cyber deception*. En este caso, este procedimiento permite crear señuelos en las señales de RF. El objetivo de este procedimiento es simular la comunicación de un dron de mayor nivel de seguridad respecto de los drones que usan comunicación wifi y generar una segunda capa de seguridad para el CyberDrone. El dron virtual se comunica utilizando los mismos mensajes de un dron real, a excepción que los mensajes van desencriptados y en una frecuencia diferente. Este procedimiento permite crear un señuelo atractivo para los atacantes experimentados en la etapa de reconocimiento del ataque. Al explorar las señales de RF, podrán detectar las comunicaciones pensando que se trata de un dron real.

Figura 3. Menú de opciones de la herramienta PenTBox. Se selecciona la opción 2-Network Tools

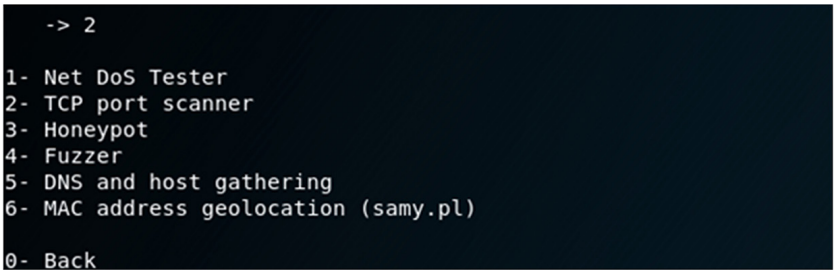

Figura 4. PenTBox (2-Network Tools). Aquí se seleccionó la opción tres (3-Honeypot) para crear el señuelo Wi-Fi

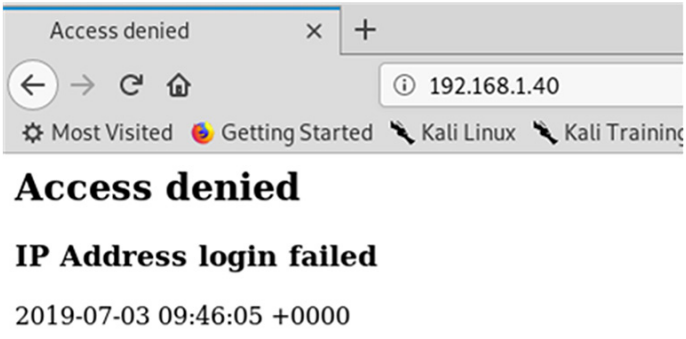

Figura 5. Mensaje de alerta obtenido al ingresar a la dirección IP del honeypot creado con la herramienta PenTBox

En la figura 6, se muestra el modelo conceptual del procedimiento de comunicación con RF. Primero, se utiliza el simulador DJI para extraer datos de comunicación reales del dron DJI Matrice 100. Luego, se carga el archivo en un microcontralador de prototipado Raspberry Pi 3B+, y mediante un algoritmo en Python, se lee el archivo y se transmiten los datos, se modifica la estampa de tiempo, de manera que se emita una real, para evitar que el atacante sospeche que los mensajes son falsos. Para probar el señuelo, se utilizó otro microcontrolador donde fue simulado el atacante, se recibió la información, se verificó que la trama se comunica correctamente y, por último, se enviaron comandos falsos desde el atacante, los cuales hacen que el dron virtual active un sistema de alerta.

