Ataque MitM a puntos de recarga AC

Javier Jarauta Gastelu, Roberto Gesteira-Miñarro, Javier Matanza, Rafael Palacios, Gregorio López
Instituto de Investigación Tecnológica, ICAI - Universidad Pontificia Comillas, Madrid, España

jjarauta@alu.comillas.edu,
rgesteira@comillas.edu, javier.matanza@iit.comillas.edu, rafael.palacios@iit.comillas.edu, gllopez@comillas.edu

***Resumen*—En este artículo presentamos un ataque MitM a puntos de recarga AC que permite controlar la carga del vehículo sin que el punto de recarga lo detecte. El ataque se ha llevado a cabo tanto en entorno de laboratorio como en entorno real. Este ataque pone de manifiesto que es necesario mejorar la seguridad en los puntos de recarga AC.**

***Index Terms*—Vehículos electricos, Recarga AC, Man-in-the-Middle, Ciberseguridad**

Tipo de contribución: *Investigación original*

I. Introducción

Los ataques coordinados y simultáneos contra la demanda o el suministro de energía a través de dispositivos IoT (*Internet of Things*) se han identificado como un riesgo más difícil de controlar y mitigar por parte de las distribuidoras y los operadores de sistema que otros más convencionales como los APT (*Advanced Persistent Threats*) o el *phishing* [1]. En consecuencia, dichos ataques han atraído el interés de la comunidad investigadora y su impacto en la red eléctrica se ha analizado, principalmente, a través de una serie de artículos publicados en *USENIX Security* [2] [3] [4]. En el primero de ellos [2], inspirados por el ataque a DYN de finales de 2016, se acuña el término ataques MaDIoT (*Manipulation of Demand via IoT*) y se demuestra mediante simulación que dichos ataques pueden provocar apagones locales o incluso a gran escala. En el segundo [3], los autores prueban mediante simulaciones más sofisticadas que la probabilidad de éxito de este tipo de ataques no es tan alta porque las protecciones existentes en la red eléctrica lo impiden. Por último, el tercer artículo de la saga [4] demuestra que un atacante con conocimientos privilegiados puede llevar a cabo ataques más sofisticados (p.ej., teniendo en cuenta el tiempo y la localización geográfica) cuya tasa de éxito e impacto serían mayores, pero que es poco probable que esto ocurra.

Estos tres artículos presentan las siguientes limitaciones, que dan lugar unas preguntas de investigación:

- Se centran en modelos de red eléctrica americanos (en el primer artículo se estudia el caso de una red polaca, pero no es representativa a nivel europeo).
- No estudian el impacto de controlar también dispositivos de generación distribuida, aunque si aparece como trabajos futuros en los últimos artículos.
- Asumen que pueden comprometer tantos dispositivos como quieran, sin entrar a valorar cómo de difícil es hacer esto.

Estas preguntas de investigación se abordan como parte del proyecto europeo eFORT [5], cuyo objetivo es la mejora de la resiliencia y fiabilidad de las redes eléctricas europeas, en el que se enmarca esta investigación. Más concretamente, en este artículo se pretende responder a la siguiente pregunta de investigación:

- ¿Es posible controlar la carga de un vehículo eléctrico de manera maliciosa?

El dispositivo elegido ha sido un punto de recarga de vehículo eléctrico debido al auge actual de este tipo de infraestructuras y a las altas potencias a las que los vehículos eléctricos pueden cargar. De hecho, los artículos de la saga publicada en *USENIX Security* comienzan considerando dispositivos como aires acondicionados, pero acaban centrándose en vehículos eléctricos y [1] también elige como ejemplo representativo el vehículo eléctrico, indicando el número de puntos de recarga que sería necesario controlar para desbalancear la red eléctrica europea dependiendo de la carga del punto.

El resto del artículo se organiza de la siguiente manera. El Apartado II busca desarrollar el proceso de carga de un vehículo eléctrico. Incluye un breve desarrollo sobre los protocolos y estándares necesarios para la recarga del vehículo, las tipologías de recarga, y el funcionamiento de carga en AC como secciones principales. El Apartado III-B2 desarrolla todas las pruebas de laboratorio y de campo necesarias para realizar satisfactoriamente el ataque, incluyendo los sistemas utilizados y los resultados de las pruebas. Finalmente, el Apartado IV desarrolla la afección, resumen y trabajos futuros con otros protocolos de recarga.

II. Carga de un Vehículo Eléctrico

Para realizar la recarga de los vehículos eléctricos, existen dos mecanismos principales, carga en corriente alterna (AC) y carga en corriente continua (DC). Además, teniendo en consideración ambos mecanismos de recarga, existe una clasificación que depende de la velocidad de carga, es decir, la potencia máxima a la que puede realizar la carga el vehículo. Esta limitación máxima se puede dar tanto por el equipamiento que provee la energía o por el propio vehículo.

Este trabajo ha sido parcialmente financiado por el Programa de Investigación e Innovación Energética de *Horizon Europe* de la Unión Europea en el marco del proyecto eFORT (Acuerdo de Subvención no. 101075665). El contenido del artículo refleja únicamente las opiniones de los autores. La Comisión Europea no se hace responsable del uso que se pueda hacer de la información contenida en el mismo.

