Secure and Privacy-Preserving Networking Strategy for Dynamic Wireless Charging of EVs

Mahmoud Abouyoussef*, Muhammad Ismail§, and Shady Refaat‡
*Department of Computer Science and Engineering, University of Central Arkansas, Conway, AR, USA
§Department of Computer Science, Tennessee Technological University, Cookeville, TN, USA
‡Department of Engineering and Technology, University of Hertfordshire, UK
Emails: *mabouyoussef@uca.edu, §mismail@tntech.edu, and ‡s.khalil3@herts.ac.uk

***Abstract*—Electric vehicles (EVs) that use dynamic wireless charging (DWC) rely on charging pads (CPs) placed along the road. For a group of mobile EVs, coordination of DWC requests can be adopted to indicate (a) the set of CPs at which each EV can charge and (b) the amount of supplied energy to each EV. Given a limited energy supply, this coordination can maximize the number of satisfied charging requests. However, this coordination requires the EV to exchange private information (i.e., identity and location) with the operator to schedule the charge. In literature, blockchain has been used to develop a privacy-preserving networking strategy that provides user anonymity and data unlinkability for DWC coordination. This paper shows that such a blockchain-based strategy is vulnerable to denial of service (DoS) attacks. Hence, we propose an approach based on blockchain and a modified K-times group signature to provide user anonymity, data unlinkability, and security against DoS attacks. A case study of Nashville, TN, USA is investigated showing that the proposed strategy can serve all the publicly charging EVs in Nashville within a DWC coordination period of 30 min while offering the required security and privacy features.**

***Index Terms*—Blockchain, smart grid, dynamic charging.**

I. Introduction

The global electric vehicles (EVs) market has been growing rapidly over the last decade. The expected number of EVs on the road will reach 125 million in 2030 [1]. In this context, EV charging can be carried out either statically or dynamically. To obtain energy through static charging, the EV is plugged into a charger in a charging station (CS). On the other hand, in dynamic wireless charging (DWC), each CS consists of a collection of charging pads (CPs) that are deployed along the road. Magnetic induction between coils at the bottom of the EV and the CP coils charges the EV while it is moving [2].

EVs that are charged dynamically have more appealing characteristics than statically charged ones. First, dynamically charging EVs does not require a lengthy period of time to charge. Second, EVs can use smaller batteries than static charging EVs, making the EV lighter and inexpensive [2].

Despite the advantages of DWC of EVs, their utilization of small batteries requires more frequent charging, which leads to more frequent energy demand to satisfy the charging requests of such EVs. This frequent energy demand adds an extra load to the power grid. One way to tackle this issue is by coordinating the charging requests of EVs so that they are not served at the same times and locations. However, this charging coordination requires each EV to send some information (i.e., current location, preferred route, destination, battery state of charge (SoC)) to the charging service provider (CSP). Then, the CSP runs a charging coordination algorithm considering the available energy and all the EV requests. The algorithm results in the charging schedule (i.e., specific CSs to each EV at a specific time and a specific amount of energy to charge). Spreading this load over space and time will increase the success rate of serving all the charging requests [3]. However, sending the EV's private information (i.e., current location, SoC, etc.) to the CSP is considered a privacy threat. Hence, a privacy-preserving strategy is needed that supports charging coordination and protects the privacy of EV owners.

Related Works: The literature that studies the DWC of EVs has mostly focused on authentication and payment methods that protect users' privacy. For example, in [4], the EV owner's identity is concealed from the CS during authentication, yet the CSP is capable of knowing the EV owner's true identity. For privacy-preserving authentication, the work in [5] depends on a trusted platform module linked to each EV. A secure payment system for DWC of EVs is presented in [6]. Although the system protects privacy, the trusted authority (TA) participates in the communication between each EV and the CSP. As a result, there is an additional communication burden as each EV must interact with the TA every time it requires charging.

Due to their inherent user-anonymity characteristic, blockchain technology has recently been investigated to support EV charging. A blockchain-based privacy-preserving authentication mechanism for EVs doing static charging was proposed in [7]. In order to achieve minimal latency, [8] proposed an EV static charging coordination mechanism based on blockchain and fog computing. In [9], a consortium blockchain is proposed that permits charging coordination for static charging EVs while protecting privacy. Unfortunately, existing blockchain platforms such as hyperledger adopt a public/private key pair for each user. This guarantees only user anonymity but does not guarantee data unlinkability (i.e., linking different messages to the same user), which is considered a privacy threat. For instance, the authors in [10] successfully linked a number of transactions to the same

This work is supported by the National Science Foundation under Award No. 2220346.

