Article

Not peer-reviewed version

Securing Wireless Charging Ecosystems in Intelligent Transport Systems: An OCPP-Based Cybersecurity Impact Analysis

Zacharenia Garofalaki *, Dimitrios Kallergis *, Ioannis Voyiatzis, Christos Douligeris

Posted Date: 12 May 2026

doi: 10.20944/preprints202605.0706.v1

Keywords: Intelligent Transportation Systems (ITS); Advanced Wireless Power Transfer (WPT); cybersecurity; Open Charge Point Protocol (OCPP); Stochastic Petri nets (SPN); EV charging networks

 doi:10.20944/preprints202605.0706.v1

Article

Securing Wireless Charging Ecosystems in Intelligent Transport Systems: An OCPP-Based Cybersecurity Impact Analysis

Zacharenia Garofalaki [1,*], Dimitrios Kallergis [1,*], Ioannis Voyiatzis [1] and Christos Douligeris [2]

[1] University of West Attica, Ag. Spyridonos str., Aegaleo, 12243, Athens, Greece
[2] University of Piraeus, 80, M. Karaoli & A. Dimitriou str., 18534, Piraeus, Greece
* z.garofalaki@uniwa.gr (Z.G.); d.kallergis@uniwa.gr (D.K.)

Abstract

As Intelligent Transportation Systems (ITS) transition towards automated ecosystems, the deployment of advanced wireless charging technologies becomes a critical infrastructure requirement. Central to the management of these networks is the Open Charge Point Protocol (OCPP), which ensures interoperability across diverse hardware vendors. However, the reliance on digital communication for power transfer introduces significant cybersecurity vulnerabilities. This paper presents a methodology for evaluating the impact of cyber-threats on urban transport services, with a specific focus on the communication layers that support these Advanced Wireless Power Transfer (WPT) environments. Utilising Stochastic Petri net (SPN) ontology, we model the operational states of an Electric Vehicle (EV) service—including the activation and the arrival phases—to quantify how protocol-level vulnerabilities affect service reliability. We introduce an Extended Vulnerability List (EVL) and analyse two distinct scenarios: a public transport service and a weather forecasting integration. Our results demonstrate that as wireless charging moves towards standardization, the security of the OCPP-based backbone is a fundamental necessity for preventing service disruption. The proposed assessment framework provides a roadmap for securing the next generation of dynamic wireless charging infrastructures against evolving cyber-physical threats.

Keywords: Intelligent Transportation Systems (ITS); Advanced Wireless Power Transfer (WPT); cybersecurity; Open Charge Point Protocol (OCPP); Stochastic Petri Nets (SPN); EV charging networks

1. Introduction

In the framework of Intelligent Transport Systems (ITS), the integration of IoT-based solutions provides the architectural interoperability required to improve service availability and quality. These intelligent layers transform the ITS decision-support system by enabling real-time, secure data exchange between vehicles, infrastructure, and third-party stakeholders. While this data-driven approach accelerates the decision-making cycle, it fundamentally redefines the operational logic of ITS functions. By incorporating complex external variables and edge-computed data into the system, the original execution models of key services—most notably automated fleet management and traffic flow optimisation—are structurally altered to accommodate a more dynamic and interconnected operational environment.

The security of the fleet-management process is vital for the greater acceptance and development of an IoT-based transportation service. Because such a service incorporates many devices and applications, the overall security depends on the individual vulnerabilities of each hardware or software component within the service. When data from a third-party service is integrated, the third-party vulnerabilities also become security factors for the transportation service.

 doi:10.20944/preprints202605.0706.v1

Fleet management in an IoT-based transportation service also includes the important subprocess of fleet charging, when the fleet consists of smart electric vehicles (EVs). EVs are part of smart transportation and operate within the smart electrical infrastructures to which they connect, forming a complex system composed of a variety of entities and technologies [1–4]. Although security technologies have already been integrated into certain Vehicle-to-Infrastructure (V2I) systems [5–7], specific challenges of the EV charging infrastructure have not been adequately addressed.

The rapid expansion of Electric Vehicle (EV) infrastructure is being accelerated by global sustainability goals and supportive government policies. In the European context, this growth is driven by new legislative frameworks such as the EU AFIR [8] for the deployment of alternative fuel infrastructures, which require standardised communication and secure data exchange for all public charging points. Consequently, the transition towards advanced wireless charging within ITS must now comply with strict regulatory requirements for interoperability and resilience. Within this framework, the Open Charge Point Protocol (OCPP) has emerged as the primary standard.

OCPP stands out as the de facto protocol among the protocols used for the communication within an EV charging network, also known as Plug-in Electric Vehicle (PEV) network. The protocol is used in 148 countries, supported by more than 65,000 installed and operational charging stations [9]. More than 40 charger manufacturers have also been reported to incorporate OCPP into their products [10,11]. OCPP is supported by the global consortium of public and private EV-infrastructure leaders, the Open Charge Alliance (OCA), which consists of more than 220 member companies active in the field of electric mobility [12].

As the industry shifts towards the standardisation of Advanced Wireless Power Transfer (WPT) systems [13,14], the role of OCPP becomes even more critical. It serves as the primary communication backbone that ensures interoperability between various hardware vendors and charging infrastructures. However, this interoperability—while essential for the scaling of Intelligent Transportation Systems—also creates a broader unified attack surface by expanding the set of ITS vulnerabilities. Ensuring the security of the protocol is therefore not just a software requirement but a fundamental necessity for the safe and reliable deployment of automated wireless charging ecosystems. The recent development and release of the protocol indicate that the study of the level of OCPP security is ongoing [15,16]. Equally worthy of study is the level of security for an overlying ITS and the impact of the OCPP-based PEV network on the transport service.

Although OCPP 1.6 offered only basic security, the transition to OCPP 2.0.1 and the subsequent standardisation of IEC 63584:2024 [17] introduced mandatory security profiles that prioritise encrypted transport via TLS and certificate-based authentication. Although these architectural changes are designed to mitigate legacy threats, the slow industry adoption of 2.0.1 means that older high-impact vulnerabilities—such as those analysed in this paper—remain prevalent in current operational fleets. Analysing these *indicative* vulnerabilities provides a baseline for evaluating whether modern security profiles effectively close these persistent gaps.

The contributions of this paper regarding the security problem under study in the vehicle-fleet charging subprocess are summarised as follows:

(a) the modelling and security evaluation of the fleet-management process of the formerly proposed iBuC IoT-based transport service in two data-exchange scenarios, each involving a different third-party service;
(b) the description of the entities involved in the OCPP-based PEV network within the iBuC service;
(c) the presentation of the extended vulnerability list of the iBuC service considering the OCPP-based PEV network active components;
(d) the security evaluation of the proposed iBuC transport service on the basis of the extended vulnerability list.

The paper is structured as follows; in Section 2, related work on ITS and OCPP-based PEV network security issues is presented; in Section 3, the formerly proposed security assessment method is presented, as well as the modelling and security evaluation of the fleet-management process of

 doi:10.20944/preprints202605.0706.v1

the formerly proposed iBuC IoT-based transport service; in Section 4, the impact evaluation of the OCPP-based PEV network on the iBuC security is shown; in Section 5, the results of the OCPP-based PEV network impact evaluation on the iBuC security are further analysed. Finally, the conclusions and future research directions are presented in Section 6.

2. Related Work

Communication security in the transportation ecosystem is crucial. Recent studies attempt to identify critical security vulnerabilities in ITS [18–22]. The security issues of internal ITS processes, such as the ITS interconnection with third-party services, were noted to be of great importance [23–25]. The internal process of an ITS EV charging network was studied using a security risk assessment framework, in a high-level approach without focusing on the recorded vulnerabilities of the architectural components of ITS EV charging [26].

The modelling of an IoT-based service has to address the challenges of depicting the behaviour of distributed, heterogeneous, and interconnected nodes. Based on these grounds, the tool named Apparatus [27] was proposed for domain-specific modelling and security analysis of an IoT-based service, while a code generation framework using a respective modelling language, namely ThingML [28], provided the semantics for modelling the software components and enabled automatic code generation from the model. The Hierarchical Attack Representation Model (HARM) [29] was used to model an IoT-based network. The HARM assessment was based on the security metrics for the respective vulnerabilities, as they were provided by the National Vulnerability Database (NVD) [30]. This assessment was conducted for different time intervals and taking into account the mobility of the nodes. In [31], security metrics were classified into two categories, host-based and network-based. The former category was studied on the basis of the probability of attack success, while the latter category was studied on the basis of the proximity of the attacker to one or more assets.