En este trabajo de investigación, el enfoque se encuentra en la carga de los vehículos eléctricos en corriente alterna. Los motivos de esta decisión se basan en la facilidad de encontrar equipamiento de prueba para la recarga en corriente alterna, el menor peligro por la potencia de recarga más limitada, uso de voltajes de baja tensión, y la posibilidad de realizar modificaciones sobre un cable de recarga. Esto se debe a que el protocolo de recarga europeo permite el uso de cables provistos por el usuario, sin necesidad de que estos se encuentren permanentemente conectados al punto de recarga, facilitando la creación de un cable malintencionado. La modificación de un cable ajeno a los elementos de carga, permite que no se modifique ni el vehículo ni el punto de recarga para el ataque, siendo ambos completamente ajenos a las actividades malintencionadas que un usuario pueda realizar. Utilizando esta metodología, el vehículo no sospecha de los comandos enviados por el punto de recarga malintencionado, y el punto de recarga simplemente observa como el vehículo fluctúa la potencia de su recarga (de manera un tanto anómala). Todas estas ventajas, combinadas con una mayor complejidad del protocolo de recarga en DC, mediante el uso de comunicación por paquetes, provoca, que las pruebas se hayan ejecutado únicamente en cargadores de corriente alterna.

II-A. Clasificación de las Potencias de Recarga

La clasificación por potencias de carga máximas varía tanto en su denominación como en la división entre diferentes operadores de puntos de recarga y fabricantes, existiendo cierto consenso únicamente en cuanto a la carga lenta. A continuación se describe una posible segmentación entre dichas potencias de carga [6]:

Carga Lenta [1.3 kW - 22 kW]
Suelen ser puntos de recarga en AC, disponibles en garajes, vías públicas urbanas, centros comerciales, hogares, etc. Los tiempos de recarga fluctúan entre las 3-15 horas, dependiendo de la potencia del punto de recarga y el cargador integrado en el vehículo.

Carga Semi-Rápida [22 kW - 100 kW]
Pueden incluir puntos de recarga tanto en AC (menos comunes) y DC. Los tiempos de recarga se encuentran alrededor de 1-3 horas.

Carga Muy/Hiper/Ultra/Súper-Rápida [>100 kW]
Son puntos de recarga únicamente en DC, y presentan las potencias más elevadas, a día de hoy hasta unos 500 kW. Sus tiempos de recarga fluctúan entre los 15-45 minutos.

II-B. Estándares

En el proceso de recarga existen una serie protocolos y estándares que integran todo el proceso de carga de los vehículos eléctricos, desde la definición de conectores hasta los protocolos de comunicación. A continuación se describen los principales y necesarios para ejecutar el proceso de recarga. Además, en la Fig. 1 se observa la aplicación de cada protocolo.

IEC 62196 Define los elementos físicos y regulaciones de enchufes, conectores, puertos, cables y configuraciones de los diferentes sistemas de recarga de vehículos eléctricos. Incluye además, los tipos de recarga y potencias y voltajes para cada modalidad.

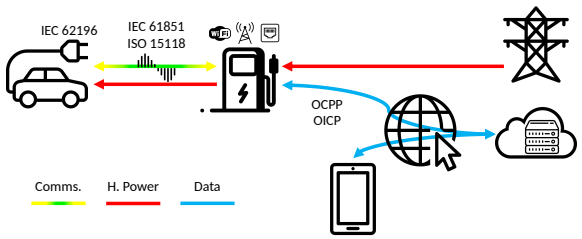

Figura 1. Sistema y protocolos de recarga.

IEC 61851 Define los requisitos eléctricos de los vehículos para la carga tanto en AC como en DC, los requisitos de las estaciones de recarga, y la comunicación básica entre ambos elementos para el comienzo y ejecución de la recarga. Define la señalización básica del sistema, como PWM y estados de carga.

ISO 15118 Define el protocolo de comunicación más avanzado entre el vehículo eléctrico y la red, incluyendo funcionalidades Vehicle-to-Grid (V2G). Además define el mecanismo de comunicación IP y Plug&Charge, que permite el uso de certificados y comunicación segura entre el vehículo y el punto de recarga, incluida la autenticación mutua y cobro automatizado.

OCPP Protocolo *de facto* para la comunicación entre las estaciones de recarga y los gestores/proveedores de estaciones de recarga. Es un estándar de código abierto, y a partir de su versión 1.6j, incluyendo la última 2.0, permite el uso de certificados para la comunicación y transmisión de información segura entre los cargadores y el sistema de gestión del operador.

II-C. Carga en AC

La carga en corriente alterna, permite carga trifásica hasta 44 kW para un vehículo que presente un cargador interno con la suficiente potencia. En este caso, este tipo de recarga, supone la mayor parte del número de puntos de carga presentes en el mercado europeo, y el más extendido entre los pequeños usuarios, ya que su instalación únicamente depende de la presencia de una mínima potencia en la red eléctrica.

La ventaja de esta tipología de recarga, es que el propio vehículo posee el cargador o conversor entre corriente alterna (red eléctrica) y corriente continua (batería). Por tanto, basta con una conexión a la red eléctrica de baja tensión para poder ejecutar la transferencia de energía.

II-C1. Conectores: Para realizar la carga en AC, en el mercado europeo se utiliza el conector denominado Tipo 2 o Mennekes (por la empresa que lo diseñó), definido en el estándar IEC 62196. Este conector presenta la característica principal que permite la carga en corriente trifásica y monofásica. Para ello, contiene siete conductores, tal y como se demuestra en la Fig. 2 [7].

