INTERNET DE LOS AUTOMÓVILES: ANÁLISIS BREVE DE LA SEGURIDAD

INTERNET OF VEHICLES: A BRIEF ANALYSIS REGARDING ITS COMMUNICATIONS SECURITY

David Israel Castillo Rodríguez
Instituto Politécnico Nacional, ESCOM, México
dcastillor1301@alumno.ipn.mx

Rubén Vázquez de Jesús
Universidad del Valle de México, Campus Querétaro, México
rubvazquezdj@gmail.com

Leonardo Palacios Luengas
Universidad Autónoma Metropolitana, Unidad Iztapalapa, México
lpl@xanum.uam.mx

Rubén Vázquez Medina
Instituto Politécnico Nacional, CICATA Unidad Querétaro, México
ruvazquez@ipn.mx

Recepción: 6/diciembre/2022 **Aceptación:** 26/diciembre/2022

Resumen

La Internet de las Cosas (IoT) ha despertado interés en aplicaciones de alta interconectividad, lo que ha traído retos que podrían superarse si se atiende la calidad en el servicio y la seguridad informática. En este trabajo se identifican y analizan ataques que pudieran ocurrir en un contexto de la Internet de los Vehículos (IoV: Internet of Vehicles). Para ello, se implementa un montaje experimental que permite analizar y atender cuatro ataques básicos: manipulación de nodos, privación del sueño, análisis de tráfico y denegación del servicio. Los primeros dos se consideraron por la facilidad con la que alguien no autorizado puede irrumpir un automóvil. El tercero se consideró por ser de los más comunes. Finalmente, el cuarto se consideró porque atenta contra la infraestructura IoV. Este trabajo muestra cómo abordar los problemas de seguridad básicos en entornos IoV, los cuales pueden derivar en ataques más complejos.

Palabras clave: Internet de los automóviles, protocolos de comunicación, seguridad.

Abstract

The Internet of Things (IoT) has raised a growing interest in various high interconnectivity applications, which poses challenges that could be surpassed if the service quality and informatics security are attended. In this paper, attacks against the Internet of Vehicles (IoV) are identified and analysed. For such purpose, an experimental setup is used to address and analyse four basic attacks: nodes manipulation, sleep deprivation attack, traffic analysis and denial of service. The first two attacks were considered due to the ease to interrupt the vehicle functionality by an unauthorized individual. The third one was considered since it is the one of the most common within the Internet. Finally, the fourth one was considered since it is the most used against the IoV infrastructure. Therefore, this paper shows how to address the problems regarding the informatics security of IoV environments with the possibility of escalating to more sophisticated attacks.

Keywords: *Communication protocols, internet of vehicles, security.*

1. Introducción

El término Internet de las Cosas (IoT: Internet of Things) data del año 1999, y se atribuye al trabajo realizado en el Instituto de Tecnología de Massachusetts cuando sentó las bases para la estandarización de la tecnología de identificación por radiofrecuencia (RFID: Radio-Frequency Identification). Desde entonces, la IoT ha continuado desarrollándose y ampliándose más allá de la tecnología RFID. Aunque se han propuesto diversas definiciones para la IoT, la Unión Internacional de Telecomunicaciones, la define como *"una infraestructura global para la Sociedad de la Información, que provee de servicios avanzados para interconectar (física y virtualmente) cosas basadas en tecnologías, existentes y en evolución, interoperables de información y comunicación"* [Wortmann, 2015]. Otras definiciones dan mayor énfasis a los dispositivos que pueden conectarse a la Internet, pero se enfocan en los protocolos de Internet y las tecnologías de red.

De forma general, se puede decir que las aplicaciones de IoT tienen tres aspectos en común: i) la recolección de información proveniente de un conjunto de sensores y otras fuentes, ii) la interpretación de la información recolectada y iii) la toma de

decisiones que mejoren el desempeño de un proceso o sistema. La IoT permite automatizar sistemas y mejorar su comportamiento, permitiendo disponer de una cantidad de información sin precedentes para la toma de decisiones [Davies, 2020]. Los sistemas IoT han tenido un desarrollo importante en seguridad, privacidad, conectividad, protocolos y arquitectura, entre otros. No obstante, aún existen retos que deben atenderse [Rehman, 2017], [Farhan, 2017], [Asghari, 2019]. Algunos de los retos por atender se encuentran en las siguientes cinco temáticas:

- **Uso de estándares:** Se requieren debido a que se trata de sistemas con dispositivos heterogéneos. A pesar de que el Grupo de Trabajo de Ingeniería de Internet (IETF: Internet Engineering Task Force) y el Instituto Europeo de Normas de Telecomunicaciones (ETSI: European Telecommunications Standards Institute) trabaja para desarrollar estándares, aún no se tiene un estándar definitivo [Rehman, 2017].
- **Conectividad:** Es un servicio que se requiere para cualquier dispositivo IoT reconocido y requiere de la definición de un identificador único para cada dispositivo autenticado.
- **Arquitectura:** Permite la interoperabilidad entre dispositivos, simplifica el desarrollo y está asociada con estándares que facilitan su implementación.
- **Seguridad:** Generalmente se considera un servicio que otorga confidencialidad, disponibilidad y autenticación, pero se debe tener en cuenta que en sistemas IoT, los dispositivos tienen menor capacidad de procesamiento y sistemas de suministro de energía de baja capacidad, por lo que requieren de algoritmos ligeros de cifrado.
- **Requerimientos energéticos:** Debido a que en muchos casos los dispositivos IoT son portátiles, se consideran de recursos energéticos, capacidad y procesamientos limitados, por ello deben considerarse mecanismos de gestión de energía.

