IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Journal Européen des Systèmes Automatisés
Vol. 56, No. 3, June, 2023, pp. 437-449
Journal homepage: http://iieta.org/journals/jesa

Enabling EV Roaming Through Cascading WebSockets in OCPP 1.6

Dwidharma Priyasta[1,2*], Hadiyanto[1], Reza Septiawan[2]

[1] School of Postgraduate Studies, Diponegoro University, Semarang 50241, Indonesia
[2] Center for Electronics Research, National Research and Innovation Agency, Jakarta 10340, Indonesia

Corresponding Author Email: dwid002@brin.go.id

https://doi.org/10.18280/jesa.560311

Received: 6 April 2023
Accepted: 11 June 2023

Keywords:
EV charging networks, roaming protocols, WebSocket cascading connection, simulation

ABSTRACT

Currently, there are four major protocols for EV roaming that support electric vehicle drivers to access charge points from different networks with a single user registration through roaming agreements between charge point operators (CPOs) and mobility service providers (MSPs): the Open Clearing House Protocol (OCHP), the Open InterCharge Protocol (OICP), the eMobility Inter-operation Protocol (eMIP), and the Open Charge Point Interface (OCPI). These protocols facilitate data exchange between CPOs and MSPs using a roaming hub or peer-to-peer connections. On the other hand, the Open Charge Point Protocol (OCPP) is the standard protocol widely used for communication between the charge point and the central system within the CPO's internal system. OCPP has been integrated into many charge point products today, where OCPP 1.6 supports Simple Object Access Protocol (SOAP) and JavaScript Object Notation (JSON) data format over the WebSocket, with the charge point acting as the WebSocket client and the central system as the WebSocket server. The aim of this study is to further enhance the functionality of OCPP by integrating the role of the WebSocket client into the central system to support EV roaming for EV drivers. This new approach describes the architecture that includes the actors and their roles, which are the Charge Point that delivers energy to electric vehicles, the Central System that manages the Charge Point and requests for EV roaming, and the National Access Point that acts as a roaming hub in the proposed EV roaming system. Additionally, three simulation models have been created, each representing an actor and their role in the proposed system. The feasibility and effectiveness of the proposed EV roaming system are evaluated through experiments during high traffic load conditions of a network using the simulation models and actual charge point products. The experiment scenarios specifically focus on cases related to user authorization and billing. This study only concern on the time consumption for user authorization. The results confirm that the proposed EV roaming system can be implemented based on the enhanced functionality of the OCPP, with the average time for user authorization over five attempts range between 3 ms for the simplest scenario one to 2200 ms for the most complex scenario four, which can be considered quite impressive.

1. INTRODUCTION

Battery Electric Vehicles (BEVs) are gaining popularity worldwide and are considered to be an important component of sustainable transportation systems. They have the potential to reduce carbon emissions, improve air quality, and stabilize power grids. According to the International Energy Agency (IEA), the number of electric cars has significantly increased globally, with 16.5 million on the roads in 2021, compared to 10 million in 2020. Predictions estimate that the global electric vehicle (EV) population will reach 85 million by 2025 and could reach as many as 270 million by 2030, not counting two- and three-wheeled vehicles [1]. The intention to adopt BEVs positively correlates with the availability of charging stations, which is driven by supportive norms [2]. Despite being more expensive than internal combustion engine vehicles (ICEVs), declining battery costs and other advancements are narrowing the gap between the two [3, 4]. The adoption is also influenced by socioeconomic factors [5-7] and government policies [8-13]. A study conducted in Indonesia in 2021 found that there were only 97 private and public charging stations across the country, but this number is expected to increase.

BEVs require recharging their batteries in order to operate. Recharging can be done using either AC or DC fast charging methods at private or public facilities. The infrastructure for charging electric vehicles generally refers to charge points that are connected to the electrical grid, enabling them to supply power to BEVs. Typically, the charge point is equipped with a socket outlet to transmit power to the electric vehicle. On the other hand, the electric vehicle has a vehicle inlet to receive power from the charge point. Both parties are connected using a cable that has an interface with the plug on one end and an interface with the vehicle connector on the other end, as shown in Figure 1. The terminology for these accessories is defined in the International Electrotechnical Commission (IEC) 62196 standard series.

The IEC 61851-1:2017 defines electric vehicle charging in four modes [14]. Mode 1 (slow) uses AC electricity with a maximum current of 16 A and a maximum voltage of 250 V or 480 V. Mode 2 (slow to semi-fast) uses AC electricity with a maximum current of 32 A and a maximum voltage of 250 V or 480 V. Mode 3 (semi-fast to fast) uses AC electricity with

a maximum current of 250 A and a maximum voltage of 250 V or 480 V. Mode 4 (fast) uses DC electricity with a maximum current of 400 A and a maximum voltage of 600 V. It is worth noting that the electric vehicle manufacturer of Tesla uses its own standards for products sold in North America, but will adapt to IEC standards for products sold in other countries.

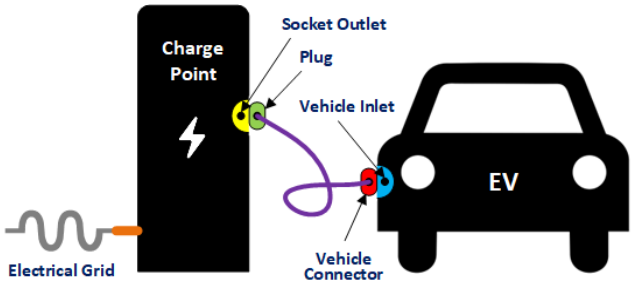

Figure 1. Accessories of an EV charging system

The IEC also defines three types of vehicle connectors for AC electric charging in IEC 62196-2:2016 [15]:

(1) Type 1, which is commonly used in North America and Japan.

(2) Type 2, which is commonly used in Germany, Spain, the United Kingdom, the Netherlands, Sweden, and China.

(3) Type 3, which is commonly used in France and Italy.

In addition, the IEC also defines the vehicle connector for DC electric charging [16], Type 4, that includes three different standardized charging systems in IEC 62196-3:2014:

(1) CHAdeMO, which is commonly used in Japan.

(2) Combined Charging System (CCS) Combo 1, which is a Type 1 with an additional connector for DC charging and is commonly used in North America.

(3) Combined Charging System (CCS) Combo 2, which is a Type 2 with an additional connector for DC charging and is commonly used in Europe.

In relation to electric vehicle charging, Afshar et al. [17] break down the electric vehicle supply equipment (EVSE) into three categories: fixed charging stations (private or public), mobile charging stations (portable, truck-mounted, or vehicle-to-vehicle power transfer), and contactless charging methods (battery swapping or wireless road charging). To access public charging stations, such as by using a contactless card or radio-frequency identification (RFID), an EV driver typically must have a contract with the corresponding charge point operator (CPO). If the driver wants to use a charge point belonging to a different CPO with whom they do not have a contract, they can still do so as long as the driver has a contract with a mobility service provider (MSP) that has an agreement with that CPO, which may also have an agreement with other CPOs. This is referred to as 'EV roaming service system' as specified [18]. Roaming in electric mobility (EV roaming) enables seamless access to charge points from multiple networks with just one user registration, rather than having to create multiple accounts [19]. This leads to a more efficient process for EV drivers.

There are four major existing EV roaming protocols [20-22], namely the Open Clearing House Protocol (OCHP), the Open InterCharge Protocol (OICP), the eMobility Inter-operation Protocol (eMIP), and the Open Charge Point Interface (OCPI). These protocols allow seamless data exchange between CPOs and MSPs during roaming transactions, and enable the transfer of essential data, such as authentication data, remote start/stop control of the charge point, details about the charge point and charging session, and billing. In addition, these protocols rely on HTTP [23-27] and, to some degree, comply with the six criteria for open standards as formulated by the Committee on Technical Barriers to Trade of the World Trade Organization (WTO TBT), which are nowadays considered as the universal reference [28-30]. These criteria are openness, impartiality and consensus, effectiveness and relevance, coherence, and developing country interests. A comprehensive explanation of how these major EV roaming protocols manage tasks such as user registration, start a charging session, stop a charging session, and billing can be found in the study [31].

On the other hand, the CPO internal system typically relies on the Open Charge Point Protocol (OCPP). This protocol has become a widely accepted standard and has been integrated into many charge point products today [32] for communication between charge points and their central management system using HTTP or WebSocket [33], where WebSocket is a full-duplex communication protocol [34]. Therefore, based on the fact that OCPP is available in many charge point products, this study aims to enhance the functionality of OCPP and explore its feasibility in supporting EV roaming between CPOs with its existing functions. This study could contribute as valuable examples that expand technology options and encourage more researchers to participate in the development of EV roaming protocols that are most suitable for their respective countries. The recent version of the protocol is OCPP 2.0.1 [35], but this paper only applies to OCPP 1.6. Thus, the term 'OCPP' without a specified version in this paper always means OCPP 1.6.

