Cristina Alcaraz and Jesus Cumplido and Alicia Trivio, "Monitorizacin Segura en Infraestructuras de Carga de Vehculos Elctricos Frente a Ciber-Ataques", *Actas del XII International Greencities Congress, Greencities, Inteligencia y Sostenibilidad Urbana, & S-Moving, Movilidad Inteligente y Sostenible*, 2021.
NICS Lab. Publications: https://www.nics.uma.es/publications

Monitorización Segura en Infraestructuras de Carga de Vehículos Eléctricos Frente a Ciber-Ataques

Cristina Alcaraz[1,2], Jesús Cumplido[2], Alicia Triviño[3]
[1]ITIS Software, Edificio de Investigación Ada Byron,
C/ Arquitecto Francisco Peñalosa 18, 29071, Málaga, España
[2]Departmento de Ciencias de la Computación, Universidad de Málaga,
Campus de Teatinos s/n, 29071, Málaga, Spain
[3]Departmento de Ingeniería Eléctrica, Universidad de Málaga,
C/ Doctor Ortiz Ramos s/n, 29071, Málaga, España

{alcaraz, cumplido}@lcc.uma.es, atc@uma.es

Resumen

Para alcanzar los objetivos de reducción de emisiones contaminantes, se está fomentando en la actualidad la inclusión de nuevas técnicas de generación, producción y consumo de energía renovable junto con el despliegue eficaz de nuevas técnicas en las redes eléctricas inteligentes. Entre estas técnicas, nos encontramos con la gestión de Vehículos Eléctricos (VE) e infraestructuras de Puntos de Carga (PC), que impulsan la movilidad sostenible y actúan como cargas controlables o como generadores potenciales. Aunque existe mucho interés por desplegar estos tipos de infraestructuras debido a los motivos anteriores, éstas son muy susceptibles a múltiples tipos de amenazas, especialmente las infraestructuras de PC al ser sistemas que se despliegan en zonas abiertas y accesibles por el público en general, lo que conlleva a diversos riesgos de seguridad. En la literatura, ya hay varios estudios realizados que demuestran cómo las infraestructuras de carga y sus modos de control pueden ser susceptibles a múltiples tipos de ataques, la mayoría de ellos causados por el modo de configuración y el despliegue de los PC y sus infraestructuras de comunicación para el control.

Dado este escenario, este artículo presenta los objetivos de "*Urban Lab II*", un proyecto de la Universidad de Málaga (UMA) que aborda todos estos problemas de seguridad, teniendo en cuenta los beneficios que las nuevas tecnologías de información pueden aportar para anticipar anomalías o el mal uso de los recursos. Dentro de este proyecto, se han identificado como dos amenazas relevantes relacionadas con las infraestructuras de carga, que son: (i) sobrecalentamiento de componentes por alteraciones maliciosas en los flujos de potencia y (ii) robo de energía y fraude económico. Para hacer frente a estas amenazas, el presente artículo también identifica, por un lado, los requisitos de seguridad más representativos que prevengan estas dos amenazas. Además, se completa este estudio detallando las tecnologías habilitadoras que faciliten no solo la gestión y la monitorización eficiente de la energía, sino los objetivos primordiales de estos desafíos de seguridad.

Abstract

In order to achieve the objectives of reducing polluting emissions, the inclusion of new techniques for the generation, production and consumption of renewable energy is currently being promoted, together with the efficient deployment of new techniques in smart grids. Among these techniques are Electric Vehicle (EV) management and Charging Point (CP) infrastructures, which drive sustainable mobility and act as controllable loads or potential generators. Although there is a lot of interest in deploying these types of infrastructures due to the above reasons, they are very susceptible to multiple types of threats, especially CP infrastructures as they are systems that are deployed in open areas and accessible by the

public, leading to various security risks. In the literature, there are already several studies that show how CP infrastructures, and their control modes can be susceptible to multiple types of attacks, most of them caused by the deployment and configuration mode of the CPs and their communication infrastructures for control.

Given this scenario, this article presents the objectives of "Urban Lab II", a project of the University of Malaga (UMA) that addresses all these security problems, considering the benefits that new information technologies can bring to anticipate anomalies or misuse of resources. Within this project, two relevant threats related to charging infrastructures have been identified as being: (i) overheating of components due to malicious alterations in power flows and (ii) energy theft and economic fraud. To address these threats, this article also identifies, on the one hand, the most representative security requirements to prevent these two threats. Moreover, it completes this study by detailing the enabling technologies that facilitate not only efficient energy management and monitoring, but also the primary targets of these security challenges.

Palabras clave: Puntos de Carga, Amenazas, Blockchain, Consciencia Situacional, Aprendizaje Automático

Keywords: Charging Points, Threats, Blockchain, Situational Awareness, Machine Learning

Área temática: *Infraestructuras y soluciones tecnológicas sostenibles*

1. Introducción

La Unión Europea se ha marcado el objetivo de reducir para 2050 las emisiones de efecto invernadero en un 80- 95% en relación a las producidas en 1990 (Horowitz, 2015). Para alcanzar este objetivo, se fijan dos estrategias fundamentales. Por un lado, se reduce la actividad de las centrales eléctricas más contaminantes, dando lugar a nuevas técnicas de generación eléctrica basadas en energías renovables que se encuentran a su vez más cercanas a los centros de consumo (la denominada generación distribuida). Por otro lado, considerando que el sector transporte es responsable de casi un 30% de las emisiones tanto en Estados Unidos como en Europa, se impulsa la penetración del Vehículo Eléctrico (VE), que es menos contaminante pero cuya carga puede representar un impacto en la red eléctrica considerable si no son controladas con técnicas como la gestión de demanda. Tanto las fuentes de energías renovables como los VE se complementan en las redes eléctricas inteligentes o Smart Grids, donde la integración de fuentes de energías renovables se beneficia de los VE como carga para las situaciones de exceso de energía sustraída. También, en las operaciones V2G (Vehicle-to-Grid), los VE se emplean como generadores móviles con tiempo de inercia prácticamente nulos descargando sus baterías y apoyando a la red eléctrica cuando existe una escasez de energía procedentes de otras fuentes (Triviño, Aguado, & Torre, 2019). Estos son unos de los grandes motivos que han impulsado el crecimiento de las infraestructuras de carga y su correspondiente demanda, existiendo ya un despliegue significativo de nuevas infraestructuras públicas de Puntos de Carga (PC) para fomentar el uso del VE (Engel, Hensley, Knupfer, & Sahdev, 2018). En la Figura 1 se puede observar la evolución del número de infraestructuras de recarga de acceso público en España (Observatory, 2021).