Un elemento clave de los sistemas IoT es la capacidad que deben tener para comunicar y conectar dispositivos autónomos, inteligentes y heterogéneos [Sikimić, 2020]. En este contexto, se debe tener en cuenta que, por consumo energético,

alcance y seguridad, podría no ser posible aplicar las tecnologías comunes de comunicación como WiFi y Bluetooth. Por ello, de acuerdo con [Sikimić, 2020], elegir la tecnología correcta podría generar un reto adicional en el diseño de sistemas IoT, en el que deben considerarse los siguientes requerimientos:

- **Rango de alcance:** En los sistemas IoT la comunicación puede ser de corto, mediano o largo alcance.
- **Ancho de banda:** Dependiendo del entorno de aplicación, en una red de datos, los dispositivos IoT podrían demandar más tiempo o mayor ancho de banda en el canal de comunicaciones. Esta condición afectaría rango de alcance en la comunicación, el consumo energético y consecuentemente la rentabilidad del sistema completo.
- **Confiabilidad:** Es una condición importante para la mayoría de las aplicaciones, y debe tenerse en cuenta que fortalecer la confiabilidad impacta significativamente en la demanda de ancho de banda y costo de operación-mantenimiento del sistema.
- **Eficiencia energética:** Debido a que los dispositivos IoT son, en su mayoría, autónomos, es de vital importancia optimizar el consumo energético.

Los protocolos de comunicación toman relevancia en sistemas heterogéneos, puesto que definen un marco de trabajo universal que permite a los dispositivos coexistir. También contribuyen en el rendimiento de los sistemas IoT y deben ser ligeros y eficaces. En este sentido, existen algunos protocolos especialmente diseñados para sistemas IoT. Entre los más comunes se pueden mencionar los siguientes [Naik, 2017]: MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol) y AMQP (Advanced Message Queuing Protocol). A pesar de no ser un protocolo diseñado específicamente para IoT, HTTP (Hypertext Transfer Protocol) es un protocolo que se ha tenido que adaptar a partir de sus versiones de carga ligera para dispositivos móviles.

En congruencia con lo planteado por [Andrea, 2015], un sistema IoT puede ser atacado considerando los dos escenarios siguientes:

I. Ataques físicos:

- Manipulación de nodos: El atacante puede causar daños a un nodo sensor al reemplazar físicamente el nodo completo o parte de él, o al interrogar electrónicamente a los nodos para obtener acceso y alterar la información sensible, como claves criptográficas o tablas de enrutamiento (si las hay).
- Inyección de nodos maliciosos: El atacante puede, físicamente, desplegar un nuevo nodo malicioso entre dos o más nodos del sistema IoT, logrando controlar tanto el flujo de datos, desde y hacia los nodos, así como su operación. Este es conocido como el ataque del hombre en el medio.
- Ingeniería social: El atacante manipula a los usuarios del sistema IoT para obtener información privada o realizar algunas acciones que podrían servir a sus propósitos.
- Ataque de privación del sueño: La mayoría de los nodos en el sistema IoT se alimentan por baterías y están programados para ejecutar rutinas de reposo que les permite extender la vida de la batería. Este ataque mantiene despierto al nodo, lo cual resulta en un mayor consumo de energía, provocando que el nodo se apague**.**

II. Ataques a la red

- Ataques de análisis de tráfico: Un atacante puede captar información sensible que esté circulando en el medio común de comunicaciones. Esto se logra utilizando aplicaciones de sniffing.
- Ataque de sumidero: El atacante atrae todo el tráfico de una red, creando un sumidero metafórico. Este tipo de ataque viola la confidencialidad de los datos. Además, deniega el servicio a la red a través del desvío de todos los paquetes en lugar de direccionarlos hacia su destino.
- Ataque de hombre en el medio: El atacante consigue interferir entre dos nodos, accediendo a datos restringidos, violando la privacidad de ambos nodos, espiando y controlando la comunicación entre ellos.
- Denegación de servicio: Un atacante puede inyectar en una red IoT más tráfico del que puede manejar, resultando en un ataque exitoso de denegación de servicio.

Por otro lado, la Internet de los vehículos (IoV: Internet of Vehicles) se define como una plataforma que permite el intercambio de información entre los automóviles y su medio circundante, usando para ello diferentes medios de comunicación [Contreras-Castillo, 2018]. Como resultado de la integración con la tecnología IoT, los sistemas IoV permiten crear redes integradas, como las redes vehiculares adhoc (VANET: Vehicular Adhoc Networks) que permiten el soporte a la conducción inteligente, el control inteligente de vehículos y los servicios de información dinámica, entre otros; todo ello para mejorar la seguridad y eficiencia vial. En este tipo de redes IoV, los vehículos se conectan a la Internet a través de puertas de enlace colocadas a lo largo de las vías vehiculares, lo que permite a los conductores conectarse a los servicios comunes de la Internet y aplicaciones IoV específicas [Sandonis, 2016]. La arquitectura de red heterogénea de la IoV incluye cinco tipos de comunicación vehicular, dentro de los que se encuentran los siguientes: V2V (Vehicle to Vehicle). - Comunicación vehículo a vehículo, V2R (Vehicle to Roadside Unit). - Comunicación vehículo a unidad de apoyo vial, V2I (Vehicle to Infraestructure). - Comunicación vehículo a infraestructura, V2P (Vehicle to Personal devices). - Comunicación vehículo a dispositivos personales o redes móviles y V2S (Vehicule-to-Sensors). - Comunicación vehículo a sensores.

