Article

Authentication and Billing for Dynamic Wireless EV Charging in an Internet of Electric Vehicles

Eiman ElGhanam, Ibtihal Ahmed, Mohamed Hassan * and Ahmed Osman

Department of Electrical Engineering, American University of Sharjah, Sharjah P.O. Box 26666, United Arab Emirates; eelghanam@aus.edu (E.E.); g00070409@aus.edu (I.A.); aosmanahmed@aus.edu (A.O.)
* Correspondence: mshassan@aus.edu

Abstract: Dynamic wireless charging (DWC) is a promising technology to charge Electric Vehicles (EV) using on-road charging segments (CS), also known as DWC pads. In order to ensure effective utilization of this on-the-road charging service, communication and coordination need to be established between the EVs and the different network entities, thereby forming an Internet of Electric Vehicles (IoEV). In an IoEV, EVs can utilize different V2X communication modes to enable charging scheduling, load management, and reliable authentication and billing services. Yet, designing an authentication scheme for dynamic EV charging presents significant challenges given the mobility of the EVs and the short contact time between the EVs and the charging segments. Accordingly, this work proposes a fast, secure and lightweight authentication scheme that allows only authentic EVs with valid credentials to charge their batteries while ensuring secure and fair payments. The presented scheme starts with a key pre-distribution phase between the charging service company (CSC) and the charging pad owner (PO), followed by a hash chain and digital signature-based registration and authentication phase between the EV and the CSC, before the EV reaches the beginning of the charging lane. These preliminary authentication phases allow the authentication between the EVs and the charging segments to be performed using simple hash key verification operations prior to charging activation, which reduces the computational cost of the EVs and the CS. Symmetric and asymmetric key cryptography are utilized to secure the communication between the different network entities. Analysis of the computational and transmission time requirements of the proposed authentication scheme shows that, for an EV traveling at 60 km/h to start charging at the beginning of the charging lane, the authentication process must be initiated at least 1.35 m ahead of the starting point of the lane as it requires ≈ 81 ms to be completed.

Keywords: Internet of Electric Vehicles (IoEV); dynamic wireless charging (DWC); authentication; billing; cryptography; signature; hashing

Citation: ElGhanam, E.; Ahmed, I.; Hassan, M.; Osman, A. Authentication and Billing for Dynamic Wireless EV Charging in an Internet of Electric Vehicles. *Future Internet* **2021**, *13*, 257. <https://doi.org/10.3390/fi13100257>

Academic Editor: Paolo Bellavista

Received: 17 June 2021

Accepted: 12 July 2021

Published: 8 October 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

With the increasing global concerns on fuel consumption and global warming, extensive research and development activities are currently ongoing to encourage large-scale adoption of electric vehicles (EVs) as an alternative to internal combustion engine (ICE) vehicles, aiming to reduce pollution and conserve energy, while ensuring driver satisfaction [1,2]. This has motivated increasing global investments in the development of EV charging infrastructures, as well as in advanced battery technologies, to help reduce the range anxiety experienced by EV drivers due to limited EV battery capacities. Furthermore, government subsidies and the utilization of renewable energy sources for electricity generation, together with the high efficiency of EV motors, all help reduce the total cost of operation (TCO) of EVs. This helps compensate for the higher EV purchase prices compared to their ICE counterparts and further motivates the adoption of EVs [3,4].

EV charging can take place using plug-in charging cables or wireless charging pads. Plug-in charging, also known as wired charging, involves a direct physical connection

between the EV and the charging socket. This requires effective yet costly electrical isolation solutions to mitigate risks of electrocution, particularly during harsh weather conditions [3]. Furthermore, the need for hardware compatibility and/or interoperability between the EV charging connector and the charging inlet point impacts the convenience of EV users and may contribute to their range anxiety for fear of running out of charge without reaching a compatible charging point [5]. Accordingly, to reduce the risks associated with wired (plug-in) charging and improve charging flexibility and convenience, wireless EV charging solutions are becoming increasingly popular, in which the charging power is wirelessly transferred, typically using inductive coupling, between a primary charging pad laid on the ground and a secondary receiver pad fitted at the bottom of the EVs [6,7]. Nevertheless, range anxiety remains the key drawback for any stationary charging solution including static wireless charging systems, as EV drivers fear running out of charge before reaching the charging station and/or without completing their desired journeys on time.

Dynamic wireless charging (DWC) systems offer an effective solution to the issue of range anxiety. This is because, by laying charging segments in dedicated lanes along extended roadways, EVs can be charged wirelessly during their motion [2,6,8]. This ensures charge ubiquity during extended journeys, thereby reducing range anxiety and eliminating driving delays due to the EV charging downtime [9,10]. Furthermore, large-scale deployments of DWC lanes across different cities enable EV battery downsizing and reduces EV production costs by increasing the dependence on the energy received during the vehicle's motion [11,12]. This energy can also be wirelessly exchanged between traveling vehicles, using direct vehicle-to-vehicle (V2V) wireless energy transfer, given effective coordination and alignment between the EVs [13,14].

With the increasing penetration of EVs and the corresponding advantages and drawbacks of the different charging systems, these systems need to be integrated and collectively utilized within the city infrastructure to address the increasing demand for EV charging facilities. This requires effective energy management and coordination to avoid grid disturbance and overload from unregulated and/or unscheduled charging [15–17]. Accordingly, a network of electric vehicles, also referred to as the Internet of EVs (IoEV), needs to be established, in which EVs can communicate and exchange information securely with one another and with the surrounding infrastructure and the power grid, to enable charging coordination, effective energy management, grid load balancing and traffic optimization [18–20]. Hence, an IoEV consists of the different EVs and the corresponding charging infrastructure, including plug-in charging stations, static and dynamic wireless charging units and vehicle-to-vehicle (V2V) energy exchange facilities. These are shown in Figure 1.

Figure 1. Overview of EV charging solutions in an Internet of Electric Vehicles (IoEV) [21].

The concept of an IoEV leverages on the capabilities of vehicular ad hoc networks (VANETs) by defining each EV as an intelligent entity that communicates with other surrounding entities using V2X communications, to ultimately establish a framework for reliable EV charging coordination and effective demand management. Accordingly, the key requirements of V2X communications in an IoEV are high-speed communications, ultra-low latency and ultra-high reliability, particularly for DWC systems due to their relatively short charging durations compared with static charging [21–23]. Different V2X communication technologies are addressed in the literature, including Dedicated Short Range Communication (DSRC), cellular-V2X (C-V2X) and 5G-V2X communications [24,25], each of which offers different features to address the different requirements for effective EV communication and coordination in an IoEV [21]. A heterogeneous network integrating the different radio access technologies (RATs) with other 5G advanced technologies such as MIMO, mmWaves and D2D communications, further improves the capabilities of vehicular communications in an IoEV and helps satisfy the requirements of the different use cases in terms of throughput, reliability, latency, security and quality-of-service (QoS).

In addition to effective vehicular communications, accurate authentication algorithms with fair and efficient billing schemes are essential to establish effective EV charging coordination and demand management strategies. This is because, whether the coordination strategy is implemented using game theory as in [26,27] or fuzzy logic inferences as in [17,28,29], accurate user authorization is crucial to ensure reliable scheduling of the charging resources among the EVs demanding energy, while ensuring protection against free riders and other unauthorized drivers. Fair billing, on the other hand, maximizes EV drivers' satisfaction and motivates their participation in EV charging coordination programs. The effective operation of these programs ultimately helps reduce power network congestion and overloading, and ensures grid load balancing between the different charging points [30,31].

Nevertheless, the implementation of effective authentication and billing schemes for dynamically charged EVs is a challenging task. This is mainly due to the continuously varying charging rate during the vehicle's motion and the charging "handover" from one charging pad to another. In addition, the fast EV traveling speeds impose the need for low latency communications, and fast authentication protocols to guarantee accurate billing during the EV motion over the charging lanes. Hence, in an Internet of EVs in which different entities are interconnected with the charging infrastructure, the charging service provider (CSP) needs to ensure the authenticity of the EVs requesting the dynamic charging service and to verify the corresponding billing credentials before initiating the charging service. This needs to be achieved while preserving the privacy of EV user information and minimizing the computational overhead to ensure fast and lightweight communications during the vehicle's motion.