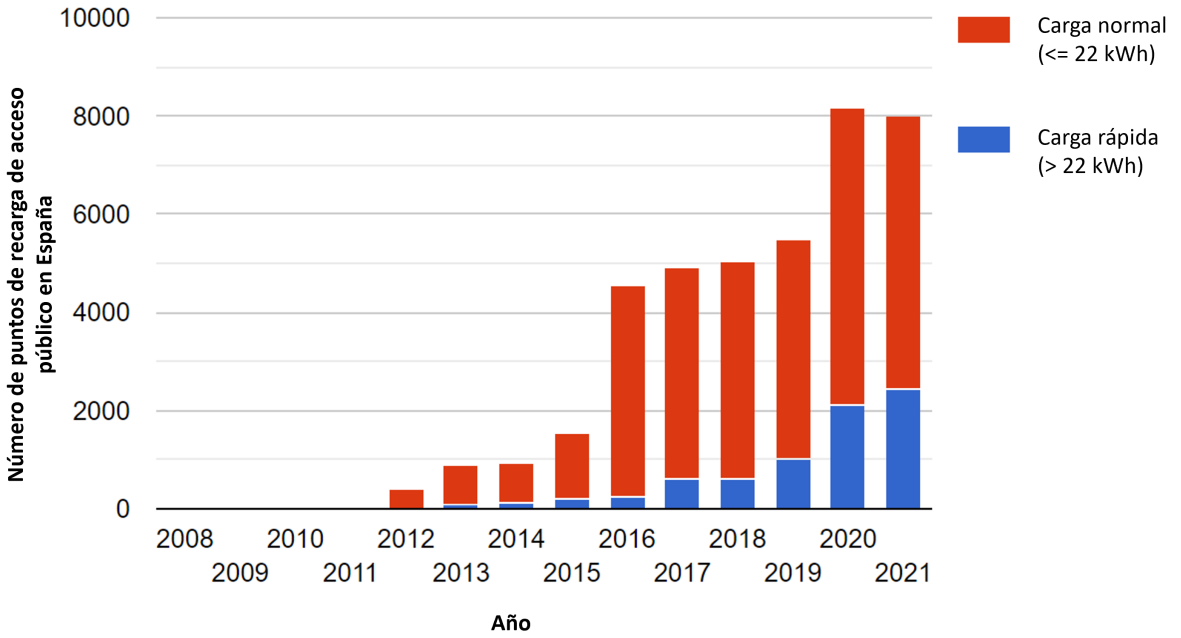

Figura 1. Evolución del número de PC de VE de acceso público en España (fuente: (Observatory, 2021)

Estas infraestructuras de carga están integradas mayoritariamente con la red eléctrica. Estas redes se componen de recursos eléctricos y de un control avanzado basados en Tecnologías de Información (TI) (Vaccaro, Pisica, Lia, & Zobaa, 2019). Se implementan con ello, tareas típicas de un sistema de potencia como el control de tensión o de frecuencia y otras adicionales como: el control de carga/componentes. Las TI deben monitorizar, controlar y gestionar eficientemente una infraestructura avanzada (compuesta por sensores, actuadores y contadores eléctricos, los bien conocidos *smart meters*) y que se apoye en algoritmos avanzados para la decisión sobre cómo actuar con los activos eléctricos, entre los que se encuentran las plataformas de carga de VE. Estos algoritmos requieren información como son el estado de la generación distribuida (fuentes de energías renovables cercanas a los puntos de consumo), los estados de algunas cargas, estimaciones de carga o generación, entre otros. Para el control, es necesario un intercambio seguro de datos sobre el estado de los activos de la entera red eléctrica (Gunduz & Das, 2020). De hecho, un requisito a cumplir en estos sistemas de información es proporcionar una comunicación segura y fiable entre los componentes para su control centralizado o distribuido con algoritmos eficientes que reduzcan los retardos de las comunicaciones y los recursos computacionales en los que se apoyan. En este sentido, las infraestructuras de carga de VE también deben satisfacer estos requisitos para permitir la confluencia entre tecnologías (Tecnologías Operativas (TO) y TI), de manera que se pueda efectuar un control y mantenimiento eficiente de la energía (Pratt, 2019).

Debido a que los PC cuentan tanto con componentes eléctricos como con sistemas de comunicación, estas infraestructuras se encuentran, por lo tanto, sujetas a las mismas amenazas que los tradicionales sistemas ciberfísicos, cuyas amenazas se extienden al dominio físico y al cibernético. Además, las amenazas en este sistema podrían ocasionar consecuencias severas y críticas, poniendo en riesgo la reputación, confianza y economía de una organización, e incluso, la seguridad y el bienestar de los ciudadanos (Reeh, y otros, 2019). Según el informe elaborado por IBM Security, las plataformas de control industrial estuvieron asociadas a un 20% más de vulnerabilidades en 2020 que en el año anterior (IBM

Security, 2021). Es por ello, que estos sistemas ciberfísicos son objeto de estudio e investigación debido a los nuevos problemas de seguridad que ocasionan.

Existe ya una taxonomía propuesta por la ENISA (*European Union Agency for Cybersecurity*) (Marinos, 2013) para clasificar los ataques físicos y cibernéticos aplicables a activos de una Smart Grid. En el presente trabajo, extendemos esta taxonomía para incluir dos amenazas específicas contra al buen uso de los recursos energéticos y centradas en los PC. En particular, añadimos un estudio sobre amenazas que tengan por objeto (i) el sobrecalentamiento de componentes al alterar deliberadamente el flujo de potencia y (ii) el robo de energía y fraude económico. Ambas amenazas se ilustran en la Figura 2. Para hacer frente a estas amenazas, el presente artículo también identifica, por un lado, los requisitos de seguridad más representativos que prevengan estas dos amenazas, y, por otro lado, las tecnologías habilitadoras que faciliten no solo la gestión y la monitorización eficiente de la energía, sino los objetivos primordiales de estos desafíos de seguridad.