En los sistemas IoV, un automóvil es un dispositivo IoT móvil que se comunica con el sistema y otros automóviles [Contreras-Castillo, 2018]. Los sistemas IoV traen consigo retos y requerimientos similares a los que se han descrito de manera general para los sistemas IoT, tales como son: la arquitectura, la conectividad y la seguridad. Pero, específicamente para sistemas IoV, se pueden mencionar los trabajos reportados por [Sun, 2017], [Sakiz, 2017] y se refieren a los virus y gusanos informáticos, los caballos de Troya y el software espía (*spyware*).

En cuanto a las características generales que se deben observar en un sistema IoV se pueden mencionar los siguientes:

- **Distribución no uniforme de los automóviles:** La distribución de vehículos se ve afectada por múltiples factores, incluyendo la topología de la red de vías, localización geográfica y hábitos de manejo, entre otros. Por ello, las subredes IoV también son dinámicos, ya que un vehículo

podría formar parte de una subred IoV y más tarde de otra, dependiendo de su localización.

- **Topologías dinámicas:** Debido a que un automóvil tiene alta movilidad y cortos ciclos de conexión, la topología de un sistema IoV es intrínsecamente dinámica, por lo tanto, difíciles de predecir y modelar.
- **Alta movilidad de los automóviles:** Esta condición genera múltiples conexiones y desconexiones de los automóviles a las subredes IoV.
- **Limitaciones en los tiempos de retardo en la comunicación:** Para evitar consecuencias catastróficas y por cuestiones de seguridad, las redes IoV deben operar en tiempo real, esto evitaría incidentes/accidentes viales o el retraso en la ejecución de operaciones de rescate o emergencia.

El diseño de una arquitectura estratificada para una red universal compuesta de redes heterogéneas resulta una tarea desafiante. Se debe identificar y agrupar funcionalidades similares. Esta red universal se debe considerar interoperable, escalable, confiable y modular. Debería permitir que se interconecten múltiples vehículos y dispositivos heterogéneos. A continuación, se describe la arquitectura propuesta en cinco capas por [Kaiwartya, 2016] para los sistemas IoV:

- **Capa de percepción:** Se representa por los diferentes tipos de sensores y actuadores en vehículos, teléfonos inteligentes y otros dispositivos personales en el sistema. La mayor dificultad de esta capa es la recolección y diferenciación eficiente, en términos de costo y energía, de la información capturada, la cual incluye posición, dirección, velocidad, aceleración, densidad de vehículos en la vía y condiciones meteorológicas, entre otras.
- **Capa de coordinación:** Se representa por una red virtual universal que coordina las redes heterogéneas involucradas, a través de las cuales se envía, de forma segura, la información recolectada por la capa de percepción y se envía bajo un formato unificado hacia capas superiores para su procesamiento. Una de las principales dificultades en esta capa reside en la interoperabilidad y cooperación entre los diferentes tipos de redes, como consecuencia de la falta de estándares.

- **Capa de inteligencia artificial (IA):** Se considera el cerebro de la IoV, ya que es responsable del almacenamiento, procesamiento y análisis de la información recibida de capas inferiores. Permite un proceso de toma de decisiones a partir de un análisis crítico que puede usar cómputo en la nube, análisis de *big data* y sistemas expertos.
- **Capa de aplicación:** Es responsable de proveer servicios inteligentes a los usuarios finales, basados en la información que recibe de la capa de IA.
- **Capa de negocios:** Es la responsable de proveer estrategias para el desarrollo de modelos de negocio basados en los datos de utilización de aplicaciones y el análisis estadístico de los datos. También considera otras responsabilidades como la toma de decisiones relacionada con la inversión económica y utilización de recursos, el presupuesto general para operación, la fijación de precios por uso de aplicaciones y la administración de datos.

Según el modelo STRIDE de amenazas presentado por [Sun, 2015], las amenazas, ataques y seguridad de la información pueden clasificarse en las siguientes seis categorías: suplantación de identidad, manipulación de datos, repudio, revelación de información, denegación de servicio y elevación de privilegios. La afectación a la seguridad de un sistema IoV podría evitarle proveer sus servicios, lo que podría causar accidentes por causa de la topología dinámica, limitaciones de ancho de banda, distribución no uniforme de los nodos y el alcance de la red, entre otras. A continuación, se describen algunos ataques en la IoV según se definen en [Sun, 2015], [Sun, 2017] y [Sharma, 2018].

Ataques a la autenticación

De este tipo de ataques se pueden describir esencialmente los tres siguientes:

- **Ataque de agujero de gusano:** Con este ataque se pretende modificar la topología de la red para colectar y/o modificar grandes cantidades de tráfico en la red. Este ataque requiere de dos o más nodos comprometidos, los cuales provocan que los protocolos de enrutamiento prefieran la conexión entre ellos como la mejor ruta, en lugar de rutas cercanas. Como resultado,

la información enviada a los nodos comprometidos podría no ser transmitida al resto de la red.