The remainder of this paper is organized as follows. Section 2 briefly reviews the OCPP and the four major EV roaming protocols: OCHP, OICP, e-MIP, and OCPI. Section 3 presents simulation models development, actual products utilization, and describes scenarios for the experiment. Section 4 presents the experiment results of the proposed system, and Section 5 discusses the results and relevant topics. Section 6 concludes this paper.

2. PROTOCOLS OVERVIEW

2.1 Open Charge Point Protocol (OCPP)

The first version of OCPP, OCPP 1.5, was released in 2009 by the E-Laad foundation in the Netherlands. The latest version to date is OCPP 2.0.1, which was released in 2018 and is based on JSON over WebSocket only. Currently, OCPP is maintained by the Open Charge Alliance (OCA), a global consortium of public and private electric vehicle infrastructure leaders from Europe, North America, and other regions.

OCPP provides two methods of data exchange between the charge point and the central management system: either using Simple Object Access Protocol (SOAP) or JavaScript Object Notation (JSON) data format over the WebSocket. Within the OCPP framework, the charge point plays the role of a client, while the central system plays the role of a server. Interactions between the charge point and the central system are based on a request-response mechanism. OCPP provides a set of messages that can be initiated either by the charge point or by the central system, such as Authorize to validate an identifier for charging, StartTransaction to inform when a charging session has started, MeterValues to periodically report the charge point's electrical meter values or other sensor values, StopTransaction to notify that a charging session has ended, RemoteStartTransaction to start a charging session from the central system, and so forth.

A charging session that begins at the charge point might be

illustrated as in Figure 2 and described as follows:

(1) EV drivers can initiate charging at the charge point by presenting an RFID tag or a smart card, which the central system recognizes as a valid user token. To obtain the token, prior registration with the central system is required. Once the central system confirms the token's validity, the charge point will start charging the electric vehicle.

(2) The charge point informs the central system when a charging session begins.

(3) The charge point reports the energy consumption data to the central system periodically.

(4) To stop the charging session, the charge point needs to verify whether or not the person is the one that initiated the charging session. Therefore, EV drivers must present the same token again to be authorized by the central system.

(5) Once authorized and the event stop, the charge point notifies the central system that the charging session has ended.

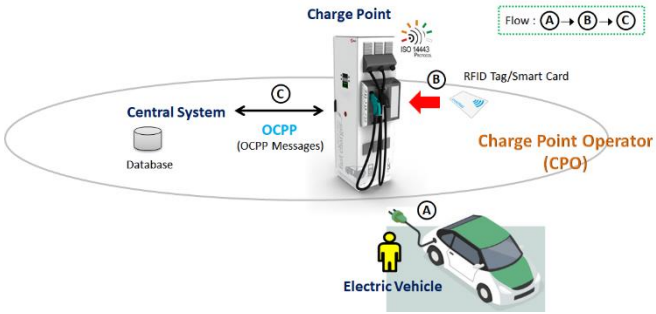

Figure 2. EV charging based on OCPP

2.2 Existing EV roaming protocols

This study focuses on EV roaming protocols currently in use, for which the complete protocol documentation is in a final form and publicly accessible, and which can be implemented by any party. The fact that these protocols are widely used in Europe is not surprising, as the region was the birthplace of the first protocols and remains the leader in EV roaming protocol development. Other parts of the world have also adopted some of these protocols. It is important to note that a global standard body, the International Electrotechnical Commission (IEC), has also released a standard in this area (IEC 63119 series). However, the standard has been excluded in this paper, as the full parts are still in progress at the time of writing.

2.2.1 Open Clearing House Protocol (OCHP)

The first publicly available EV roaming protocol, OCHP, was released in 2013 by Smartlab Innovationgesellschaft and ElaadNL, two organizations founded by German and Dutch utilities, respectively. It is used by e-clearing.net, a not-for-profit roaming hub that is operated by the same parties, which has now become a privately held company. The most recent version is OCHP 1.4, which was released in 2016, along with its extension, OCHPDirect 0.2, that supports peer-to-peer (p2p) connectivity. OCHP is licensed under the MIT License.

2.2.2 Open InterCharge Protocol (OICP)

In 2013, Hubject, a joint venture of German organizations, including BMW Group, Bosch, Mercedes-Benz, Volkswagen Group, EnBW, Siemens, innogy, and Enel X created OICP to facilitate EV roaming through the Hubject roaming hub. The most recent version, OICP 2.3, was released in 2020. OICP is licensed under the Creative Commons Attribution Share Alike 4.0 International License.

2.2.3 eMobility Inter-operation Protocol (eMIP)

The eMIP protocol was designed by GIREVE, a consortium of French organizations that includes EDF, Renault, CNR, and Caisse des Dépôts. The first operational version, eMIP 0.7.4, was released in 2015, and GIREVE remains the only operating roaming hub, requiring certification to connect to its platform. While the eMIP has been subject to many updates to add new features, as reflected in the frequent release of new description and implementation guide documents up to 2020, this did not require an update to the protocol itself. eMIP's users obtained a usage license from GIREVE.

2.2.4 Open Charge Point Interface (OCPI)

The OCPI protocol was initially developed by eViolin, a collaboration of Dutch CPOs and MSPs, in partnership with ElaadNL. The first official release of the protocol, OCPI 2.0, was published in 2015. Currently, the protocol is managed by the EVRoaming Foundation, which is a consortium consisting of Freshmile, Chargepoint, Google Maps, GIREVE, Last Mile Solutions, and NKL. Unlike the other EV roaming protocols discussed here, OCPI is the only protocol not managed by a party that also manages a roaming hub. The latest version, OCPI 2.2.1, was released in 2021, and the protocol is licensed under the MIT License.

Table 1. The actors involved in EV roaming and their roles

Roles	OCHP 1.4 & OCHPDirect 0.2	OICP 2.3	eMIP 0.7.4	OCPI 2.2.1
Provides services for charging EVs	EVSP	EMP	eMSP	eMSP
Operates the charge point	EVSE Operator	CPO	CPO	CPO
Delivers energy to EVs	EVSE	EVSE	Charge Point	Charge Point
Uses the charge point	EV user	User	User	EV user

Table 2. The basic functionalities of EV roaming protocols

Basic Functionality	OCHP 1.4 & OCHPDirect 0.2	OICP 2.3	eMIP 0.7.4	OCPI 2.2.1
Remote start/stop	●	●	●	●
Authorization	●	●	●	●
Billing	●	●	●	●
Synchronous (real-time) data exchange		●	●	●
Asynchronous data exchange	●	●	●	●

2.2.5 Actors, roles, and functionalities

The four major EV roaming protocols define similar actors but use different terminology to refer to them, as presented in Table 1. Please note that the information given in this section is limited to the actors that will be featured in the experiment of the proposed system. It is also important to note that the EV roaming protocols discussed here may define additional actors, roles, and functionalities not mentioned in this section.

The basic functionalities needed to support EV roaming are presented in Table 2, and these include giving remote start/stop commands to the charge point, authorization of the charge point user, and billing. The remaining functionalities consist of two methods that serve as the basis for authenticating charge point users: synchronous (real-time) and asynchronous approaches. These methods typically involve data exchange between MSPs and CPOs, either directly or via a roaming hub. Each protocol has its own preference for user authorization, such as OCHP, which does not support real-time authentication.

User authorization is the most important functionality in any EV roaming protocol. This process involves authenticating the user's identifier and verifying their eligibility to use the charge point, such as by ensuring that they have a valid user token and the payment status is clear. The earliest protocol, OCHP, uses an asynchronous approach to verify the identity of users. This method relies on a 'whitelist' of authorized users that the MSP shares with the roaming hub, which is then downloaded from the roaming hub by the CPO. Although this approach is robust against some network failures, such as when communication between the CPO and the MSP is lost, its potential drawback is that it may not always provide the most up-to-date information about a user's eligibility at the time of charging. As a result, users who are no longer authorized may still be able to use the charge point. To prevent this, frequent updates of the whitelists are necessary. On the other hand, the recent protocols OICP, eMIP, and OCPI utilize a synchronous approach. This method allows for real-time authentication of users using the most up-to-date information present at the MSP, ensuring that recently blocked users are promptly identified and prevented from using the charge point. The drawback of the synchronous approach arises when user authentication needs to be performed by the owner of the user data, such as the MSP, through a roaming hub instead of a peer-to-peer connection. This process takes more time as the authentication data must be sent to the roaming hub before being forwarded to the destination. Nevertheless, OICP, eMIP, and OCPI also support an asynchronous data exchange for business reasons, possibly to increase the availability of the charge points and to improve the reliability of the EV roaming system. However, it is important to note that when it comes to scalability in accessing networks outside your own, using a roaming hub offers greater availability.