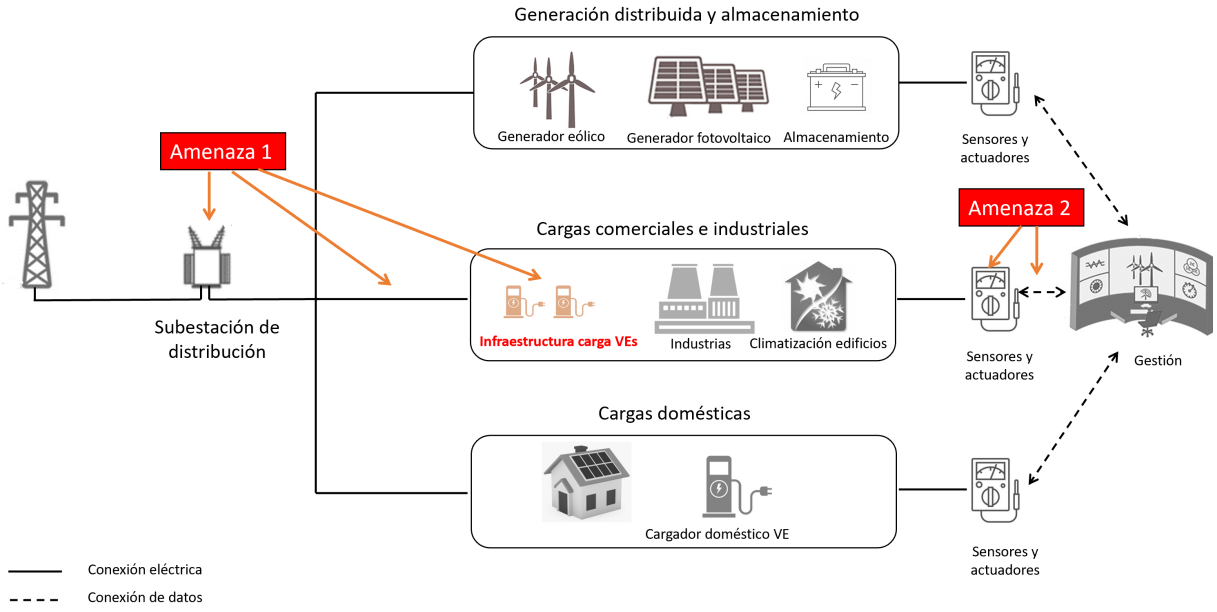

Figura 2. Esquema simplificado para representar las amenazas consideradas en el presente estudio dentro de la red de distribución de una Smart Grid.

El resto del artículo se estructura tal y como sigue. En primer lugar, se muestran los objetivos generales de este artículo en la Sección 2. A continuación, en la Sección 3, se detalla el caso de estudio analizado en este trabajo para, posteriormente, realizar el análisis e identificación de los dos tipos de amenazas asociadas a los componentes energéticos de este tipo de infraestructura en la Sección 4. En la Sección 5, se describen los desafíos de seguridad que presentan y las tecnologías habilitadoras para hacer frente a las amenazas anteriores. Por último, la Sección 6 explica las principales conclusiones de este trabajo.

2. Objetivos

A continuación, se lista los objetivos generales de este artículo que se encuentran enfocados en la ciberseguridad de las infraestructuras de carga:

- Estudio detallado de dos amenazas en infraestructuras de carga y centradas en: (1) sobrecalentamiento de recursos energéticos y (2) robo de energía y fraude económico
- Identificación de los desafíos y requisitos de seguridad necesarios en infraestructuras de carga
- Identificación de las tecnologías habilitadoras para una gestión y monitorización segura y eficiente de la energía en infraestructuras de carga

3. Caso de estudio

En este artículo, se ha realizado un estudio del estado del arte sobre las características de seguridad en una infraestructura de puntos de carga, donde se ha identificado dos amenazas potenciales y que, a partir de ellas, se ha extraído un conjunto de desafíos y requisitos de seguridad. Para el estudio de estos requisitos, se ha tenido en cuenta las visiones de expertos europeos en el campo de la seguridad de sistemas críticos y, en especial, en el campo de la cadena de suministro dado que comparte ciertas características con una infraestructura de carga. Dicha infraestructura pone a disposición recursos energéticos esenciales producidos y distribuidos por toda una red eléctrica, y cuya distribución es parte gracias por las infraestructuras de carga.

4. Amenazas en infraestructuras basadas en puntos de carga

Para comenzar, la mayoría de los PC se desarrollan en entornos abiertos y con una alta exposición al público. Esto facilita el acceso y la interacción por parte del atacante a liderar subsecuentes vectores de ataques (Shahriar Saadat, 2020). Uno de ellos puede ser los típicos ataques físicos, que incluye desde sabotajes contra el funcionamiento de los PC y sus componentes, lo que conlleva consecuentemente a pérdidas de control, falta de suministro o la exposición deliberada de datos críticos (Lopez, Huerta, & Sargolzaei, 2015), a robo de componentes o datos. Por otro lado, los atacantes pueden también preparar acciones más sofisticadas tanto en el PC como en sus comunicaciones, con el objetivo de acceder al sistema para robar información, manipular recursos o denegar el acceso o el servicio a los PC (Reeh, y otros, 2019). En los artículos (Alcaraz, Lopez, & Wolthusen, 2017) y (Shahriar Saadat, 2020) se muestran diferentes escenarios de ataques llevados a cabo por las vulnerabilidades en las propias comunicaciones y sus protocolos, como puede ser el protocolo *Open Charge Point Protocol* (OCPP), especializado en la comunicación entre el sistema de control y los PC.

Para resumir el alcance de los problemas de seguridad en estos tipos de infraestructuras, se ha considerado las amenazas presentadas en la taxonomía dada por la agencia ENISA en (Marinos, 2013). La taxonomía propuesta, ilustrada también en la **Tabla 1**, clasifica las amenazas de acuerdo con el dominio o capa donde se producen los vectores de ataque, que pueden ser en la capa física, cibernética o en ambas.