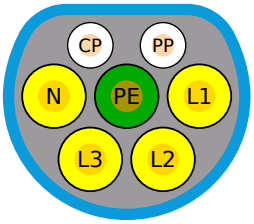

Figura 2. Conector Tipo 2.

En este caso N (Neutro), L1, L2 y L3 (Líneas) proveen la corriente correspondiente para la recarga. PE (Tierra) protege la instalación y sirve como voltaje de referencia para la señalización. PP (Piloto de Presencia) indica a la estación de recarga que existe un vehículo conectado y finalmente CP (Piloto de Control) indica al vehículo la conexión de una estación de recarga, y es el conductor por el cual se transmite la información codificada de manera bidireccional.

II-C2. Señalización: Para la comunicación entre el vehículo y la estación de recarga, el estándar indica el uso de señales PWM (Pulse Width Modulation) o modulación por ancho de pulsos en la línea CP, para indicar los diferentes estados y potencias. Esta señal PWM será la señal sobre la que los protocolos superiores se basarán para el envío de información más compleja, en el caso de la carga en DC [8].

Dentro de la señal PWM, existe comunicación tanto por parte de la estación de recarga como del vehículo. En una comunicación básica, la estación de recarga necesita indicar al vehículo la potencia máxima disponible y el estado del punto de recarga, incluyendo escenarios de fallos. En el caso del vehículo, este deberá comunicar el estado actual de la recarga, y cualquier requisito que pueda poseer dentro de esta.

La información sobre la potencia disponible/limitada que posea el punto de recarga se codifica mediante el ciclo de trabajo de la señal PWM. Además, y en el caso de paro, un ciclo de trabajo inválido, como 0 % indica, paro en la carga o en algunos casos fallo, de tal manera que se tienen en consideración estados de error.

El ciclo de trabajo de la señal PWM viene definido para valores entre 6...50 A [8]:

$$Ciclo\ de\ Trabajo\ =\ \left(\frac{Corriente}{0{,}6}\right)\ \%\qquad(1)$$

Y para valores entre 51...80 A:

$$Ciclo\ de\ Trabajo\ =\ \left(\frac{Corriente}{2{,}5}\ +\ 64\right)\ \%\qquad(2)$$

Además, existen ciertos rangos de valores con significados diferentes. En la Tabla I se presenta una relación limitada de valores para la señal PWM [9].

Conociendo la codificación de la potencia máxima disponible, es necesario tener en consideración la comunicación bidireccional de los diferentes estados de carga mediante la línea CP. Para ello, se utiliza el voltaje de la señal PWM para indicar el estado actual de la recarga. Como se muestra en Apartado II-C3, la señal PWM provista por el punto de recarga, siempre presenta unos valores entre $\pm$ 12 V, y es el vehículo a través de la introducción de resistencias entre la línea CP y PE el que modifica el valor máximo superior de la señal PWM para indicar el estado actual de la recarga. Los diferentes estados se encuentran en la Tabla II [8].

Tabla I
RELACIÓN CICLO DE TRABAJO / CORRIENTE

Ciclo de Trabajo	Corriente/Información
<3,00 %	Carga no permitida
3,00 - 7,00 %	ISO 15118
7,00 - 8,00 %	Carga no permitida
10,00 %	6 A
26,67 %	16 A
53,33	32 A
96,00 %	80 A

Tabla II
ESTADOS DE RECARGA Y VOLTAJES

Estados	Voltaje de la señal PWM	Resistencia entre CP/PE
Vehículo desconectado	$+12\ V$	$\infty\ \Omega$
Vehículo preparado	$+9/-12\ V$	2740 Ω
Cargando	$+6/-12\ V$	882 Ω
Cargando - Ventilación necesaria	$+3/-12\ V$	246 Ω
Apagado	$0\ V$	
Fallo	$-12\ V$	

II-C3. Circuitería: Para que ambos elementos presenten una comunicación básica, es necesario que se encuentren correctamente definidos los elementos de comunicación entre ambos sistemas. Sin embargo, y debido a la simpleza de los sistemas, la circuitería se basa en medición de las líneas de control, resistencias, diodos, y un número limitado de elementos activos. Un esquema de la conexión de los elementos del vehículo y el punto de recarga, mediante un cable independiente se muestra en la Fig. 3 [9].

II-C4. Proceso de Recarga: El proceso de recarga del vehículo eléctrico en corriente alterna se basa en las siguientes acciones:

1. **Conexión del vehículo con el punto de recarga**
   Por medio de un cable independiente o permanentemente conectado al punto de recarga se realiza la conexión entre ambos elementos. Los pines PE (Tierra) realizarán su conexión primero por motivos de seguridad, y el punto de recarga detectará la presencia del vehículo/cable, ya que este está manteniendo un voltaje de 5 V en la línea PP. La presencia por parte del ambos elementos se detecta de dos maneras diferentes. Si el cable está integrado en el punto de recarga, el voltaje emitido por el vehículo será detectado por el punto de recarga, y este añade una resistencia entre PE y PP para indicar su conexión. En este caso, siempre se asume que el punto de recarga conoce los límites de carga permitidos por el cable al