A stochastic modelling approach was evaluated using Petri nets for the security analysis of an IoT-based service [32]. The Petri net ontology was used for the model of a well-known malware infection and the evaluation of a mitigation method [33]. Furthermore, the Petri net ontology was used to model the orchestrating mechanisms within IoT-based services [34]. Changes in IoT entities and the IoT environment were shown to be unable to fully rely on static modelling methods. In addition, operational representations of the IoT in meta-models were found to enable verification and simulation in various fields, such as cybersecurity [35].

OCPP was studied as the main communication protocol amongst the components of a PEV network, namely the Charging Station (CS), the Electric Vehicle Supply Equipment (EVSE) and the Charging Station Management System (CSMS) [7,36,37]. A more recent study identified the vulnerabilities of the OCPP and the main components of the PEV network [38,39]. In other cases, a mathematically orientated model was analysed on the basis of vulnerabilities in the components of the PEV network to produce a security metric [40]. However, the identification of all the vulnerabilities in an OCPP-based PEV network is still in progress mainly due to the spread of PEV networks. Moreover, the security evaluation of the OCPP-based PEV network is usually not focused on the impact of the network on the overlying ITS.

3. Modelling and Security Assessment Method

In [41], we applied a modelling and security assessment method in the fleet management of the Intelligent Transportation Service (ITS), namely the intelligent Bus on Campus (iBuC), which we previously proposed in [42], that facilitates electric vehicle transit between internal campus nodes and peripheral public transport interchanges. We studied the service in two scenarios, in each scenario, the integrated third-party IoT service was different. The fleet management process model for each scenario was based on the Stochastic Petri net (SPN) service model. The models were compared and contrasted in terms of states and transitions to provide a baseline indicator of how data flows shift between the two scenarios and how third-party IoT integration impacts the service life cycle.

 doi:10.20944/preprints202605.0706.v1

Moreover, in [41], we investigated how the IoT third-party service affects the service life-cycle. In this context, the SPN models of the two service scenarios were then used as the basis for the security assessment, leading to a numeric representation of the security level of each case, as another indicator of how data flows shift between the two scenarios.

The security assessment process resulted in the security metric of the service, based on the components participating in every state and the associated weaknesses, expressed by indicative vulnerabilities. The findings indicated that shifts in the service life cycle and security posture are directly associated with the incorporation of third-party IoT services.

The security assessment process included three phases; *(a)* Stochastic model of the service in each scenario and analysis of the models, *(b)* compilation of the vulnerability list of the iBuC service and identification of actors within the service, and *(c)* security assessment of each model.

In this work, the security assessment process will demonstrate the impact of the OCPP-compliant PEV charging infrastructure on the iBuC service.

3.1. Stochastic Modelling of the Service

The actors in the fleet management process of the iBuC service are: *(a)* the autonomous vehicle (AV) fleet; *(b)* the Control Unit (CU) of the service that gathers fleet data (e.g., the position, direction, and speed of the EV, the number of passengers on-board and pending service requests) and supports the decision-making process [43]; *(c)* the client application, which is accessible via smartphone devices and the web and offers a user interface to place and monitor itinerary requests; and *(d)* the third-party services.

The iBuC fleet management was implemented considering two scenarios: in the first scenario, the data from the Public Transportation System (PTS) was integrated, and in the second scenario, the data from a Weather Forecasting Service (WFS) was integrated.

The third-party data integration feature introduces events that cannot be fully and timely predicted. Nevertheless, the lack of a detailed time-sequence for events and the inherent complexity of an IoT service can be sufficiently depicted by employing the Stochastic Petri net (SPN) modelling method [44]. The SPN formalism allows for modelling the duration of activities and the delay between events by using tokens and the firing settings of the transitions [45,46]. Thus, the adoption of the SPN model can form the basis of the IoT service security assessment method [47] at the service design phase.

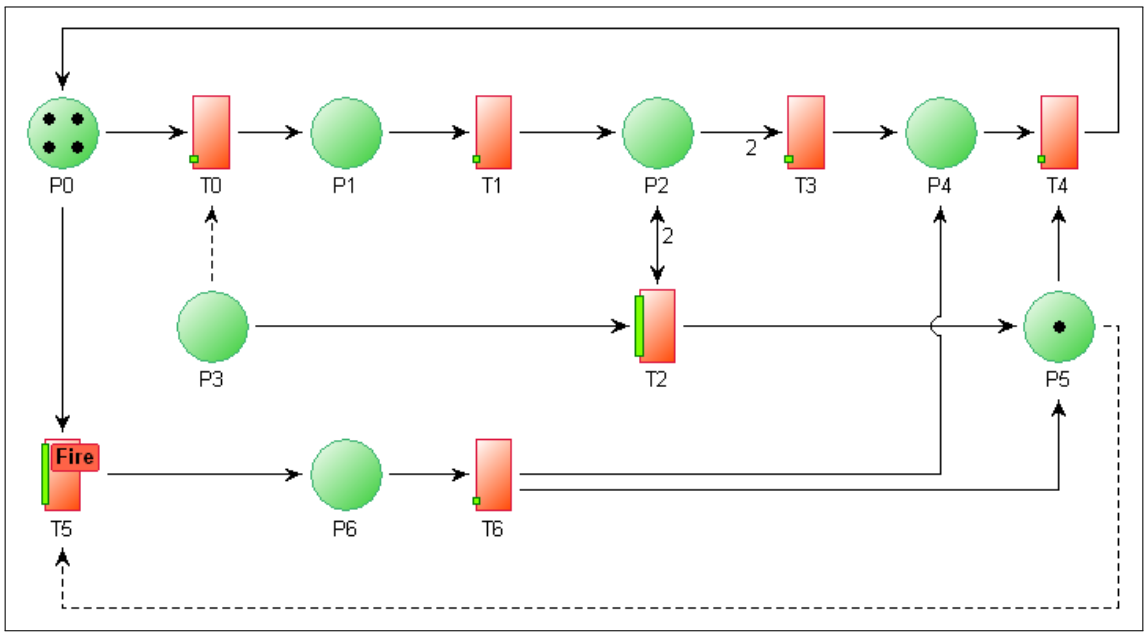

Figure 1. iBuC-PTS fleet management model

 doi:10.20944/preprints202605.0706.v1

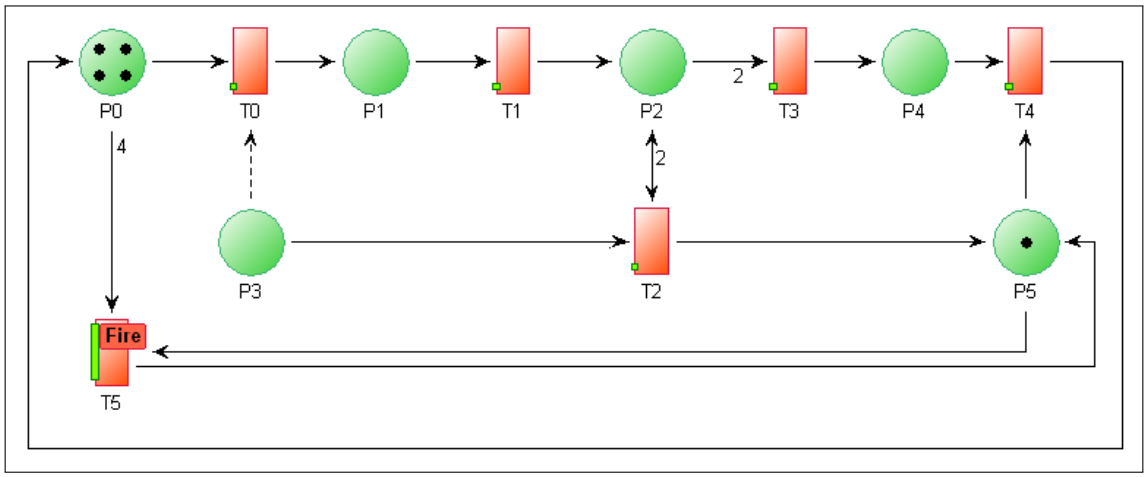

Figure 2. iBuC-WFS fleet management model

In the iBuC-Public Transport Service (iBuC-PTS) scenario (Figure 1), the service life cycle was dynamically adjusted based on real-time PTS itinerary data to optimize *(a)* passenger wait times at interchange nodes and *(b)* the on-time arrival rate per PTS route. Under this adjustment, the EV fleet was triggered to navigate a comprehensive route through all service boarding nodes (BNs) within the local network, terminating at the destination node (DN) closest to the public transit hub.

Conversely, in the scenario of the iBuC-Weather Forecasting Service (iBuC-WFS) (Figure 2), the service life cycle adapted to the incoming WFS alerts regarding extreme weather to prioritise passenger and fleet safety. These tactical adjustments included *(a)* the expedited completion of all active routes based on real-time EV positioning and service status, and *(b)* the suspension of operations by the iBuC Control Unit (CU) as a protective measure.