Tabla 1. Amenazas en infraestructuras de PC (Marinos, 2013)

Dominio	Amenaza	Impacto
Físico	Desastres naturales	Pérdidas de energía y daños físicos, denegación de servicio
	Vandalismo, golpes, robo de equipos	Pérdidas de energía y daños físicos, robo de información, denegación de servicio
	Cortes de luz	Apagones (denegación de servicio)
Cibernético	Denegación de servicio	Falta de suministro de energía

	Inyección de programas maliciosos	Manipulación, comando y control, desconfiguración, fraude económico, denegación de servicio
	Man-in-the-Middle (MitM), espionaje, hijacking	Robo de información o configuraciones, escuchas ilícitas, FDI, denegación de servicio
Físico / Cibernético	Fallos, mal funcionamiento	Desconfiguración, denegación de servicio
	Acceso no autorizado	Robo de información o configuraciones, escuchas ilícitas, FDI, denegación de servicio
	Inyección de datos falsos (FDI)	Manipulación, desconfiguración, fraude económico

Sin embargo, esta taxonomía deja fuera algunos otros ataques también relevantes en los ecosistemas de carga, cuyas consecuencias van más directamente al uso real del consumo de energía como son, por ejemplo, el robo de energía, la desestabilización y el sobrecalentamiento de recursos energéticos (ej. transformadores, líneas eléctricas, convertidores de potencia, baterías de apoyo o baterías de VE). Por tanto, este artículo identifica y presenta dos nuevas amenazas potenciales que se deben tener en cuenta en el futuro y complementan la taxonomía dada en (Marinos, 2013):

1. ***Amenaza 1***: sobrecalentamientos de recursos energéticos.
2. ***Amenaza 2*****:** robo de energía y fraude económico, con impacto directo en el usuario final.

A continuación, se explica en detalle estas dos amenazas, definiendo sus posibles vectores de ataque, así como las consecuencias y riesgos que conllevarían en el sistema, para posteriormente, en la siguiente sección, mostrar los principales requisitos de seguridad junto con las tecnologías habilitadoras que lograrían ayudar a paliar ambas amenazas.

4.1. Amenaza 1: sobrecalentamientos de recursos energéticos

La primera amenaza muestra cómo los atacantes alteran los flujos de potencia para arremeter contra los recursos energéticos para así desestabilizar la generación y modificar el consumo del usuario final. En este caso, adversarios avanzados pueden preparar diversos vectores de ataques ejecutados y sincronizados en diversos PC conectados a la misma subestación de energía y en horas punta (intervalo de mayor demanda en la conexión a la red eléctrica) con la intención de revertir la energía y ocasionar significantes apagones a nivel local o destrucciones en VE.

En la Figura 3, se ilustran dos vectores de ataque que pueden ser ejecutados para comprometer diferentes PC y, posteriormente, realizar acciones maliciosas a través de ellas:

1. La primera forma de comprometer los PC es a través de la manipulación de manera física y controlar así diferentes PC de manera estratégica y coordinada para, posteriormente, inyectar en estos dispositivos comprometidos datos falsos (del inglés, False Data Injection (FDI)) o ejecutar comandos de control (del inglés, Command and Control (C&C)) con el objetivo de desestabilizar los recursos energéticos y sobrecalentar los dispositivos energéticos, como los generadores locales (en PC alimentados con fuentes de energía renovable, por ejemplo) o transformadores de la red de distribución. Atacantes pueden inyectar datos falsos o controlar remotamente diferentes componentes software/hardware de un PC, como sensores, controladores o clientes OCPP (que se encargan de recibir operaciones y enviar la información energética al servidor OCPP, situado en el sistema de control).

Por ejemplo, si un atacante inserta datos falsos en alguno de estos componentes y logra disminuir los valores reales de potencias consumidas en los cargadores de un PC, esto provocaría que el sistema de control analice y monitorice una demanda de energía total menor a la real y, por tanto, asuma que puede servir mayor energía. Este aumento puede no ser apropiado y podría desestabilizar el estado general de la red. Esta desestabilización puede impactar, a largo plazo, en los dispositivos energéticos de los PC, que, por una mala gestión, son sobrecalentados y empiezan a mostrar un funcionamiento incorrecto con errores en el sistema.

2. Otra forma de comprometer el sistema es inyectar un malware en diferentes PC de forma cautelosa para que, de manera sincronizada y en horas pico de demanda, se tome el control de los PC y sus controladores a fin de ejecutar posteriormente acciones que cambien el flujo natural de la potencia, bien hacia la red eléctrica o hacia los VE, sobrecargando sus recursos, provocando con ello la interrupción del suministro de energía.

   Por ejemplo, si se compromete un controlador de carga de un conector (en inglés, EV Charge Control (EVCC)), encargado principalmente de establecer la intensidad (en Amperios) a la que se carga un determinado VE según el tipo de EVCC, y el atacante logra incrementar la potencia de este conector, esto podría sobrecalentar y dañar los componentes de carga de los VE, debido a que seguramente no soporten el nivel de intensidad de carga, e incluso, saturar también las líneas eléctricas y recursos energéticos provocando interrupciones del suministro eléctrico, debido a que los componentes de la red de distribución afectados no son capaces de soportar la actual demanda de energía (más alta de lo habitual), sobre todo, si el ataque es realizado en horas pico.

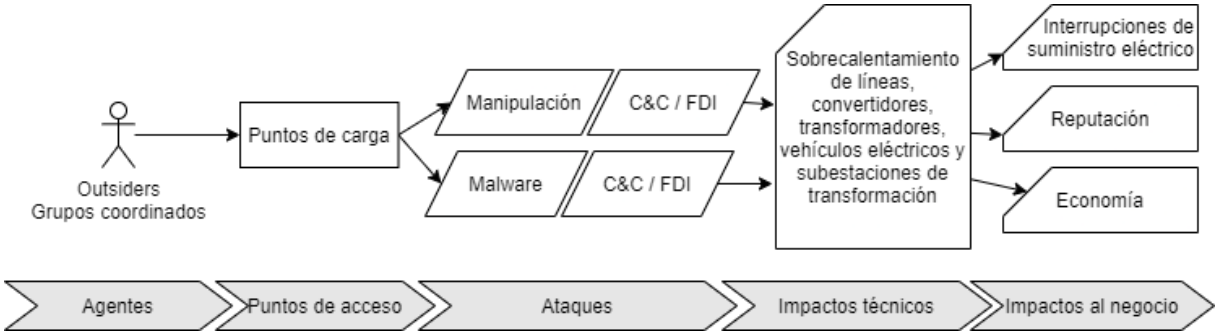

Figura 3. Vectores de ataque de la amenaza 1

4.2. Amenaza 2: robo de energía y fraude económico en los puntos de carga

La segunda amenaza consiste en mentir sobre el consumo total de energía tras la finalización de una transacción de carga, con el objeto de pagar menos (o no pagar) la energía realmente consumida. Los PC cuentan con contadores inteligentes que computan de forma lógica la cantidad de potencia consumida. En sistemas avanzados estos contadores actúan como sensores y actuadores, para controlar la carga (véase Figura 1). La información medida por los sensores se envía al *backend* del sistema de control, que se encarga de reenviar el consumo a las infraestructuras correspondientes para la gestión del pago. Esta información puede ser manipulada de diferentes formas, bien modificando las salidas del consumo real de los contadores al sistema de control, suplantando la identidad de otra persona, o robando energía de conectores físicamente comprometidos. Estos tipos de ataques son normalmente llevados a cabo por adversarios avanzados, que, con un fin económico, pretendan robar energía de los PC para recargar las baterías de sus VE.