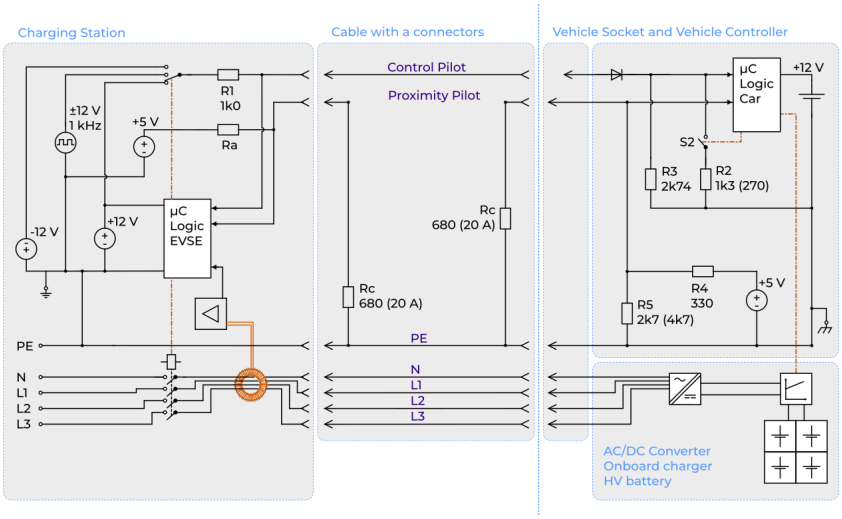

Figura 3. Circuitería de conexión entre el vehículo y la estación de carga.

que está conectado. En el caso que sea un cable independiente, la línea PP no presenta una conexión directa entre ambos elementos, y es una resistencia interna en el cable en cada extremo, la que indica la potencia máxima de recarga. Esta resistencia varía entre 1500 Ω y 100 Ω aproximadamente, e indica la corriente máxima [8].

2. **Inicio del proceso de recarga**
   El punto de recarga comienza con una señal PWM de $\pm 12\ V$ indicando la máxima potencia de carga en el ciclo de trabajo, indicando que se encuentra preparado para la carga. Una detectada la señal, el vehículo indica por medio de una resistencia de 2740 Ω que se encuentra preparado para la carga.
3. **Carga**
   Habiendo obtenido respuesta del vehículo, el punto de recarga cierra los relés/contactos para suplir la energía al vehículo, y cuando este detecta una corriente positiva, indica, por medio de una resistencia de unos 1200 Ω que está cargando correctamente. Cabe destacar que si el vehículo necesitase ventilación para la carga (extremadamente raro para cualquier vehículo moderno) indicaría una resistencia menor. Sin embargo, este modo de carga prácticamente no esta soportado/garantizado por ningún punto de recarga actual.
4. **Desconexión/Interrupción**
   Para realizar la desconexión, el vehículo interrumpirá la carga, y desconectará el voltaje en la línea de presencia, indicando al punto de recarga la desconexión. En el caso del punto de recarga, si este necesita interrumpir la carga sin dar fallo, simplemente indicará una señal PWM con un ciclo de trabajo del 0 %.

II-D. Carga en DC

Aún no siendo objeto de esta investigación, para la carga en DC, el protocolo subyacente utiliza la misma comunicación básica que la carga en AC para realizar la conexión entre el punto de recarga y el vehículo. Además, utiliza un conector modificado, denominado CCS 2 (Combined Charging System) que utiliza la misma estructura que el Tipo 2, pero con dos pines adicionales que permiten la carga en DC, con una conexión directa a la batería del vehículo.

Teniendo en cuenta que el protocolo para carga en DC, utiliza una señal PLC (Power Line Communication) en la misma línea CP, utilizando para la comunicación superior TCP/IP, es necesario que la señal subyacente PWM esté presente en esa línea para que la carga sea satisfactoria. Además, en cualquier situación, una desconexión de la señal PWM supone una parada de la carga en DC [10].

III. Ataque MitM a un Punto de Recarga

Para realizar el ataque al sistema de carga de vehículos eléctricos en AC, se realizaron las pruebas e investigación de manera sistemática, comenzando en el laboratorio simulando un sistema de recarga completo, incluyendo tanto el punto de recarga como el vehículo. Una vez obtenidos unos resultados satisfactorios, y tras realizar las comprobaciones necesarias, se procede a desarrollar un cable malintencionado que pueda ser fácilmente desplegado en pruebas de campo, para comprobar la señalización y la posibilidad de realizar un ataque de demanda a un vehículo eléctrico en proceso de recarga.

La búsqueda de una simulación fidedigna del protocolo guía las pruebas y circuitería realizadas. La intención es evitar la detección del sistema, mejorando la portabilidad y escalabilidad de los componentes utilizados para la realización del ataque.

III-A. Pruebas de Laboratorio

En las pruebas de laboratorio, el objetivo es la verificación de los componentes, circuitería y la posibilidad de realizar el ataque MitM de manera satisfactoria en elementos simulados.

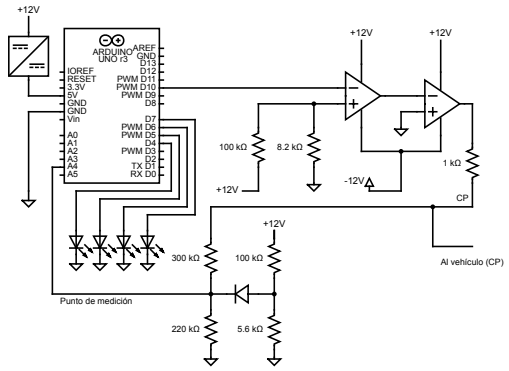

Figura 4. Simulador de la estación de carga.