This work particularly focuses on the authentication and billing aspects of EVs utilizing the DWC infrastructure. Given the stringent requirements for low latency and high reliability due to the short lane-crossing duration, and assuming an efficient underlying communication network, this paper proposes a fast, secure and lightweight authentication and billing scheme for EVs requesting dynamic wireless charging. The proposed scheme allows each EV user to receive a single, aggregated bill instead of segment-by-segment payment, in a DWC network consisting of multiple charging lanes owned by different pad owners (PO) and coordinated using a Centralized Management and Coordination System (CMCS) in an IoEV within a smart grid. A charging service company (CSC) is responsible for EV registration and authentication with the DWC network. This scheme uses pseudonyms, symmetric and asymmetric encryption, and lightweight hashing to authenticate the EVs to the charging segments, after registration and authentication with the CSC and the PO. In the proposed model, the amount of energy demanded by the EV needs to be announced before the EV enters the charging lane. A heterogeneous communication network that integrates different communication technologies has been adopted, including 5G cellular networks, wired connections and Direct Short Range Communications (DSRC)

to meet the communication requirements of the different entities. The performance of the proposed model is analyzed in terms of security, communication overhead, computational cost and system delay.

The remainder of this paper is organized as follows: Section 2 provides a description of some of the cryptographic techniques used in this work. Section 3 then outlines the related works on authentication and billing of EVs in DWC systems. The system model, including the network entities and the communication and cryptographic protocols, is then presented in Section 4, and the proposed authentication and billing scheme is detailed in Section 5. Security analysis and performance evaluation of the proposed scheme are presented in Sections 6 and 7, respectively, before the paper is concluded in Section 8.

2. Preliminaries

This section explains some of the techniques used for information security and user authentication.

2.1. Symmetric and Asymmetric Cryptography

Asymmetric cryptography or public-key cryptography is a technique that uses pairs of keys, namely public and private keys, for encryption and decryption. In public-key cryptography, a message is encrypted using the receiver's public key, and only the intended receiver is able to decrypt the message using its private key [32]. In contrast, symmetric-key cryptography is based on a shared key that is used for both encryption and decryption [33]. Since a single shared key is utilized, the execution of symmetric key cryptography is faster and simpler than asymmetric cryptography protocols.

2.2. Digital Signatures

A digital signature is a cryptographic protocol that verifies the authenticity of a digital document or a message. This protocol is used in asymmetric cryptography to send information over an insecure channel, and the receiver can verify that the message is transmitted by the claimed sender [34]. The widely used digital signature techniques are Rivest, Shamir, and Adleman (RSA), Digital Signature Algorithm (DSA), and Elliptic Curve Digital Signature Algorithm (ECDSA) [35–37]. ECDSA is the recommended digital signature scheme in the IEEE 1609.2 standard, as it offers a lower computational overhead compared to RSA-based schemes [38,39]. Three steps are involved in digital signature schemes, namely: key generation, algorithm signing, and signature verification.

2.3. Hash Chains

A hash function is a mathematical one-way function that maps a message of an arbitrary size into a fixed-sized message that can be used for efficient authentication. A hash chain is a chain of multiple one-way hash functions generated using hash algorithms such as Secure Hash Algorithms-1 (SHA-1) or SHA-2 [40]. The first key is selected randomly and the remaining keys are calculated using the hash function, $\mathcal{H}$. Each key is found by $k_i = \mathcal{H}(k_{i-1})$ for $i = 1, 2, 3, \dots, n$ [40]. A sample 4-key hash chain is shown in Figure 2. For verification, the keys are verified in opposite order to the order of generation, i.e., k_n is the first key to be verified [35,40].

Figure 2. Sample 4-key hash chain.

3. Related Works

3.1. EV Authentication in DWC Systems

Different authentication techniques are proposed in the literature for DWC systems. A fast authentication for a dynamic EV charging (FADEC) model is proposed in [41], to provide fast message signatures, fast signature verification, and low communication overhead. The proposed system utilizes DSRC for the information exchange between the EVs and the road side units (RSUs). The cryptographic techniques employed for authentication include hash-based message authentication code (HMAC), Elliptic Curve Digital Signature Algorithm (ECDSA), and Just Fast Keying (JFK), which is a key exchange protocol based on the Diffie-Hellman protocol. The scheme is designed such that the same key is used to authenticate each EV to multiple RSUs, based on EV driving route estimation from traffic statistics, to avoid re-authentication and reduce handover latency. Nevertheless, this scheme does not preserve the privacy of the EV as the charging pad owners can determine the exact location of the EVs and can use this data for vehicle tracking.

To address the issue of EV location privacy, an anonymous authentication scheme is proposed by the authors in [42] using verifiable encryption, authenticated pairwise-keys and coin hash chains. The EV identity is preserved by using pseudonyms instead of its real identity, and a hash chain is used for verification purposes. A similar approach is also adopted in [9] and fast authentication is achieved using symmetric keys involving the spatiotemporal location of the EV. The scheme proposed in [9] further enhances the privacy of EV information and ensures lightweight authentication by eliminating the need for communication between the charging segments, allowing the EV to exchange the corresponding encrypted messages securely with each segment as it approaches it.

The authors in [43] also propose an efficient authentication protocol for dynamic charging using blind signatures and hashing. The process is initiated when the charging company generates keys and the EV purchases these keys and un-blinds them, while they are being verified by the charging management controller. The EV then uses a hash chain to authenticate itself to the charging segments and starts charging. Hence, the charging pads do not need to share any keys with the pad owner, and the EV anonymously authenticates itself to the pad owner using the blind signatures. Another authentication approach is proposed in [44,45], using partial blind signatures, hashing, and one-time tokens to formulate a secure and privacy-preserving physical-layer-assisted authentication model. However, while hash key verification is computational efficient for authentication between the EVs and the charging segments, the verification of blind signatures requires exponential operations and bilinear pairing, which increases the overall computational cost of the authentication models presented in [43–45].

A lightweight authentication and charging management scheme for DWC systems is also proposed in [46], involving EV registration and power negotiation with the charging controller, referred to as power supply station (PSS), and hierarchical token-based authentication with the RSUs. The DWC system in [46] assumes the charging energy is harvested from renewable energy sources (RES) and hence, power negotiation is essential to guarantee energy availability. The proposed system utilizes pseudonyms and digital signatures to first register the EVs with the PSS, then uses asymmetric key cryptography for power negotiation and demand management. The mutual authentication between the EVs and different system entities, using signature verification and public/private key pairs, ensures reliability and security of the message exchange process.

3.2. Billing Models in DWC Systems

In addition to authentication schemes, fair and privacy-preserving billing models are also reported in the literature, some of which utilize segment-by-segment billing [47,48] while others adopt a single bill approach [9,49].

In [47,48], the authors assume that a tamper-resistant module is installed on each EV to perform secure calculations required for authentication and billing. Segment-by-segment billing is performed with a bidirectional audit between the CSP and the EV, while assuming

that a constant amount of energy is supplied per segment. A key disadvantage of segment-by-segment billing is that it enables free-riders to charge before and after authenticated EVs by utilizing the associated handover delay from one segment to another. This particular problem is addressed by the authors in [50]. The proposed privacy-preserving billing approach in [50] uses token authentication and tamper-proof meters, and requests each authenticated EV to securely share its power levels before and after the charging lane with N segments. These levels are then compared to the actual energy supplied by the charging pads, and the difference in readings helps identify free-riders while preventing over-billing of authorized EVs.

Another lightweight and secure billing approach using hash functions and symmetric key cryptography is proposed in [49]. The process starts with a pre-registration phase using symmetric keys, followed by hashing with the different charging segments. At the end of the charging process, the EV communicates its received energy level with all the associated entities and is billed accordingly. A single bill approach is also adopted by the authors in [9], to achieve the required computational efficiency given effective privacy-preserving authentication protocols to ensure data security.