Bitcoin user. In summary, none of the aforementioned works offered a DWC framework that offers authentication, charging coordination, and billing while protecting users' privacy.

In [11], a framework for charging coordination, authentication, and billing that guarantees user anonymity and data unlinkability was proposed. The system is secure against external attacks. However, due to user anonymity and data unlinkability, the system is vulnerable to internal attacks. Our paper will show that a malicious EV owner can launch a denial of service (DoS) attack against the framework in [11]. This is done when the EV owner submits multiple fake charging requests to overwhelm the blockchain network. Hence, the time taken to prepare the charging schedules will exceed the system requirement to release such schedules to the users in the network. To fill this gap, our paper proposes an approach that preserves user anonymity and data unlinkability while at the same time standing robust against internal DoS attacks.

Contributions: The following contributions are carried out:

- We present a DoS attack that targets blockchain-based DWC coordination strategies that support user anonymity and data unlinkability. The presented DoS attack prevents the CSP from processing the charging requests and reporting the charging schedules in the required time frame.
- We propose a blockchain network that uses a modified unlinkable K-times group signature scheme instead of the known public/private key pair in blockchain architecture. The proposed networking strategy ensures (a) user anonymity, (b) data unlinkability, and (c) security against DoS attacks applied by malicious EV owners.
- We implement and test the proposed blockchain-based strategy. Our demonstration shows that the proposed strategy can coordinate the requests from the total number of publicly charging EVs in Nashville city in Tennessee, USA with a charging coordination period of 30 mins.

This paper is structured as follows: Section II discusses the functionality, security goals, and network/threat models. Section IV proposes a DoS attack on the strategy in [11]. Section IV details the blockchain-based approach. Implementation, performance assessment, and security analysis are covered in Section V. Section VI concludes the paper.

II. System Model and Design Objectives

This section explains the network and threat models, and the functionality and security objectives of the proposed strategy.

A. Network Model

The system consists of a set of CSs distributed all over the power grid, the participating EVs, a CSP, a certificate authority (CA), and a bank, as shown in Fig. 1. A private network is adopted since specific customers (i.e., EV owners) are allowed to join. The role assigned to each entity is described as follows:

- Certificate Authority (CA): It generates the cryptographic material and reveals the identity of a malicious EV owner. The CA does not participate in the blockchain network.

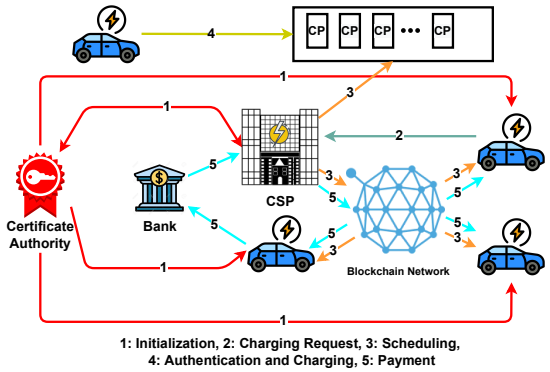

Fig. 1. Illustration of the system model under consideration.

- CSP: It receives EV charging requests and employs a smart contract to schedule a CS (i.e., group of CPs) to charge each EV with a specific amount of energy.
- CS: Each CS authenticates and charges scheduled EVs.
- EV: Each EV sends a charging request to the CSP and receives the assigned CS to charge.
- Bank: It collects the bill value from charged EVs.

B. Threat Model

The following threat model is considered:

- CSP: It is not aiming to attack the network availability because it owns the infrastructure. However, it is curious to know private information about EV owners.
- EVs: Malicious EV owners can (a) launch DoS attacks to affect the network availability and/or (b) reduce the bill value requested for the amount of received energy.
- External attackers: They aim to either (a) attack the network to affect its availability and/or (b) reveal private information about the EV owners.

C. Functionality and Security Objectives

The proposed networking strategy aims to achieve the following functionalities:

(F1) The CSP can coordinate charging requests to assign EVs to each CS according to energy availability.
(F2) The EV is able to perform fast authentication (i.e., less than 20 ms for DWC [12]) with the CS.
(F3) The CSP can accurately record the energy delivered to each EV at the end of the charging process.
(F4) The CSP can reveal the identity of any malicious EV owner.