The states P0:[Fleet idle - EV charging] to P5:[Third-party incoming data] were common for both the iBuC-PTS and iBuC-WFS models. However, P6:[Full-route service triggered] was the state in which a full-route service was activated for all EVs in the fleet and the state that preceded the activation of state P5 in the iBuC-PTS model. The state that preceded the activation of the P5 state in the iBuC-WFS model was the P0 state, as is the case where an incoming alert leads to a service suspension.

Table 1. Fleet Management States

	States	iBuC-PTS	iBuC-WFS
P0	Fleet idle - EV charging	●	●
P1	EV activated	●	●
P2	EV arrives at BN	●	●
P3	Service request is placed	●	●
P4	EV arrives at DN	●	●
P5	Third-party incoming data	●	●
P6	Full-route service triggered	●	○

The states P1:[EV activated] and P2:[EV arrives at BN] were critical transition points in the operational lifecycle of the EV fleet. In the context of dynamic WPT (charging-while-driving), these states require near-instantaneous and secure OCPP handshakes as the vehicle moves across various charging segments. Unlike static charging, where time-delays in authentication are manageable, the mobility inherent in states P1 and P2 requires a communication framework that can handle rapid, secure authentication to maintain continuous energy transfer without compromising the service cybersecurity.

 doi:10.20944/preprints202605.0706.v1

3.2. Weaknesses and Vulnerability List

The next phase of the service assessment process was the identification of service weaknesses, using the Architectural Concepts list provided by the Massachusetts Institute of Technology Research & Engineering (MITRE) database [48]. This weakness list also included an indicative vulnerability for every weakness, chosen based on the following two criteria; *(a)* the relevance between a vulnerability and the component of the service, and *(b)* the impact of a vulnerability on the integrity and privacy of the service data, represented by the vulnerability security score [30]. These criteria ensured that the selected vulnerabilities were the most significant for the service weaknesses.

The relevance of a vulnerability was defined by the logical association of the vulnerability with the state of the service. The relevance criterion helped to select the group of vulnerabilities that were inherent in the software and in the hardware included in the service. Within this group of relevant vulnerabilities, some had a rather greater impact, due to their more frequent exploitation. The use of the Common Vulnerability Scoring System (CVSS) Base Score [30] showed the level of impact for the specific entity (i.e., software, hardware component and OS, among others) that suffered from the vulnerability. The CVSS Base Score represented the severity of the vulnerability on a scale of 0 to 10, where 10 was the most critical value. The impact criterion limited the group of relevant vulnerabilities to the most critical ones.

The security issues of the iBuC service depend on the weaknesses of the CU, the EV fleet, and the consumers (i.e., their smart device or the service's passenger application). The selection of the iBuC Vulnerability List (VL) was made taking into account the vulnerabilities of the service weaknesses (Table 2). Each vulnerability was represented by the CVE-ID and had metrics that reflected the exploitability and the impact of the vulnerability [30]. The CVSS Temporal Score was a numeric representation of the mitigation of vulnerability in the case of applying patches or fixes, if available. In case no patches or fixes existed, the CVSS Temporal Score had the same value as the CVSS Base Score.

Table 2. Vulnerability List (VL)

CVE	Description	CVSS	
		BS	TS
CVE-2017-7214	Information Exposure	9.8	9.1
CVE-2018-4878	(Resource) Use After Free	9.8	9.1
CVE-2018-8174	Failure to Constrain Operations	7.5	7.3
CVE-2017-0199	Access Control (Authorization) Issues	7.8	6.6
CVE-2018-7600	Improper Input Validation	9.8	8.5
CVE-2018-12942	OS Command Injection	8.8	8.1
CVE-2018-14643	Improper Authentication	9.8	8.8
CVE-2018-10635	Missing Critical Function Authentication	9.8	7.9
CVE-2016-6829	Use of Hard-coded Credentials	9.8	8.7
CVE-2016-5788	Improper Authorisation	10	8.3
CVE-2016-5062	Incorrect Resource Transfer	9.8	8.3
CVE-2016-8209	Improper Check	7.5	6.6
CVE-2017-5239	Inadequate Encryption Strength	7.5	7.1
CVE-2017-17717	Broken Cryptographic Algorithm	9.8	9.3
CVE-2017-7901	Use of Insufficiently Random Values	8.6	7.6
CVE-2017-18146	Improper Crypto Verification	9.8	8.5
CVE-2016-5069	Insufficient Session Expiration	9.8	9.1
CVE-2016-7124	Deserialization of Untrusted Data	9.8	8.5
CVE-2018-12689	LDAP Injection	9.8	9.3

***BS**: Base Score* ***TS**: Temporal Score*

3.3. Security Metric Calculation

The final phase of the assessment provides a quantitative representation of the service security level by calculating the Frequency of Occurrences (R), Severity (W), and Risk (P). This process is taking under consideration the Common Vulnerability Scoring System (CVSS) values from the Vulnerability

 doi:10.20944/preprints202605.0706.v1

List (VL) to derive the Security Metric (SM_{VL}). The aforementioned metrics were calculated with the following equations:

$$R = \frac{K}{\sum_{i=1}^{n} A_i}, \tag{1}$$

where K is the number of vulnerabilities per weakness, n is the number of model SPN states, and the denominator is the sum of states affected by the K vulnerabilites of the weakness [49].

$$W = \sum_{i=1}^{K} \frac{V_i}{K \cdot CR \cdot IR \cdot AR}, \tag{2}$$

where V_i is the CVSS base score of each vulnerability, and CR, IR, and AR are the Environmental Metrics of the vulnerability. The Environmental Metrics quantify how specific deployment contexts influence the likelihood of vulnerability mitigation versus exploitation [30].

$$P = \frac{R}{\sum_{j=1}^{m} R}, \tag{3}$$

where R is calculated using Eq.1, and the denominator is the total Frequency of Occurrences of the m number of weaknesses.

$$SM_{VL}(0) = \sum_{i=1}^{m} (P \cdot W), \tag{4}$$

where P is the result of Eq.3 and W is the result of Eq.2 respectively, for the m number of the weaknesses. As the value of $SM_{VL}(0)$ increases, a more critical level of service security is depicted. As the vulnerabilities are mitigated or even eliminated, the Environmental Metrics vary, the vulnerability severity decreases, leading to a mitigated security metric $SM_{VL}(t)$.

Table 3. Security Metrics

Models	**Metrics**	
iBuC-PTS	$SM_{VL}(0) = 9.14$	$SM_{VL}(t) = 8.15$
iBuC-WFS	$SM_{VL}(0) = 9.09$	$SM_{VL}(t) = 8.09$

$SM_{VL}(0)$: Based on CVSS Base Scores *$SM_{VL}(t)$: Based on CVSS Temporal Scores*

The security assessment process was conducted separately for the iBuC-PTS and iBuC-WFS models, in both cases considering the iBuC VL. The results of the evaluation process are shown in Table 3. The metrics $SM_{VL}(0)$ are the result of the evaluation based on the CVSS Base Score of the VL items, whilst the metrics $SM_{VL}(t)$ are the result of the evaluation based on the CVSS Temporal Score of the VL items. It is noted that $SM_{VL}(0)$ is 0.5% lower in the iBuC-WFS model compared to the iBuC-PTS model. This small value deviation of the two $SM_{VL}(0)$ metrics is caused by the additional state of the iBuC-PTS model compared to the iBuC-WFS model. So, the dynamic adaptation of the iBuC to the third-party service affects the security, even if only one new state (i.e., the P6 state) arises. By comparing the two metrics $SM_{VL}(t)$, a deviation in mitigation is also observed. More specifically, in iBuC-PTS the mitigated metric $SM_{VL}(t)$ is 10.8% lower than the respective $SM_{VL}(0)$ metric, and in iBuC-WFS the mitigated metric $SM_{VL}(t)$ is 11% lower than the respective $SM_{VL}(0)$ metric. This differentiation is also associated with the one additional state and the degree of mitigation for the VL items that affect that specific state. Hence, the dynamic adaptation of the iBuC to the third-party service affects the security more if the additional states are affected by critical vulnerabilities.

The above showed that the security assessment process can be used to highlight the data flow changes in the two scenarios and how the IoT third-party service affects the service life-cycle. In this vein, the same method will be followed to highlight the impact of the PEV network on the security level of the service.

 doi:10.20944/preprints202605.0706.v1

4. PEV Network Security Impact

In this section, the security assessment method presented in the previous section is implemented to evaluate the impact of the PEV network security level on the ITS security level. In the first phase, the list of weaknesses and the list of selective vulnerabilities of the PEV network and its active components will be presented. The former iBuC VL is expanded to include the PEV network entries and to form the iBuC Extended Vulnerability List (EVL). Then, the security assessment process is applied to iBuC-PTS and iBuC-WFS, this time based on the EVL to highlight the impact of the PEV network on the security level of the service.