- **Ataque Sybil:** En las redes inalámbricas, un nodo con múltiples identificaciones puede dañar el sistema controlando la mayoría de sus nodos. Debido a que en la IoV los vehículos tienen alta movilidad y acceden a las redes en tiempo cortos, los nodos Sybil pueden generar un ataque efectivo.
- **Engaño GPS:** El engaño GPS puede proveer a un nodo de información falsa acerca de su localización y velocidad. En un sistema IoV, la información GPS es importante para evitar una localización imprecisa que cause una operación falsa o de fraude.

Ataques a la disponibilidad

Se refiere a los ataques de seguridad física, denegación de servicio e interferencia en el canal. Este tipo de ataques atentan contra la integridad física de los sistemas, o explotan las limitaciones de ancho de banda con la intención de colapsar a un sistema IoV.

La mayoría de los componentes significativos de la IoV se encuentran expuestos al exterior, con poco o nula protección, resultando en una significativa facilidad de ser interferidos, controlados o destruidos.

- **Ataques a la secrecía:** El atacante intercepta información para comprometer un vehículo o una unidad de apoyo vial (RSU: Road Side Units), de modo que podría acceder a recursos sensibles para usuarios válidos.
- **Ataques de enrutamiento:** Con ellos se busca el espionaje, así como el enmascaramiento y la modificación de la ruta. Son relativamente complejos a causa de las limitaciones de ancho de banda y la movilidad vehicular, ocasionando vulnerabilidades en el sistema.
- **Denegación de servicio:** El atacante busca atentar contra la red IoT para deshabilitar los accesos establecidas por las RSU, o bien, detener sus comunicaciones, lo que ocasionaría consecuencias desastrosas.
- **Ataques a la integridad física:** Son muy comunes; y podrían permitir el establecimiento de una conexión directa con los componentes del vehículo

generando un acceso ilegítimo al sistema de diagnóstico utilizado para mantenimiento o al firmware del sistema.

Ataques a la autenticidad de los datos

Este tipo de ataques pueden clasificarse en cuatro tipos: ataque de repetición, ataque de camuflaje, ataque de fabricación y manipulación con mensajes y ataque de ilusión. Dado que la IoV debe ser abierta, el flujo de datos puede, fácilmente, ser capturado, modificado y enviado, especialmente en el enrutamiento y en las comunicaciones inalámbricas.

2. Métodos

Con el propósito de proseguir hacia una propuesta de mejora de seguridad para las comunicaciones IoV, en este trabajo se propone un montaje experimental llamado Sistema IoT-WiFi-ODB-II, el cual se aplica en un entorno IoV. Este sistema incluye una tarjeta de desarrollo Arduino UNO WiFi Rev. 2 sobre la cual se implementa el protocolo de comunicación HTTP. Esta tarjeta Arduino se seleccionó dada su conocida facilidad para el desarrollo de proyectos, así como la cantidad de sensores y accesorios disponibles para su utilización en proyectos de electrónica, de IoT e incluso industriales. Además, esta tarjeta incluye por defecto un módulo de comunicación WiFi NINA W102, del fabricante U-blox, con la cual es posible conectarse a una red WiFi de forma segura a través de una conexión cifrada. En este caso, el dispositivo IoT considerado es un automóvil; por ello, el Sistema IoT-WiFi-ODB-II incluye una interfaz OBD-II para lograr la comunicación con la Unidad de Control del Motor (ECU: Engine Control Unit), utilizando el protocolo CAN. Para implementar el protocolo CAN se usa el módulo de comunicación CAN-BUS Shield V2.0 (en adelante, CAN-Bus), especialmente diseñado para las tarjetas de desarrollo Arduino UNO. Este módulo, a través de la Interfaz Periférica en Serie (SPI: Serial Peripheral Interface), utiliza los pines de conexión CAN-High y CAN-Low, especificados en el conector OBD-II, según el estándar SAE J1962, para establecer comunicación con la ECU del automóvil. Cabe mencionar que el conector OBD-II debe instalarse en todos los automóviles fabricados a partir de 1996, por lo

que es posible encontrarlo en cualquier automóvil puesto a la venta posterior a tal año.

En cuanto a la forma en que la tarjeta Arduino se conecta con el automóvil, se debe mencionar que se utilizó un cable de conexión que tiene en un extremo un conector macho OBD-II y en el otro extremo únicamente se toman los cables correspondientes a los pines CAN-High y CAN-Low, mismos que son conectados a la terminal de conexión del módulo CAN-Bus. Una vez que se ha realizado la conexión del puerto OBD-II del automóvil con el módulo CAN-Bus, este último se configura para el envío y recepción de paquetes, y así comenzar con el envío de peticiones a la ECU. En este proceso se utilizan identificadores definidos por el estándar OBD-II; cabe aclarar que, para el envío y recepción de peticiones, el automóvil debe estar encendido (no necesariamente con el motor arrancado) y la tarjeta Arduino con el programa para ejecutar lograr la comunicación del automóvil con la Internet. Los datos que se recolectan de la ECU del automóvil son: temperatura del anticongelante, velocidad del motor, velocidad del automóvil, nivel del depósito de combustible, temperatura ambiente. Los datos leídos a través del módulo se envían a un servicio web REST habilitado con un programa de desarrollo propio en Python y desplegado a través de la plataforma Heroku.