Table 3. Technology features and supported business models

EV Roaming Protocol	Messaging Format	Communication Protocol	Supported Business Models
OCHP 1.4 OCHPDirect 0.2	SOAP	HTTP	Only via e-clearing.net peer-to-peer (p2p)
OICP 2.3	SOAP/REST APIs	HTTP	Only via Hubject
eMIP 0.7.4	SOAP	HTTP	Only via GIREVE
OCPI 2.2.1	JSON	HTTP	Both p2p and roaming hub

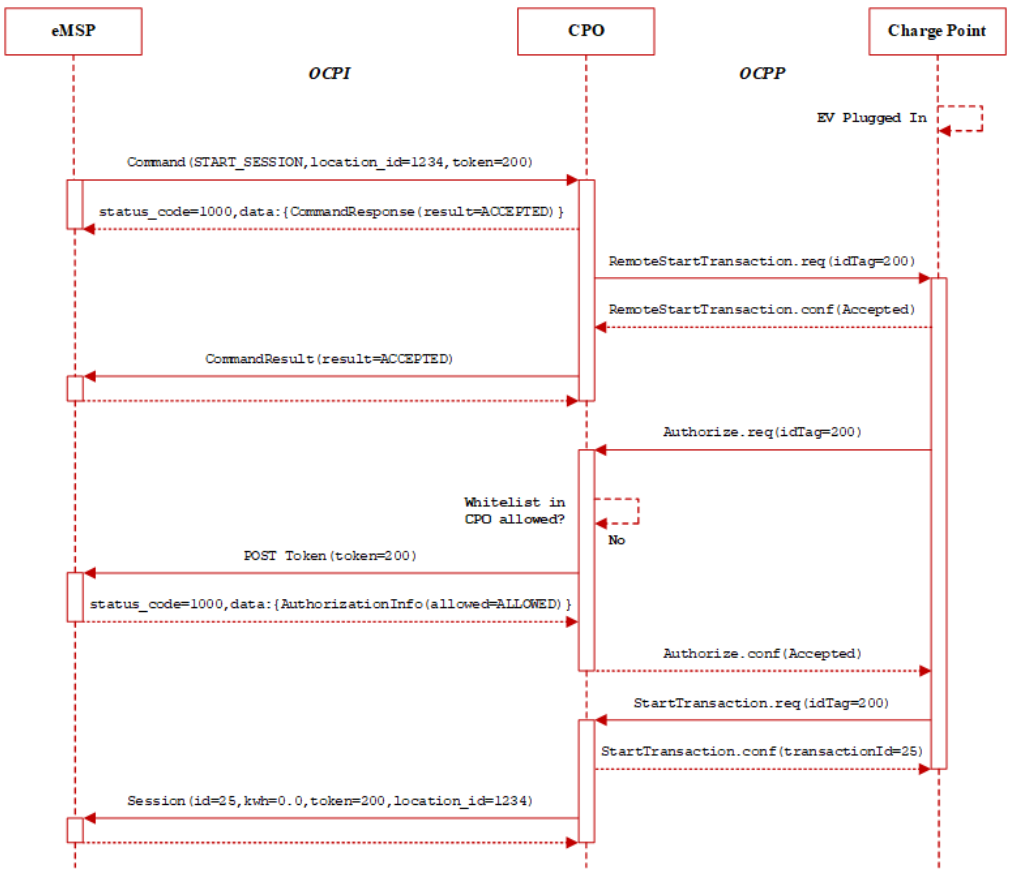

Figure 3. Synchronous data exchange in OCPI to start a charging session

Hypertext Transfer Protocol (HTTP) is used as the primary communication protocol for OCHP, OICP, eMIP, and OCPI, as presented in Table 3. This protocol enables the exchange of request-response messages between MSPs and CPOs, such as messages for remote start/stop commands, authorization, and billing. Figure 3 illustrates an example of synchronous data exchange between the MSP and the CPO to initiate a charging session in OCPI with the peer-to-peer topology. It is important to note that the communication between the charge point and the CPO (typically represented by the central system) uses the OCPP protocol. Thus, in an EV roaming system where OCPP has been integrated into the charge point, there are two different communication protocols in use – HTTP and WebSocket. This can be considered inefficient for many reasons.

The transactions illustrated in Figure 3 might be described as follows:

(1) The eMSP sends an OCPI request called 'Command', which includes parameters about the request intent, the charge point location, and the token to be authenticated in order to start a charging session. Subsequently, the CPO sends a response to confirm that the request has been accepted.

(2) After receiving the request from the eMSP, the CPO sends an OCPP request called 'RemoteStartTransaction' to the charge point. This message includes the token data received from the eMSP. In response, the charge point confirms that the request was accepted. The CPO then forwards the information about the successful initiation of the charging session to the eMSP using an OCPI request called 'CommandResult'.

(3) After the 'RemoteStartTransaction' request-response, the charge point may send an 'Authorize' request that contains the token data, now referred to as the tag id, to be authenticated by the central system. It is important to highlight whether the 'RemoteStartTransaction' request-response is followed by the 'Authorize' request depends on a particular configuration key described in the OCPP specification document.

(4) After receiving the 'Authorize' request containing the tag id from the charge point, the CPO forwards the tag id (now referred to as the token) to the eMSP for authentication using the actual user data that the eMSP has. This occurs in the case of a synchronous approach. However, this mechanism can be confusing because the eMSP is the origin of the token data. It is expected that the EVRoaming Foundation will soon release a solution to this issue.

(5) Once authorized by the eMSP, the charge point can start charging the electric vehicle. The charge point then sends the 'StartTransaction' request to the central system to inform that a charging session has started, which in return responds with the given transaction id to the charge point and also sends the 'Session' request to the eMSP to inform about the start of the requested charging session for the given token.

Table 4. The OICP's CDR

Field Name	Description
ChargingEnd	The date and time at which the charging process stopped.
EvseID	The ID that identifies the charging spot.
Identification	Authentication data used to authorize the user or car.
SessionID	The Hubject SessionID that identifies the process.
SessionStart	The date and time at which the session started, e.g. swipe of RFID.

After a charging session has ended, the CPO can prepare a Charge Detail Record (CDR) to share with the eMSP. The CDR contains the description of the completed charging session and is the only object relevant for billing purposes. Although there is no requirement to share CDRs in real-time, it is considered good practice to do so promptly.

An example of a CDR specified by OICP that includes the mandatory fields only is shown in Table 4.

2.3 Related communication protocols

HTTP is a request-response protocol where the client sends a request to the server, which then responds with the requested information. With HTTP, the client initiates a new connection with the server for each request, which can create additional overhead in terms of time and resources. This method has been revised by HTTP/2 and the most recent HTTP/3 by supporting bidirectional communication between the client and the server over a single connection. A study conducted by Priyasta et al. [31] overviews how the four major EV roaming protocols utilize HTTP for roaming purposes.

WebSocket, on the other hand, is a full-duplex, bidirectional protocol that enables continuous communication between the client and server over a single connection. This means that the client can send messages to the server, and then the server can send messages back to the client as a response, or the server can send messages to the client, and then the client can send a response to the server, without requiring the client to initiate a new connection for each message. This approach can reduce the overhead associated with establishing a new connection for every request-response cycle and enables any party to start the communication. As an example, OCPP provides messages for operations initiated by the charge point, such as Authorize and StartTransaction, as well as messages for operations initiated by the central system, such as RemoteStartTransaction.

HTTP request messages must use specific methods listed below to indicate the desired operations:

- GET - retrieves a resource from a server.
- POST - submits data to create/update a resource.
- PUT - uploads a new resource to a server.
- DELETE - deletes a resource from a server.
- HEAD - retrieves only the headers of a resource.
- OPTIONS - retrieves the options for a resource.

In addition, HTTP messages are limited in size, typically a few kilobytes, and are used to send structured data such as HTML, XML, and JSON.

On the other hand, WebSocket is designed to transmit both binary and text data in real-time using a flexible and extensible protocol that allows for the use of proprietary methods. The messages can be large enough, but their size may be limited by factors such as network bandwidth, message fragmentation, and implementation-specific limits.

Handling both HTTP and WebSocket simultaneously in a system can be a complicated task for any party, including the CPO. The differences in the way that these protocols work can create challenges for both developers and administrators who are responsible for implementing and maintaining the system that uses both protocols. However, experienced developers can use best practices and libraries to simplify the task of handling both protocols and mitigate potential issues. Similarly, system administrators can take advantage of network management best practices in order to improve their ability to monitor and debug network issues related to these protocols. In conclusion, if a single protocol can provide all the necessary functionality for a system, it is often the most efficient solution.