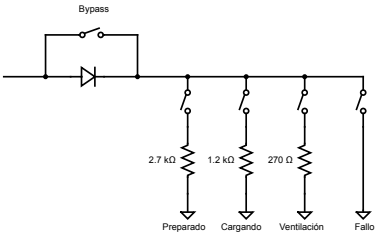

Figura 5. Simulador del vehículo.

Para poder realizar la simulación correctamente, se realizaron los siguientes componentes:

III-A1. Simulador del punto de recarga: Utilizando un Arduino UNO como controlador de la lógica, se procedió a realizar una simulación de un punto de recarga, capaz de ajustar la potencia de carga con respecto a unos parámetros preestablecidos. Incluye la simulación del comportamiento de los diferentes estados de carga mediante una máquina de estados y el ajuste de los ciclos de trabajo de la señal PWM. Además, tiene la capacidad de realizar todas las mediciones en el voltaje de línea, mediante un circuito adaptador, de manera que puede reaccionar a los errores y estados del vehículo. Adaptando la información en la Fig. 3 se desarrolló el sistema presente en la Fig. 4.

III-A2. Simulador del vehículo: Para simular los estados de carga del vehículo, se realizó un pequeño circuito operado mediante interruptores de manera manual (Fig. 5), que pudiese indicar al punto de recarga simulado el estado del vehículo para su detección. Todo esto se muestra a través de diodos LED en el simulador del punto de recarga.

III-A3. Creación del sistema malicioso: Utilizando otro Arduino UNO y circuitería, fue posible realizar un sistema malicioso, combinando ambos circuitos superiores, y realizando el control de los interruptores mediante relés, como se muestra en Fig. 6.

Este sistema es capaz de interceptar la señal enviada por el punto de recarga verdadero, descifrar el ciclo de trabajo para obtener la potencia disponible y el estado y modificar dicha capacidad, para indicar al vehículo una potencia disponible diferente, e incluso una falta de potencia. También es capaz de leer la línea de control enviada al vehículo, determinar los estados que este comunica y reenviar esos estados en un periodo de tiempo menor a 200 ms al cargador, simulando el comportamiento del vehículo.

Siguiendo este proceso, el sistema malicioso es capaz de modificar la potencia que el coche cree que esta disponible y realizar fluctuaciones periódicas, o incluso parar la carga por completo, todo ello sin necesidad de alterar ninguno de los dos elementos del proceso. La lógica del sistema presenta tres elementos básicos que permiten su funcionamiento.

1. **Sistema de medición** El sistema de medición presenta dos funciones principales: medición de los estados de ambas líneas y medición del ciclo de trabajo de la señal PWM. Para determinar el estado que envía el vehículo, este sistema mide el voltaje máximo de la línea, tras pasar por un conversor de voltaje, y determina el estado en el que se encuentra el vehículo. Así, es capaz de retransmitir dicha información al punto de recarga, mediante el uso de los relés aguas arriba. Para determinar el ciclo de trabajo que indica la potencia máxima a retransmitir al coche, este sistema posee lógica de filtrado de señal, para evitar que distorsiones y resistencias internas modifiquen el valor, y asigna, según *Ec.* (1) o *Ec.* (2) la potencia máxima de la línea que puede proveer el punto de recarga.
2. **Máquina de estados** La máquina de estados transmite la información desde el vehículo hasta el punto de recarga, y altera su valor interno en base a las mediciones de ambos pilotos. Es la encargada de modificar valores de salidas, monitorizar ambos cables de información y controlar que a pesar de realizar un ataque, se mantiene el sistema dentro de los parámetros habituales. En el caso de esta implementación, existen dos máquinas de estados paralelas, para cada uno de los cables que existen al vehículo y al punto de recarga. El objetivo es que cualquier cambio de una se vea reflejado instantáneamente en la otra.
3. **Sistema de ataque** Este es el sistema encargado de recibir las órdenes malintencionadas, y ejecutar el ciclo de fluctuación de la potencia de carga en un intervalo de segundos modificable. A través de este mecanismo, un usuario malintencionado es capaz de alterar en base a un patrón la demanda y carga del vehículo.

III-A4. Integración de los componentes en un simulador: Todos los sistemas anteriores se integraron en un simulador, para demostrar su correcto funcionamiento mediante la sensorización de las líneas de control CP y la medición de estados y potencias máximas. Utilizando para ello: dos Arduinos, para controlar un punto de recarga bueno y otro para controlar el sistema malintecionado; y un simulador de vehículo manual. Con este sistema de simulación se realizaron los ajustes necesarios en los sistemas de medición y la máquina de estados, para que la transmisión de información fuese lo más rápida posible por motivos de seguridad.