En la Figura 4, se ilustran cuatro posibles vectores de ataque donde los usuarios pueden llegar a modificar el resultado del consumo total de energía, el método de pago o usar los conectores de forma no autorizada. Estos cuatro vectores dependen principalmente del punto de acceso comprometido y pueden derivar en la amenaza anterior, con la desestabilización de la red energética.

1. El primer vector de ataque se sitúa en el sistema de autenticación, donde un atacante podría aprovechar una vulnerabilidad de este sistema y suplantar la identidad (ID) de otro usuario, bien robando la ID de la víctima o creando una cuenta falsa usando datos personales y financieros de otra persona. Esto permite al atacante el robo de energía y causar fraude económico, si el sistema reconoce a la víctima como el único responsable de la transacción de carga y, por tanto, del pago del consumo total de energía. Este vector de ataque repercute tanto en la reputación de la organización como en la confianza de los usuarios afectados.
2. Otra forma de fraude económico es a través de los contadores eléctricos, situados en los PC, con el fin de alterar intencionadamente sus salidas (ej. dejar el valor de consumo kWh al valor anterior antes del consumo), o bien, inyectarles valores incorrectos antes de ser enviados al sistema de control, ya sea para fines de monitorización o pago. Este vector de ataque se basa, entonces, en la manipulación física de los contadores para, posteriormente, alterar el resultado final del consumo de energía de un usuario y enviar al sistema central una cantidad errónea de energía total consumida.
3. Las tomas de conexión eléctricas del PC pueden ser manipuladas físicamente y abusar de ellas con el objetivo de robar energía. Este vector de ataque permite al atacante el uso no autorizado de los PC y, por tanto, la carga e, incluso, la descarga de las baterías de sus VE.
   Por ejemplo, en un escenario donde los conectores son activados ante una previa autenticación en el sistema y evitar así posibles fraudes, un atacante podría manipular o inyectar un malware en los EVCC para alterar su funcionamiento y lograr así activar o desactivar un determinado conector de los PC tanto de forma remota, a través de mensajes maliciosos de comando y control (ataques C&C), o bien, de forma física, a través de una manipulación física del dispositivo EVCC, encargado de activar y establecer la potencia de carga del conector.
4. Por último, las comunicaciones (ej. las transacciones OCPP) son otro foco de posibles ataques de fraude, donde el atacante puede modificar el valor del consumo real que se envía desde el PC al sistema de control. Este vector de ataque no tiene la necesidad de comprometer de forma física los PC, sino que, a través de diferentes técnicas, el atacante logra comprometer y acceder a la red de comunicación del sistema. Es cierto, que en la última versión de OCPP, versión 2.01, se han incorporado nuevas medidas de seguridad como son actualizaciones de firmware, registro de seguridad, notificación de eventos, perfiles de seguridad para la autenticación y, sobre todo, el uso de certificados TLS. Sin embargo, en (Alcaraz, Lopez, & Wolthusen, 2017) se demuestra como el protocolo OCPP sobre TLS sigue siendo susceptible a amenazas MitM, permitiendo a atacantes liderar acciones maliciosas como, por ejemplo, eliminar y modificar los paquetes asociados a la facturación y el consumo procedentes de un PC, evitando así que el sistema de control proceda a facturar al usuario correspondiente el pago real del consumo de energía.

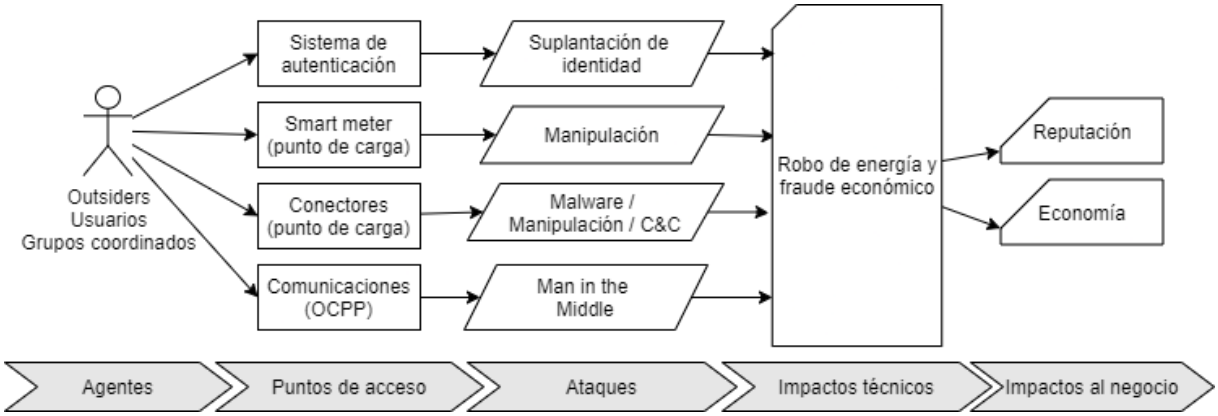

Figura 4. Vectores de ataque de la amenaza 2

5. Requisitos de seguridad y tecnologías habilitadoras

Para hacer frente a los problemas de seguridad comentados en la sección anterior, es necesario identificar los principales requisitos de seguridad que deben ser tenidos en cuenta en el futuro, y, aprovechar la tendencia actual de las TI para identificar las tecnologías habilitadoras que sirvan de soporte a dicha seguridad. Ambos aspectos son abordados en mayor detalle en las dos siguientes subsecciones.