The following security objectives should be guaranteed:

(S1) EV Owner's Anonymity: The charging requests should not be linked to any EV owner by any entity.
(S2) Data Unlinkability: Any entity should not link two charging requests to the same EV owner.
(S3) Transparency: The consumed energy and the calculated bill should be available for the EVs.
(S4) Protection against DoS attack: The network availability must be secure against DoS attacks.

III. DoS attack on blockchain-based privacy-preserving strategies for DWC of EVs

This section summarizes the blockchain-based networking strategy for DWC of EVs in [11]. In addition, it proposes a DoS attack that can be launched by a malicious EV owner on this strategy, hence, motivating the need for a secure strategy.

A. Summary of the Networking Strategy in [11]

The strategy in [11] replaced the public/private key pair in the traditional blockchain architecture by an anonymous group signature to solve the data linkability limitation. Hence, any EV can send its private information to the CSP anonymously. Then, the CSP can broadcast the scheduling information on the blockchain network to all EVs. The security analysis in [11] showed that any entity cannot link any charging request to an EV owner. Moreover, no entity can link two charging requests submitted by the same EV owner over time.

To test the scalability of the strategy, a case study of Nashville city in the state of Tennessee, USA, is considered. By taking into consideration (a) the total number of EVs in Nashville is 1885 and (b) the fact that 65% of EV owners prefer to charge in public CSs [13], the capacity of the networking strategy should be $1885 \times 65/100 = 1230$ charging requests per charging coordination period. By taking a charging coordination period of 30 mins (because this is the commonly used period for demand side management in smart grids [14]), the capacity of the strategy in [11] is found to be 1400 EVs (i.e., the blockchain network can broadcast charging schedules for 1400 EVs every 30 mins). The time taken by the CSP to process different numbers of charging requests from different EVs and broadcast the scheduling block is shown in Fig. 2. The details of calculating this time are in [11].

B. Proposed DoS Attack

Due to the anonymity offered by the group signature scheme in [11], malicious EV owners can overwhelm the network with multiple fake charging requests, that can affect its availability. The CSP should handle 1230 charging requests within a charging coordination period. Hence, a malicious EV owner can apply a DoS attack by sending many requests to the CSP such that the total number of requests exceeds 1400. As shown in Fig. 2, if 100 fake requests are sent such that a total of 1500 requests are received within the charging coordination period, the preparation of the charging scheduling information would require 38 mins. This violates the charging coordination period of 30 mins. By injecting more fake charging requests, the network availability is jeopardized as the charging schedules would not be broadcasted in due time. To overcome this malicious act, we propose herein to limit the number of charging request sent by the same EV to 1 per charging coordination period. The challenge is how to achieve this goal while preserving the privacy of the EV owner.

IV. Secure and Privacy-Preserving Networking Strategy for Dynamic Charging of EVs

The proposed strategy uses a novel unlinkable K-times group signature scheme on top of a blockchain network. The details of the novel scheme and the complete networking strategy are discussed below.

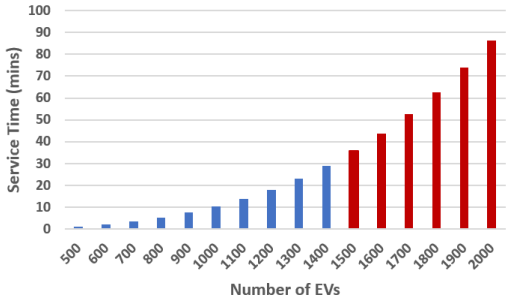

Fig. 2. Illustration of the time taken to serve different number of EVs in [11].

A. Unlinkable K-Times Group Singature Scheme

This scheme is adopted to ensure: (1) EV owner's anonymity, (2) unlinkability of the charging requests sent by the same EV owner, and (3) each EV owner can generate only one request within a charging coordination period. This scheme is based on the K-times group signature scheme introduced in [15]. However, our proposal modifies some of the parameters in [15] to ensure unlinkability of the signatures to protect the user's privacy. The scheme consists of a group manager (GM), an open authority, a verifier, and group members. The GM is responsible for generating the keys. The open authority can reveal the identity of any member who signed a request. The verifier is responsible for ensuring that the number of signatures do not exceed a predetermined value (K) within a certain period of time (i.e., charging coordination period). The group members sign the messages anonymously. The details of the unlinkable K-times group signature are summarized by describing its five main functions as follow.