3. METHODS

3.1 Simulation models development

Actors and roles involved in the experiment to simulate the proposed EV roaming system are defined as follows:

- The **National Access Point (NAP)** facilitates EV roaming in the proposed system. The NAP acts like a roaming hub and is assigned the role of both the WebSocket client and the WebSocket server.
- The **Central System (CS)** manages charge points and connects to the National Access Point to provide EV roaming services for EV drivers. This allows them to communicate and exchange data with other CSs. The CS is assigned the role of both the WebSocket client and the WebSocket server.
- The **Charge Point (CP)** delivers energy to an EV and allows it to recharge its battery. The CP is assigned the role of the WebSocket client.

Three simulation models for the experiment, which includes the National Access Point Model, the Central System Model, and the Charge Point Model, have been developed using Java, each representing an actor in the proposed EV roaming system. The development sequence as shown in Figure 4 was followed to ensure reliability. In addition, an open-source central system platform called SteVe [36], as shown in Figure 5, which was developed at RWTH Aachen University, was utilized as the benchmark for creating the models. SteVe supports OCPP up to version 1.6 and is distributed under the General Public License (GPL).

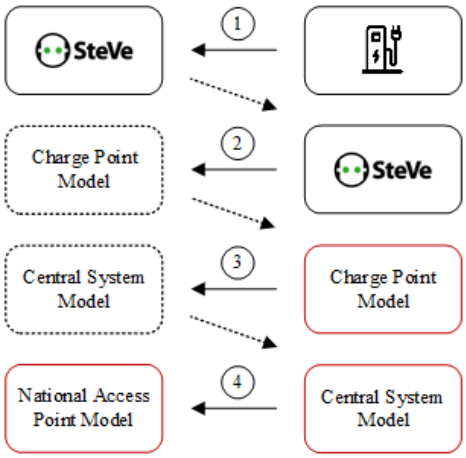

Figure 4. Simulation models development sequence

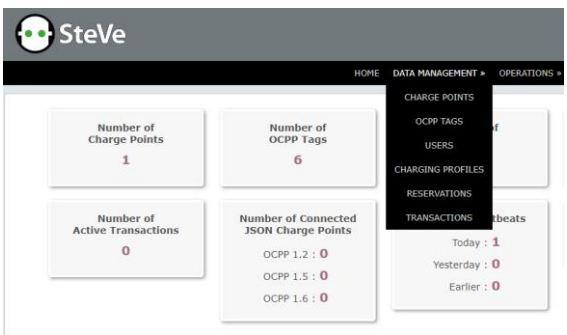

Figure 5. SteVe user interface

Figure 4 illustrates that once it is confirmed that SteVe can exchange data with the actual charge point product, it could be used as a reference for creating the Charge Point Model. The same method applies when creating both the Central System Model, which uses the fully functional Charge Point Model as a reference, and the National Access Point Model, which uses the fully functional Central System Model as a reference. It is important to note that both the Central System and the Charge Point are entities operated by the CPO, where, in best practice, the Central System is also responsible for managing users.

3.2 Simulation models interconnection

The three simulation models were designed to be connected to each other as shown in Figure 6. This connection technique, commonly found in distributed systems, enables seamless data exchange between the models. When a client sends a message to a WebSocket server, that server can forward the message to another server using another WebSocket connection, and so on, until the message reaches its appropriate destination. This will allow the models to work together effectively and efficiently, facilitating simulation of EV roaming activities.

Cascading the WebSocket connection is a technique used to pass WebSocket messages from one connection to another. It shares similarities with the cascading replication described by Red Hat, where a server acts both as a consumer and a supplier [37]. In both cases, the aim is to ensure that data is efficiently and reliably distributed across multiple connections, thereby improving the performance and reliability of the system. In the context of WebSocket connections, cascading can be useful in scenarios where a large number of clients need to receive real-time transactions in a system.

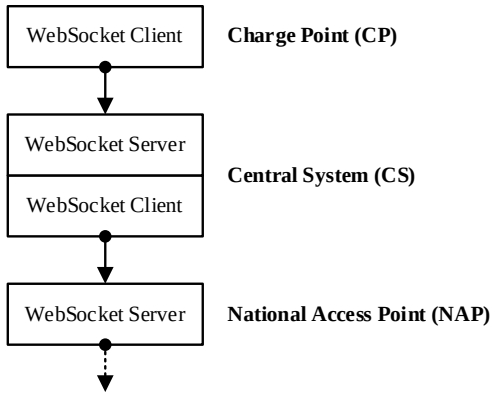

Figure 6. Cascading the WebSocket connection

3.3 Actual products utilization in the experiment

In addition to the simulation models, this study also utilizes actual charge point products in the experiment, including one charge point developed in-house and one manufactured by the industry. The in-house developed charge point has a maximum charging power of 22 kW and is equipped with Type 1 (J1772) connector, while the industry-manufactured charge point has a maximum charging power of 50 kW and is equipped with two connectors, CHAdeMO and CCS Combo 2. The objective of using these actual products is to ensure that the proposed EV roaming system can be implemented in real-world scenarios. Figures 7(a) and (b) show the visual representations of the two charge point products.

Furthermore, in order to simulate EV roaming using actual charge point products, this study utilizes an electric vehicle as shown in Figure 8. The car supports both Type 1 (J1772) and CHAdeMO connectors.

(a) Made in-house

(b) Made by the industry

Figure 7. Charge point products used in the experiment

Figure 8. EV used in the experiment

3.4 Scenarios and evaluation

The experiment will be conducted based on five scenarios mentioned below. Qualitative evaluation determines whether the scenarios can be successfully simulated, while quantitative evaluation measures the time required for user authorization processes using both the completed simulation models and the actual products. In this study, the user authorization process is defined as the duration between the request message and the corresponding response message, which is used to authorize a user for using the charge point. Furthermore, it was decided to conduct the experiment during high traffic load conditions of a network where normal subscriber expectations would not be met, but for which a reduced level of performance should still be achieved to prevent excessive repeat calling and spread of network congestion, as described in the study [38].

The high traffic load conditions are chosen for the following reasons:

- **Realistic testing**: High traffic load conditions create a more realistic testing environment. If a system is intended to be used in a high traffic scenario, it is important to test it under such conditions to ensure that it can perform optimally in the intended use case. The objective is to ensure that EV roaming between CPOs remains available even during periods of high traffic load, such as peak hours.
- **Performance evaluation**: Conducting an experiment under high traffic load conditions is useful in order to evaluate the performance of the system under stress. This approach can help to identify any potential weaknesses that may not be seen under normal conditions. For instance, the network connection between CPOs remains stable, and user authorization is within the acceptable time limit.
- **Optimization**: High traffic load conditions can create an opportunity to improve system performance by identifying specific areas for optimization. For instance, new methods for user authorization that are more effective and efficient can be well-measured and introduced.
- **Risk mitigation**: Conducting experiments under high traffic load conditions can help to mitigate the risk of system failure and improve reliability by identifying potential issues in high load conditions that can be addressed to reduce the risk of system failure. In this case, the decision whether to increase the scalability of EV roaming networks can be obtained based on the endurance under high traffic load conditions.

The following are the five scenarios used for the experiment. Each scenario is coupled with its respective flow chart, which depicts user authorization to grant access to the Charge Point based on a valid user token, up to the provision of the CDR.

3.4.1 Scenario one

"An EV driver, *D*, registered with CPO 1, C_1, and received a valid user token, *T*, for accessing Charge Points operated by C_1, which then shares *T* with the National Access Point, *N*. Currently, *D* needs to access a Charge Point operated by C_2 using *T*, where C_2 has a 'whitelist' of valid user tokens from *N*. Thus, *D* can be granted access to the Charge Point."

Figure 9 shows the decision whether or not to grant access to the Charge Point for scenario one.

3.4.2 Scenario two

"An EV driver, *D*, registered with CPO 1, C_1, and received a valid user token, *T*, for accessing Charge Points operated by C_1. Currently, *D* needs to access a Charge Point operated by CPO 2, C_2, using *T*. Both C_1 and C_2 have shared their 'whitelist' of registered user tokens with the National Access Point, *N*, for authenticating EV drivers who require Charge Points from CPOs they are not yet registered with. *D* can be granted access to the Charge Point operated by C_2 through authentication by *N*. After *D* finishes using the Charge Point, C_2 will send the payment details to *N*, which then shares them with C_1."

Figure 10 shows the decision whether or not to grant access to the Charge Point for scenario two.

3.4.3 Scenario three

"An EV driver, *D*, registered with CPO 1, C_1, and received a valid user token, *T*, for accessing Charge Points operated by C_1. Currently, *D* needs to access a Charge Point operated by CPO 2, C_2, using *T*. Both C_1 and C_2 have shared their endpoint with the National Access Point, *N*, enabling other parties to authorize EV drivers who require access to their Charge Points. *D* can be granted access to the Charge Point operated by C_2 based on the following processes: 1) *N* provides the endpoint of C_1 to C_2, and 2) C_2 requests authentication of *D* from C_1. After *D* finishes using the Charge Point, C_2 will send billing information to C_1."

Figure 11 shows the decision whether or not to grant access to the Charge Point for scenario three.