4. System Model

Different entities constitute the DWC infrastructure within the IoEV modeled in this work, namely: the charging service company (CSC), the charging pad owners (PO), the charging segments (CS), and the EVs. Each pad owner, PO_i , owns S_i charging segments. For simplicity, it is assumed that the charging segments are numbered $1, 2, 3, \dots, S_i$ and that the EVs always enter the charging lane at segment 1 and are charged subsequently by the following segments. Each EV has to register and sign a contract with a specific CSC before a registered pad owner, PO_i , provides dynamic charging to EVs. The EVs are, however, not billed directly by the PO. Instead, the PO submits the bills to the CSC, which pays for the EVs and then bills the subscribers accordingly. Each EV is assumed to be equipped with a tamper-proof device that carries out cryptographic computations, including message signatures, encryption and decryption. The proposed authentication and billing strategies in this work are developed to leverage on the advantages of the different approaches discussed in Sections 2 and 3 to provide fast, lightweight and privacy-preserving authentication with fair and efficient billing.

4.1. Communication Model

For the communication model, a wired connection is assumed between the charging segments and the pad owners, to provide a reliable and high-speed communication link. A 5G cellular communication link is used to exchange information between the EVs and the CSC, and between the EVs and the PO, through 5G base stations, also known as 5G g-Node-B (gNB). By using 5G communications, EVs benefit from the wide cellular coverage, ultra-low latency, high capacity, and the support for unicast, groupcast and broadcast messages [51–53]. This enables each EV to simultaneously initiate multiple dedicated communication sessions with different entities within the charging infrastructure. For the direct communication between the EVs and the charging segments, DSRC is utilized to benefit from the short operation range of DSRC links and avoid interference from adjacent channels. Utilizing DSRC between the EV and the CS also reduces the physical-layer latency due to the small air gap between the EV and the underlying segment. A summary of the different communication technologies utilized in the proposed model is shown in Figure 3.

Figure 3. Overview of the different communication technologies utilized in the proposed model.

4.2. Cryptography

In order to develop a secure and privacy-preserving authentication and billing scheme, different cryptographic methods are utilized in this work. In particular, the following cryptographic protocols are used:

- The SHA-256 algorithm is adopted for the hash function with 256 bits (32 bytes) output.
- The Advanced Encryption Standard (AES) algorithm is used for symmetric encryption of messages exchanged with the charging segments, with a 256-bit key and an output size of 16 bytes.
- The RSA algorithm is used for asymmetric encryption of messages exchanged between the EVs, the CSC and the PO, with a 2048-bit key and an output size of 256 bytes.
- The elliptic-curve digital signature algorithm (ECDSA) is used to sign the messages exchanged between the EVs, the CSC and the PO, resulting in 448-bit signatures.

Furthermore, additional communication security can be achieved by implementing advanced physical-layer security (PLS) techniques on the 5G wireless communication link [21,54,55], but this is beyond the scope of this work.

Table 1 lists each symbol used in the proposed authentication and billing strategy and the corresponding symbol length given the aforementioned cryptographic protocols.

Table 1. Description and length, in bytes, of the different symbols used in the proposed authentication and billing model.

Symbol	Description	Length (bytes)
C	ID of the charging service company	8
PO_i	Pad Owner ID	8
s	charging segment ID	8
I_e	Real identity of EV e	128
p	Pseudo identity of EV e	32
k_p	Session key for the EV with pseudo identity p	32
t_x	Time stamp of the message generated by x	8
$reqE$	Required energy by EV e	8
SIG_{gk_x}	Message signature with the signing key of x	56
$\varepsilon_{k_p}(\cdot)$	Symmetric key encryption using session key, k_p	16
$E_{pk_x}(\cdot)$	Asymmetric key encryption using public key, pk_x	256
$HashChReq$	Hash chain request	8
$\mathcal{H}_i()$	Hash function	32
h_n	Hash key for authentication with the n th segment	32
$param$	Charging parameters	32
$cost$	Unit cost of the charging energy, in \$/kWh	8
$P_{s,p}$	Power supplied by s to the EV with pseudonym p	8
E_p	Total energy supplied to the EV, calculated by the PO	8
E	Actual energy received by the EV	8

5. Proposed Authentication and Billing Scheme

Each entity in the DWC system at hand, namely the EV, the CSC and the PO, has its public and private key pair for encryption, (pk_x, sk_x) . The function $E_{pk_x}(\cdot)$ means encrypt the message with the public key of entity x . A pair of signing/verification keys is also used for each entity. The function $SIG_{sk_x}(\cdot)$ denotes signing the message with the signing key of x .

5.1. Key Pre-Distribution Phase

To begin with, the CSC generates pseudonyms and the corresponding key sets, $\mathcal{P}_i$ and $\mathcal{K}_i$, daily based on the traffic volume and sends the message $m_1: \{\mathcal{P}_i, \mathcal{K}_i, t_C, SIG_{gk_C}\}$ to each PO, denoted as PO_i , where the subscript i is the index of the PO owning the DWC lane, and the subscript C indicates that the message is initiated by the CSC. This message is signed using the signing key of the CSC and is encrypted using the public key of PO_i . Therefore, only the PO is able to decrypt the message using its private key. After receiving the message, PO_i verifies the signature of the CSC and forwards the pseudonyms and the corresponding key sets to the charging segments under its control in a message $m_2: \{\mathcal{P}_i, \mathcal{K}_i, t_{PO_i}\}$. This phase can be done during light traffic hours.

5.2. Registration and Authentication Phase

When EV e enters the charging lane, it has to communicate with the CSC to obtain a pseudonym, $p \in \mathcal{P}_i$, and a session key, $k_p \in \mathcal{K}_i$. To authenticate with the CSC and obtain the session key, EV e sends its real identity and its energy demand, $reqE$, in $m_3: \{I_e, t_e, reqE, SIG_{gk_e}\}$. To ensure the privacy of EV information, the calculation of the energy demand is performed on the on-board unit (OBU) of the EV, based on the current EV SoC, SoC_0 , the desired final SoC, SoC_f , and the maximum EV battery capacity, E_{max} , using the expression,

$$reqE = (SoC_f - SoC_0)E_{max}, \quad (1)$$

where the desired final SoC is estimated by each EV based on its remaining trip distance, its average traveling velocity and the average EV energy consumption rate [6,28]. The message m_3 is then signed using the signing key of EV e and is encrypted using the public key of the CSC, $E_{pk_C}(m_3)$. In response, the CSC calculates the estimated number of charging segments, N , that need to be activated to meet the energy demand of the EV, given the rated power of each charging segment owned by PO_i , P_{rated_i} , and the nominal driving velocity on the charging lane, v_i , using the expression,

$$N = \left\lceil \frac{reqE}{P_{rated_i}} \frac{v_i}{L_i} \right\rceil, \quad (2)$$

where L_i is the length of each charging segment assuming equally sized segments, and $\lceil \cdot \rceil$ is used to round up to the nearest integer value of N . The rated segment power and the nominal lane crossing velocity, v_i , are assumed to be predetermined by the Charging Management and Coordination System (CMCS), which runs different supply and demand management programs to ensure grid load balancing and maximal demand coverage. Nevertheless, since this work particularly focuses on proposing a fast, reliable and privacy-preserving authentication and billing scheme for DWC systems, the specifications of the charging coordination process including load distribution and scheduling are beyond the scope of this work.

Upon verifying that the EV energy demand can be addressed by $N \leq S_i$ segments on the DWC lane owned by PO_i , the CSC selects a pseudonym p from the list of unassigned pseudonyms and sends it back to the EV e with the corresponding session key, k_p , after signing the message with its key, $m_4: \{I_e, t_C, p, k_p, SIG_{gk_C}\}$, and encrypting it with the EV public key, $E_{pk_e}(m_4)$. The CSC then activates a countdown timer, T , and waits for a response from the EV, which shall include the hash chain request in $m_5: \{HashChReq, p, t_e, SIG_{gk_e}\}$. In case of timer expiry, a timer expiry flag, f_T , is shared with the EV, and the authentication process

is terminated. The value of the timer, T , must acknowledge the expected transmission delay for the communication between the EV and the CSC, yet must not be excessively long to avoid undesirable channel occupancy, which allows unauthorized channel access and leads to network congestion.