5.1. Requisitos de seguridad en infraestructuras de carga

Para abordar los nuevos frentes, y en especial las amenazas definidas en las Secciones 4.1 y 0, se tendrá en cuenta los análisis hechos en (Fischer-Hübner, y otros, 2021), en el que se incluyen los principales retos de investigación más comunes en los sectores críticos, entre ellos, la cadena de suministro. En este caso, asociamos la infraestructura de carga como un elemento más de la propia cadena de suministro de energía, ya que es un elemento clave para la distribución de recursos al usuario final. Para complementar el estudio, se añaden, además, otras medidas relevantes para la monitorización segura, resultando en la siguiente lista de Requisitos de Seguridad (RS):

- ***Defensa en profundidad y "security-by-design"*** **[RS1]:** como cualquier infraestructura crítica, la defensa en profundidad se convierte en un requisito prioritario, en el que se debe abordar los servicios de seguridad mínimos como es la protección de los datos mediante la criptografía y el control de acceso siguiendo la política del mínimo privilegio. Sin embargo, este tipo de protección se debe extender para incluir marcos regulatorios y mecanismos que faciliten la prevención, detección y resiliencia de sistemas TI y TO en tiempo real, los cuales deben ser integrados siguiendo los principios de "seguridad por diseño" y de acuerdo a las existentes complejidades e interacciones de una infraestructura de carga.
- ***Control de acceso dinámico*** **[RS2]:** cualquier infraestructura de carga, ya sea local o federada, debe adaptar mecanismos de control acceso automatizados que favorezcan la gestión automática de identidades y permitan reformular políticas de acceso de acuerdo a un conjunto de factores (Alcaraz, Lopez, & Wolthusen, 2016): el tipo de usuario y sus permisos, el grado de abuso en la infraestructura de carga (ej. abusos en EVCC o de ID robado - ver Secciones 4.1 y 4.2) y las condiciones del contexto (ej. el estado real de los recursos y las subestaciones).
- ***Evaluación dinámica de riesgos*** **[RS3]:** la tendencia actual de interconectar sistemas TI con sistemas TO conlleva a múltiples conexiones y dependencias en componentes hardware y software, creando ecosistemas de carga cada vez más complejos, donde se suman diversas infraestructuras (la de monitorización, la de carga

y de VE). Es por ello, que se hace necesario crear soluciones inteligentes que sean capaces de gestionar de manera automática la salud de los activos TI/TO y computar los riesgos de forma dinámica.

- ***Prevención y resiliencia dinámica*** **[RS4]:** como se ha mencionado, cualquier infraestructura de carga debe estar basada de servicios de seguridad ligeros (en términos de computación y de almacenamiento) que garanticen medidas preventivas, reactivas y correctivas. Sin embargo, ofrecer tales medidas en tiempo lineales requieren de una mayor investigación, ya que las complejidades del entorno hacen difícil desplegar este tipo de soluciones, especialmente las reactivas y las correctivas (Alcaraz & Wolthusen, 2014). Además de esto, no podemos olvidar que existe aún el hándicap adicional de que las industrias todavía no confían en la automatización de las respuestas, especialmente en la parte del control.
- ***Monitorización y conciencia situacional*** **[RS5]:** ya en el estándar NISTIR 7628 (Lee & Brewer, 2010) se estableció que la monitorización y la conciencia situacional de área amplia debían considerarse como un requisito primordial para la protección de infraestructuras que componen una red eléctrica inteligente incluyendo las infraestructuras de carga (Alcaraz & Lopez, 2013). Once años después sigue siendo una condición prioritaria (McCarthy, y otros, 2019). Para dar soporte a la conciencia situacional, el sistema debe soportar mecanismos avanzados de predicción y de detección para monitorizar eventos anómalos dentro de un determinado contexto, y localizar y trazar la secuencia para mostrar el avance y la secuencia de la amenaza.
- **Auditoría y responsabilidad [RS6]:** más allá de la conciencia situacional, la gestión de controles, la especificación de políticas de seguridad y la harmonización de interacciones siguiendo los actuales estándares (ej. NIST 7628, IEC-62351), es también fundamental dotar al sistema de medidas que expliquen de primera mano la ocurrencia de eventos en los dominios de carga, indicando qué ha ocurrido, dónde (localización del PC, tipo de conector), cuándo, cómo y quién es el responsable. Por esta razón, es esencial también mantener un registro de hechos que evidencien dichas ocurrencias.

Tabla 2. Requisitos de seguridad para hacer frente a las amenazas 1 y 2

	[RS1]	**[RS2]**	**[RS3]**	**[RS4]**	**[RS5]**	**[RS6]**	**[RS7]**	**[RS8]**
Amenaza 1		X	X	X	X	X	X	X
Amenaza 2	X	X	X	X	X	X	X	X

La Tabla 2 ilustra cómo estas medidas pueden ayudar a prevenir las amenazas de tipo 1 y 2, destacando su viabilidad para todas ellas. Sin embargo, las características técnicas (en términos de procesamiento y almacenamiento) de muchos de los dispositivos desplegados en una infraestructura de carga, como son los controladores o los contadores inteligentes, hace complicado adaptar dichas soluciones de seguridad. Es por ello que es necesario investigar soluciones ligeras y/o desacopladas de las tareas operativas, de forma que garanticen seguridad, interoperabilidad y escalabilidad. Por esta razón, el proyecto "*Smart and Secure EV Urban Lab II*" pretende desplegar un laboratorio de experimentación, Urban Lab II, con el objeto de facilitar la investigación en el plano de la ciberseguridad industrial y extender los recursos de protección en los dominios de carga (Universidad de Málaga, 2021). El éxito de este laboratorio, a disposición de la comunidad científica del Smart Campus de la Universidad de Málaga, nos va a llevar a otros dos requisitos a abordar en el futuro:

- ***Diseño de soluciones de seguridad ligeras y precisas*** **[RS7]:** este requisito debe considerar las capacidades hardware y software de los elementos operacionales que

conforman el ecosistema de una infraestructura de carga, y probar dichas soluciones para comprobar el nivel de acoplamiento, precisión y eficiencia de las soluciones.

- ***Concienciación y educación*** **[RS8]**: para hacer frente a cualquier amenaza, es aconsejable definir planes de formación y concienciación para mostrar los riesgos que pueden traer los nuevos ecosistemas inteligentes y las consecuencias que conlleva un mal uso de los recursos de protección. Aprovechando el despliegue de Urban Lab II, será entonces posible extraer ejemplos claros que justifiquen estos objetivos, promoviendo formación, educación y concienciación. Si este proceso, además, se desarrolla dentro de una comunidad universitaria en donde se forman los futuros expertos en la materia, el buen uso y la protección de infraestructuras de carga estarán garantizados.