1) Key Generation: The GM runs this function to generate the public parameters of the scheme. It selects three cyclic groups ($\mathbb{G}_1, \mathbb{G}_2,$ and $\mathbb{G}_T$) and a bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$. Moreover, it randomly chooses $g_1,\ h \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$ as the generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively, so that $g_1 \leftarrow \psi(g_2)$. Moreover, it randomly selects $\zeta_1,\ \zeta_2 \in \mathbb{Z}_p^*$ and calculates $u \in \mathbb{G}_1$, such that $u^{\zeta_1} = h$ and $u^{\zeta_2} = g_1$. Both ζ_1 and ζ_2 are saved only with the open authority. In addition, it selects $\gamma \in_R \mathbb{Z}_p^*$ and calculates $w = g_2^{\gamma}$. Afterwards, it selects two hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_T$ and $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_p$. Finally, the public parameters (i.e., group key) are $< \mathbb{G}_1, g_1, \mathbb{G}_2, g_2, \mathbb{G}_T, e, \psi, h, u, H_1, H_2 >$.
2) Group Joining: Each group member n selects a random variable $y_n \in_R \mathbb{Z}_p$, calculates $C_n = h^{y_n}$, and sends C_n to the GM. Upon receiving C_n, the GM generates private parameters (A_n, x_n) for group member n, such that $A_n = (g_1 C_n)^{\frac{1}{\gamma + x_n}}$. Afterwards, the GM saves a list $\mathcal{U}$ including the user identification ID_n and its private parameters. Hence, the saved data for member n is (ID_n, A_n, x_n). By the end of this function, each group member saves its own private key, $\Upsilon_n = (A_n, x_n, y_n)$.

3) Sign: This is our proposed modification to [15]. The verifier broadcasts a pseudo random number, r_t, each period. Each group member uses its private key, $\Upsilon_n = (A_n, x_n, y_n)$, the group key, and r_t to sign a given charging request. The group member calculates $M_{\{n,i\}} = h_{\{n,i\}}^{y_n}$, such that $h_{\{n,i\}} = H_1(r_t, i)$, where $i \in [1, \ldots, K]$ Hence, $M_{\{n,i\}}$ is calculated by encrypting the hash of r_t and i with the group member's private parameter y_n. This ensures that any group member can generate only one $M_{\{n,i\}}$ each i. Accordingly, the number of signatures per member does not exceed K. Moreover, the group member uses non-interactive zero-knowledge proof, $\pi_{\{i,n\}} = \text{ZKP}\{(A_n, x_n, y_n) : M_n = h_n^{y_n} \wedge e(A_n, g_2)^{x_n}.\ e(A_n, w).\ e(h, g_2)^{-y_n} = e(g_1, g_2)\}$, to sign the message. Finally, the group member sends $(i, M_{\{n,i\}}, \pi_{\{i,n\}})$ as its signature. The details of calculating $\pi_{\{i,n\}}$ can be found in [15].
The scheme in [15] uses the period T at which each group member is allowed to sign K times instead of r_t to calculate $h_{\{n,i\}}$. The work of [15] adopts scenarios where different periods with different K value for each period is used. However, since in the DWC of EVs the charging coordination period is constant, using the scheme in [15] will lead to repeating the same $M_{\{n,i\}}$ for every member in all the periods. Hence, the signatures at different time periods can be linked to the same group member. This is avoided in our scheme by using a random number r_t broadcasted by the verifier.
4) Verify: Upon receiving $(i, M_{\{n,i\}}, \pi_{\{i,n\}})$, the verifier checks that $1 < i < K$ and ensures that it is the first time to receive $M_{\{n,i\}}$ within the same period. This proves that the number of signatures does not exceed the threshold. Moreover, the verifier checks the signature validity [15].
5) Identity Reveal: The open authority uses ζ_1 and ζ_2 to find the private parameter, A_n, of a malicious signer to reveal the identity of the signer if needed as in [15].

B. Blockchain-based Networking Strategy

The proposed strategy uses the unlinkable K-times group signature such that (a) the CA represents the GM and the open authority, (b) the CSP is the verifier, and (c) the EV owner is the group member. The value of K is 1, allowing an EV owner to submit one charging request each charging coordination period. Hence, a malicious EV owner cannot overwhelm the network with multiple fake charging requests to cause a DoS. The proposed strategy is divided into five phases, namely: (1) initialization, (2) charging request, (3) scheduling, (4) authentication and charging, and (5) payment. The details of these phases are discussed below and shown in Fig. 1.