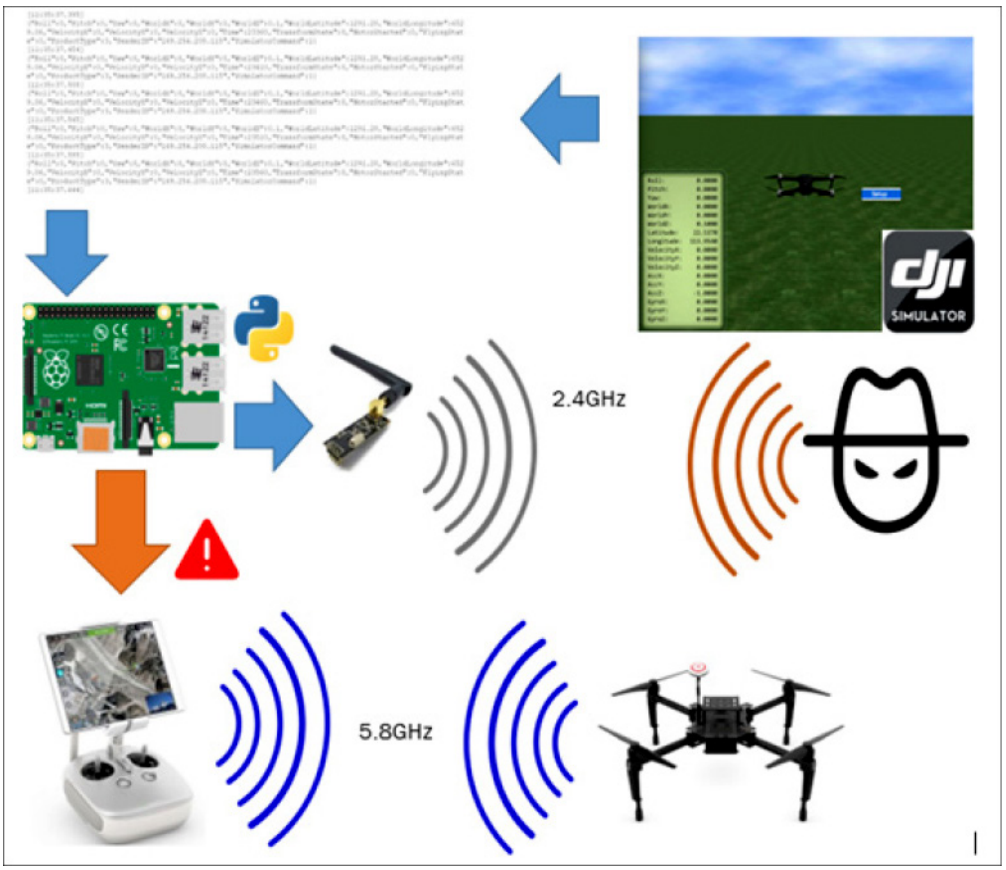

Figura 6. Modelo conceptual del procedimiento de comunicación con radiofrecuencia CyberDrone

Para lograr engañar al atacante, es necesario que el dispositivo de señuelo cuente con mensajes UDP similares al dispositivo real. Por tanto, se utiliza la herramienta DJI Simulator conectada al dron real, por medio de la cual se realiza una ruta simulada,

que permite almacenar la información simulada de la ruta y sus respectivos mensajes UDP en un archivo de texto. A fin de extraer la información, se conecta el dron al PC y se ejecuta la herramienta DJI Simulator (figura 7). Se debe encender el dron al igual que el control remoto y, luego, es necesario ingresar en la pestaña de configuración de la herramienta. Aquí se verifica que la herramienta de simulación detectó el dron. Hecho esto, se selecciona la opción UDP Broadcast y se inicia la simulación. Luego de iniciar la simulación, es necesario ingresar en las opciones de configuración UI. Una vez en la ventana, se activan las opciones para mostrar y guardar la ruta, y se selecciona el directorio donde se desea almacenar los datos de la ruta simulada.