3.4.4 Scenario four

"An EV driver, *D*, registered with CPO 1, C_1, and received a valid user token, *T*, for accessing Charge Points operated by C_1. Currently, *D* needs to access a Charge Point operated by CPO 2, C_2, using *T*. Both C_1 and C_2 have shared their endpoint with the National Access Point, *N*, enabling *N* to redirect any authentication request to the corresponding CPOs. *D* can be granted access to the Charge Point operated by C_2 based on the following processes: 1) *N* redirects the authentication of *D* to C_1, and 2) C_1 sends the authentication result of *D* to *N*, which then forwards it to C_2. After *D* finishes using the Charge Point, C_2 will send an invoice to *N*, which then shares it with C_1."

Figure 12 shows the decision whether or not to grant access to the Charge Point for scenario four.

3.4.5 Scenario five

"An EV driver, *D*, registered with CPO 1, C_1, and received a valid user token, *T*, to access Charge Points operated by C_1. Currently, *D* needs to access a Charge Point operated by CPO 2, C_2, using *T*. However, only C_1 is connected to the National Access Point, *N*, to enable EV roaming for EV drivers, while C_2 does not have an agreement with and is not yet connected to *N*. Therefore, *D* cannot be granted access to the requested Charge Point operated by C_2."

Figure 9 also shows the decision to not grant access to the Charge Point for scenario five.

4. RESULTS

The experiment results presented in this section are based on the methods described earlier. The National Access Point Model and the Central System Model were run on personal computers, while the Charge Point Model was run on a laptop. All devices used in the experiment, including the charge point products, were connected to a single network service provider via a Wi-Fi modem. This modem also functioned as a hub for communication between components within the system, using a star topology as shown in Figure 13.

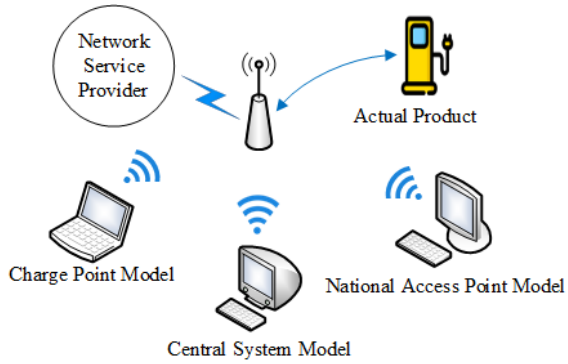

Figure 13. Network topology used in the experiment

4.1 Qualitative and quantitative evaluations

The experiment successfully simulated the given scenarios. The user authorization time was assessed when using only the simulation models and when the actual products were included. The evaluation results are presented in Table 5, which clearly indicate that the user authorization time was relatively similar for both cases.

Table 5. The experiment's evaluation results

Scenarios	Simulatable	Average Time for User Authorization over Five Attempts (ms)		
		CP Model	CP In-house	CP Industry
Scenario one	Yes	2.6	3.0	2.6
Scenario two	Yes	1021.0	1022.6	1020.8
Scenario three	Yes	2032.2	2181.2	2091.2
Scenario four	Yes	2032.8	2186.8	2049.4
Scenario five	Yes	N/A	N/A	N/A