1) Initialization Phase: This phase takes place at network setup and for key refreshment. In this phase, the CA generates the public parameters in the unlinkable K-times group signature scheme (i.e., $(\mathbb{G}_1, g_1, \mathbb{G}_2, g_2, \mathbb{G}_T, e, \psi, w, u, h, H_1, H_2)$) and distributes these parameters to all the EVs. In addition, it generates the private keys for N EVs. Moreover, it stores the identity revealing parameters (ζ_1 and ζ_2) in its memory.

2) Charging Request Phase: In this phase, the CSP broadcasts a random number r_t to all EVs on the blockchain network. EV n submits an anonymous charging request, Ω_{nt}, at time t to the CSP. Ω_{nt} includes the GPS location of the origin, $l_{\text{o},n}$, and destination of the EV owner, $l_{\text{d},n}$, battery SoC B_n, the starting time of the journey T_n, energy needed E_n, route preference P_n, and two unique and untraceable random numbers (R_{nt1} and R_{nt2}) (generated in a distributed fashion according to Algorithm 1 in [11]). Afterward, the message is encrypted using the CSP's public key, a timestamp, $\tilde{t}_n$, is added, and the full message is signed using the unlinkable K-times group signature, σ_{nt}. Hence, the charging request is

$$\Omega_{nt} = \text{Enc}_{\text{PK}}(l_{\text{o},n} \,||\, l_{\text{d},n} \,||\, B_n \,||\, T_n \,||\, E_n \,||\, P_n \,||\, R_{nt1} \,||\, R_{nt2}) \,||\, \tilde{t}_n \,||\sigma_{nt}, \quad (1)$$

where Enc represents an encryption function, P_n can be given as $\mathcal{D}$ for smallest duration, $\mathcal{P}$ for shortest path, or $\mathcal{F}$ for least traffic. This request is an anonymous back-channel message from the EV to the CSP and is not included in the blockchain.

After receiving Ω_{nt}, the CSP checks the signature and the timestamp. Checking the signature is achieved by: (1) ensuring that the signer is a legitimate EV owner and (2) ensuring that it is the first message sent by this EV owner within this charging request period. The timestamp is checked to ensure that the message is generated within the charging period. If valid, the CSP processes all the charging requests to assign the optimal CS to each EV aiming to maximize the charging success rate while balancing supply and demand. This processing is performed via the charging coordination algorithm. If the signature is not validated, the request is dropped.

3) Scheduling Phase: After assigning the best CS for each EV, the CSP generates a block including the scheduling transactions. Since the CSP cannot know the identity of the EVs sending the charging requests, it uses the random numbers R_{nt1} to point each EV to its scheduling transaction. Hence, a scheduling transaction, Ψ_{nt}, includes R_{nt1}, the location of the assigned CS $l_{\text{CP},n}$ and its public key PK_s, the amount of energy dedicated to charge the EV, $E_{\text{sp},n}$, and the CSP's signature, σ. Hence, the scheduling transaction is given by

$$\Psi_{nt} = R_{nt1} \,||\, l_{\text{CP},n} \,||\, \text{PK}_s \,||\, E_{\text{sp},n} \,||\, \sigma. \quad (2)$$

All the generated scheduling transactions are added into a block and broadcasted to all the EVs. The block contents are:

1) Index ($\tilde{I}$): The block number in the blockchain. It starts with block zero, which is the genesis block.
2) Previous Hash ($H_{\tilde{I}-1}$): The hash of the preceding block.
3) Transactions (Ψ_{nt}): The set of scheduling messages for the group of EVs requesting to charge at time t.
4) Timestamp ($\tilde{t}$): The time when the block is generated.

Thus, the block of scheduling transactions can be given by

$$\Psi_{\tilde{I}} = \tilde{I} \,||\, H_{\tilde{I}-1} \,||\, \Psi_{nt} \;\forall n \in \{1, \ldots, \breve{\mathcal{N}}\} \,||\, \tilde{t}, \quad (3)$$

given that $\breve{\mathcal{N}}$ is the total number of EVs requesting a charge.