5.2. Tecnologías de soporte a la seguridad de infraestructuras de carga

Como se ha indicado en la sección anterior, la elección de las TI en estos tipos de entornos es clave para facilitar la gestión eficiente de la seguridad. Es por ello, que en esta sección se identifica las siguientes cuatro tecnologías habilitadoras que mejor se ajustan a los objetivos de los RS de la Sección 5.1:

- ***Inteligencia Artificial*** (IA): básicamente consiste en la combinación de un conjunto de algoritmos que favorecen la autonomía y la inteligencia de los servicios de seguridad, y, especialmente, aquellos relacionados con **[RS2-RS5]**. En este nivel destacamos los algoritmos de aprendizaje máquina, conocidos comúnmente como Machine-Learning (ML). A través de estos algoritmos es posible aprender de manera automática un determinado hecho, identificando o extrayendo patrones de comportamiento y prediciendo hechos futuros (Shaukat, Luo, Varadharajan, Hameed, & Xu, 2020). Dependiendo del algoritmo y del contexto, podemos desplegar sistemas de ML supervisados (con intervención humana), no supervisados (sin intervención) y semi-supervisados. La elección de uno u otro dependerá del grado de supervisión de los PC, el nivel de autonomía del sistema frente amenazas y del grado de precisión de la técnica.
- **Big Data** (BD): normalmente el volumen de datos esperados de un entorno como puede ser una infraestructura de carga y sus elementos de monitorización puede ser muy elevada, por lo que se puede requerir de técnicas específicas de BD para limpiar aquellos datos inválidos o redundantes, y una vez saneados, aplicar técnicas de ML para detectar o predecir situaciones anómalas (Saravanan & Prakash, 2021), lo que favorece principalmente a **[RS3-RS4]**.
- ***Distributed Ledger Technology*** (DLT): esta es una de las tecnologías más extendidas y aplicadas en escenarios que requieran de una mayor gestión distribuida de entidades independientes (Zhuang, Zamir, & Liang, 2020)(Zhuang, Zamir, & Liang, 2020). Ofrece un conjunto de servicios ideales para cubrir principalmente los servicios **[RS2-RS6]** como, por ejemplo: (i) el almacenamiento distribuido de datos - lo que favorece la redundancia de datos y su disponibilidad -; (ii) la inmutabilidad de datos frente amenazas que traten de ocultar un hecho ocasionado dentro de un sistema (ej. cambiar los ID de los registros para liderar la amenaza 2); y (iii) la transparencia necesaria para llevar a cabo acciones específicas como la trazabilidad, de lo que se benefician las tareas de control de acceso (ej. detectar abusos), monitorización, conciencia situacional, auditoría y responsabilidad. Dentro de la DLT, destacamos la red de blockchain, el cual es una tecnología ideal que ofrece un gran histórico inmutable que permite a otros sistemas a detectar, prevenir o mitigar un problema.
- ***Opinión Dinámica*** (OD) ***y agentes software***: consiste en desplegar un conjunto de agentes cooperando entre sí para alcanzar un objetivo común: (i) detectar y localizar desviaciones, y (ii) trazar en tiempo real el avance de una amenaza (Rubio, Roman,

Alcaraz, & Zhang, 2019). Para ello, cada agente software integrado dentro de un nodo debe ser capaz de detectar variaciones correspondientes a su estado de salud usando, por ejemplo, técnicas de ML, y en base a esta información, extraer un nivel de salud (por área) por compartir dicha información con el resto de los agentes de la vecindad. Dependiendo de cómo se gestione estos valores se puede calcular un indicador de salud global que caracterice en todo momento el estado de salud de toda la infraestructura de carga. Esta característica tan potencial, es útil para llevar a cabo las propuestas de trazabilidad correspondiente a la conciencia situacional, **[RS5]**.

La Tabla 3 recoge todo lo comentado, mostrando la utilidad del ML y de una red de blockchain para la mayoría de las soluciones de seguridad, aunque no tanto para la **[RS1]**. Esto se debe a que en **[RS1]** se pretende diseñar soluciones eficientes y ligeras, cuyo objetivo se desarrolla específicamente en **[RS7]**. También es importante subrayar la importancia de dar visibilidad a estas soluciones a través de la educación, ya que expertos en ciberseguridad industrial deben conocer de primera mano la utilidad de las actuales TI para garantizar un mínimo de seguridad.

Tabla 3. Relación de las tecnologías con los requisitos de seguridad

	[RS1]	[RS2]	[RS3]	[RS4]	[RS5]	[RS6]	[RS7]	[RS8]
IA y ML		X	X	X	X		X	X
BD			X	X		X	X	X
DLT – blockchain		X	X	X	X	X	X	X
OD y agentes SW					X		X	X

6. Conclusiones y líneas futuras

El despliegue real de una flota representativa de VE requiere de infraestructuras de carga para dar soporte a estos vehículos. Las infraestructuras de VE están integradas en la red eléctrica, sistema que está experimentando grandes cambios con controles más sofisticados y mayores carga en la red de distribución por la presencia de generación distribuida. La gestión de los activos de la red requiere de una monitorización y control adecuados, apoyados principalmente en la adquisición de datos sobre el estado de la red o de los elementos gestionados. En concreto, las infraestructuras de VE de acceso público son sistemas ciberfísicos, donde se integran elementos hardware (incluidos los eléctricos) y software, siendo susceptibles a ataques de seguridad. En el presente artículo identificamos dos amenazas destacadas que pueden sufrir este tipo de infraestructuras, para a continuación determinar los desafíos de seguridad de dichas amenazas y las tecnologías habilitadoras que permiten mejorar la monitorización y la gestión de los PC desde el plano de la seguridad.

Este estudio revela que la inclusión de técnicas habilitadoras es imprescindible para garantizar la correcta operación de las infraestructuras de carga, tanto en el plano energético como en el plano de los datos del sistema de información en el que se basan, y especialmente el ecosistema de carga tiende a ser complejo y altamente interconectado. Esta condición guiará las líneas futuras de diseño y desarrollo de las infraestructuras de carga de VE.

Agradecimientos

Financiado por el proyecto "*Smart and Secure EV Urban Lab II*", perteneciente al II Plan Propio Smart Campus de la Universidad de Málaga.

Referencias

Alcaraz, C., & Lopez, J. (2013). Wide-area situational awareness for critical infrastructure protection. *Computer, 46(4)*, 30-37.