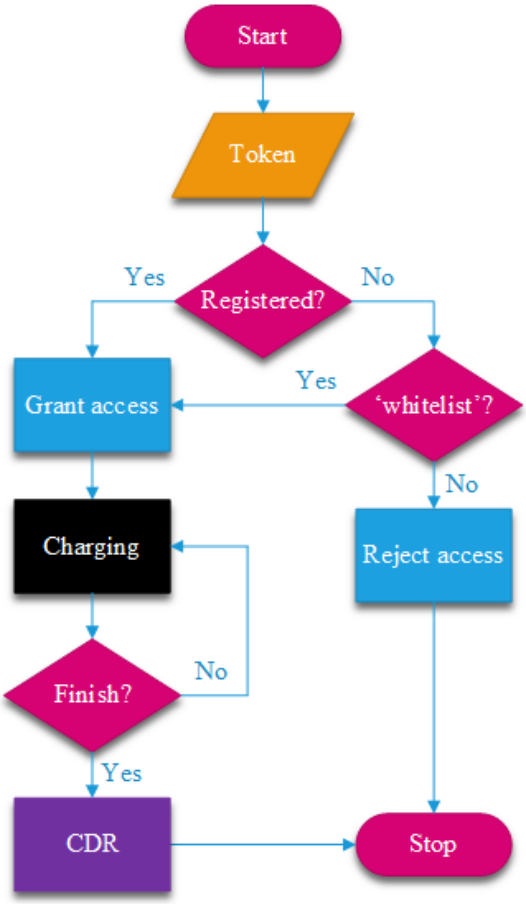

Figure 9. Scenario one access decision at C_2

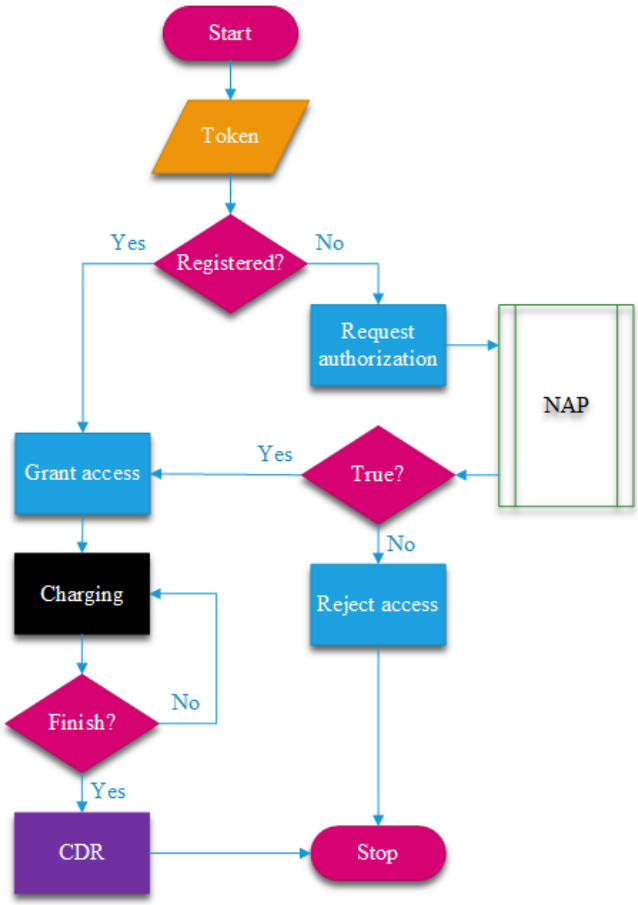

Figure 10. Scenario two access decision at C_2

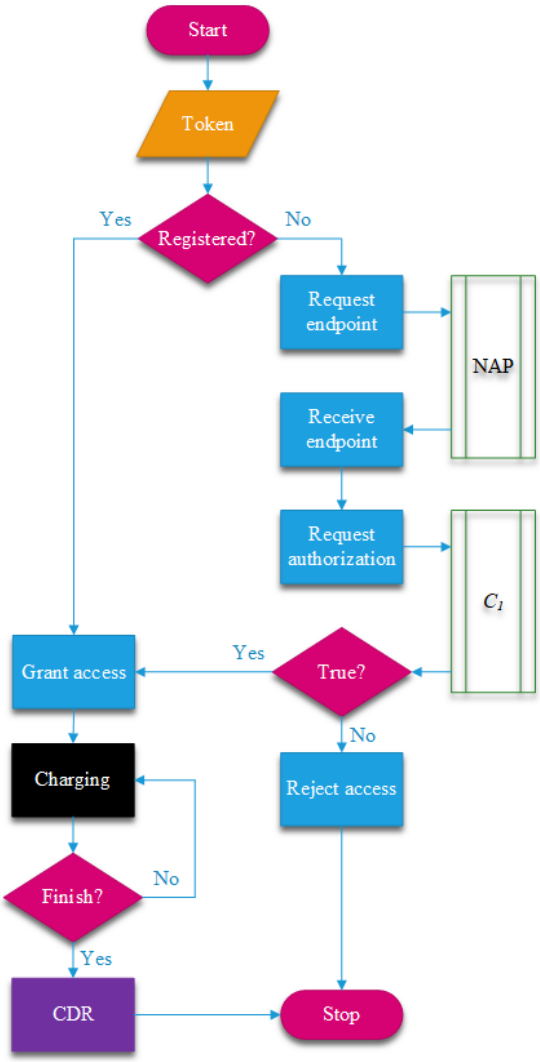

Figure 11. Scenario three access decision at C_2

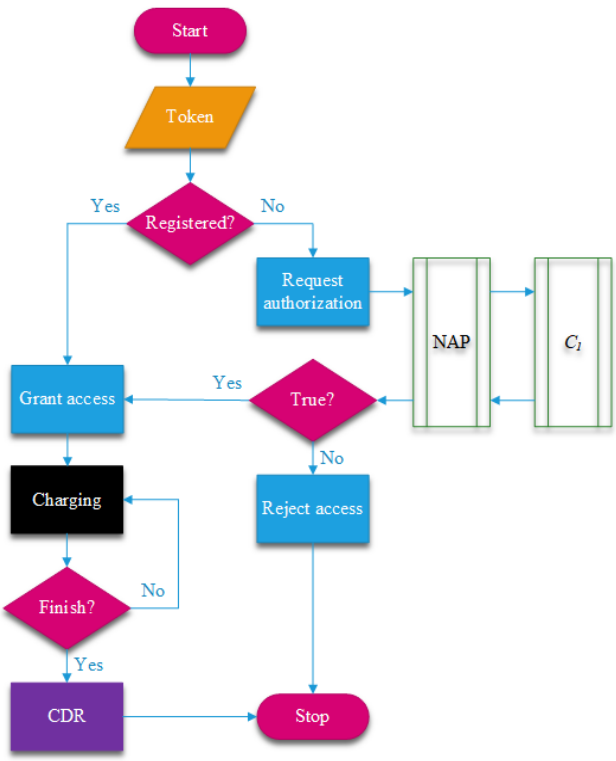

Figure 12. Scenario four access decision at C_2

4.2 Sharing CDRs

The 'DataTransfer' message, which is a user-defined OCPP message, is used to encapsulate CDRs for inter-central system billing purposes. The Central System sends this message to the National Access Point, which then shares it with the relevant Central System. Figure 14 shows the implementation of CDRs in this experiment. It is important to note that the CDRs in this experiment are simulated for experimental purposes only, but they are based on the actual charging sessions and can be used as the basis for billing in real-world scenarios.

```
[09:37:28] Receiving message DataTransfer.
[09:37:28] Request:
[2,"0b3YZGFGLTHw9dkC7nghVb42OXjZilC6LZWB","DataTransfer",{
    "data": {
        "sessionStart": "2023-03-14T02:36:54.786Z",
        "idTag": "01020304050609",
        "meterStart": 0,
        "operatorId": "DSICPO",
        "transactionId": 100,
        "meterStop": 20000
    },
    "vendorId": "ev_roaming",
    "messageId": "cdr"
}]
```

Figure 14. The simulated CDR in JSON data format

The details of the simulated CDR are presented in Table 6, with field names aligned with the OCPP as much as possible. It is important to underline that the simulated CDR is located in the 'data' field of the 'DataTransfer' message.

4.3 Proposed EV roaming system's architecture

The experiment results in this study lead to a proposed EV roaming system that enables seamless access to charge points from different operators with a single user registration, rather than having to create multiple accounts. The architecture of the proposed EV roaming system, which consists of the National Access Point, the Central System, and the Charge Point, is illustrated in Figure 15. The experiment has demonstrated the effectiveness of the proposed EV roaming system, indicating that it could have significant impacts for the future of electric vehicle charging infrastructure.

Table 6. The simulated CDR content

Field Name	Description
sessionStart	The date and time at which the session started, e.g. swipe of RFID.
idTag	Token data that needs to be authorized.
meterStart	The meter value in Wh at start of the charging session.
operatorId	Unique ID that identifies the charge point operator.
transactionId	Unique ID that identifies the session.
meterStop	The meter value in Wh at end of the charging session.

Figure 15 presents information indicating that the EV driver has a direct contract with CPO 1, but not with CPO 2 and CPO 3. Moreover, both CPO 1 and CPO 2 have individual contracts with the National Access Point and are connected to it through their Central Systems. This connectivity allows the EV driver to utilize the Charge Point operated by CPO 1 as well as CPO 2. However, CPO 3, which does not have a contract with the National Access Point, remains inaccessible to the EV driver.

By having one contract with a single CPO within the proposed system, the EV driver benefits from increased access and use of EV charging infrastructure across different CPOs, making it easier for them to drive their electric vehicle with confidence.

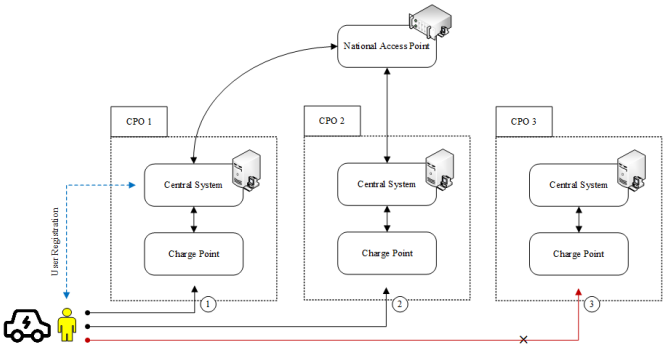

Figure 15. The proposed EV roaming system's architecture

5. DISCUSSION

The provided scenarios for the conducted experiment in this study outline potential business models for the proposed EV roaming system, which can be described as follows:

- Scenario one, which demonstrates asynchronous data exchange, is the fastest user authorization in the experiment. This scheme requires CPOs to share their authorized user data with the NAP, which then shares the 'whitelist' of valid user tokens with all CPOs. This allows for local user authentication for EV roaming. However, as mentioned earlier, the drawback of this approach is that the system may not always have the latest information regarding a user's eligibility during the EV roaming process. Sharing valid user tokens with the roaming hub, which can then be shared with the CPO, is also provided by OCHP, eMIP, and OCPI. In this case, it is important to note that security and privacy issues must be taken into account and that the user agrees to the sharing of their data.
- Scenario two, which also demonstrates asynchronous data exchange, requires CPOs to connect to the NAP for user authentication. This scheme also requires CPOs to share their authorized user data with the NAP for authentication purposes. This scenario significantly demands more user authorization time than scenario one, and similarly, the system might not be updated with the latest user eligibility information during the EV roaming process. In this case, the NAP does not share the valid user tokens with the CPO, and user authentication is done by the NAP. Thus, the responsibility for data security is in the hands of the NAP solely, and also the CPO where the user was initially registered.
- Scenario three, which demonstrates synchronous data exchange, doubles the time required for user authorization in comparison with scenario two. This scenario requires CPOs to share their endpoint for the user authentication service with the NAP, which then shares it with the requesting CPO. This CPO needs to connect to the corresponding CPO using the provided endpoint for user authentication purposes. In scenario three, the NAP's task is completed after sending the endpoint to the requesting CPO. This approach can be considered new and for experimental only, as it was not found in OCHP, OICP, eMIP, and OCPI. There are no issues with data security and privacy concerns in this approach. However, the requesting CPO must find the relevant CPO to request for user authentication.
- Scenario four provides a user authorization time that is approximately the same as in scenario three. Moreover, this scenario also demonstrates synchronous data exchange, which reflects real-time user authentication. However, in scenario four, user authentication is performed by the CPO that owns the user data, whereas the NAP serves as a roaming hub for authentication. This is similar to those in OCHP, OICP, eMIP, and OCPI.
- Scenario five demonstrates that if a CPO is currently not supporting EV roaming (i.e., does not have a contract with the NAP), then the users belonging to other CPOs might not be granted access to charge points belonging to that CPO.

The effectiveness of the proposed EV roaming system starts with the establishment of connections between all components within the system. In this context, the connection between the WebSocket clients and the WebSocket servers are established from the CP to the CS up to the NAP. This arrangement creates a virtual channel for bidirectional data exchange that enables seamless communication for EV roaming or other purposes. It is clear from this paper that the proposed EV roaming system does not yet include any MSP, as in other existing EV roaming protocols discussed in this paper. However, this does not mean there is no room for the MSP in the proposed system, as this paper is intended to present the simplest architectural solution. In fact, the role of an MSP can be taken over by the CPO, such as for handling user registration, contract, and payment. In the case where an actual MSP exists, the business model could be similar as those described in OCHP, OICP, eMIP, and OCPI, with the NAP becoming a roaming hub that has an agreement with the MSP.

Payment details in an EV roaming protocol typically relies on CDRs. After the end of a charging session, a CDR is sent by the local CPO to the EV driver's home CPO, which then calculates the cost of the charging session based on the tariffs agreed upon with the local CPO. The EV driver is then charged by the home CPO for the charging session, and the home CPO pays the local CPO for the service. This method is useful for those who frequently use public charging stations and prefer only their home CPO for billing and payment. On the other hand, ad-hoc payments (pay directly using credit cards, mobile payment apps, etc.) are useful for those who do not frequently use public charging stations and do not want to commit to a subscription plan. Both CDR and ad-hoc payment have their pros and cons. CDR provides a more convenient and efficient payment process for EV drivers, as they only need to deal with their home CPO for billing and payment. Ad-hoc payment, in contrast, provides more flexibility and can be more convenient for EV drivers who do not want to be restricted to a particular CPO. However, ad-hoc payment can also be more expensive, as CPOs may charge higher fees to cover the cost of processing ad-hoc payments.