If m_5 is received before timer expiry, the CSC responds by generating a hash chain, $\mathcal{H}_i^N(h_0)$, where h_0 is selected randomly. The CSC accordingly generates a number of hash keys sufficient to charge EV e according to the value of N estimated earlier by the CSC using Equation (2), based on the EV energy demand shared by the EV in m_3 . The message sent by the CSC is, $m_6: \{h_0, h_1, h_2, \dots, h_N, t_C, \text{SIG}_{gk_C}\}$ and is encrypted as $E_{pk_e}(m_6)$. When the EV receives the packet, it decrypts the message and verifies the signature of the CSC. If the verification succeeds, the EV stores the N hash keys to be used for authentication with the charging segments. Algorithm 1 presents the detailed procedure taking place at the CSC to register and authenticate the EVs. Assuming the EV energy demand can be fully covered by the DWC lane owned by PO_i , the message exchange sequence between the different entities up to this step is shown in Figure 4.

Algorithm 1 Proposed EV registration and authentication algorithm at the CSC.

Given P_{rated_i} and v_i for PO_i are provided to the CSC by the CMCS.
Input $E_{pk_C}(m_3: \{I_e, t_e, reqE, \text{SIG}_{gk_e}\})$ from EV e .

- 1: Decrypt $E_{pk_C}(m_3)$ using the private key of the CSC.
- 2: Calculate the number of charging segments, N , required to provide $reqE$ using Equation (2).
- 3: **if** $N \leq S_i$ **then**
- 4: Select a pseudonym $p \in \mathcal{P}_i$ for EV e .
- 5: Send m_4 to EV e with pseudonym, p , and session key, k_p .
- 6: Activate countdown timer, T .
- 7: **while** $T > 0$ **do**
- 8: Listen for incoming messages from EV e and other nearby EVs.
- 9: **if** $E_{pk_C}(m_5)$ is received from e **then**
- 10: Randomly generate h_0 .
- 11: Run the hashing algorithm to generate the hash chain, $\mathcal{H}_i^N(h_0)$.
- 12: Send the N hash keys back to the EV in $E_{pk_e}(m_6)$.
- 13: EV e is now authenticated and ready to communicate with PO_i and the N segments for charging activation.
- 14: **end if**
- 15: **end while**
- 16: **if** $T = 0$ and no message is received from e **then**
- 17: Send timer expiry flag, f_T , to EV e and terminate the authentication process.
- 18: **end if**
- 19: **else if** $N > S_i$ **then**
- 20: Set $N = S_i$.
- 21: Calculate maximum energy that can be provided from the S_i segments connected to PO_i .
- 22: Communicate the remaining EV energy demand with CMCS to recommend nearest available DWC lane.
- 23: Send charge insufficiency flag, f_{nc} , to EV e with the ID of the new PO, PO_j , shared by the CMCS.
- 24: Calculate the number of segment to be activated from the DWC lane owned by PO_j , N_j .
- 25: Upon EV approval, share the pseudonyms and session keys to register EV e with PO_i and PO_j .
- 26: Repeat steps 6-18 for N_j segments belonging to PO_j .
- 27: **end if**

Figure 4. Message sequence for key pre-distribution, registration and authentication messages.

5.3. Charging Activation Phase

After getting the hash key set from the CSC, EV e starts to communicate with PO_i by sending the N th hash key assigned by the CSC with the charging parameters and the ID of the CSC who generated the hash chain, in $m_7: \{h_N, p, C, t_e, param, SIG_{gk_e}\}$, encrypted using $E_{pk_{PO_i}}(m_7)$. The charging parameters field, $param$, includes the EV energy requirement, $reqE$, as well as the desired charging rate, EV speed, EV charging coil model, battery type, etc. The privacy of this information is maintained as it is linked to the pseudonym p assigned to the EV, not to the real EV identity. Hence, even if this message is compromised, this information cannot be traced back to the EV.

Upon receiving $E_{pk_{PO_i}}(m_7)$, the PO replies by sending its ID, the unit cost of charging and the time stamp to the EV, as $m_8: \{cost, PO_i, t_{PO_i}, SIG_{gk_{PO_i}}\}$. The PO also publishes the N th hash key shared by the EV to the charging segments, in $m_9: \{h_N, t_{PO_i}\}$. Once the EV enters the communication range of the first charging segment, it sends a message containing its pseudonym, the next hash key, h_{N-1} , the CSC ID, C , and the time stamp generated by EV. This is denoted as $m_{10}: \{p, h_{N-1}, C, t_e\}$. The message is encrypted using the session key, k_p , as $\varepsilon_{k_p}(m_{10})$. CS_1 decrypts the message and verifies the hash key by finding $h_N = \mathcal{H}(h_{N-1})$, which has to be equal to the root key sent by the PO in m_9 . If verification succeeds, CS_1 is activated and the EV starts charging. The segment also adds the received pseudonym, p , and corresponding key, k_p , to the revocation list to avoid reuse by free-riders.

In addition, CS_1 forwards the verified hash key received from the EV, h_{N-1} , in a message, m_{11} , to the next segment, CS_2 , which includes the EV pseudonym, p , the segment index, s , and h_{N-1} , encrypted using the segment-to-segment session key, k_s , as $\varepsilon_{k_s}(p, s, h_{N-1})$. The second segment stores the hash key and waits for the incoming message from the EV with pseudonym, p . As soon as the next message is received from the EV with h_{N-2} , CS_2 performs one hashing operation to verify that $h_{N-1} = \mathcal{H}(h_{N-2})$ before activating the charging process. This process continues until EV e finishes the required number of charging segments by sending h_0 to the last charging segment, CS_N . The use of dedicated short range communication (DSRC) between the EVs and the CSs ensures that the message transmitted by the EV only reaches the nearest charging segment before fading out, which minimizes the interference between the different messages shared between the EVs and the CSs.

5.4. Billing Phase

The billing process is performed during light traffic. Each charging segment, $s \in \mathcal{S}_i$, reports its supplied power levels for the vehicle with pseudonym p , $P_{s,p}$, to the PO along with the charging duration, i.e., the start and end charging times, $t_{s,p}^s$ and $t_{s,p}^e$, respectively, in the message $m_{12}:\{p, s, t_{s,p}^s, t_{s,p}^e, P_{s,p}\}$. The PO then calculates the total energy received by EV e by integrating the power supplied by each pad over time and finds the total energy using,

$$E_p = \sum_{s=1}^N E_{s,p} = \sum_{s=1}^N \left(\int_{t_{s,p}^s}^{t_{s,p}^e} P_{s,p} dt \right). \quad (3)$$

The PO sends the total energy calculated using Equation (3) with the start and end times to the CSC, in $m_{13}:\{p, t_p^s, t_p^e, E_p, \text{SIG}_{gk_{PO_i}}\}$, encrypted using $E_{pk_C}(m_{13})$. On the other hand, EV e reports its received energy when it leaves the charging lane by sending a packet that contains its real identity and the total energy received. The corresponding message is $m_{14}:\{I_e, E, t_e, \text{SIG}_{gk_e}\}$, encrypted using $E_{pk_C}(m_{14})$. The CSC then compares these two messages and pays the due amount to PO_i , then charges the EV at the end of the charging cycle. The message exchange between the charging entities during the charging activation and billing processes is presented in Figure 5.

Figure 5. Message sequence of charging activation and billing messages.

6. Security Analysis

This section assesses the security of the proposed scheme, in terms of message integrity, information privacy and protection against different types of attacks, including double-spending attacks, man in the middle (MITM) attacks and impersonation attacks.

6.1. Message Integrity

Message integrity is an important metric in vehicular authentication schemes to ensure the accuracy of the information exchanged between the different entities and guarantee that the messages have not been altered by unauthorized users. In the proposed schemes, digital signatures are employed to ensure the integrity of messages exchanged between the EVs, the CSC and the PO. Furthermore, hash functions are utilized for communications between the EV and the charging segments to verify message integrity before initiating the charging process. If an attacker modifies the message in transition, the hash value generated by the CS for the altered message shall be different from the value for the original message. Accordingly, the altered message shall be dropped by the CS, and the charging process is terminated.