En la figura 1 se muestra el Sistema IoT-WiFi-ODB-II conectado a la Internet, y este incluye: automóvil, tarjeta Arduino y servicio web REST. Este sistema se usa para reproducir los cuatro ataques a la disponibilidad considerados: manipulación de nodos, privación del sueño, análisis de tráfico y denegación del servicio.

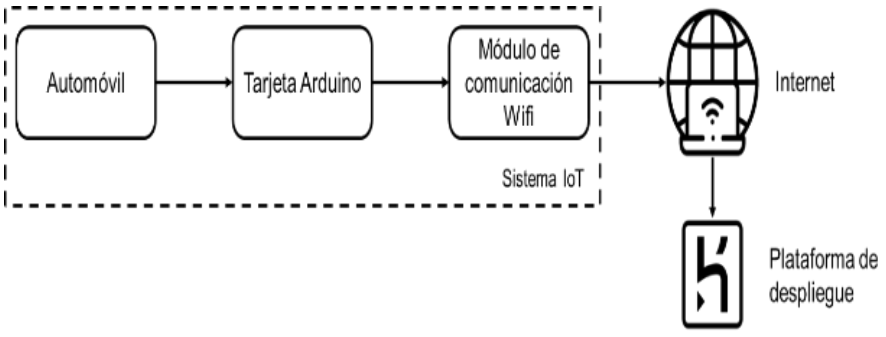

Figura 1 Diagrama a bloques del montaje experimental del sistema IoT-WiFi-ODB-II.

3. Resultados

A continuación, se describen los resultados obtenidos del análisis realizado para cada uno de los ataques considerados.

Manipulación de nodos

Es un ataque a la disponibilidad que afecta a las comunicaciones V2V, V2I, V2S, V2R y V2T. También es un ataque a la confidencialidad, ya que si se tiene acceso al sistema pudiera tener acceso a información sensible del vehículo. En este caso se plantea el hecho de que el funcionamiento de un automóvil sea ilegalmente irrumpido. Aquí se tiene como premisa que el Sistema IoT-WiFi-ODB-II del automóvil no está protegido con técnicas de seguridad física y se encuentra expuesto a la vista del perpetrador. Esta premisa es factible debido a que un automóvil comúnmente se encuentra expuesto a manipulación en una estación de servicio, un estacionamiento o lavado de autos. En ese contexto, el Sistema IoT-WiFi-ODB-II del automóvil puede ser sustraído y afectado por alguna persona no autorizada. Adicionalmente, en manos de un conocedor en electrónica y/o programación, el Sistema IoT-WiFi-ODB-II puede representar una fuente de información valiosa, ya que en la memoria se encuentran el programa principal y datos necesarios para su ejecución (parámetros de conexión para una red WiFi, credenciales de acceso al servidor web).

El ataque a la disponibilidad se puede resolver a través del aseguramiento físico del el Sistema IoT-WiFi-ODB-II. No obstante, la vulnerabilidad en la confidencialidad se puede resolver a través de la tarjeta Arduino. En este caso, el microcontrolador de la tarjeta requiere de un archivo compilado para ser ejecutado, por lo que el código legible para el ser humano no se encuentra en la memoria de la tarjeta. Así, el archivo compilado se graba en el microcontrolador, y por defecto el fabricante permite activar una opción que impide acceder al archivo grabado, aún al propio desarrollador. De esta manera, el Sistema IoT-WiFi-ODB-II propuesto evita que alguien malintencionadamente tenga el código legible, ya que cuenta con esta opción habilitada impidiendo el acceso al código fuente. Así, en caso de que el sistema sea robado o sustraído temporalmente, únicamente se tendría acceso al

archivo compilado, y el proceso de ingeniería inversa para obtener el código fuente podría ser una tarea altamente compleja de lograr.

Ataque de privación del sueño

Este es otro ataque a la disponibilidad, ya que tiene en cuenta el consumo energético como un problema para el desarrollo e implementación de aplicaciones IoT, y en particular de IoV. Así, se debe considerar que el Sistema IoT-WiFi-ODB-II propuesto ejecuta rutinas de reposo periódicas, las cuales se ejecutan para reducir el consumo de energía proveniente de la batería del automóvil. Ahora bien, considerando que la interfaz OBD-II permite obtener energía directamente de la batería del automóvil, y sabiendo que el ataque de privación del sueño tiene como objetivo evitar que un nodo IoV entre en un estado de reposo, se puede identificar un escenario en el que un atacante pudiera acceder al Sistema IoT-WiFi-ODB-II haciéndose pasar por personal autorizado para manipularlo por medio de un circuito externo para lograr su reinicio. Una alternativa para dicho circuito externo únicamente requeriría de un módulo de relevadores y un generador de pulsos de reloj, el cual podría energizarse a través de los dos pines de alimentación dispuestos en la tarjeta Arduino del Sistema IoT-WiFi-ODB-II. Así, el módulo de relevadores, con ayuda del generador de pulsos de reloj, provocará que la tarjeta esté constantemente reiniciándose. Con base en lo anterior, la tarjeta Arduino no será capaz de ejecutar las rutinas de reposo y requerirá consumir más energía, ya que estará suministrando energía a los dos módulos adicionales (módulo de relevadores y módulo generador de pulsos de reloj). Suministrar energía a ambos módulos podría ser una forma de causar daños a la tarjeta Arduino, ya que las terminales usadas para obtener suministro de energía tienen un límite de corriente máxima. Si se sobrepasa tal límite, entonces se podría dejar incomunicado a ese nodo IoT, lo que llevaría a un ataque adicional. No obstante, considerando solamente el ataque de la privación del sueño, existe la posibilidad de drenar energía innecesaria de la batería del automóvil. Sin energía suficiente, el automóvil podría quedar desprotegido y propenso a un ataque de manipulación del nodo. La efectividad de este ataque se puede reducir si el Sistema IoT-WiFi-ODB-II se asegura físicamente.