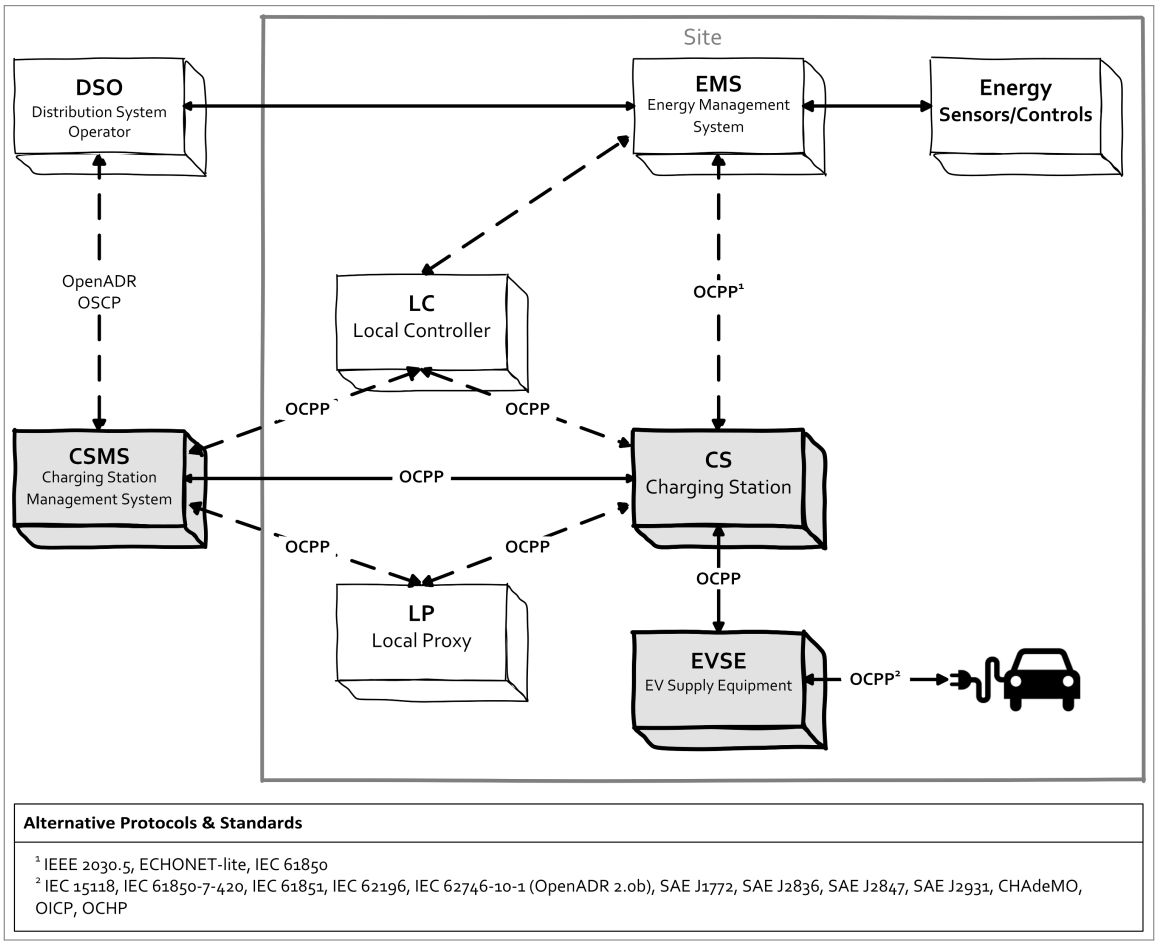

Figure 3. Architecture of an OCPP-based PEV network

As proposed by the architecture of a PEV network supported by the Open Charge Point Protocol (OCPP) [50], the components of the PEV network within an ITS such as iBuC are *(a)* the Charging Station (CS), *(b)* the Charging Station Management System (CSMS), *(c)* the Electric Vehicle Supply Equipment (EVSE), *(d)* the Energy Management System (EMS) if existing, *(e)* the Electric Vehicle (EV) and *(f)* the OCPP protocol (Figure 3). In the case of the iBuC service, as with other ITS, the CSMS serves as the iBuC CU system. Consequently, CSMS vulnerabilities are excluded from this specific study, as they were considered within the previously discussed iBuC VL security assessment of the CU. Additionally, communication between the components of the iBuC PEV network complies exclusively with the OCPP.

4.1. Security Weaknesses and Vulnerabilities

The following list includes vulnerabilities that are directly related to the active components of the OCPP-based PEV network of the iBuC fleet.

- **CVE-2018-7800** - This vulnerability allows the attacker to access the EVSE with full privileges. With these access privileges, the attacker gains full control and can affect the availability of the

 doi:10.20944/preprints202605.0706.v1

service by enforcing the following [51,52]; *(a)* stopping any ongoing charging process, *(b)* falsely setting the CS status to 'not availiable' or 'charging', and *(c)* unlocking the charging cable to allow malicious or uncontrolled use.
CVE-2018-7800 falls under the weakness [CWE-798: Use of Hard-coded Credentials] and is classified as *critical* severity (CVSS Base score: 9.8) [30].

- **CVE-2018-7801** - This is a high-risk vulnerability, the exploitation of which allows the attacker to access the EVSE with full privileges, using some arbitrary code. With these access privileges, the attacker gains full control of the charging station operating system [51,52]. CVE-2018-7801 falls under the [CWE-94: Improper Control of Generation of Code ('Code Injection')] weakness and it is classified as of *high* severity (CVSS Base score: 8.8) [30].
- **CVE-2018-7802** - This vulnerability allows the attacker to access the EVSE with full privileges, using Structured Query Language (SQL) code injection [51],[52]. CVE-2018-7802 falls under the [CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')] weakness and is classified as of *high* severity (CVSS Base score: 8.8) [30].
- **CVE-2020-27813** - This vulnerability allows attacks against OCPP messages, through manipulated JSON messages, which are used to violate the constraints governing the charging site. These messages may also include circular or encapsulated code structures [53]. CVE-2020-27813 falls under the weaknesses [CWE-190: Integer Overflow or Wrap-around] and [CWE-400: Uncontrolled Resource Consumption] and is classified as of *high* severity (CVSS Base score: 7.5) [30].
- **CVE-2021-22706** - This vulnerability allows the attacker to impersonate a trusted user of the charging station and to submit malicious parameters to the charging station web server [54]. CVE-2021-22706 falls under the [CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')] weakness and is classified as of *medium* severity (CVSS Base score: 6.1) [30].
- **CVE-2021-22722** - This vulnerability allows the attacker to change the operating parameters of the charging station by injecting malicious code through CSV files [54]. CVE-2021-22722 falls under the [CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')] weakness and is classified as of *medium* severity (CVSS Base score: 5.4) [30].
- **CVE-2021-22729** - This vulnerability allows the attacker to bypass authorisation checks and access the charging station web server with administrative rights [54]. CVE-2021-22729 falls under the [CWE-259: Use of Hard-coded Password] weakness and is classified as of *critical* severity (CVSS Base score: 9.8) [30].
- **CVE-2021-22730** - This vulnerability allows the attacker to bypass authorisation checks and access the charging station web server with administrative rights [54]. CVE-2021-22730 falls under the [CWE-798: Use of Hard-coded Credentials] weakness and is classified as of *critical* severity (CVSS Base score: 9.8) [30].
- **CVE-2018-16669** - This vulnerability allows the attacker to discover the administrator credentials of the service, as they are stored in XML files [30]. CVE-2018-16669 falls under the weakness [CWE-259: Use of Hard-coded Password] and is classified as of *critical* severity (CVSS Base score: 9.8) [30].

These vulnerabilities were incorporated into the vulnerability list of the iBuC service. Regarding this integration, the following should be noted:

(a) CVE-2021-22730 replaced the iBuC vulnerability CVE-2016-6829, which falls under the same weakness [CWE-798: Use of Hard-coded Credentials]. CVE-2021-22730 prevailed for being more contemporary and having a better CVSS Temporal Score. CVE-2021-22730 was chosen over CVE-2018-7800, which also falls under CWE-798 for being more contemporary;

(b) CVE-2018-7802 replaced CVE-2018-12942, which falls under the same weakness [CWE-89: SQL Injection]. CVE-2018-7802 prevailed for having a better CVSS Temporal Score, while also being relevant to the charging process;

 doi:10.20944/preprints202605.0706.v1

(c) CVE-2021-22706 replaced CVE-2021-22722 which falls under the same weakness [CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')], due to higher severity (i.e., CVE-2021-22706 has CVSS Base score: 6.1 while CVE-2021-22722 has CVSS Base score: 5.4).