6.2. Man in the Middle (MITM) Attack

This happens when an attacker secretly relays and possibly alters the communication between two parties who believe that they are directly communicating with one another. In addition to using the hash function to ensure message integrity, asymmetric key cryptography is utilized in this work to provide mutual authentication between the EV, the CSC and the PO, and help in protecting against MITM attacks. That is, by encrypting the messages using the public key of the receiver, only the intended receiver can decrypt the message using his private key. Assuming the private key of the receiver is not compromised, this encryption scheme provides protection against MITM attacks.

6.3. Impersonation Attack

Another common concern during wireless communications is that anyone can pretend to be the sender and encrypt the messages using the receiver's public key. This is acknowledged in the proposed model by using digital signatures, implemented using ECDSA. The message is signed using the signing key of the sender, which cannot be generated by any other entity, and the receiver has to verify the signature before establishing the communication link.

6.4. Double Spending and Free Rider Attacks

In this case, the attacker tries to listen to the message sent over the public channel and uses it during another time slot. The attacker can be an EV that has already received an amount of energy and would like to use the message to charge again without paying, i.e., double spending, or a free rider who aims to charge without being authenticated. The proposed system avoids this issue by using time stamps and revocation lists. Each time a hash key is sent to the charging segment, it has to validate t_e by calculating $|t_e - t_s| \in \Delta t$, where Δt represents the permitted tolerance time. If the time t_s by which the segment s receives a key exceeds the limit, the message is invalid. Revocation lists, on the other hand, are particularly beneficial against free riders. This is because once an EV starts receiving energy from the CS, its corresponding pseudonym and session key are added to the revocation list of the charging segment. Accordingly, any EV attempting to reuse the same pseudonym or key would be detected and prevented from charging.

6.5. EV Privacy

One of the most important considerations in vehicular communications is the privacy of vehicular information. In the proposed model, the identities of the EVs requesting charge are kept confidential during the communication. This is achieved by utilizing pseudonyms that are assigned randomly each time an EV decides to charge, thereby eliminating the need to reveal the real identity of the EV. Furthermore, EV-related information such as current SoC and distance until the charging lane are not explicitly shared by the EV in any of the messages exchanged with the CSC or with the PO. During communication with the CSC, only the EV energy demand is shared as a single value, $reqE$, in the encrypted message, m_3 , together with the EV identity. Upon receiving its pseudonym from the CSC, the EV shares its charging parameters, $param$, in m_7 using its pseudonym without revealing its real identity to the PO. Hence, the privacy of EV information is preserved in the proposed scheme.

7. Performance Evaluation

In addition to security analysis, the performance of the proposed model is evaluated using:

- Communication overhead: The communication overhead associated with the process of authentication and billing is measured by estimating the sizes of the different messages exchanged in the process.
- Computational cost: The computational cost is the time taken by the network entities to execute the different cryptographic techniques.

- Authentication delay: The authentication process needs to be performed within a few milliseconds to provide sufficient time for dynamic wireless charging, given the relatively short lane crossing time. This is evaluated by calculating the total time required for EV registration and authentication with the different network entities before starting the charging process. This is calculated using the estimated computational cost of the different cryptographic protocols and the transmission delay of the underlying communication networks.

7.1. Communication Overhead

The communication overhead is estimated by calculating the number of bytes transmitted during the message exchange process. In order to compute the size of each packet, the size of each message is calculated using the information in Table 1, as shown in Table 2, excluding the size of symmetric and asymmetric encryption and the messages exchanged offline between the CSC, the PO and the CS.

Table 2. Calculation of message sizes for message m_3 to m_{14} exchanged during EV registration, authentication, charging activation and billing.

Message	Message Content	Message Size (bytes)
m_3	$\{I_e, t_e, reqE, SIG_{gk_e}\}$	$128 + 8 + 8 + 56 = 200$ bytes
m_4	$\{I_e, p, k_p, t_c, SIG_{gk_c}\}$	$128 + 32 + 32 + 8 + 56 = 256$ bytes
m_5	$\{HashChReq, p, t_e, SIG_{gk_e}\}$	$8 + 32 + 8 + 56 = 104$ bytes
m_6	$\{h_0, h_1, h_2, \dots, h_N, t_c, SIG_{gk_c}\}$	$32N + 8 + 56 = 32N + 64$ bytes
m_7	$\{h_N, p, C, t_e, param, SIG_{gk_e}\}$	$32 + 32 + 8 + 8 + 32 + 56 = 168$ bytes
m_8	$\{cost, PO, t_{PO}, SIG_{gk_{PO}}\}$	$8 + 8 + 8 + 56 = 80$ bytes
m_9	$\{h_N, t_{PO}\}$	$32 + 8 = 40$ bytes
m_{10}	$\{p, h_{N-1}, C, t_e\}$	$32 + 32 + 8 + 8 = 80$ bytes
m_{11}	$\{p, s, h_{N-1}\}$	$32 + 8 + 32 = 72$ bytes
m_{12}	$\{p, s, t_{s,p}^s, t_{s,p}^e, P_{s,p}\}$	$32 + 8 + 8 + 8 + 8 = 64$ bytes
m_{13}	$\{p, t_p^s, t_p^e, E_p, SIG_{gk_{PO}}\}$	$32 + 8 + 8 + 8 + 56 = 112$ bytes
m_{14}	$\{I_e, E, t_e, SIG_{gk_e}\}$	$128 + 8 + 8 + 56 = 200$ bytes

As observed in Table 2, the size of m_6 depends on the number of segments, N , that need to be activated to satisfy the charging requirements of the EV, which means that the communication overhead increases as N increases. Nevertheless, although the EV needs to allocate sufficient memory to store N hash keys, the computational complexity of its authentication module is reduced as it does not need to run the hashing algorithm or generate the hash chain, as this is performed by the CSC. On the other hand, the hash key verification is performed on the CS side using a single hashing operation per CS. This offers lightweight authentication, particularly due to the robustness and low computational complexity of the SHA-256 algorithm used for hashing. This is further clarified in the computational cost calculation that follows. Furthermore, the inherent sequentiality of the hash keys formed in the chain structure allows the EV to authenticate with the CSs in order, which improves the security of the proposed model.

7.2. Computational Cost

Using the message exchange sequences described in Figures 4 and 5, the total computational cost of each entity in the proposed DWC authentication and billing system is analyzed, excluding the key pre-distribution phase, and is compared to the computational cost of the scheme proposed in [46], as shown in Table 3, with the following notation:

- N is the number of charging segments,
- x is the number of EVs,
- T_s and T_v are the time durations for signature and verification, respectively,

- T_E and T_{dE} are the time durations to encrypt and decrypt messages using RSA, respectively,
- T_ϵ and $T_{d\epsilon}$ are the time durations to encrypt and decrypt the message using AES, respectively,
- T_h is the time for one hashing operation, $\mathcal{H}(\cdot)$, and
- T_r is the time for random number generation, required for generating h_0 at the CSC.

In addition, T_{MAC} and T_{pm} are the times for one message authentication code (MAC) and for one point multiplication operation, respectively, which are utilized in the model proposed in [46]. The model in [46] is particularly selected for comparison with the proposed scheme in this work because it utilizes similar cryptographic protocols and hashing operations to achieve lightweight authentication. Nevertheless, the message structures and the underlying authentication and billing algorithms are different between the two schemes and the corresponding computational efficiencies are compared accordingly.

Table 3. Computational cost calculation for each network entity.