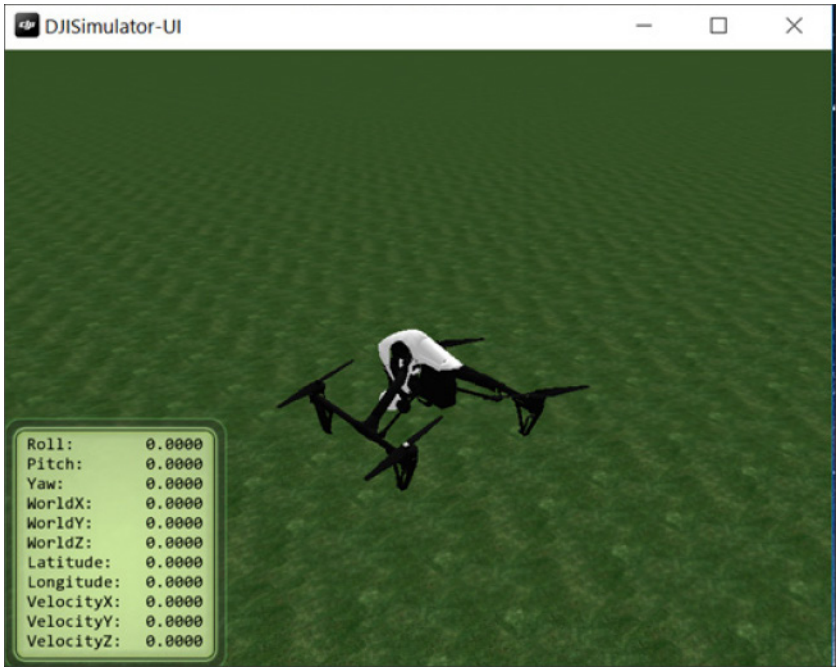

Figura 7. Herramienta de simulación de DJI para elaborar rutas de prueba. En la esquina inferior izquierda, se puede ver el reporte de las coordenadas actuales del dron

Para iniciar la simulación, se utiliza el control del Matrice 100, y se llevan ambos *joysticks* hacia los extremos inferiores externos. Una vez despegue el dron en la simulación, puede pilotearse y crear los datos de la ruta simulada. Luego de realizar un recorrido con el dron en la herramienta, y de aterrizarlo satisfactoriamente, es posible acceder a los archivos derivados de la simulación. La simulación arroja tres tipos de archivos: el primero es un archivo de *log* de los eventos del dron, el segundo es un archivo que muestra la ruta realizada por el dron y el tercero es un archivo con los mensajes UDP transmitidos por el dron. En la figura 8, se observa el archivo de

simulación donde se registraron las coordenadas de la trayectoria realizada por el dron. El archivo muestra la estampa de tiempo y las coordenadas x, y, z.