The aforementioned vulnerabilities were added to the list of vulnerabilities of the iBuC service, forming the Extended Vulnerability List (EVL) shown in Table 4. The EVL includes two new vulnerabilities related to the OCPP-based charging process. In addition, the EVL includes five new vulnerabilities.

It is important to note that while the vulnerabilities listed in Table 4 are based on historical exploits recorded in earlier OCPP implementations, they represent the very *security concerns* that the *Advanced Security* module of OCPP 2.0.1 [55] was developed to address. Specifically, features such as secure firmware updates and encrypted security logging in 2.0.1 were introduced to prevent the unauthenticated access and code injection scenarios described in CVE-2018-7801 and CVE-2018-7802. By modelling these specific weaknesses, this study evaluates the robustness of transport services that may still rely on legacy protocol versions or incomplete security profile implementations.

Table 4. Extended Vulnerability List (EVL)

CVE	Description	CVSS	
		BS	TS
CVE-2017-7214	Information Exposure	9.8	9.1
CVE-2018-4878	(Resource) Use After Free	9.8	9.1
CVE-2018-8174	Out-of-bounds Write	7.5	7.3
CVE-2017-0199	Access Control (Authorization) Issues	7.8	6.6
CVE-2018-7600	Improper Input Validation	9.8	8.5
~~CVE-2018-12942~~	~~SQL Injection~~	~~8.8~~	~~8.1~~
CVE-2018-7802	**SQL Injection**	**8.8**	**7.9**
CVE-2018-14643	Improper Authentication	9.8	8.8
CVE-2018-10635	Missing Critical Function Authentication	9.8	7.9
~~CVE-2016-6829~~	~~Use of Hard-coded Credentials~~	~~9.8~~	~~8.7~~
CVE-2021-22730	**Use of Hard-coded Credentials**	**9.8**	**8.8**
CVE-2016-5788	Improper Authorisation	10	8.3
CVE-2016-5062	Incorrect Resource Transfer	9.8	8.3
CVE-2016-8209	Improper Check	7.5	6.6
CVE-2017-5239	Inadequate Encryption Strength	7.5	7.1
CVE-2017-17717	Broken Cryptographic Algorithm	9.8	9.3
CVE-2017-7901	Use of Insufficiently Random Values	8.6	7.6
CVE-2017-18146	Improper Crypto Verification	9.8	8.5
CVE-2016-5069	Insufficient Session Expiration	9.8	9.1
CVE-2016-7124	Deserialization of Untrusted Data	9.8	8.5
CVE-2018-12689	LDAP Injection	9.8	9.3
CVE-2018-7801	**Code Injection**	**8.8**	**8.2**
CVE-2020-27813	**Uncontrolled Resource Consumption**	**7.5**	**6.7**
CVE-2021-22706	**Cross-site Scripting**	**6.1**	**5.7**
CVE-2021-22729	**Use of Hard-coded Password**	**9.8**	**8.8**
CVE-2018-16669	**Insufficiently Protected Credentials**	**9.8**	**8.7**

***BS**: Base Score* ***TS**: Temporal Score*

4.2. Impact on the iBuC Service Security

The security of the iBuC fleet management is affected by the security of the PEV network and the vulnerabilities of the actors of the charging process.

In the iBuC-PTS scenario, the states P0:[Fleet idle - charging of EV], P4:[EV arrives at DN] and P6: [triggered Full-route service] are mostly affected by vulnerabilities in the PEV network, that is, a percentage of 43% of the service states (i.e., three of seven model states). In the iBuC-WFS scenario,

 doi:10.20944/preprints202605.0706.v1

only the states P0:[Fleet idle - EV charging] and P4:[EV arrives at DN] are affected by the vulnerabilities of the PEV network, that is, a 33% percentage of service states (i.e., two of six model states).

Table 5. Comparative analysis of security metrics for iBuC scenarios.

Scenario	Operational State	SM_{VL}	SM_{EVL}	ΔSM
iBuC-PTS	Initial ($t = 0$)	9.14	8.93	0.21
	Mitigated (t)	8.15	7.99	0.16
iBuC-WFS	Initial ($t = 0$)	9.09	8.87	0.22
	Mitigated (t)	8.09	7.94	0.15

SM_{VL}: iBuC metric considering the Vulnerability List; SM_{EVL}: iBuC metric considering the Extended Vulnerability List; $\Delta SM = SM_{\mathrm{EVL}} - SM_{\mathrm{VL}}$

This time, the security of the iBuC service is evaluated on the basis of the EVL that includes vulnerabilities in the OCPP-based EV charging process. Table 5 resumes the security metrics of the previous evaluation process on the vulnerability list of the iBuC service (Table 5, column SM_{VL}) and of the last evaluation process based on the extended vulnerability list of the iBuC service (Table 5, column SM_{EVL}).

In both scenario models of the iBuC service, the metrics based on the EVL are improved in relation to the respective metrics based on the VL by 0.15 to 0.22. This decrease is associated with the following factors.

(a) EVL includes more vulnerabilities than VL for the same service states, resulting in an increased frequency of occurrence R), an inversely reduced proportional risk P, and, finally, reduced security metrics $\mathrm{SM}_{VL}(0)$ and $\mathrm{SM}_{VL}(t)$.

(b) The majority of the EVL additions (i.e., four of seven vulnerabilities) have a CVSS Base Score of less than 8.9 and are therefore classified as of high severity, rather than of critical severity, and two out of seven of the EVL additions have a CVSS Temporal Score of even less than 6.9, which classifies them as vulnerabilities of medium severity.

(c) The EVL additions are affecting 43% of the iBuC-PTS states and 33% of the iBuC-WFS states and the impact of the added vulnerabilities increases.

In summary, the fact that *(a)* the PEV network vulnerabilities are included in the iBuC vulnerability list (i.e., the EVL), *(b)* the new entries of the EVL have lower CVSS scores than the existing entries, and *(c)* the new EVL entries affect nearly half of the service life-cycle states are the factors that lead to the reduced metrics.

In the context of advanced wireless charging, $\mathrm{SM}_{VL}(0)$ represents the initial risk profile of the inductive charging service, while $\mathrm{SM}_{VL}(t)$ reflects the improved security posture after implementing protocol-level mitigations such as those defined in IEC 63584:2024.

Although the mathematical results derived from the SPN models provide the formal basis for the analysis, a visual comparison of steady-state probabilities (P) reveals how the integration of external IoT data, such as weather forecasting, fundamentally alters the operational profile of the service. This shift is particularly relevant for advanced wireless charging infrastructures within ITS, where timing and synchronisation are critical for both energy efficiency and communication security. Figure 4 illustrates the probability distribution in the seven identified states for both iBuC-PTS and iBuC-WFS scenarios.

The steady-state analysis illustrated in Figure 4 reveals that the probability that the system resides in the P3:[Service request is placed] state where the EV is in charging mode increases from 0.35 in the PTS model to 0.50 in the WFS model. From a cybersecurity perspective, this increased residence time in the charging phase expands the "exposure window" for protocol-level attacks. In advanced

 doi:10.20944/preprints202605.0706.v1

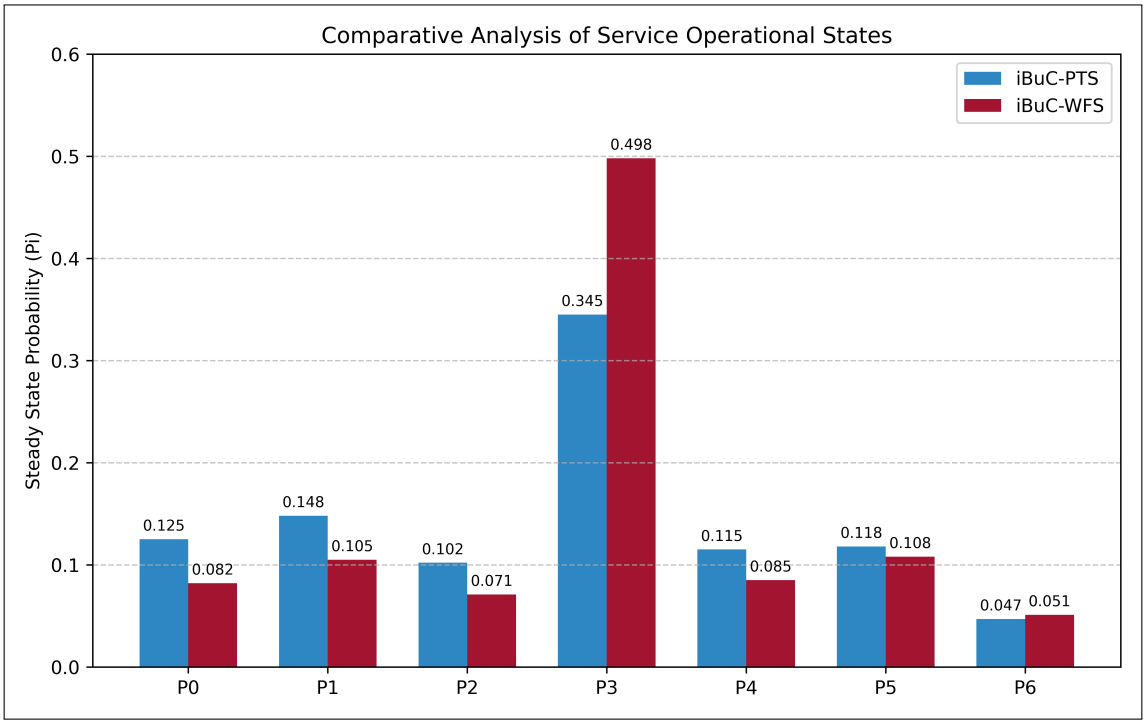

Figure 4. Comparison of steady-state probability distributions (Pi) for the iBuC-PTS (PublicTransport-integrated) and iBuC-WFS (Weather-integrated) models