The CDR can contain data about start and stop meter values, and hence can be considered a source of energy consumption data. This data is important for various stakeholders, including the local government, as they may want to develop a predictive machine learning model to forecast energy consumption for the next day based on data from previous days for optimizing energy distribution, increasing energy efficiency, and reducing energy costs. Furthermore, such a model could potentially lead to dynamic pricing, which can benefit both energy consumers and suppliers. Consumers could save money by using energy during off-peak demand, while suppliers could manage their energy resources more efficiently, reduce peak demand, and ensure a stable supply of energy. Studies [39-41] provide

information on the study that explores predictive models for energy consumption based on machine learning.

Calculating payments based on the CDR can be as follows:

$$B = (EC \times BR) + TX \quad (1)$$

where,

B = billing price
EC = stop meter – start meter
BR = base electricity rate
TX = government tax

The NAP is the central element of the proposed EV roaming system, without which EV roaming cannot be carried out. In non-continental countries, such as Indonesia, where electric mobility in transportation occurs only within the country, an appointed government institution can participate as the NAP. Whereas in other countries where electric mobility in cross-border transportation is frequent, another business model may be preferred. Furthermore, it is important for regulations to be established that ensure cooperation between different charging networks and guarantee fair and transparent pricing for EV drivers. This will help to promote the growth of the EV market and increase adoption of electric mobility.

User authentication to authorize EV drivers who want to use a charge point can be achieved in several ways, including the plain verification and approaches that involve security. Plain verification could include methods such as checking the user's identifier, whereas security approaches might involve N-factor authentication, or encryption to protect the user's information and prevent unauthorized access.

Aydin [42] proposes an authentication and billing scheme for EV charging that includes mutual authentication based on a MAC calculated from random numbers and the encrypted user's identifier using the AES algorithm. ElGhanam et al. [43] propose a fast, secure, and lightweight authentication and billing scheme using symmetric and asymmetric cryptography for dynamic wireless charging of EVs in an Internet of Electric Vehicles (IoEV) that integrates EVs into the Internet of Things (IoT) ecosystem. From all available sources, a comprehensive reference that discusses the authentication and billing scheme using OCPP can be found in the study [44].

The traffic load of the communication network could affect the performance of an EV charging session, with higher traffic loads increasing the chance of collisions and requiring more connection attempts for the session to complete. To guarantee quality of service (QoS) and quality of experience (QoE), it is important to classify the traffic on the communication channel between all entities involved in the session: the Charge Point, the Central System, and the National Access Point. In the study [45], traffic classification and prediction of network traffic load are discussed for a software-defined network with high prediction accuracy. The traffic load of the communication network also increases with the number of EVs in vicinity with the charge points. The populations of EVs in the residential, business, and working area, along with the corresponding load comparison of charge points under different forecast methods and the number of queuing vehicles, finish queuing time, and idle time are discussed in the study [46].

6. CONCLUSIONS AND FUTURE WORK

This paper presents a novel EV roaming system based on the enhanced functionality of the OCPP. The system integrates the role of the WebSocket client into the central system, which already acts as the WebSocket server, to provide EV roaming services for EV drivers. The system's actors and architecture are presented, along with the introduction of three simulation models that represent each actor in the proposed EV roaming system: the Charge Point, the Central System, and the National Access Point. The proposed EV roaming system was evaluated through experiments that focused on user authorization and billing, using both simulation models and actual charge point products. The results confirm that the proposed EV roaming system is feasible for implementation.

Certainly, there is still much work that needs to be done to complete this study. One possibility for future study could be expanding the scope of the evaluation to further challenging scenarios, such as involving infrastructure diversity, instability, network communication errors, and interoperability with other EV roaming systems. In addition, it is important to elaborate by providing complete functionalities of the proposed system, while current assumption is already enough to only utilize the multipurpose DataTransfer message provided by the OCPP for EV roaming purposes. It may also be necessary to investigate potential security vulnerabilities and implementing measures to ensure that the proposed system is secure against potential attacks.

The current study had been conducted internally, without involving potential stakeholders, including existing CPOs and related government bodies. Therefore, in the near future, they should be included to gain more realistic real-world scenarios and conformity with the government regulations. Furthermore, it is worth introducing the role of the National Access Point to the government, as they have the potential to fulfill this role.

The current study only focuses on the implementation of EV roaming in Indonesia, where the authors live. The findings of this study could be shared with neighboring ASEAN countries to promote the development of a unified ASEAN solution for electric mobility accross the region. The initial output could be in the form of technical reports that cover, for instance, similar works done by the evRoaming4EU project in Europe, which explore topics to maximize interoperability of the EV charging market and to promote the adoption of a standardized protocol for EV charging [20-22]. This initiative could also be extended to a wider region, covering Asia, which would include China, the world's largest EV market.

ACKNOWLEDGEMENT

The authors would like to thank Wahyu Cesar and Firson Satriasta for their contribution in the development of the work.

REFERENCES

[1] International Energy Agency. (2022). Global EV Outlook 2022. https://www.iea.org/reports/global-ev-outlook-2022, accessed on September 11, 2022.
[2] White, L.V., Carrel, A.L., Shi, W., Sintov, N.D. (2022). Why are charging stations associated with electric vehicle adoption? Untangling effects in three United States metropolitan areas. Energy Research & Social Science, 89: 102663. https://doi.org/10.1016/j.erss.2022.102663
[3] Nykvist, B., Sprei, F., Nilsson, M. (2019). Assessing the

progress toward lower priced long range battery electric vehicles. Energy Policy, 124: 144-155. https://doi.org/10.1016/j.enpol.2018.09.035

[4] Lander, L., Kallitsis, E., Hales, A., Edge, J.S., Korre, A., Offer, G. (2021). Cost and carbon footprint reduction of electric vehicle lithium-ion batteries through efficient thermal management. Applied Energy, 289: 116737. https://doi.org/10.1016/j.apenergy.2021.116737

[5] Ruoso, A.C., Ribeiro, J.L.D. (2022). The influence of countries' socioeconomic characteristics on the adoption of electric vehicle. Energy for Sustainable Development, 71: 251-262. https://doi.org/10.1016/j.esd.2022.10.003

[6] Munshi, T., Dhar, S., Painuly, J. (2022). Understanding barriers to electric vehicle adoption for personal mobility: A case study of middle income in-service residents in Hyderabad city, India. Energy Policy, 167: 112956. https://doi.org/10.1016/j.enpol.2022.112956

[7] Haidar, B., Rojas, M.T.A. (2022). The relationship between public charging infrastructure deployment and other socio-economic factors and electric vehicle adoption in France. Research in Transportation Economics, 95: 101208. https://doi.org/10.1016/j.retrec.2022.101208

[8] Langbroek, J.H.M., Franklin, J.P., Susilo, Y.O. (2016). The effect of policy incentives on electric vehicle adoption. Energy Policy, 94: 94-103. https://doi.org/10.1016/j.enpol.2016.03.050

[9] Choi, S., Kwak, K., Yang, S., Lim, S., Woo, J. (2022). Effects of policy instruments on electric scooter adoption in Jakarta, Indonesia: A discrete choice experiment approach. Economic Analysis and Policy, 76: 373-384. https://doi.org/10.1016/j.eap.2022.08.015

[10] Sahoo, D., Harichandan, S., Kar, S.K., Sreejesh. (2022). An empirical study on consumer motives and attitude towards adoption of electric vehicles in India: Policy implications for stakeholders. Energy Policy, 165: 112941. https://doi.org/10.1016/j.enpol.2022.112941

[11] Ramesan, S., Kumar, P., Garg, S.K. (2022). Analyzing the enablers to overcome the challenges in the adoption of electric vehicles in Delhi NCR. Case Studies on Transport Policy, 10(3): 1640-1650. https://doi.org/10.1016/j.cstp.2022.06.003

[12] Mohammadzadeh, N., Zegordi, S.H., Kashan, A.H., Nikbakhsh, E. (2022). Optimal government policy-making for the electric vehicle adoption using the total cost of ownership under the budget constraint. Sustainable Production and Consumption, 33: 477-507. https://doi.org/10.1016/j.spc.2022.07.015

[13] Alali, L., Niesten, E., Gagliardi, D. (2022). The impact of UK financial incentives on the adoption of electric fleets: The moderation effect of GDP change. Transportation Research Part A: Policy and Practice, 161: 200-220. https://doi.org/10.1016/j.tra.2022.04.011

[14] International Electrotechnical Commission. (2017). Electric vehicle conductive charging system - Part 1: General requirements. IEC 61851-1:2017

[15] International Electrotechnical Commission. (2016). Plugs, socket-outlets, vehicle connectors and vehicle inlets - Conductive charging of electric vehicles - Part 2: Dimensional compatibility and interchangeability requirements for a.c. pin and contact-tube accessories. IEC 62196-2:2016.