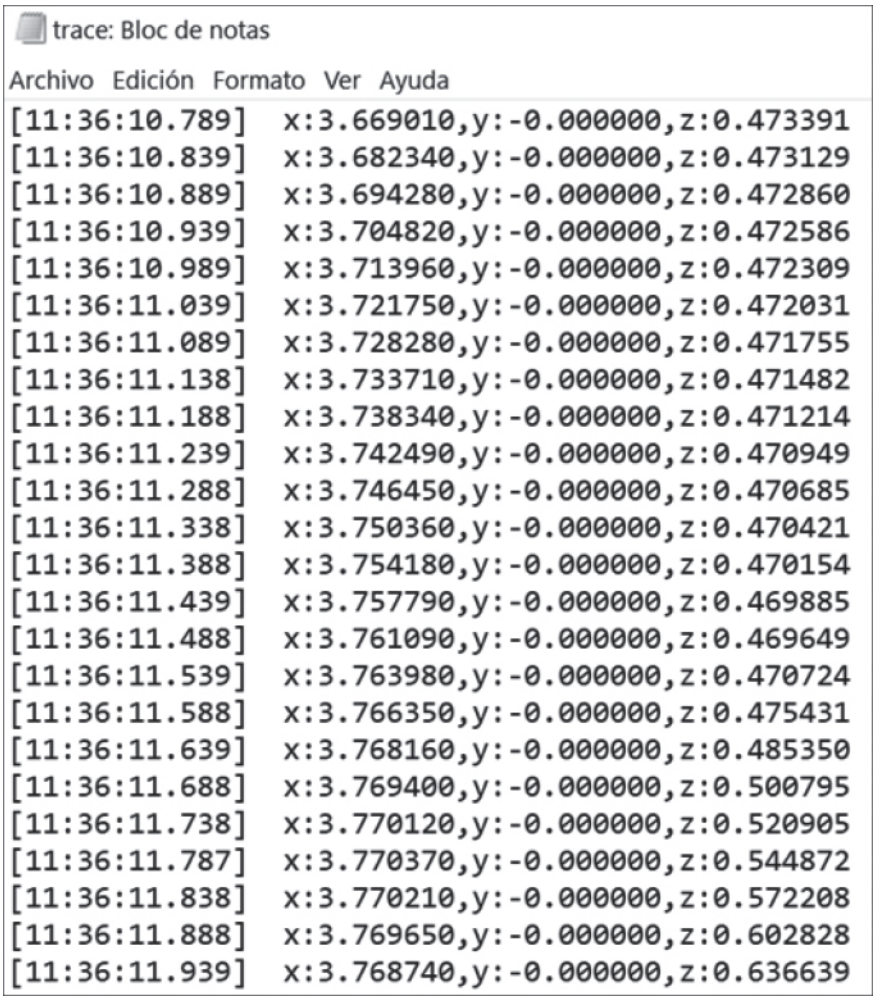

Figura 8. Archivo que muestra el registro de las coordenadas de la ruta simulada en la herramienta de DJI

El CyberDrone será simulado utilizando una Raspberry Pi a efectos de prueba y prototipado, a la que se le agrega un módulo embebido de RF de 433 MHz. A pesar de que el dron real utiliza una frecuencia de 5,8 GHz, el objetivo es utilizar a propósito una banda de frecuencia común, para que el atacante encuentre fácilmente las señales transmitidas por el CyberDrone. Utilizando librerías de Python 3, se logra transmitir los mensajes UDP simulados y reemplazar la estampa de tiempo por una real en el momento de la transmisión. Por otro lado, en el algoritmo de recepción de señales de RF del dron, se configura de tal forma que, al obtener un mensaje de confirmación (a

ACK) de lectura o un comando de cualquier fuente, el dispositivo genere automáticamente una alarma que advierte que se ha encontrado un agente no autorizado en el sistema que intenta acceder a las señales de RF de los drones.

En tercer lugar, se propone el despliegue del procedimiento de GPS Spoofing. Para el despliegue de este procedimiento, se usó el equipo Hackrf One. Este equipo es un SDR (por sus siglas en inglés), o radio definido por *software*, que también puede ser descrito como un sistema de radiocomunicaciones donde gran parte de los componentes son implementados usando *software* en lugar de *hardware*, para lo cual emplea un dispositivo embebido que trata la información y la transmite a un computador.

Este dispositivo permite capturar señales de RF en una banda entre 1 MHz y 6 GHz. Según la antena que se conecte al dispositivo, es posible procesar estas señales por medio de *software* y a su vez replicar (transmitir) estas señales en el mismo rango de frecuencias con las respectivas modificaciones. La principal ventaja de este tipo de sistema es el uso de un microprocesador multipropósito para el procesamiento de las señales, lo que reduce la complejidad del sistema al no ser necesaria la implementación de *hardware* de bloque completo y, además, ofrece la flexibilidad del uso de múltiples configuraciones.

El Hackrf One es una plataforma de *hardware* libre que puede ser usada como un periférico vía USB o programada para operar de manera autónoma. Este dispositivo es un transceptor con capacidad de operación *half duplex*. Tiene un rango de operación de frecuencia desde 1 MHz hasta 6 GHz, lo que le da una gran flexibilidad, potencia y aplicabilidad a la hora de realizar cualquier envío o recepción de información en un gran rango de frecuencias comerciales de uso diario. Tiene una capacidad de muestreo de hasta 20 millones de muestras por segundo y logra alcanzar 21,5 millones de muestras en función del tipo controlador USB 2.0 HS (*high-speed*) que incluya el computador al que se conecta.