wireless charging environments, this prolonged state suggests that the synchronisation between the OCPP handshake and the physical inductive power transfer is more susceptible to latency-induced vulnerabilities or signal-jamming. The data indicates that as ITS becomes more interconnected with external data providers, the complexity of the service chain directly impacts the vulnerability surface of the service, necessitating more robust high-speed authentication protocols to maintain service continuity.

5. Discussion

The security within an Intelligent Transport Service is affected by the characteristics of the third-party service which the ITS shares data with, in the context of the IoT interoperability. The service security is also affected by the internal sub-processes, such as the fleet parking and charging. The majority PEV networks are based on the OCPP protocol. OCPP security vulnerabilities have not yet been fully recorded, as the study and development of the protocol began the last decade.

The purpose of this work was to evaluate the level of security of the transport service considering the challenges of the service vehicle charging process. The iBuC service was used as a testbed. The vulnerabilities related to active components of the PEV network [50] were embedded in the respective list of iBuC fleet management vulnerabilities (iBuC VL), forming the iBuC Extended Vulnerability List (iBuC EVL).

The first step was the collection of the PEV network vulnerabilities that are relative to the two service cases already presented, namely iBuC-PTS and iBuC-WFS. This led to a list of nine (9) vulnerabilities. The majority (78%) of these vulnerabilities were added to the iBuC VL forming the iBuC EVL based on the following criteria:

(a) Every vulnerability has the highest CVSS Base score within the respective weakness;

(b) Every vulnerability has the highest discrepancy between CVSS Base and Temporal scores (respectable mitigation rate);

(c) Every vulnerability affects service components which participate in several or, even better, the majority of the service states.

 doi:10.20944/preprints202605.0706.v1

The 29% of the seven (7) PEV network vulnerabilities included in the iBuC EVL replaced the vulnerability entries in the iBuC VL that were less contemporary or felt short according to the aforementioned criteria. The 71% of the seven (7) PEV network vulnerabilities included in the iBuC EVL are new entries in the iBuC VL.

In general, the vulnerabilities of the PEV network are 29% of the iBuC EVL entries, which is related to the fact that the PEV network subprocess is vital for the life-cycle of the transport service. The importance of the PEV network subprocess is shown by the level to which security issues in the subprocess affect the security of the transport service.

Each vulnerability was correlated with the individual actors within the PEV network architecture, to ensure that the security assessment of the PEV charging process was feasible. Related countermeasures or good practice suggestions were also considered, and a correlation was made between the EVL contents and the affected service lifecycle states, as described by the security assessment method.

As already mentioned, in the iBuC-PTS case 43% of the total service states, and in the iBuC-WFS case 33% of the total service states are affected by the vulnerabilities of the PEV network. These rates show that nearly half of the service life-cycle is affected by the PEV network security issues, another indicator of the latter criticality.

The iBuC-PTS and the iBuC-WFS were finally evaluated on the basis of EVL. In both scenario models of the iBuC service, the metrics based on the EVL were improved in relation to the respective metrics based on the VL by a mean percentage of 18%.

In summary, the security assessment of the two service cases based on the EVL was found to have metrics with lower values. The decreased metrics are due to the fact that the EVL increases the sum of the Frequency of Occurrence (R) for each vulnerability, inversely decreases the Proportional Risk (P_i) of each vulnerability and consequently reduces both Security Metrics, the basic $SM_{EVL}(0)$ and the mitigated $SM_{EVL}(t)$. In addition, it was observed that most vulnerabilities introduced by the EVL were classified as high rather than critical severity, and all mitigated to be classified as medium severity. In conclusion, it was shown that the security level of the IoT transport service is further affected by the security issues of the PEV network.

Our results indicate that the system transitions into state P2 with a high degree of frequency in both the PTS and WFS models. In a real-world ITS deployment, this state is no longer merely a physical arrival but a complex digital interaction; for instance, modern infrastructures are now utilising the Differential Inductive Positioning System (DIPS) as defined in the latest SAE J2954 update [56] to ensure precise coupling during P2 state. Although this standard optimises power transfer efficiency, our analysis suggests that this automated alignment phase also represents a critical point where secure OCPP handshakes must be maintained to prevent unauthorised access during the positioning sequence.

6. Conclusions

The security of the various functions within an Intelligent Transport Service is affected by the internal sub-processes, such as the fleet parking and charging processes. The purpose of this work was to evaluate the level of security of the transport service considering the challenges of the service vehicle charging process. The iBuC, an OCPP-based Intelligent Transport Service, was used as a testbed. The vulnerabilities in the PEV network were embedded in the respective list of iBuC fleet management vulnerabilities, and a security assessment was undertaken, considering the security challenges introduced by the fleet charging sub-process.

The fleet management security metrics of the two service cases already presented, namely iBuC-PTS and iBuC-WFS, were evaluated based on the EVL of the service. Although the two IoT-based transport services have functional differences (e.g., the third-party service and the number of service states), in both cases the security metrics were decreased. Therefore, it is safe to conclude that the evaluation of an IoT-based transport service in terms of security is more robust if the vulnerabilities of the PEV network are considered.

 doi:10.20944/preprints202605.0706.v1

The majority of PEV networks are based on the OCPP protocol, as happens with the iBuC-PTS and the iBuC-WFS. The OCPP security vulnerabilities have not yet been fully recorded, as the study and development of the protocol began the last decade. Until now, the list of recorded vulnerabilities has not been exhaustive. However, related research efforts are intensive and the more vulnerabilities recorded, the more mitigation measures will be suggested, making the assessment of the security level of IoT-based transport services more accurate.

The results of the security assessment can be evaluated to suggest changes within the service so that the level of security improves without affecting the nature of the service. The integration of Artificial Intelligence (AI) algorithms in the future could assist the process of finding the key-changes needed to reach higher service security levels. Moreover, the application on the service of Reinforcement Learning (RL) features can be considered, so that the service decision-making will be able to continuously adapt based on interaction with the environment.

The security assessment methodology presented in this study offers a scalable framework to address the unique signal-security challenges of wireless inductive charging pads. Unlike physical plug-in stations, wireless systems rely on proximity-based handshakes and inductive communication channels that are susceptible to specialised man-in-the-middle (MitM) attacks and signal jamming. By applying our Stochastic Petri net (SPN) model to these wireless scenarios, researchers can quantify the impact of 'foreign object detection' spoofing or unauthorised power-draw requests on the overall stability of the Intelligent Transportation System. Integrating OCPP-based security profiles with the physical-layer authentication of wireless pads will be a critical step in ensuring the resilience of future autonomous charging ecosystems against both digital and signal-level intrusions.

This study presented a robust methodology to evaluate the cybersecurity resilience of ITS by focusing on the OCPP-based communication backbone. Through the application of SPNs, we have quantified how the integration of external IoT data—such as weather forecasting—impacts the steady-state probabilities of charging services, notably increasing the *exposure window* during the critical charging phase. As the industry moves towards global standardisation of Advanced WPT in frameworks such as IEC 63584:2024 [17] and SAE J2954 [57],[56], the security of the underlying protocols ceases to be a secondary concern and becomes a fundamental requirement for system safety. Our findings demonstrate that protecting the digital handshake is as vital as the physical efficiency of the inductive coils. Future work will extend this assessment framework to dynamic wireless charging scenarios, where high-speed mobility and rapid authentication handshakes will present new challenges for the cyber-physical security of automated transport ecosystems.