III-A5. Creación del cable malicioso: Una vez se integran todos los componentes, fue necesario modificar el cable utilizado para la recarga del vehículo eléctrico. La modificación no supone la alteración de ninguno de los cables de potencia (L1,

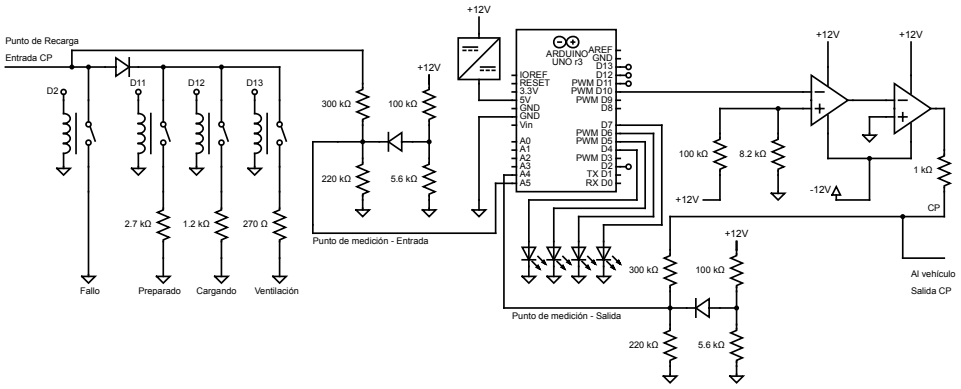

Figura 6. Simulador del sistema malicioso.

L2, L3, N), y únicamente es necesario interceptar el cable CP mediante unas clemas y obtener el voltaje de referencia para todos los componentes de medición mediante una pequeña perforación en el aislante de PE. De esta manera, el riesgo a la persona realizando el ataque o usuario del punto se minimiza, ya que las señales por el piloto CP son de bajo voltaje, y la apariencia de alteración del cable es mínima.

Este sistema se integra en una pequeña PCB con fácil portabilidad, siendo su apariencia final parecida a aquella de un cargador móvil/emergencia provisto por los fabricantes de vehículos eléctricos para la carga en enchufes domésticos (schuko - CEE 7/3 Tipo F) o industriales (Cetac - IEC 60309).

III-B. Pruebas de Campo

Una vez realizadas las pruebas de laboratorio, se procedió a realizar las pruebas de campo, con puntos de recarga y vehículos sin alterar, en un entorno en producción. Para realizar las pruebas de campo, se utilizaron: el cable malintencionado, lógica malintencionada, sistemas de medición (osciloscopio, pinza amperimétrica, multímetro) y fuente de alimentación.

III-B1. Eavesdropping: La primera aproximación a la realización del ataque es la comprobación que el sistema real funciona tal y como indican las especificaciones [8]. Este paso fue necesario para incluir en el ataque cualquier implementación específica del fabricante del punto de recarga o peculiaridad necesaria, sin embargo, no fue necesario realizar ningún ajuste significativo.

En un principio, se realizó el análisis de la señal PWM en el cable, sin interceptar la línea CP. Así, se observó que no existiese ninguna distorsión extra introducida por la modificación del cable de carga, tanto en el tramo de la línea hacia el punto de recarga como en el tramo del vehículo. Este análisis conlleva la verificación primero, de los niveles de carga, es decir, cuando está desconectado, un voltaje continuo de $+12\ V$, una vez se detecta la presencia del cable, una señal PWM $\pm 12\ V$ y al iniciar la carga entre $+9\ V / -12\ V$. No se comprobó el estado de fallo por no forzar ningún error en la línea que supusiese algún daño [8].

Además, se verificó que el ciclo de trabajo para los valores de corriente esperados fuesen adecuados. Se comprobó como para los $6\ A$ de corriente ($3{,}6\ kW$), el ciclo de trabajo era alrededor del $10\,\%$, al igual que $\sim 50\,\%$ para $32\ A$ de corriente por fase ($22\ kW$). En este caso, la distorsión que existe en la línea, bien por el ruido introducido por el cable o por su modificación es insignificante para las distancias de un cable de carga de vehículo eléctrico, y la medición de amperaje recibido por el sistema se encontraba dentro de los valores esperados según la especificación.

III-B2. Ataque: Una vez realizadas las comprobaciones de las señales en el cable, sin realizar ninguna modificación malintencionada en ellas (*eavesdropping*), se procedió con la realización del ataque en el entorno de pruebas real.

El ataque de demanda consiste en, estando activa la carga del vehículo, modificar periódicamente la potencia de carga, desde el máximo disponible por el punto de recarga, hasta el mínimo admisible por el protocolo ($6\ A$(. Este ciclo se repetiría cada cierto intervalo de tiempo, que puede fluctuar desde pocos segundos hasta periodos largos de tiempo.

El objetivo de este ataque es verificar, que efectivamente, se puede modificar la carga activa de un vehículo eléctrico sin necesidad de reconexión o parada, permitiendo así generar ataques de demanda a elementos de alta potencia. Además, la ventaja de este ataque es no solo poder interrumpir su recarga, ya que es fácilmente detectable si el vehículo o el punto de recarga interrumpen la carga, si no fluctuar periódicamente la potencia. Esta fluctuación es mucho más difícil de detectar, ya que se puede asumir como un comportamiento semi-anómalo de alguno de los elementos del proceso. Es decir, el vehículo puede modificar la potencia de recarga en base a las necesidades de este como el estado de carga de la batería, horarios de carga, etc. Además, el punto de recarga podría estar modificando la potencia debido a una limitación de la línea, carga mediante sistemas fotovoltaicos, o por potencia compartida entre diferentes puntos, entre otros.

Así, se procedió a insertar el dispositivo malintencionado, interceptando la línea de control del cable. Una vez insertado, se procedió a realizar una batería de pruebas que verificasen el correcto funcionamiento, manteniendo los elementos de medida tanto en los conductores como en las líneas para

Figura 7. Estado normal.