Entity	This Work	Ref. [46]
EV	$NT_\epsilon + 4T_s + 3T_v + 4T_E + 3T_{dE}$	$T_\epsilon + T_{d\epsilon} + 2T_s + 3T_v + 2T_E + 3T_{dE}$ $+ 2T_{MAC} + 2NT_h + 2T_r + 2T_{PM}$
CSC (PSS in [46])	$2xT_s + 4xT_v + 2xT_E + 4xT_{dE}$ $+ NT_h + T_r$	$2xT_s + xT_v + 2xT_E + xT_{dE} + 2xT_\epsilon$ $+ xT_{d\epsilon} + 2T_{MAC} + T_h + 2T_r + 3T_{PM}$
PO (RSU in [46])	$2xT_s + xT_v + 2xT_E + xT_{dE} +$ $xT_\epsilon + xNT_{d\epsilon}$	$xT_s + xT_v + xT_E + xT_{dE} + xT_{d\epsilon}$ $+ (2 + N)T_h + T_{MAC} + T_r + 2T_{PM}$
CS	$3xT_{d\epsilon} + 2xT_\epsilon + xT_h$	Negligible

As observed in Table [46], the scheme proposed in [46] requires additional operations of MAC, hashing, random number generation and point multiplication by the EV, the CSC and the PO. This increases the computational cost incurred by these entities, in comparison with the proposed scheme in this work, despite the additional encryption and decryption operations incurred in this work compared to [46].

The scheme proposed in [46] requires N hashing operations to be performed by the EV and the PO, which increases their computational requirements. In contrast, N hash keys are generated by the CSC only in the scheme proposed in this work. Furthermore, the additional operations in [46] aim to minimize the role of the CS to a pure comparison of the hash keys generated and shared by the PO and the EV, respectively, without performing any hashing operations. This, however, introduces additional delay, in the computational time required to run the hashing algorithm on the EV side, and in the transmission of messages with hash keys from both the EV and the PO, to be compared and verified by the CS prior to charging activation. In this work, on the other hand, hash keys are generated once by the CSC in a hash chain, and are shared to the EV, which shares them with the respective charging segments without having to run any hashing algorithm. Each CS then performs a single hashing operation to verify that $h_n = \mathcal{H}(h_{n-1})$, where n is the index of the received hash key such that $n = 1, 2, 3, \dots, N$.

7.3. Authentication Delay

In order to evaluate the system delay of the proposed authentication and billing scheme, the computational time for the different cryptographic protocols needs to be estimated. Accordingly, the different cryptographic protocols used in the proposed model are implemented using OpenSSL library on a system with Intel Core i7-3537U processor, 16-GB RAM, 256-GB SSD hard drive and a 64-bit Windows 10 operating system. To validate the results, the obtained computational time for the different protocols is compared with the time reported in Reference [56], which uses a machine with similar hardware specifications,

namely an Intel Core i7-4702MQ processor, 16-GB RAM, 256-GB SSD hard drive and 64-bit Ubuntu 16.04 operating system. This comparison is presented in Table 4.

Table 4. Computational time for the cryptographic protocols.

Operation	This Work	Ref. [56]
SHA-256 (16 bytes)	225 ns	255 ns
AES-256 CBC Encryption (16 Bytes)	109 ns	192 ns
AES-256 CBC Decryption (16 Bytes)	122 ns	-
256-bit ECDSA (nistp256) signature	30 μ s	46 μ s
256-bit ECDSA (nistp256) verification	100 μ s	116 μ s
RSA 2048 Encryption	651 μ s	728 μ s
RSA 2048 Decryption	20 μ s	32 μ s

As observed in Table 4, the computational time for executing the different cryptographic protocols on the machine used for this work is comparable and reasonably lower than the values reported in [56]. This validates the reliability of the utilized processor and its effectiveness for running the different cryptographic protocols. Nevertheless, the aforementioned hardware specifications are typically utilized at the CSC and the PO but are quite costly to be implemented on EV OBUs and at the charging segments. Hence, to account for the limited computational capabilities of the EV and the charging segments, the computational time for the cryptographic protocols in Table 4 is increased by 60% when used to compute the time required to run these protocols on the OBUs of the EV and at the CS.

The short computational times reported in Table 4, in microseconds and nanoseconds, confirm that the adopted protocols are sufficiently lightweight and can be efficiently implemented for the proposed authentication scheme in an IoEV. For the protocols executed by the charging segments in particular, namely the hash function algorithm and symmetric key encryption/decryption, a significantly low computational time is required, which is around two orders of magnitude less than that needed for the digital signatures and asymmetric cryptography protocols. This is also significantly lower than the expected transmission delay in the DSRC link between the EV and the CS, which proves the advantage of off-loading the hashing verification operation from the EV and PO sides to the CS side, to enable faster authentication between the EV and the CS and faster charging activation as the EV approaches the charging lane.

In order to accurately assess the speed of the authentication process, the total time required to execute the proposed authentication scheme needs to be evaluated, including the time taken to sign and encrypt messages, the transmission delay of the wireless communication channel, and the time taken to decrypt the messages and verify the signatures. Accordingly, the communication links between the different network entities in the proposed model are simulated on ns-3 network simulator, using the 5G-K SimNet tool developed by [57]. For the conducted simulations, equally-sized charging segments, each of length $L = 1$ m, are deployed on a road of 500 m length with segment-to-segment spacing, $d = 0.25$ m, and a 5G g-Node-B (gNB) is assumed to be located in the middle of the road. A total of 400 charging segments, one EV, one CSC and one PO are simulated and a constant EV speed of 60 km/h is considered throughout the EV motion along the charging lane.

When the EV enters the charging lane, it starts to communicate with the different network entities using different communication technologies shown in Figure 3. Using the message length calculations in Table 2, the transmission delay, T_d , for sending a message between the EV and the CSC (or the PO) using the 5G network modeled on ns-3 is found to be 11.75 ms. Furthermore, the wired link between the CSC and the PO, and between the PO and each charging segment has an average communication delay of 4.28 ms.

Hence, the total computational and transmission time requirements of the proposed scheme up to message m_9 , i.e., before the EV starts communicating with the charging segments, is shown in Figure 6. To acknowledge the difference in the computational capabilities between the different entities, an additional subscript c is used to indicate the computational time for the CSC and the PO, while the subscript e indicates the time for the EV and the CS, which is 60% higher than the values reported in Table 4.

Figure 6. Time required for EV registration and authentication with the CSC and the PO before reaching the first charging segment.

As shown in Figure 6, the time required to authenticate the EV to the PO and the CSC before reaching the first charging segment is 81.22 ms. Hence, for an EV traveling with a constant speed of 60 km/h, the authentication protocol proposed in this work needs to be executed at least 1.35 m before the EV reaches the first charging segment. Furthermore, the delay for the DSRC link between the EVs and the charging segments is measured by ns-3 simulations to be 0.24 ms. The time required by the EV to encrypt the message shared to the CS is $T_{e_e} = 0.17 \mu s$ and the time required by the CS to decrypt the EV message, verify the hash key sent by the EV and encrypt the message forwarded to the next segment is $T_{d_{e_e}} + T_{h_e} + T_{e_e} = 0.73 \mu s$, which are negligible compared to the DSRC transmission delay. Accordingly, for a CS of length 1 m, the EV-segment crossing time at 60 km/hr is ≈ 60 ms, of which ≈ 0.241 ms shall be used for message encryption/decryption and transmission, while the remaining time is allocated for charging.

8. Conclusions

In this paper, an efficient, lightweight and privacy-preserving authentication and billing scheme is proposed to be utilized for dynamic wireless charging of vehicles in an IoEV. The model preserves the user's information by using pseudonyms and supports a single aggregated bill for efficient and fair payment. Due to the limited computation capabilities of the charging segments, a lightweight EV-to-segment authentication model is employed, while major EV registration and authentication operations are performed with the charging service provider entities before the EV approaches the charging lane. In particular, hash chain generation is assigned to the entities with higher computational capabilities, namely the charging service company (CSC), while only simple hash key verification is required by the charging segments. Furthermore, the computationally extensive public key encryption and digital signature algorithms are employed by the entities with higher computational resources, namely the CSC and the PO, while the charging segments are only required to perform symmetric key encryption and decryption with lower computational

requirements. This guarantees faster authentication as the EV approaches the charging lane. The proposed approach is also analyzed against different possible attacks and is considered robust against double-spending attacks, MITM attacks and impersonation attacks. Future research shall study the utilization of advanced asymmetric cryptography techniques with lower computational costs to reduce the overall execution time of the proposed scheme. In addition, integrating the proposed scheme with an EV charging coordination system shall leverage on its advantages to ensure reliable and effective energy management in an IoEV.