Author Contributions: Conceptualization, Z.G. and C.D.; methodology, Z.G.; software, Z.G.; validation, Z.G., D.K., I.V. and C.D.; formal analysis, Z.G.; investigation, Z.G.; resources, Z.G.; data curation, Z.G.; writing—original draft preparation, Z.G., D.K., I.V. and C.D.; writing—review and editing, Z.G., D.K., I.V. and C.D.; visualization, Z.G.; supervision, Z.G.; project administration, Z.G.; funding acquisition, D.K. and I.V. All authors have read and agreed to the published version of the manuscript.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Acknowledgments: The publication of this article was financially supported by the Special Account for Research Grants of the University of West Attica. Open access funding provided by HEAL-Link Greece. The authors have reviewed and edited the output and take full responsibility for the content of this publication.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

 doi:10.20944/preprints202605.0706.v1

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
AV	Autonomous Vehicle
BN	Boarding Node
CS	Charging Station
CSMS	Charging Station Management System
CU	Control Unit
CVSS	Common Vulnerability Scoring System
DN	Destination Node
EMS	Energy Management System
EV	Electric Vehicle
EVL	Extended Vulnerability List
EVSE	Electric Vehicle Supply Equipment
HARM	Hierarchical Attack Representation Model
iBuC	intelligent Bus on Campus
IoT	Internet of Things
ITS	Intelligent Transportation Service
MITRE	Massachusetts Institute of Technology Research & Engineering
NVD	National Vulnerability Database
OCA	Open Charge Alliance
OCPP	Open Charge Point Protocol
PEV	Plug-in Electric Vehicle
PTS	Public Transportation System
RL	Reinforcement Learning
SPN	Stochastic Petri net
V2I	Vehicle-to-Infrastructure
VL	Vulnerability List
WFS	Weather Forecasting Service
WPT	Wireless Power Transfer

References

1. Bhargavi, K.; Jayalaksmi, N.; Malagi, S.; Jadoun, V.K. Integration of Plug-in Electric Vehicles in Smart Grid: A Review. In Proceedings of the IEEE International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), 28-29 Feb, Mathura, India, 2020; pp. 214–219. https://doi.org/10.1109/PARC49193.2020.236595.
2. Ortiz-Aguilar, L.; Palacios-Ortega, M.; Carpio, M.; Funes-Tapia, J. A Systematic Review of Electric Vehicle Optimization Problems: Taxonomy, Methods, and Research Challenges. *Automation* **2026**, *7*. https://doi.org/10.3390/automation7020061.
3. Resilient Electric Vehicle Charging Stations in Urban Areas: A Systematic Literature Review. *World Electric Vehicle Journal* **2026**, *17*, 148. https://doi.org/10.3390/wevj17030148.
4. Yu, H.; Wu, C.; Liu, Y. Vehicle-to-Grid Integration in Smart Energy Systems: An Overview of Enabling Technologies, System-Level Impacts, and Open Issues. *Machines* **2026**, *14*. https://doi.org/10.3390/machines14040418.
5. Kim, K.; Kim, J.S.; Jeong, S.; Park, J.H.; Kim, H.K. Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers and Security* **2021**, *103*, 102150. https://doi.org/10.1016/j.cose.2020.102150.
6. Karras, A.; Theodorakopoulos, L.; Karras, C.; Theodoropoulou, A. Towards LLM-Driven Cybersecurity in Autonomous Vehicles: A Big Data-Empowered Framework with Emerging Technologies. *Machine Learning and Knowledge Extraction* **2026**, *8*. https://doi.org/10.3390/make8020043.
7. Naseem, H.; Goswami, P.; Choi, K.; Iqbal, A.; Hakami, H. Smart Charging and Vehicle-to-Grid Integration of Electric Vehicles: Technical Insights, Cybersecurity Risks, and Mobility-OrientedControl Strategies. *Applied Sciences* **2026**, *16*, 1748. https://doi.org/10.3390/app16041748.

 doi:10.20944/preprints202605.0706.v1

8. European Union. Regulation (EU) 2023/1804 of the European Parliament and of the Council of 13 September 2023 on the deployment of alternative fuels infrastructure, and repealing Directive 2014/94/EU. *Official Journal of the European Union* **2023**, *L 234*, 1–47.
9. Open Charge Alliance. *Open Charge Alliance - Annual Report 2025*. Open Charge Alliance (OCA), Arnhem, The Netherlands, 2025.
10. Ampeco LTD. *Enable innovation and cost efficiency with OCPP*. Ampeco LTD, 2022.
11. Current AS. *Innovation and cost-efficiency in four letters: OCPP*. Current AS, 2021.
12. Open Charge Alliance. *Open Charge Alliance - Our mission*. Open Charge Alliance (OCA), 2022.
13. Van Mulders, Jarne and Delabie, Daan and Lecluyse, Cédric and Buyle, Chesney and Callebaut, Gilles and Van der Perre, Liesbet and De Strycker, Lieven. Wireless power transfer: Systems, circuits, standards, and use cases. *Sensors* **2022**, *22*, 5573.
14. Pairindra, W.; Phongsawat, S.; Phophongviwat, T.; Khomfoi, S. The Development of a 1 kW Mid-Range Wireless Power Transfer Platform for Autonomous Guided Vehicle Applications Using an LCC-S Resonant Compensator. *World Electric Vehicle Journal* **2025**, *16*. https://doi.org/10.3390/wevj16060322.
15. Open Charge Alliance. *Open Charge Point Protocol 1.6*. Open Charge Alliance (OCA), Arnhem, The Netherlands, 2015.
16. Open Charge Alliance. *Open Charge Point Protocol 2.0.1*. Open Charge Alliance (OCA), Arnhem, The Netherlands, 2018.
17. International Electrotechnical Commission (IEC). Electric vehicle supply equipment – Open Charge Point Protocol (OCPP). Standard IEC 63584:2024, IEC, Geneva, CH, 2024.
18. Alsaleh, A. Toward a conceptual model to improve the user experience of a sustainable and secure intelligent transport system. *Acta Psychologica* **2025**, *255*, 104892. https://doi.org/10.1016/j.actpsy.2025.104892.
19. Arachchige, K.G.; Alkaabi, G.; Murtaza, M.; Haq, Q.E.U.; Abualkishik, A.Z.; Lee, C.C. Threat Landscape and Integrated Cybersecurity Framework for V2V and Autonomous Electric Vehicles. *World Electric Vehicle Journal* **2025**, *16*, 469. https://doi.org/10.3390/wevj16080469.
20. Durlik, I.; Miller, T.; Kostecka, E.; Zwierzewicz, Z.; Łobodzińska, A. Cybersecurity in Autonomous Vehicles—Are We Ready for the Challenge? *Electronics* **2024**, *13*, 2654. https://doi.org/10.3390/electronics13132654.
21. Muslam, M.M.A. Enhancing Security in Vehicle-to-Vehicle Communication: A Comprehensive Review of Protocols and Techniques. *Vehicles* **2024**, *6*, 450–467. https://doi.org/10.3390/vehicles6010020.
22. Giannaros, A.; Karras, A.; Theodorakopoulos, L.; Karras, C.; Kranias, P.; Schizas, N.; Kalogeratos, G.; Tsolis, D. Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions. *Journal of Cybersecurity and Privacy* **2023**, *3*, 493–543. https://doi.org/10.3390/jcp3030025.
23. Walch, M.; Schirrer, A.; Neubauer, M. Impact assessment of cooperative intelligent transport systems (C-ITS): a structured literature review. *European Transport Research Review* **2025**, *17*, 11.
24. Khanmohamadi, M.; Guerrieri, M. Smart Intersections and Connected Autonomous Vehicles for Sustainable Smart Cities: A Brief Review. *Sustainability* **2025**, *17*, 3254. https://doi.org/10.3390/su17073254.
25. Puzio, E.; Drożdż, W.; Kolon, M. The Role of Intelligent Transport Systems and Smart Technologies in Urban Traffic Management in Polish Smart Cities. *Energies* **2025**, *18*, 2580. https://doi.org/10.3390/en18102580.
26. Shirvani, S.; Baseri, Y.; Ghorbani, A. Evaluation framework for electric vehicle security risk assessment. *IEEE transactions on intelligent transportation systems* **2023**, *25*, 33–56. https://doi.org/10.1109/TITS.2023.3307660.
27. Mavropoulos, O.; Mouratidis, H.; Fish, A.; Panaousis, E. Apparatus: A framework for security analysis in internet of things systems. *Ad Hoc Networks* **2019**, *92*, 101743. https://doi.org/10.1016/j.adhoc.2018.08.013.
28. Harrand, N.; Fleurey, F.; Morin, B.; Husa, K.E. ThingML: A Language and Code Generation Framework for Heterogeneous Targets. In Proceedings of the Proceedings of the ACM/IEEE 19th International Conference on Model Driven Engineering Languages and Systems, New York, NY, USA, 2016; MODELS '16, p. 125–135. https://doi.org/10.1145/2976767.2976812.
29. Samandari, A.; Ge, M.; Hong, J.B.; Kim, D.S. Evaluating the Security of IoT Networks with Mobile Devices. In Proceedings of the IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC). IEEE, 2018, pp. 171–180. https://doi.org/10.1109/PRDC.2018.00028.
30. National Institute of Standards and Technology (NIST). *National Vulnerability Database (NVD)*. National Institute of Standards and Technology (NIST), 2019.
31. Hali, A.; Zirra, P. Reward Based Metrics for Assessing the Effectiveness of Shuffled Based Moving Target Defense. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)* **2025**, *17*, 7–18. https://doi.org/10.11591/jtec.v17i1.6395.