Ataque de análisis de tráfico

Es un ataque a la confidencialidad, ya que permite el espionaje e incluso la intercepción de las comunicaciones V2V, V2I o V2R. Para analizar este ataque se ha considerado un sistema complementario funcionando en modo monitor, el cual permite que las comunicaciones del Sistema IoT-WiFi-ODB-II puedan interferirse generando un ataque de *sniffing* a las comunicaciones V2V, V2R o V2I. Para este sistema complementario de prueba se usó el Sistema en Chip (SoC: System-on-Chip) Raspberry Pi 3B+, el cual permite ejecutar sistemas operativos basados en Linux. En particular, se usó la distribución diseñada especialmente para pruebas de hacking ético Linux Kali (en adelante, Kali). Dicha distribución está disponible para arquitecturas de procesador ARM, como es el caso del Raspberry. Con ayuda de una tarjeta microSD, es posible crear un disco de arranque para ejecutar el sistema operativo. Kali ofrece herramientas de *sniffing*, como "*Wireshark*", que permite capturar y analizar paquetes dentro de la red inalámbrica IoV en la que participe el vehículo. Dado que la tarjeta Arduino utiliza el protocolo IEEE 802.11 para comunicarse, fue necesario configurar el módulo WiFi del SoC Raspberry Pi 3B+para operar en modo monitor. Cabe mencionar que, para reproducir este ataque se ha considerado que el *sniffer* tenga acceso a la misma red WiFi que la tarjeta Arduino, por lo que será capaz de capturar todos los paquetes ahí transmitidos.

Se debe recordar que el ataque de análisis de tráfico captura información de forma no autorizada en una red. Por lo que, con ayuda del software "*Wireshark*" se ha logrado capturar paquetes de datos. En la figura 2 se muestran ocho paquetes capturados mientras la tarjeta Arduino se comunicaba con el servicio web REST. Se puede constatar que los datos viajan cifrados. Nótese que un ataque de análisis de tráfico es el primer reto que un atacante debe superar para ejecutar ataques más sofisticados como el ataque para lograr las claves de cifrado en la comunicación.

A partir de este ataque podría ocurrir que, conociendo los datos de conexión, se puedan descifrar los datos y extraer la información sensible transmitida por el dispositivo. El software utilizado ofrece la posibilidad de descifrar los datos si se dispone del nombre del punto de acceso y la contraseña. Sin embargo, habilitar esta funcionalidad no es parte del alcance de este trabajo, ya que se busca evitar la

infracción de las políticas de utilización de la red institucional en la que hizo el experimento. Nótese que para ejecutar ataques más sofisticados se requiere un montaje experimental más amplio y diverso en cuanto a infraestructura y servicios de red.

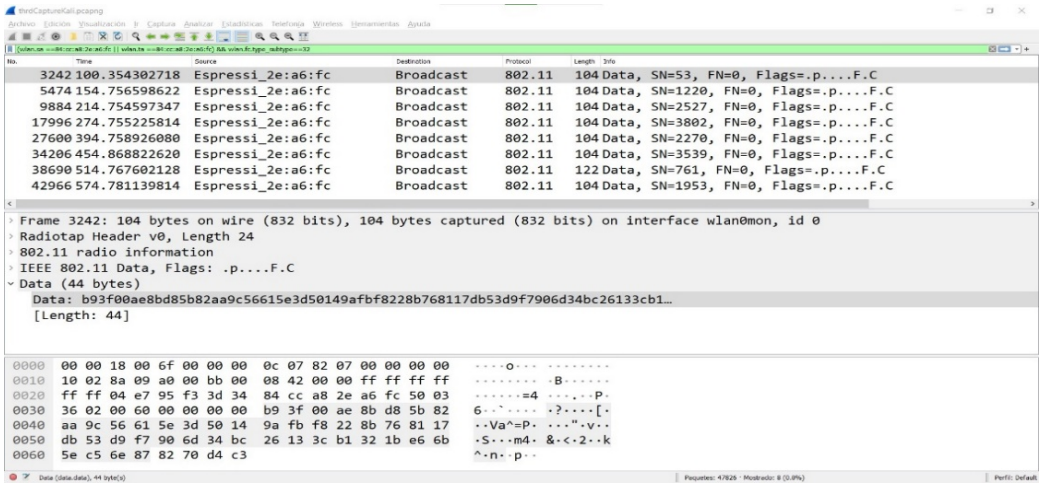

Figura 2 Captura de paquetes con “Wireshark” en un SoC Raspberry Pi 3B+.