Alcaraz, C., & Lopez, J. (2013). Wide-area situational awareness for critical infrastructure protection. *Computer, 46(4)*, 30-37.

Alcaraz, C., & Wolthusen, S. (2014). Recovery of structural controllability for control systems. *In International Conference on Critical Infrastructure Prottection* (págs. 47-63). Berlin, Heidelberg: Springer.

Alcaraz, C., Lopez, J., & Wolthusen, S. (2016). Policy enforcement system for secure interoperable control in distributed smart grid systems. *Journal of Network and Computer Applications, 59*, 301-314.

Alcaraz, C., Lopez, J., & Wolthusen, S. (2017). OCPP Protocol: Security threats and challenges. *IEEE Transactions on Smart Grid, 8(5)*, 2452-2459.

Comisión Europea. (11 de Junio de 2021). *Un Pacto Verde Europeo*. Obtenido de Comisión Europea: https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_es

Dileep, G. (2020). A survey on smart grid technologies and applications. *Renewable Energy, 146*, 2589-2625.

Engel, H., Hensley, R., Knupfer, S., & Sahdev, S. (2018). Charging ahead: Electric-vehicle infrastructure demand. *McKinsey Center For Future Mobility, 8*.

ENISA. (2015). *Communication network interdependencies in smart grid.*

Fischer-Hübner, S., Alcaraz, C., Ferreira, A., Fernandez-Gago, C., Lopez, J., Markatos, E., . . . Akill, M. (2021). Stakeholder perspectives and requirements on cybersecurity in Europe. *Journal of Information Security and Applications, 61, 102916*.

Gottumukkala, R., Merchant, R., Tauzin, A., Leon, K., Roce, A., & Darby, P. (2019). Cyber-physical system security of vehicle charging stations. *IEEE Green Technologies Conference* (págs. 1-5). IEEE.

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, 107094.

Horowitz, C. A. (2015). *Paris Agreement.* International Legal Materials.

IBM Security. (2021). *X-Force Threat Intelligence Index.*

Institute of Standards, National. (2012). Roadmap for smart grid interoperability standards, release 2.0. *NIST special publication 1108R2*, 1-225.

Lee, A., & Brewer, T. (2010). Guidelines for smart grid cyber security: Vol. 1, smart grid cyber security strategy, architecture, and high-level requirements. *NISTIR, 7628, 14*.

Lopez, C., Huerta, C., & Sargolzaei, A. (2015). Smart grid cyber security: an overview of threats and countermeasures. *Journal of Energy and Power Engineering, 9(7)*, 632-647.

Marinos, L. (2013). Smart Grit threat landscape and good practice guide. *White Paper, European Network and Information Security Agency (ENISA).* Attiki, Greece: ENISA.

McCarthy, J., Alexander, O., Edwards, S., Faatz, D., Peloquin, C., Symington, S., . . . Viani, K. (2019). Situational Awareness. *NIST Special Publication*, 7B-1800.

Mollah, M. B., Zhao, J., Niyato, D., Lam, K. Y., Zhang, X., Ghias, A. M., & Yang, L. (2020). Blockchain for future smart grid: A comprehensive survey. *IEEE Internet of Things Journal, 8(1)*, 18-43.

Musleh, A. S., Chen, G., & Dong, Z. Y. (2019). A survey on the detection algorithms for false data injection attacks in smart grids. *IEEE Transactions on Smart Grid, 11(3)*, 2218-2234.

Observatory, E. A. (2021). *Total number AF infrastructure* . Obtenido de https://eafo.eu/

Open Charge Alliance. (04 de 08 de 2021). *OCPP 2.0.1, Protocols, Home - Open Charge Alliance*. Obtenido de https://www.openchargealliance.org/protocols/ocpp-201/

Pratt, R. M. (2019). Vehicle Charging Infrastructure Security. *In 2019 IEEE International Conference on Consumer Electronics (ICCE)* (págs. 1-5). IEEE.

Reeh, D., Tapia, F. C., Chung, Y. W., Khaki, B., Chu, C., & Gadh, R. (2019). Vulnerability analysis and risk assessment of EV charging system under cyber-physical threats. *In 2019 IEEE Transportation Electrification Conference and Expo (ITEC)* (págs. 1-6). IEEE.

Rubio, J., Roman, R., Alcaraz, C., & Zhang, Y. (2019). Tracking apts in industrial ecosystems: A proof of concept. *Journal of Computer Security, 27(5)*, 521-546.

Saravanan, S., & Prakash, G. (2021). A Comprehensive Survey on Big Data Technology Based Cybersecurity Analytics Systems. *Applied Soft Computing and Communication Networks*, 123-143.

Shahriar Saadat, S. M. (2020). Electric Vehicle Charging Station Security. *5th IEEE Workshop on the Electronic Grid (eGRID)*, 1-8.

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. *IEEE Access, 8*, 222310-222354.

Triviño, A., Aguado, J. A., & Torre, S. d. (2019). Joint routing and scheduling for electric vehicles in smart grids with V2G. *Energy*, 113-122.

Universidad de Málaga. (15 de marzo de 2021). *Smart and Secure EV Urban II - Plan Propio de Smart-Campus*. Obtenido de https://eventos.uma.es/63025/detail/smart-and-secure-ev-urban-ii-plan-propio-de-smart-campus.html?private=1da34ddc2ebc057ac5b3

Vaccaro, A., Pisica, I., Lia, L., & Zobaa, A. F. (2019). A review of enabling methodologies for information processing in smart grids. *International Journal of Electrical Power & Energy Systems*, 516-522.

Wu, J., Ota, K., Dong, M., Li, J., & Wang, H. (2016). Big data analysis-based security situational awareness for smart grid. *IEEE Transactions on Big Data, 4(3)*, 408-417.

Zhuang, P., Zamir, T., & Liang, H. (2020). Blockchain for cibersecurity in smart grid: A comprehensive survey. *IEEE Transactions on Industrial Informatics, 17(1)*, 3-19.

Cesión de derechos

Por la presente, y como autor del trabajo mencionado arriba, cedo al Palacio de Ferias y Congresos de Málaga una licencia no-exclusiva irrevocable para imprimir, reproducir, distribuir, transmitir o comunicar de cualquier manera dicho trabajo, incluyendo el derecho de hacer modificaciones de formato. Además, afirmo que esta cesión no lesiona los derechos de terceros.