Author Contributions: Conceptualization, E.E., I.A., M.H. and A.O.; methodology, I.A. and E.E.; software, I.A.; validation, M.H. and A.O.; formal analysis, E.E. and I.A.; investigation, I.A. and E.E.; resources, M.H. and A.O.; data curation, I.A.; writing—original draft preparation, E.E.; writing—review and editing, M.H. and A.O.; visualization, E.E., I.A., M.H. and A.O.; supervision, M.H. and A.O.; project administration, M.H. and A.O.; funding acquisition, M.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work is jointly supported by the American University of Sharjah through SCRI grant number SCRI 18-CEN-10, and by Sharjah Research Academy (SRA), Sharjah, United Arab Emirates. This work is also supported by the American University of Sharjah OAP Program # OAPCEN-1410-E00002.

Data Availability Statement: The data presented in this study are available upon request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Jayakumar, A. Review of prospects for adoption of fuel cell electric vehicles in New Zealand. *IET Electr. Syst. Transp.* **2017**, *7*, 259–266. [\[CrossRef\]](#)
- Patil, D.; McDonough, M.K.; Miller, J.M.; Fahimi, B.; Balsara, P.T. Wireless Power Transfer for Vehicular Applications: Overview and Challenges. *IEEE Trans. Transp. Electr.* **2018**, *4*, 3–37. [\[CrossRef\]](#)
- Habib, S.; Khan, M.M.; Abbas, F.; Sang, L.; Shahid, M.U.; Tang, H. A Comprehensive Study of Implemented International Standards, Technical Challenges, Impacts and Prospects for Electric Vehicles. *IEEE Access* **2018**, *6*, 13866–13890. [\[CrossRef\]](#)
- Javaid, N.; Hafeez, G.; Iqbal, S.; Alrajeh, N.; Alabed, M.S.; Guizani, M. Energy Efficient Integration of Renewable Energy Sources in the Smart Grid for Demand Side Management. *IEEE Access* **2018**, *6*, 77077–77096. [\[CrossRef\]](#)
- Electric Power Research Institute. *Interoperability of Public Electric Vehicle Charging Infrastructure*; Electric Power Research Institute: Palo Alto, CA, USA, 2019.
- ElGhanam, E.; Hassan, M.; Osman, A. Design of a High Power, LCC-Compensated, Dynamic, Wireless Electric Vehicle Charging System with Improved Misalignment Tolerance. *Energies* **2021**, *14*, 885. [\[CrossRef\]](#)
- Corti, F.; Reatti, A.; Piccirilli, M.C.; Grasso, F.; Paolucci, L.; Kazimierczuk, M.K. Simultaneous Wireless Power and Data Transfer: Overview and Application to Electric Vehicles. In Proceedings of the 2020 IEEE International Symposium on Circuits and Systems (ISCAS), Seville, Spain, 17–20 May 2020; pp. 1–5. [\[CrossRef\]](#)
- Abou Houran, M.; Yang, X.; Chen, W. Magnetically Coupled Resonance WPT: Review of Compensation Topologies, Resonator Structures with Misalignment, and EMI Diagnostics. *Electronics* **2018**, *7*, 296. [\[CrossRef\]](#)
- Li, H.; Dán, G.; Nahrstedt, K. Portunes+: Privacy-preserving fast authentication for dynamic electric vehicle charging. *IEEE Trans. Smart Grid* **2016**, *8*, 2305–2313. [\[CrossRef\]](#)
- Liu, Z.; Song, Z. Robust planning of dynamic wireless charging infrastructure for battery electric buses. *Transp. Res. Part C Emerg. Technol.* **2017**, *83*, 77–103. [\[CrossRef\]](#)
- Jeong, S.; Jang, Y.J.; Kum, D. Economic Analysis of the Dynamic Charging Electric Vehicle. *IEEE Trans. Power Electron.* **2015**, *30*, 6368–6377. [\[CrossRef\]](#)
- ElGhanam, E.A.; Hassan, M.S.; Osman, A.H. Deployment Optimization of Dynamic Wireless Electric Vehicle Charging Systems: A Review. In Proceedings of the 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Vancouver, BC, Canada, 9–12 September 2020; pp. 1–7. [\[CrossRef\]](#)
- Mou, X.; Zhao, R.; Gladwin, D.T. Vehicle to Vehicle Charging (V2V) Bases on Wireless Power Transfer Technology. In Proceedings of the IECON 2018—44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, USA, 21–23 October 2018; pp. 4862–4867.
- Kosmanos, D.; Maglaras, L.A.; Mavrovouniotis, M.; Moschyiannis, S.; Argyriou, A.; Maglaras, A.; Janicke, H. Route Optimization of Electric Vehicles Based on Dynamic Wireless Charging. *IEEE Access* **2018**, *6*, 42551–42565. [\[CrossRef\]](#)
- Zhang, J.; Pei, Y.; Shen, J.; Wang, L.; Ding, T.; Wang, S. Charging Strategy Unifying Spatial-Temporal Coordination of Electric Vehicles. *IEEE Access* **2020**, *8*, 74853–74863. [\[CrossRef\]](#)