La propuesta de implementación de esta tecnología en el proyecto CyberDrone se orientó inicialmente hacia la realización de un ejercicio de suplantación de señal de GPS o, como se conoce en el mundo de la seguridad digital, un GPS Spoofing. Con la suplantación de GPS, se intenta engañar a un receptor GPS mediante la retransmisión de una señal falsa desde la superficie, que hace que todos los navegadores o dispositivos que usen señal GPS muestren una ubicación errónea [19]. La suplantación de GPS actualmente se usa para secuestrar UAV, lo que representa un riesgo inminente o una oportunidad de defensa. Para realizar una suplantación de GPS usando el Hackrf One, se requiere que este dispositivo haga llegar la señal que enviaría normalmente un satélite. Esta señal es una señal de radio continua que envía el código del satélite y el tiempo preciso de transmisión. Los dispositivos que reciben esta señal analizan el tiempo de recepción y con esto calculan la distancia respecto del origen de la señal.

Con varias de estas señales y unos cálculos matemáticos rápidos, el dispositivo receptor puede determinar su ubicación precisa en relación con los satélites.

El Hackrf One sería el transmisor de radio que emite una señal de GPS falsa pero técnicamente sólida, que anule la señal de los satélites y cause que todos los receptores cercanos calculen las coordenadas incorrectas. Para visualizar las alertas de los eventos, y poder consultar el listado de registros almacenados en el contrato inteligente de la cadena de bloques de Ethereum, se diseñó una interfaz gráfica, por medio de la cual un supervisor podrá ver los reportes en tiempo real.

En la figura 9, se observa la pantalla inicial de la plataforma, donde se visualizan algunas de las variables principales relacionadas con el monitoreo de los señuelos. También se observa el listado de los intentos de intrusión detectados por el CyberDrone. Una vez desplegados el *honeypot* wifi y el *honeypot* de RF, se procede con la configuración de servicios API (por sus siglas en inglés), los cuales son consultados mediante diferentes algoritmos configurados en la plataforma de visualización. Una vez que la plataforma recibe reporte de actividad en alguno de los señuelos por medio de los servicios API, genera una señal de alerta en el momento en el cual un intruso intenta comunicarse con alguno de los señuelos. Una vez detectado el intruso, la plataforma reporta el incidente realizando un registro con los detalles del evento en una cadena de bloques mediante un contrato inteligente, y así garantizar la disponibilidad, integridad y confidencialidad de los eventos registrados en la plataforma.

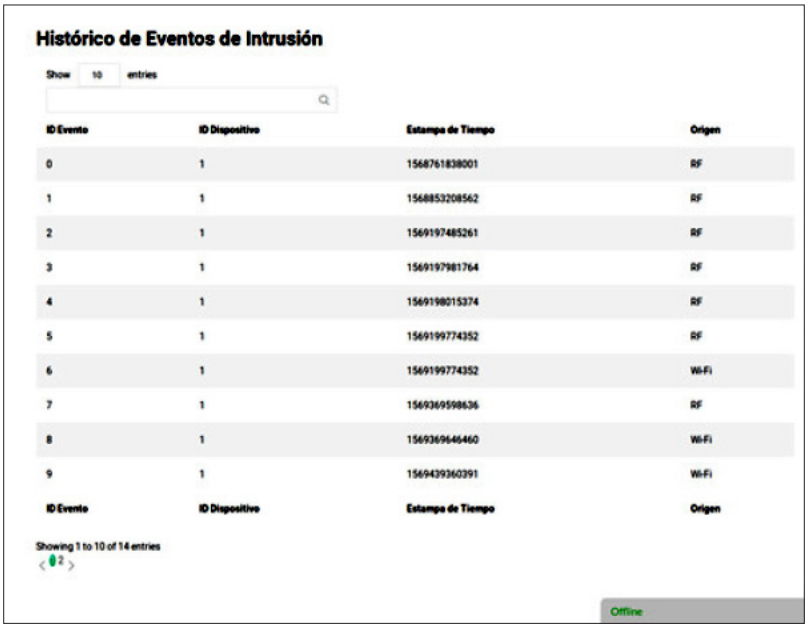

Figura 9. Interfaz gráfica de la plataforma web para el monitoreo de los honeypot activos y el registro de los intentos de intrusión. Estos eventos se almacenan en una blockchain privada creada en Ethereum