[16] International Electrotechnical Commission. (2014). Plugs, socket-outlets, vehicle connectors and vehicle inlets - Conductive charging of electric vehicles - Part 3: Dimensional compatibility and interchangeability requirements for d.c. and a.c./d.c. pin and contact-tube vehicle couplers. IEC 62196-3:2014.

[17] Afshar, S., Macedo, P., Mohamed, F., Disfani, V. (2021). Mobile charging stations for electric vehicles – A review. Renewable and Sustainable Energy Reviews, 152: 111654. https://doi.org/10.1016/j.rser.2021.111654

[18] International Electrotechnical Commission. (2019). Information exchange for electric vehicle charging roaming service - Part 1: General. IEC 63119-1:2019.

[19] Ferwerda, R., Bayings, M., Van der Kam, M., Bekkers, R. (2018). Advancing E-roaming in Europe: Towards a single "language" for the European charging infrastructure. World Electric Vehicle Journal, 9(4): 50. https://doi.org/10.3390/wevj9040050

[20] Van der Kam, M., Bekkers, R. (2020). Comparative analysis of standardized protocols for EV roaming - Report D6.1 for the evRoaming4EU project. https://evroaming.org/app/uploads/2020/06/D6.1-Comparative-analysis-of-standardized-protocols-for-EV-roaming.pdf, accessed on July 8, 2021.

[21] Van der Kam, M., Bekkers, R. (2020). Achieving interoperability for EV roaming: Pathways to harmonization - Report D6.2 for the evRoaming4EU project. https://evroaming.org/app/uploads/2020/06/D6.2-Achieving-interoperability-for-EV-roaming-Pathways-to-harmonization.pdf, accessed on July 8, 2021.

[22] Van der Kam, M., Bekkers, R. (2020). Design principles for an 'ideal' EV roaming protocol - Report D6.3 for the evRoaming4EU project. https://evroaming.org/app/uploads/2020/06/D6.3-Design-principles-for-an-ideal-EV-roaming-protocol.pdf, accessed on July 8, 2021.

[23] Smartlab, ElaadNL. (2016). Open Clearing House Protocol 1.4. https://github.com/e-clearing-net/OCHP

[24] Hubject. (2020). Open InterCharge Protocol for Charge Point Operators 2.3. https://github.com/hubject/oicp/tree/master/OICP-2.3/OICP%202.3%20CPO.

[25] Hubject. (2020). Open InterCharge Protocol for Emobility Service Providers 2.3. https://github.com/hubject/oicp/tree/master/OICP-2.3/OICP%202.3%20EMP.

[26] GIREVE. (2020). eMIP Protocol - Protocol Description 1.0.14. https://www.gireve.com/wp-content/uploads/2022/09/Gireve_Tech_eMIP-V0.7.4_ProtocolDescription_1.0.14-en.pdf, accessed on September 11, 2021.

[27] EVRoaming Foundation. (2021). Open Charge Point Interface 2.2.1. https://evroaming.org/app/uploads/2021/11/OCPI-2.2.1.pdf, accessed on November 10, 2021.

[28] Van der Kam, M., Bekkers, R. (2022). Mobility in the smart grid: roaming protocols for EV charging. IEEE Transactions on Smart Grid, 14(1): 810-822. https://doi.org/10.1109/TSG.2022.3202608

[29] World Trade Organization Committee on Technical Barriers To Trade. (2000). Second triennial review of the operation and implementation of the agreement on technical barriers to trade, document G/TBT/9.

[30] Institute of Electrical and Electronics Engineers. (2020). IEEE Position Statement: IEEE Adherence to the World

Trade Organization Principles for International Standardization. http://globalpolicy.ieee.org/wp-content/uploads/2020/08/IEEE20013.pdf, accessed on March 15, 2023.
[31] Priyasta, D., Hadiyanto, H., Septiawan, R. (2022). An overview of EV roaming protocols. In Proceedings of the 7th ICENIS 2022, Semarang, Indonesia. https://doi.org/10.1051/e3sconf/202235905006
[32] Van Amstel, M., Ghatikar, R., Wagers, A. Importance of open charge point protocol for the electric vehicle industry. Open Charge Alliance. https://www.openchargealliance.org/uploads/files/OCA-EN_whitepaper_OCPP_vs_proprietary_protocols_v1.0.pdf, accessed on April 4, 2023.
[33] Open Charge Alliance. (2017). Open Charge Point Protocol 1.6. https://www.openchargealliance.org/protocols/ocpp-16.
[34] Danny Coward. (2014). Java WebSocket Programming. Oracle Press, pp. xviii.
[35] Open Charge Alliance. (2018). OCPP 2.0. https://www.openchargealliance.org/protocols/ocpp-201
[36] The Intelligent Distributed Systems Group, RWTH Aachen University. SteVe. https://rwth-i5-idsg.github.io/about/steve, accessed on February 7, 2020.
[37] Red Hat. (2023). 15.5. Cascading Replication. https://access.redhat.com/documentation/en-us/red_hat_directory_server/11/html/administration_guide/cascading_replication, accessed on March 1, 2023.
[38] International Telecommunication Union. (1988). E.500: Traffic intensity measurement principles. https://www.itu.int/rec/T-REC-E.500-198811-S/en.
[39] Ullah, I., Liu, K., Yamamoto, T., Zahid, M., Jamal, A. (2021). Electric vehicle energy consumption prediction using stacked generalization: An ensemble learning approach. International Journal of Green Energy, 18(9): 896-909. https://doi.org/10.1080/15435075.2021.1881902
[40] Renata, D.A., Fauziah, K., Aji, P., Larasati, A., Halidah, H., Tasurun, D.P., Astriani, Y., Riza. (2021). Modeling of electric vehicle charging energy consumption using machine learning. In Proceedings of the 2021 International Conference on Advanced Computer Science and Information Systems (ICACSIS), Jakarta, Indonesia. https://doi.org/10.1109/ICACSIS53237.2021.9631324
[41] Shapi, M.K.M., Ramli, N.A., Awalin, L.J. (2021). Energy consumption prediction by using machine learning for smart building: Case study in Malaysia. Developments in the Built Environment, 5: 100037. https://doi.org/10.1016/j.dibe.2020.100037
[42] Aydin, O. (2022). Authentication and billing scheme for the electric vehicles: EVABS. International Journal of Management Information Systems and Computer Science, 6(1): 29-42. https://doi.org/10.33461/uybisbbd.1075481
[43] ElGhanam, E., Ahmed, I., Hassan, M., Osman, A. (2021). Authentication and billing for dynamic wireless EV charging in an internet of electric vehicles. Future Internet, 13(10): 257. https://doi.org/10.3390/fi13100257
[44] Garofalaki, Z., Kosmanos, D., Moschoyiannis, S., Kallergis, D., Douligeris, C. (2022). Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (OCPP). IEEE Communications Surveys & Tutorials, 24(3): 1504-1533. https://doi.org/10.1109/COMST.2022.3184448
[45] Raikar, M.M., Meena, S.M., Mulla, M.M., Shetti, N.S., Karanandi, M. (2020). Data traffic classification in software defined networks (SDN) using supervised-learning. Procedia Computer Science, 171: 2750-2759. https://doi.org/10.1016/j.procs.2020.04.299
[46] Zhuang, Z., Zheng, X., Chen, Z., Jin, T., Li, Z. (2022). Load forecast of electric vehicle charging station considering multi-source information and user decision modification. Energies, 15(19): 7021. https://doi.org/10.3390/en15197021

NOMENCLATURE

BEV	Battery Electric Vehicle
IEA	International Energy Agency
EV	Electric Vehicle
ICEV	Internal Combustion Engine Vehicle
EVSE	Electric Vehicle Supply Equipment
RFID	Radio-Frequency Identification
CPO	Charge Point Operator
MSP	Mobility Service Provider
OCHP	Open Clearing House Protocol
OICP	Open InterCharge Protocol
eMIP	eMobility Inter-operation Protocol
OCPI	Open Charge Point Interface
WTO	The World Trade Organization
TBT	Technical Barriers to Trade
OCPP	Open Charge Point Protocol
OCA	Open Charge Alliance
SOAP	Simple Object Access Protocol
JSON	JavaScript Object Notation
IEC	International Electrotechnical Commission
EVSP	Electric Vehicle Service Provider
EMP	EMobility Service Provider
eMSP	eMobility Services Provider (in eMIP) e-Mobility Service Provider (in OCPI)
HTTP	Hypertext Transfer Protocol
CDR	Charge Detail Record
HTML	HyperText Markup Language
XML	eXtensible Markup Language
NAP	National Access Point
CS	Central System
CP	Charge Point
GPL	General Public License
MAC	Message Authentication Code
AES	Advanced Encryption Standard