Denegación de servicio

Este ataque puede afectar toda o parte de la infraestructura IoV, y se puede lograr a partir de perjudicar la comunicación V2I desde el lado de la infraestructura. Para mostrar la viabilidad de este ataque se ha habilitado el servidor web estilo REST (el despacho de peticiones HTTP) utilizando un micro-framework llamado *Flask*, el cual se ha elegido por su sencillez al ofrecer la funcionalidad básica HTTP requerida. Esta funcionalidad cuenta con herramientas para la conexión con bases de datos, validación de formularios y autenticación de usuarios, entre otras. Por otro lado, también permite una integración sencilla con elementos básicos de desarrollo web, como documentos HTML, hojas de estilo y *JavaScript*. Para mostrar la viabilidad del ataque se desplegó el servicio web en la plataforma “Heroku”. Sin embargo, para evitar la infracción de las políticas institucionales, se decidió ejecutar el servicio de forma local utilizando una computadora de escritorio con sistema operativo macOS, a través una dirección IP no enrutable. Cabe aclarar que, aunque limitado, este escenario de prueba no hace que se pierda generalidad en la ejecución del ataque.

Así, para emular el ataque, se usó una computadora personal portátil con el sistema operativo Windows 10 con un programa en Python para crear sockets que realizan solicitudes al servicio web.

Se pudo observar que, al realizar 200 peticiones consecutivas, el servicio web es capaz de manejarlas. Sin embargo, al utilizar un navegador en la misma computadora portátil, la consulta al sitio web demoró algunos segundos en ser atendida por el servidor. Cuando el número de peticiones se aumentó a 230, también aumentó el tiempo de respuesta y los problemas en el servidor para atender la solicitud del navegador. Esto quedó manifestado en que la página principal mostró algunos elementos que no habían sido enviados correctamente (hoja de estilos o imágenes). Aumentando la cantidad de peticiones a 250, el servidor no fue capaz de atender la solicitud del navegador, indicando que no se pudo alcanzar. Con base en lo expuesto, como se observa en la figura 3, se puede constatar la necesidad de proveer mecanismos de seguridad que eviten este tipo de ataque. Es importante mencionar que *Flask* es vulnerable a la denegación de servicio; por lo que es importante elegir cuidadosamente cada uno de los componentes que conforman el sistema IoV.

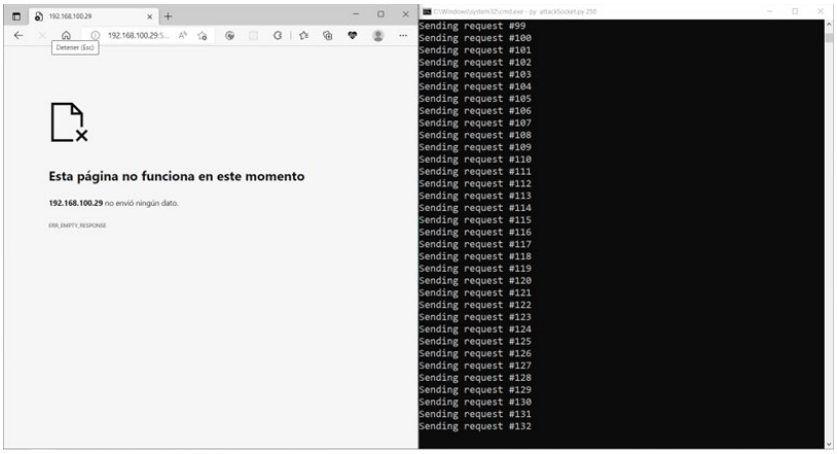

Figura 3 Comunicación interrumpida con el servidor a causa del ataque.

4. Discusión

Las demostraciones de la viabilidad de los ataques presentados en la Sección 3. Resultados son congruentes con el montaje experimental desarrollado. Es

importante mencionar que para ampliar la diversidad de los ataques presentados es necesario contar con un montaje experimental más amplio y de mayores capacidades, incluso se debe disponer de más recursos de red. Con estas precisiones, se puede decir que, en la demostración de la viabilidad de los ataques, se encontraron algunas dificultades. Una de ellas fue la selección del dispositivo que actuaría como el nodo IoT dentro del contexto de una red IoV. En este caso, la primera opción considerada fue una tarjeta Arduino sin un módulo WiFi integrado, asumiendo que la comunicación inalámbrica se realizaría por medio de un módulo de comunicación celular. Esto no pudo ser posible, ya que estos módulos requerían el mismo puerto de comunicación que el módulo CAN-BUS. La alternativa de solución a este problema fue usar la tarjeta Arduino UNO WiFi, cuyo módulo WiFi integrado no entra en conflicto con el módulo CAN-BUS, con la obvia condición de estar en la proximidad de una red inalámbrica. Se debe mencionar que esta condición de proximidad a una red WiFi nos permitió identificar una oportunidad para realizar pruebas posteriores que involucren el consumo energético o el uso de redes con recursos limitados.

Por otro lado, se encontró una dificultad para la puesta en funcionamiento de la comunicación con el protocolo HTTP, debido a que no existe una librería bien documentada para utilizar este protocolo en tarjetas Arduino. Sin embargo, como fue descrito en la Introducción, el protocolo HTTP puede no ser la opción más conveniente de protocolo de comunicaciones para dispositivos con recursos limitados, ya que los encabezados para realizar su envío son más extensos que la carga útil del mensaje. Pero, la demostración del ataque no pierde generalidad. Un protocolo como HTTP podría requerir del dispositivo un consumo energético adicional y un ancho de banda mayor en la comunicación, lo que resulta opuesto a los requerimientos óptimos para los dispositivos IoV. A pesar de esto, fue interesante seleccionar uno de los estilos arquitectónicos de desarrollo web más populares; es decir, el desarrollo web se hizo a través de interfaces de programación de aplicaciones (API: Application Programming Interface); puesto que hoy en día, es una de las formas más comunes de comunicar dos servicios web que pretenden realizar un intercambio de información.