Figura 8. Estado reducido.

verificar que el comportamiento es similar/igual.

Se comenzó utilizando un ciclo de cambio de 3 segundos. Este ciclo de tres segundos, probado en las pruebas de laboratorio, funciona según lo esperado. Sin embargo, se encontraron problemas, ya que el vehículo sobre el que se realizaron las pruebas, al estar en un potencia de carga baja, no incrementa la potencia instantáneamente. Sin embargo, por motivos de seguridad, si que reduce la potencia instantáneamente si tiene la instrucción por parte de la estación de recarga. Para mitigar este pequeño inconveniente, las subsecuentes pruebas se realizan con un intervalo de 30 segundos entre cambios de potencia. Con esta modificación, el comportamiento del ataque en todos los elementos es el siguiente:

1. **Estado de carga normal**
   El vehículo esta cargando a la máxima potencia deseada ($11\ kW$). La señal PWM en ambos segmentos de CP posee un ciclo de trabajo de aproximadamente un 50 %, indicando una carga máxima de $22\ kW$ y el voltaje en ambos lados de la señal PWM se encuentra entre $+9/-12\ V$, indicando un estado de carga activo. En este punto el sistema no actúa, y ninguno de los dos elementos es consciente de su existencia. Esto se muestra en la Fig. 7
2. **Reducción de potencia**
   El ataque comienza en este punto. El vehículo recibe una señal malintencionada a través de CP que indica que la potencia máxima de carga es $3{,}6\ kW$ (ciclo de trabajo del 10 %), sin embargo, el punto de recarga sigue emitiendo potencia máxima (Fig. 8). EL vehículo, al recibir dicha señal, reduce la potencia instantáneamente, para evitar fallos en el "punto de recargaz comienza a cargar a $3{,}6\ kW$. En este caso, para el punto de recarga, la única visualización es que el vehículo ha reducido la potencia de carga medida en las líneas, pero no ha alterado ninguno de los estados. Para el vehículo, este ha recibido una señal directa de reducción de potencia, pero sigue cargando.
3. **Aumento de potencia**
   En este caso, una vez está reducida la potencia, el atacante envía otra vez al vehículo una señal de que el punto de recarga tiene otra vez potencia máxima, o cualquier potencia entre el mínimo y el máximo disponible. Al recibir el vehículo esta señal, comienza de manera escalonada a subir la potencia de carga tomando unos 12 segundos (este comportamiento depende de cada marca y modelo de vehículo). Para el vehículo, simplemente ha habido un aumento de potencia, sin cambio del estado de carga. Para el punto de recarga, la potencia medida comenzará a subir. Cabe destacar, que cuando al vehículo se le envíe una potencia superior a la disponible por el punto de recarga, pueden existir dos situaciones.
   - El vehículo detecta que el punto de recarga no provee más potencia sin llegar a la máxima, y considera que está defectuoso. Sin embargo, no existirá ningún fallo en el punto de recarga o vehículo, a lo sumo un mensaje de potencia de carga reducida. Esto se da si el punto de recarga puede físicamente limitar la potencia de recarga.
   - Si el punto no puede limitar la potencia, el punto de recarga interrumpiría la carga por motivos de seguridad. Esto se daría cuando el vehículo solicite más potencia de la disponible y exceda los limites.
4. **Paralización de la recarga**
   Es posible paralizar la recarga, de variadas maneras. La más adecuada sería indicando al vehículo que no existe potencia. En este caso, este detendría el proceso, y en el mismo instante, al punto de recarga se le indica que el vehículo no está cargado eliminando la resistencia en la línea. Automáticamente el punto de recarga abre los contactos de las líneas de tensión, y se paraliza todo. Aún así, existe la opción de desconectar por completo la señal, o incluso provocar la señal de fallo.
5. **Reiniciación de la recarga**
   La reiniciación de la recarga está supeditada a la implementación que tenga el fabricante del punto de recarga, y si este es público (de pago) o privado. En un punto público, la interrupción puede suponer una reinicialización del proceso de autenticación, y por tanto no ser posible. En un punto privado, esta reinicialización es posible, dependiendo de como se realice la parada. En el caso de las pruebas, no se realizó ninguna reiniciación.

Una vez verificados los casos superiores, se dan por concluidas las pruebas de campo, en las que se demuestra como es posible alterar el proceso de carga AC de un vehículo eléctrico, pudiendo realizar ataques de demanda sobre la infraestructura de carga, sin ninguna detección.

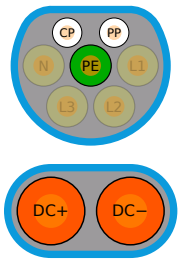

Figura 9. Conector CCS 2.

IV. Conclusiones y Trabajo Futuro

Tras la realización de las pruebas tanto de laboratorio como de campo, se ha comprobado como el modo más lento de recarga de los vehículos eléctricos (AC) es vulnerable a un ataque de demanda. Un agente malintencionado, con el suficiente número de recursos, podría modificar la demanda de los vehículos eléctricos en proceso de recarga en una amplia área geográfica, para conseguir afecciones significativas a la red eléctrica, ya sea de manera local, regional o global [1].