Antes se ilustró el modelo conceptual del sistema *cyber deception* (figura 1), donde se observa el flujo de información entre los sistemas *honeypots* y la plataforma web. Una vez que los señuelos han sido desplegados satisfactoriamente según los procedimientos descritos y un atacante intenta acceder a ellos, las variables de estado configuradas en la API cambian de 0 a 1. La plataforma web corre algoritmos JavaScript de consulta a las API periódicamente. Al recibir alguno de los cambios es posible identificar el *honeypot* bajo ataque. Y al conectar un dispositivo Hackrf y comunicarlo con la plataforma web, es posible realizar acciones de seguridad ofensiva y permitir a la estación de control detectar y controlar drones enemigos mediante GPS Spoofing.

4. CONCLUSIONES

La ciberseguridad en los UAV es un campo de investigación en auge y que está adquiriendo mayor relevancia, debido a la masiva implementación de soluciones de monitoreo y vigilancia basadas en drones y tecnologías similares. Las empresas de energía se están beneficiando de la flexibilidad de los UAV para recolectar datos de la infraestructura de sus sistemas eléctricos. Esta situación los convierte en blancos atractivos para atacantes de las comunicaciones entre los drones y las estaciones de control, por lo que desarrollar escudos para protegerse se convierte en una necesidad.

Se propusieron tres procedimientos de ciberseguridad basados en la tecnología *cyber deception*. El primero, basado en las señales wifi, crea un señuelo deliberadamente fácil de atacar, el cual busca identificar atacantes en estas redes. El segundo, basado en comunicaciones RF, emite las tramas UDP de las coordenadas de un dron comercial, para emular la presencia de un equipo y que los atacantes se sientan atraídos para intentar acceder a su control. El último procedimiento es una aproximación al GPS Spoofing, que por medio de un dispositivo SDR intenta desubicar a un dron atacante en un perímetro de seguridad, mediante el envío de señales de ubicación confusas.

Para el correcto desempeño de los señuelos y el funcionamiento de las API, fueron desarrollados diversos algoritmos en distintas tecnologías complementarias. El señuelo wifi utiliza el sistema operativo Kali Linux, que cuenta con la herramienta PenTBox, por medio de la cual se despliega el señuelo y permite configurar un mensaje de alerta o una interfaz falsa que simule la interfaz de administración de un dron. Además, se desarrollaron diversos algoritmos que hacen posible simular una comunicación bidireccional, transmitir datos a partir de los archivos de ruta extraídos de un dron real y recibir mensajes de comunicación por parte del otro extremo.

Este tema de investigación debe ser profundizado para conseguir implementar soluciones comerciales para las empresas que están usando de manera intensiva UAV

o drones en sus actividades de inspección de infraestructura crítica o, incluso, para aquellas que quieren proteger sus perímetros físicos de posibles drones intrusos o atacantes.

REFERENCIAS

[1] A. Constantin y R.-N. Dinculescu, "UAV development and impact in the power system", en *2019 8th International Conference on Modern Power Systems (MPS)*, 2019, pp. 1-5. Doi: 10.1109/MPS.2019.8759745

[2] Power Engineering International (23 febr. 2018), *How drones are playing a role in the power and utility sector* [En línea]. Disponible en: https://www.powerengineeringint.com/gas-oil-fired/om/how-drones-are-playing-a-role-in-the-power-and-utility-sector/

[3] N. Ellis, "Inspection of power transmission lines using UAVs", Tesis de grado, University of Southern Queensland, Australia, 2013 [En línea]. Disponible en: https://eprints.usq.edu.au/24719/1/Ellis, N._2013.pdf