5. Conclusiones

Con base en los ataques reproducidos, se mostró la facilidad con la que se puede afectar a un sistema IoV, ya sea desde el lado del vehículo o desde la infraestructura que le da servicio. Se puede notar entonces que para garantizar la seguridad del dispositivo se requiere, en primer lugar, establecer estrategias de seguridad física que ayuden a restringir el acceso al hardware del dispositivo y del vehículo solo al personal autorizado. Habilitar estrategias de seguridad física ayudará a evitar ataques más sofisticados como la suplantación de identidad o la manipulación del dispositivo con propósitos distintos a los establecidos.

Por otro lado, definir y establecer estrategias para la autenticación de los dispositivos también resultaría útil para evitar ataques más sofisticados, pues este tipo de estrategias contribuyen a detectar la suplantación de identidad e intrusiones.

A partir de los experimentos realizados, se ha podido mostrar la importancia de reconocer los requerimientos de software y hardware, que demanda una aplicación en función del alcance que se pretende tener. En este caso, se mostró que un atacante tiene retos que resolver para lograr que un ataque sea efectivo, pero se debe entender que solo requiere tiempo, interés y capacidad para lograrlo. En esta tarea de mostrar la viabilidad de un ataque se ha puesto en evidencia la importancia de seleccionar herramientas pertinentes sin perder de vista la función que deben desempeñar en el contexto del sistema y los dispositivos atacados. Al mostrar la viabilidad de un ataque se deben tener establecidos claramente las capacidades y fortalezas del sistema a ser atacado, así como de las herramientas que se requieren para tener éxito en el ataque. Se debe tener en cuenta que los ataques atentan contra la autenticación, la confidencialidad, y la disponibilidad en un sistema, y por ello debe existir una tarea continua para la detección y corrección de errores y vulnerabilidades, así como en la identificación y el control de las amenazas de seguridad en un sistema y los agentes que podrían ejecutarlas.

También en el diseño de un sistema IoT en general e IoV en particular se deben considerar los recursos disponibles y los requerimientos funcionales-energéticos que este sistema tenga. Finalmente, se pudo confirmar la importancia de conocer con detalle las limitaciones e implicaciones de la tecnología y el protocolo

seleccionado, ya que ese conocimiento permitirá un mejor diseño e implementación del sistema.

6. Bibliografía y Referencias

[1] Andrea, I., Chrysostomou, C., & Hadjichristofi, G. Internet of Things: Security Vulnerabilities and Challenges. 2015 IEEE Symposium on Computers and Communication (ISCC), 180-187, 2015.

[2] Asghari, P., Masoud, A., & Seyyed, H. Internet of Things applications: A systematic review. Computer Networks, No. 148, 241-261, 2019.

[3] Contreras-Castillo, J., Zeadally, S., & Guerrero-Ibañez, J. A. (2018). Internet of Vehicles: Architecture. IEEE internet of things Journal, No. 5, 3701-3709.

[4] Davies, J., & Fortuna, C. The Internet of Things: From Data to Insight. John Wiley & Sons Ltd, 1-7. Sussex, Inglaterra. 2020.

[5] Farhan, L., Shukur, S., Alissa, A., Alrweg, M., Raza, U., & Kharel, R. A survey on the challenges and opportunities of the Internet of Things (IoT). 2017 Eleventh International Conference on Sensing Technology (ICST), 1-5, 2017.

[6] Kaiwartya, O., Abdullah, A. H., Cao, Y., Altameem, A., Prasad, M., Lin, C.-T., & Liu, X. Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects. IEEE access, Vol. 4, 5356-5373, 2016.

[7] Naik, N. Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. 2017 IEEE International Systems Engineering Symposium (ISSE), 1-7, 2017.

[8] Rehman, H., Asif, M., & Ahmad, M. Future Applications and Research Challenges of IOT. International Conference on Information and Communication Technologies (ICICT), 68-74, 2017.

[9] Sakiz, F., & Sen, S. A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. Ad Hoc Networks, Vol. 61, 33-50, 2017.

[10] Sandonis, V., Soto, I., Calderon, M., & Urueña, M. Vehicle to Internet communications using the ETSI ITS. Transactions on Emerging Telecommunications Technologies, No. 3, 373-391, 2016.

[11] Sharma, N., Chauhan, N., & Chand, N. Security challenges in Internet of Vehicles (IoV) environment. 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC), 203-207, 2018.

[12] Sikimić, M., Amović, M., Vujović, V., Suknović, B., & Manjak, D. An Overview of Wireless Technologies for IoT Network. 19th International Symposium INFOTEH-JAHORINA (INFOTEH), 1-6, 2020.

[13] Sun, Y., Wu, L., Wu, S., Li, S., Zhang, T., Zhang, L., Cui, X. Attacks and countermeasures in the internet of vehicles. Annals of Telecommunications, Vol. 74, 283-295, 2017.

[14] Sun, Y., Wu, L., Wu, S., Li, S., Zhang, T., Zhang, L., Xiong, Y. Security and Privacy in the Internet of Vehicles. 2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI), 116-121, 2015.

[15] Wortmann, F., & Flüchter, K. Internet of Things. Business & Information Systems Engineering, Vol. 57, 221-224, 2015.