Con este ejemplo, la escalabilidad es reducida, ya que supone la compra de una gran variedad de dispositivos para generar la suficiente variación de demanda. Sin embargo, con un conocimiento elevado de la red eléctrica, es posible ejecutar este ataque de demanda de manera satisfactoria.

El ataque demuestra, que para el protocolo de carga AC, no existe ningún elemento de autenticación, lo que permite, que el atacante pueda realizar sus pericias maliciosas. Además, considerando que el ataque puede ser ejecutado sin el conocimiento de ninguna de las dos partes que realizan el proceso de recarga (vehículo y cargador), es posible considerar que alguno de estos dos quieran interferir maliciosamente en la recarga. Por tanto, y existiendo un protocolo superior con autenticación y verificación de certificados, sería conveniente promover la adopción de dicho protocolo también para recarga en AC.

IV-A. Trabajo Futuro

Debido a las limitaciones y peligros mencionados anteriormente, como el riesgo de la alta tensión y potencia de esos cargadores, la carga en DC no se ha tenido en consideración para la realización de este ataque. Sin embargo, con las suficientes medidas de seguridad, y a través de la creación de un enchufe sobrepuesto (al no existir cables propios en carga en DC) a modo de los estafadores de tarjetas de crédito, puede ser posible duplicar el ataque presentado en los cargadores en DC. La ventaja de este ataque es que la potencia de estos cargadores es muy superior, pudiendo llegar hasta los $500\ kW$ de potencia. Así, al afección de una menor cantidad de ellos supone un impacto mucho mayor.

Para el desarrollo del ataque en DC, cabe destacar que, el sistema de comunicación básico utiliza la misma estructura que los cargadores AC, como se observa por la estructura del conector CCS en 9 [11]. Sigue utilizando señales PWM para la conexión y la indicación de los estados de recarga, y por tanto se podría reutilizar la circuitería básica. Sin embargo, este modo de carga utiliza un protocolo superior para la comunicación (ISO 15118) [10] basado en TCP/IP. Para su activación, el ciclo de trabajo del protocolo inferior se fija en 5 % aproximadamente, y comienza el uso del protocolo superior, atendiendo a las diferentes capas de comunicación con respecto al modelo OSI:

1. Física: HomePlug Green PHY – Módem PLC – $[1{,}8 \leftrightarrow 30\ MHz]$
2. Enlace: SLAC (Signal Level Attenuation Characterization) - $[-75\ dBm/Hz]$
3. Red: IPv6 – Neighbor Broadcast Protocol + ICMPv6
4. Transporte: TCP + TLS (Opcional), UDP
5. Sesión: V2GTP (Vehicle to Grid Transfer Protocol)
6. Presentación: W3C EXI 1.0 Codificación/Decodificación
7. Aplicación: Comunicación de paquetes de carga

La ventaja que posee este protocolo, es que en su última implementación, utiliza certificados emitidos por una autoridad para la comunicación entre el vehículo y el cargador, sin embargo, esta seguridad se basa únicamente en la aplicación de *Plug&Charge*, el cual no está implementado por todos los fabricantes ni activado por todos los operadores de recarga

Por tanto, a pesar de utilizar certificados para la comunicación y TLS, estos son autofirmados y pueden ser susceptibles de MitM. En este caso, la investigación futura podría investigar la seguridad de comunicación entre el cargador y el vehículo en DC, y los mecanismos de autenticación mutua existentes.

Referencias

[1] L. Anderson, D. Dobrygowski, and S. Rajachudamani, "Cyber resilience in the electricity ecosystem: Principles and guidance for boards," 2019, publisher: World Economic Forum. [Online]. Available: https://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf

[2] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 15–32. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/soltan

[3] B. Huang, A. A. Cardenas, and R. Baldick, "Not everything is dark and gloomy: Power grid protections against IoT demand attacks," in *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA: USENIX Association, Aug. 2019, pp. 1115–1132. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/huang

[4] T. Shekari, A. A. Cardenas, and R. Beyah, "MaDIoT 2.0: Modern High-Wattage IoT botnet attacks and defenses," in *31st USENIX Security Symposium (USENIX Security 22)*. Boston, MA: USENIX Association, Aug. 2022, pp. 3539–3556. [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/shekari

[5] "eFORT Project," 2022. [Online]. Available: https://efort-project.eu/

[6] Iberdrola, "Puntos de Recarga para Coches Eléctricos." [Online]. Available: https://www.iberdrola.es/smart-mobility/puntos-de-recarga

[7] M. W. Commons. (2021) Iec 62196-2 type 2 (plug). [Online]. Available: https://commons.wikimedia.org/wiki/File:IEC_62196-2_Type_2_(plug).svg

[8] I. 61851-1:2023, "Electric vehicle conductive charging system," International Electrotechnical Commission, Geneva, CH, Standard, Feb. 2023.

[9] M. Hubinský, "EVSE - Charging of electric vehicles," Sep. 2023. [Online]. Available: https://www.elso.sk/en/blog/technologies/evse-charging-of-electric-vehicles

[10] I. 15118-1:2019, "Road vehicles - Vehicle to grid communication interface," International Organization for Standardization, Geneva, CH, Standard, 04 2019.

[11] M. W. Commons. (2021) Iec 62196 type 2 (m, dc, ccs combo 2). [Online]. Available: https://commons.wikimedia.org/wiki/File:IEC_62196_Type_2_(M,_DC,_CCS_Combo_2).svg