[4] D. Long, P. J. Rehm y S. Ferguson, "Benefits and challenges of using unmanned aerial systems in the monitoring of electrical distribution systems", *Electr. J.*, vol. 31, no. 2, pp. 26-32, mzo. 2018. https://doi.org/10.1016/j.tej.2018.02.004

[5] M. Manzur, A. Wiśniewski y J. McMillan (oct. 2017), *Clarity from above: leveraging drone technologies to secure utilities systems* [En línea]. Disponible en: https://www.pwc.com/hu/hu/kiadvanyok/assets/pdf/clarity-from-above-leveraging-drone-technologies-to-secure-utilities-systems-pwc.pdf

[6] C. G. L. Krishna y R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles", en *2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*, 2017, pp. 194-199. Doi: 10.1109/SSRR.2017.8088163

[7] H. Benkraouda, E. Barka y K. Shuaib, "Cyber-attacks on the data communication of drones monitoring critical infrastructure", *Comput. Sci. Inf. Technol.*, vol. 8, no. 17, pp. 83-93, 2018. Doi : 10.5121/csit.2018.81708

[8] K. Wesson y T. Humphreys, "Hacking drones", *Sci. Am.*, vol. 309, no. 5, pp. 54-59, nov. 2013. Doi: 10.1038/scientificamerican1113-54

[9] K. Hartmann y K. Giles, "UAV exploitation: a new domain for cyber power", en *2016 8th International Conference on Cyber Conflict (CyCon)*, 2016, pp. 205-221. Doi: 10.1109/CYCON.2016.7529436

[10] N. Falliere, L. O. Murchu y E. Chien, "W32. stuxnet dossier", *White paper, Symantec Corp., Security Response*, vol. 5, no. 6, p. 29, 2011 [En línea]. Disponible en: https://paxor.com/hh/stuxnet/Symantec-Stuxnet-Update-Feb-2011.pdf

[11] A. Cherepanov y R. Lipovsky (2 jun. 2017), *Industroyer: biggest threat to industrial control systems since Stuxnet* [En línea]. Disponible en: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

[12] G. Liang, S. R. Weller, J. Zhao, F. Luo y Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks", *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317-3318, jul. 2017. Doi: 10.1109/TPWRS.2016.2631891

[13] S. Jajodia, V. S. Subrahmanian, V. Swarup y C. Wang, *Cyber deception: building the scientific foundation*. Cham: Springer, 2016.

[14] C.-Y. J. Chiang, Y. M. Gottlieb, S. J. Sugrim, R. Chadha, C. Serban, A. Poylisher, L. M. Marvel y J. Santos, "ACyDS: An adaptive cyber deception system", en *MILCOM 2016 - 2016 IEEE Military Communications Conference*, 2016, pp. 800-805. https://doi.org/10.1109/MILCOM.2016.7795427

[15] C. De Faveri, A. Moreira y V. Amaral, "Multi-paradigm deception modeling for cyber defense", *J. Syst. Softw.*, vol. 141, pp. 32-51, jul. 2018. https://doi.org/10.1016/j.jss.2018.03.031

[16] V. E. Urias, W. M. S. Stout, J. Luc-Watson, C. Grim, L. Liebrock y M. Merza, "Technologies to enable cyber deception", en *2017 International Carnahan Conference on Security Technology (ICCST)*, 2017, pp. 1-6. Doi: 10.1109/CCST.2017.8167793

[17] V. Zabatta Galgano, "Primeras reflexiones sobre un modelo general de desarrollo tecnológico", *Investig. y Postgrado*, vol. 23, no. 2, pp. 433-446, ag. 2008 [En línea]. Disponible en: http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1316-00872008000200016

[18] J. O'Malley, "Pirates of the skies", *Eng. Technol.*, vol. 12, no. 3, pp. 32-35, abr. 2017. Doi: 10.1049/et.2017.0302

[19] T. E. Hay (1 ag. 2016), *Determining electronic and cyber attack risk level for unmanned aircraft in a contested environment* [En línea]. Disponible en: https://apps.dtic.mil/sti/citations/AD1040702.