 doi:10.20944/preprints202605.0706.v1

32. Ahmadon, M.A.B.; Yamaguchi, S.; Saon, S.; et al. On service security analysis for event log of IoT system based on data Petri Net. In Proceedings of the IEEE International Symposium on Consumer Electronics (ISCE). IEEE, 2017, pp. 4–8. https://doi.org/10.1109/ISCE.2017.7972186.
33. Yamaguchi, S.; Tanaka, H. Modeling of Infection Phenomenon and Evaluation of Mitigation Methods for IoT Malware Mirai by Agent-Oriented Petri Net PN^2. In Proceedings of the IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW). IEEE, 2018, pp. 1–2. https://doi.org/10.1109/ICCE-China.2018.8448898.
34. Ahmadon, M.A.B.; Yamaguchi, S. On service orchestration of cyber physical system and its verification based on Petri Net. In Proceedings of the IEEE 5th Global Conference on Consumer Electronics. IEEE, 2016, pp. 1–4. https://doi.org/10.1109/GCCE.2016.7800350.
35. Fortino, G.; Russo, W.; Savaglio, C.; Viroli, M.; Zhou, M. Opportunistic cyberphysical services: A novel paradigm for the future Internet of Things. In Proceedings of the IEEE 4th World Forum on Internet of Things (WF-IoT). IEEE, 2018, pp. 488–492. https://doi.org/10.1109/WF-IoT.2018.8355174.
36. Orcioni, S.; Conti, M. EV smart charging with advance reservation extension to the OCPP standard. *Energies* **2020**, *13*, 3263–3284. https://doi.org/10.3390/en13123263.
37. Kirchner, S.R. OCPP Interoperability: A Unified Future of Charging. *World Electric Vehicle Journal* **2024**, *15*, 191. https://doi.org/10.3390/wevj15050191.
38. Hamdare, S.; Brown, D.J.; Jha, D.N.; Aljaidi, M.; Cao, Y.; Kumar, S.; Kharel, R.; Jugran, M.; Kaiwartya, O. Cyber defense in OCPP for EV charging security risks. *International Journal of Information Security* **2025**, *24*, 134. https://doi.org/10.1007/s10207-025-01055-7.
39. Plaka, R.; Asplund, M.; Nadjm-Tehrani, S. Vulnerability analysis of an electric vehicle charging ecosystem. In Proceedings of the International Conference on Critical Information Infrastructures Security. Springer, 2023, pp. 155–173. https://doi.org/10.1007/978-3-031-62139-0_9.
40. Abazari, A.; Ghafouri, M.; Jafarigiv, D.; Atallah, R.; Assi, C. Developing a security metric for assessing the power grid's posture against attacks from EV charging ecosystem. *IEEE Transactions on Smart Grid* **2024**. https://doi.org/10.1109/TSG.2024.3451970.
41. Garofalaki, Z.; Kallergis, D.; Douligeris, C., A Security Assessment Platform for Stochastic Petri Net (SPN) Modelling in the Internet of Things (IoT) Ecosystem. In *Domain-Specific Conceptual Modeling: Concepts, Methods and ADOxx Tools*; Karagiannis, D.; Lee, M.; Hinkelmann, K.; Utz, W., Eds.; Springer International Publishing: Cham, 2022; pp. 289–311. https://doi.org/10.1007/978-3-030-93547-4_13.
42. Garofalaki, Z.; Kallergis, D.; Katsikogiannis, G.; Ellinas, I.; Douligeris, C. Transport services within the IoT ecosystem using localisation parameters. In Proceedings of the IEEE International Symposium on Signal Processing and Information Technology (ISSPIT). IEEE, 2016, pp. 87–92. https://doi.org/10.1109/ISSPIT.2016.7886014.
43. Garofalaki, Z.; Kallergis, D.; Katsikogiannis, G.; Ellinas, I.; Douligeris, C. A DSS model for IoT-based intelligent transportation systems. In Proceedings of the IEEE International Symposium on Signal Processing and Information Technology (ISSPIT). IEEE, 2017, pp. 276–281. https://doi.org/10.1109/ISSPIT.2017.8388655.
44. Yu, Z.; Zhou, L.; Ma, Z.; El-Meligy, M.A. Trustworthiness Modeling and Analysis of Cyber-physical Manufacturing Systems. *IEEE Access* **2017**, *5*, 26076–26085. https://doi.org/10.1109/ACCESS.2017.2764835.
45. Karagiannis, D.; Buchmann, R.A.; Burzynski, P.; Reimer, U.; Walch, M., Fundamental Conceptual Modeling Languages in OMiLAB. In *Domain-Specific Conceptual Modeling: Concepts, Methods and Tools*; Springer, 2016; pp. 3–30. https://doi.org/10.1007/978-3-319-39417-6_1.
46. Karagiannis, D.; Burzynski, P.; Miron, E.T. The Imker Case Study - Practice with the Bee-Up Tool, 2017. https://doi.org/10.5281/zenodo.345846.
47. Garofalaki, Z.; Kallergis, D. On the Security of an IoT-based Intelligent Transportation Service. In Proceedings of the 4th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). IEEE, 2019, pp. 1–5. https://doi.org/10.1109/SEEDA-CECNSM.2019.8908369.
48. MITRE Corporation. Common Vulnerabilities and Exposures: the Standard for Information Security Vulnerability Names. https://cve.mitre.org, 2007.
49. Khamparia, A.; Pandey, B. Threat driven modeling framework using petri nets for e-learning system. *SpringerPlus* **2016**, *5*, 1–16. https://doi.org/10.1186/s40064-016-2101-0.

 doi:10.20944/preprints202605.0706.v1

50. Garofalaki, Z.; Kosmanos, D.; Moschoyiannis, S.; Kallergis, D.; Douligeris, C. Electric Vehicle Charging: A Survey on the Security Issues and Challenges of the Open Charge Point Protocol (OCPP). *IEEE Communications Surveys & Tutorials* **2022**, *24*, 1504–1533. https://doi.org/10.1109/COMST.2022.3184448.
51. Harnett, K.; Watson, G.; Brown, G.; et al. *Government Fleet and Public Sector Electric Vehicle Supply Equipment (EVSE) Cybersecurity Best Practices and Procurement Language Report*, 2019.
52. Saadat, S.; Maingot, S.; Bahizad, S. Electric vehicle charging station security enhancement measures. In Proceedings of the 2020 5th IEEE Workshop on the Electronic Grid (eGRID). IEEE, 2020, pp. 1–8. https://doi.org/10.1109/eGRID48402.2020.9331557.
53. Coats, D.; Suryanarayana, H.; Wang, Z.; Brissette, A.; Zhang, Y.; Ramanan, V.; Scoffield, D.; Woodbury, D.; Haltmeyer, N.; Benzinger, A. *Final Scientific/Technical Report-Cybersecurity for Grid Connected eXtreme Fast Charging (XFC) Station (CyberX)*, 2021.
54. Nasr, T.; Torabi, S.; Bou-Harb, E.; Fachkha, C.; Assi, C. ChargePrint: A Framework for Internet-Scale Discovery and Security Analysis of EV Charging Management Systems. *Proceedings 2023 Network and Distributed System Security Symposium* **2023**, pp. 1–18. https://doi.org/10.14722/ndss.2023.23084.
55. Uribe-Pérez, N.; Gonzalez-Garrido, A.; Gallarreta, A.; Justel, D.; González-Pérez, M.; González-Ramos, J.; Arrizabalaga, A.; Asensio, F.J.; Bidaguren, P. Communications and Data Science for the Success of Vehicle-to-Grid Technologies: Current state and Future Trends. *Electronics* **2024**, *13*, 1940. https://doi.org/10.3390/electronics13101940.
56. SAE International. Dynamic Wireless Power Transfer for both Light and Heavy Duty Vehicles. Recommended Practice SAE RP J2954/3, SAE International, Warrendale, PA, USA, 2025.
57. SAE International. Wireless Power Transfer for Light-Duty Plug-In Electric Vehicles and Alignment Methodology. Standard SAE J2954_202408, SAE International, Warrendale, PA, USA, 2024.