16. Saldaña, G.; San Martin, J.I.; Zamora, I.; Asensio, F.J.; Oñederra, O. Electric Vehicle into the Grid: Charging Methodologies Aimed at Providing Ancillary Services Considering Battery Degradation. *Energies* **2019**, *12*, 2443. [\[CrossRef\]](#)
17. Hussain, S.; Ahmed, M.A.; Kim, Y.C. Efficient Power Management Algorithm Based on Fuzzy Logic Inference for Electric Vehicles Parking Lot. *IEEE Access* **2019**, *7*, 65467–65485. [\[CrossRef\]](#)
18. Shen, X.; Fantacci, R.; Chen, S. Internet of Vehicles [Scanning the Issue]. *Proc. IEEE* **2020**, *108*, 242–245. [\[CrossRef\]](#)
19. Bayram, I.S.; Papapanagiotou, I. A survey on communication technologies and requirements for internet of electric vehicles. *EURASIP J. Wirel. Commun. Netw.* **2014**, *2014*, 223. [\[CrossRef\]](#)
20. Hussain, S.S.; Ustun, T.S.; Nsonga, P.; Ali, I. IEEE 1609 WAVE and IEC 61850 standard communication based integrated EV charging management in smart grids. *IEEE Trans. Veh. Technol.* **2018**, *67*, 7690–7697. [\[CrossRef\]](#)
21. ElGhanam, E.; Hassan, M.; Osman, A.; Ahmed, I. Review of Communication Technologies for Electric Vehicle Charging Management and Coordination. *World Electr. Veh. J.* **2021**, *12*, 92. [\[CrossRef\]](#)
22. Jember, A.G.; Xu, W.; Pan, C.; Zhao, X.; Ren, X.C. Game and Contract Theory-Based Energy Transaction Management for Internet of Electric Vehicle. *IEEE Access* **2020**, *8*, 203478–203487. [\[CrossRef\]](#)
23. Cao, Y.; Kaiwartya, O.; Wang, R.; Jiang, T.; Cao, Y.; Aslam, N.; Sexton, G. Toward Efficient, Scalable, and Coordinated On-the-Move EV Charging Management. *IEEE Wirel. Commun.* **2017**, *24*, 66–73. [\[CrossRef\]](#)
24. Zhou, H.; Xu, W.; Chen, J.; Wang, W. Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities. *Proc. IEEE* **2020**, *108*, 308–323. [\[CrossRef\]](#)
25. Lu, R.; Zhang, L.; Ni, J.; Fang, Y. 5G Vehicle-to-Everything Services: Gearing Up for Security and Privacy. *Proc. IEEE* **2020**, *108*, 373–389. [\[CrossRef\]](#)
26. Liu, X.; Gao, B.; Wu, C.; Tang, Y. Demand-Side Management With Household Plug-In Electric Vehicles: A Bayesian Game-Theoretic Approach. *IEEE Syst. J.* **2018**, *12*, 2894–2904. [\[CrossRef\]](#)
27. Mediawathe, C.P.; Smith, D.B. Game-Theoretic Electric Vehicle Charging Management Resilient to Non-Ideal User Behavior. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 3486–3495. [\[CrossRef\]](#)
28. Hussain, S.; Lee, K.B.; Ahmed, M.A.; Hayes, B.; Kim, Y.C. Two-Stage Fuzzy Logic Inference Algorithm for Maximizing the Quality of Performance under the Operational Constraints of Power Grid in Electric Vehicle Parking Lots. *Energies* **2020**, *13*, 4634. [\[CrossRef\]](#)
29. Hussain, S.; Ahmed, M.A.; Lee, K.B.; Kim, Y.C. Fuzzy Logic Weight Based Charging Scheme for Optimal Distribution of Charging Power among Electric Vehicles in a Parking Lot. *Energies* **2020**, *13*, 3119. [\[CrossRef\]](#)
30. Al-Anbagi, I.; Mouftah, H.T. WAVE 4 V2G: Wireless access in vehicular environments for vehicle-to-grid applications. *Veh. Commun.* **2016**, *3*, 31–42. [\[CrossRef\]](#)
31. Gil, A.; Sauras-Perez, P.; Taiber, J. Communication requirements for dynamic wireless power transfer for battery electric vehicles. In Proceedings of the 2014 IEEE International Electric Vehicle Conference (IEVC), Florence, Italy, 17–19 December 2014; pp. 1–7.
32. Khan, A.G.; Basharat, S.; Riaz, M.U. Analysis of asymmetric cryptography in information security based on computational study to ensure confidentiality during information exchange. *Int. J. Sci. Eng. Res.* **2018**, 992–999. [\[CrossRef\]](#)
33. Bokhari, M.U.; Shallal, Q.M. A review on symmetric key encryption techniques in cryptography. *Int. J. Comput. Appl.* **2016**, 147. [\[CrossRef\]](#)
34. Atreya, M.; Hammond, B. *Digital Signatures*; McGraw-Hill, Inc.: New York, NY, USA, 2002.
35. Roman, L.F.; Gondim, P.R. Authentication protocol in CTNs for a CWD-WPT charging system in a cloud environment. *Ad Hoc Netw.* **2020**, *97*, 102004. [\[CrossRef\]](#)
36. Johnson, D.; Menezes, A.; Vanstone, S. The elliptic curve digital signature algorithm (ECDSA). *Int. J. Inf. Secur.* **2001**, *1*, 36–63. [\[CrossRef\]](#)
37. ANSI. *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*; ANSI X9.62; American National Standards Institute, Inc. (ANSI): Washington, DC, USA, 2005.
38. Azam, F.; Yadav, S.K.; Priyadarshi, N.; Padmanaban, S.; Bansal, R.C. A Comprehensive Review of Authentication Schemes in Vehicular Ad-Hoc Network. *IEEE Access* **2021**, *9*, 31309–31321. [\[CrossRef\]](#)
39. Petit, J. Analysis of ECDSA authentication processing in VANETs. In Proceedings of the 2009 3rd International Conference on New Technologies, Mobility and Security, Cairo, Egypt, 20–23 December 2009. [\[CrossRef\]](#)
40. Hu, Y.C.; Jakobsson, M.; Perrig, A. Efficient constructions for one-way hash chains. In Proceedings of the International Conference on Applied Cryptography and Network Security, New York, NY, USA, 7–10 June 2005; pp. 423–441.
41. Li, H.; Dán, G.; Nahrstedt, K. Proactive key dissemination-based fast authentication for in-motion inductive EV charging. In Proceedings of the 2015 IEEE International Conference on Communications (ICC), London, UK, 8–12 June 2015; pp. 795–801.
42. Hamouid, K.; Adi, K. Privacy-aware Authentication Scheme for Electric Vehicle In-motion Wireless Charging. In Proceedings of the 2020 International Symposium on Networks, Computers and Communications (ISNCC), Montreal, QC, Canada, 20–22 October 2020; pp. 1–6. [\[CrossRef\]](#)
43. Rabieh, K.; Wei, M. Efficient and privacy-aware authentication scheme for EVs pre-paid wireless charging services. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 1–6.
44. Gunukula, S.; Sherif, A.B.; Pazos-Revilla, M.; Ausby, B.; Mahmoud, M.; Shen, X.S. Efficient scheme for secure and privacy-preserving electric vehicle dynamic charging system. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 1–6.

45. Pazos-Revilla, M.; Alsharif, A.; Gunukula, S.; Guo, T.N.; Mahmoud, M.; Shen, X. Secure and privacy-preserving physical-layer-assisted scheme for EV dynamic charging system. *IEEE Trans. Veh. Technol.* **2017**, *67*, 3304–3318. [[CrossRef](#)]
46. Wu, X.; Li, G.; Zhou, J. A Lightweight Secure Management Scheme for Energy Harvesting Dynamic Wireless Charging System. *IEEE Access* **2020**, *8*, 224729–224740. [[CrossRef](#)]
47. Hussain, R.; Kim, D.; Nogueira, M.; Son, J.; Tokuta, A.; Oh, H. A new privacy-aware mutual authentication mechanism for charging-on-the-move in online electric vehicles. In Proceedings of the 2015 11th International Conference on Mobile Ad-hoc and Sensor Networks (MSN), Shenzhen, China, 16–18 December 2015; pp. 108–115.
48. Hussain, R.; Son, J.; Kim, D.; Nogueira, M.; Oh, H.; Tokuta, A.O.; Seo, J. PBF: A new privacy-aware billing framework for online electric vehicles with bidirectional auditability. *Wirel. Commun. Mob. Comput.* **2017**, *2017*, 5676030. [[CrossRef](#)]
49. Tajmohammadi, M.; Mazinani, S.M.; Nikooghadam, M.; Al-Hamdawee, Z. LSPP: Lightweight and Secure Payment Protocol for Dynamic Wireless Charging of Electric Vehicles in Vehicular Cloud. *IEEE Access* **2019**, *7*, 148424–148438. [[CrossRef](#)]
50. Zhao, X.; Lin, J.; Li, H. Privacy-preserving billing scheme against free-riders for wireless charging electric vehicles. *Mob. Inf. Syst.* **2017**, *2017*, 1325698, doi:10.1155/2017/1325698. [[CrossRef](#)]
51. Dong, P.; Zheng, T.; Yu, S.; Zhang, H.; Yan, X. Enhancing vehicular communication using 5G-enabled smart collaborative networking. *IEEE Wirel. Commun.* **2017**, *24*, 72–79. [[CrossRef](#)]
52. Naik, G.; Choudhury, B.; Park, J. IEEE 802.11bd 5G NR V2X: Evolution of Radio Access Technologies for V2X Communications. *IEEE Access* **2019**, *7*, 70169–70184. [[CrossRef](#)]
53. Zeadally, S.; Javed, M.A.; Hamida, E.B. Vehicular Communications for ITS: Standardization and Challenges. *IEEE Commun. Stand. Mag.* **2020**, *4*, 11–17. [[CrossRef](#)]
54. Martin-Vega, F.J.; Aguayo-Torres, M.C.; Gomez, G.; Entrambasaguas, J.T.; Duong, T.Q. Key Technologies, Modeling Approaches, and Challenges for Millimeter-Wave Vehicular Communications. *IEEE Commun. Mag.* **2018**, *56*, 28–35. [[CrossRef](#)]
55. ElHalawany, B.M.; El-Banna, A.A.A.; Wu, K. Physical-Layer Security and Privacy for Vehicle-to-Everything. *IEEE Commun. Mag.* **2019**, *57*, 84–90. [[CrossRef](#)]
56. Abbasinezhad-Mood, D.; Nikooghadam, M. An anonymous ECC-based self-certified key distribution scheme for the smart grid. *IEEE Trans. Ind. Electron.* **2018**, *65*, 7996–8004. [[CrossRef](#)]
57. Dabukke, A.K. 5G Korea—Network Simulator v1.0 User Manual; 5G Wireless Innovative Systems Engineering Research Center. Available online: <https://pdfcoffee.com/qdownload/5g-k-simnetusermanual-pdf-free.html> (accessed on 13 July 2021).