Moreover, the CSP sends encrypted messages to the CSs including the set of EVs that are scheduled to charge at them. These messages are encrypted using the CS's public key PK_s. Each message, Σ_{st}, includes a set of tuples, $\breve{\mathcal{N}}_{\text{sT}}$. Each tuple includes R_{nt2} that was sent by EV n in the charging request and the energy calculated to charge EV n $E_{\text{sp},n}$. A timestamp, $\tilde{t}_{\text{s}}$, is added and the message is signed σ by the CSP. This message is not part of the blockchain but is sent on a back channel. Hence, Σ_{st} can be given by

$$\Sigma_{st} = \text{Enc}_{\text{PK}_s}((R_{nt2} \mid\mid E_{\text{sp},n} \ \forall n \in \{1, \ldots, \breve{\mathcal{N}}_{\text{sT}}\})) \mid\mid \tilde{t}_{\text{s}} \mid\mid \sigma. \tag{4}$$

Thus, the proposed strategy fulfills the functionality (F1).

4) Authentication and Charging Phase: In this phase, EV n uses R_{nt2} to authenticate itself to the CS. The authentication process is done after the EV sends an encrypted message Λ_{nt} to the CS including R_{nt2}. Λ_{nt} is not part of the blockchain and is sent on a back-channel. Λ_{nt} is given by

$$\Lambda_{nt} = \text{Enc}_{\text{PK}_s}(R_{nt2}). \tag{5}$$

The CS decrypts Λ_{nt} and looks for R_{nt2} in Σ_{st} that is already acquired from the CSP. If R_{nt2} is located, the authentication of EV n is successful, and the CS begins to charge EV n until it obtains the $E_{\text{sp,n}}$ assigned in Σ_{st}. Hence, the functionality (F2) is successfully fulfilled.

5) Payment Phase: Each CS calculates the amount of energy delivered to each EV, $E_{\text{dv},n}$, after the charging process. $E_{\text{dv},n}$ along with the corresponding random identifier R_{nt2} are then encrypted to be reported to the CSP. In addition, a timestamp $\tilde{t}_{\text{p1}}$, and the CS's signature σ_s are added. Hence, the reported message to calculate the payment is given by

$$\Theta_s = \text{Enc}_{\text{PK}_c}(R_{nt2} \mid\mid E_{\text{dv},n}) \mid\mid \tilde{t}_{\text{p1}} \mid\mid \sigma_s. \tag{6}$$

According to Θ_s, the CSP can calculate the bill value for EV_n. By this way the proposed strategy satisfies the functionality (F3). Afterwards, the CSP prepares a transaction including the random number R_{nt2}, the delivered energy $E_{\text{dv},n}$, and the bill value γ_n, which is given by

$$\Gamma_n = R_{nt2} \mid\mid E_{\text{dv},n} \mid\mid \gamma_n. \tag{7}$$

A set of billing transactions are collected in a block and broadcasted to all the EVs. The block includes a block number, previous block's hash, the billing transactions, a timestamp, and a signature. Hence, the billing block is given by

$$\Gamma_{\hat{I}} = \hat{I} \mid\mid H_{\hat{I}-1} \mid\mid \Gamma_n \ \forall n \in \{1, \ldots, \breve{\mathcal{N}}\} \mid\mid \hat{t} \mid\mid \sigma. \tag{8}$$

Each EV can extract its bill value using R_{nt2}. Moreover, the CSP sends to the bank encrypted messages containing R_{nt2} along with its corresponding bill amount γ_n. A timestamp $\tilde{t}_{\text{p2}}$ and a signature are added to the encrypted message. Hence, the bill message to the bank is given by

$$\Gamma_B = \text{Enc}_{\text{SK}}(R_{nt2} \mid\mid \gamma_n) \mid\mid \tilde{t}_{\text{p2}} \mid\mid \sigma. \tag{9}$$

TABLE I
EV COMPUTATION TIME TO GENERATE A MESSAGE & PROCESS A BLOCK

Sending Operations	Time (ms)	Equation	Receiving Operations	Time (ms)	Equation
Encrypt	3.5	Eq.(1, 5)	Verify	12.8	Eq.(3, 8)
Group Sign	32	Eq.(1)	Searching for R_{nt}	6.35	Eq.(3, 8)

TABLE II
CSP COMPUTATION TIME TO RECEIVE REQUESTS AND SEND MESSAGES

Receiving Operations	Time (ms)	Equation	Sending Operations	Time (ms)	Equation
Decrypt	2.8	Eq.(1, 6)	Encrypt	3.5	Eq.(4, 9)
Group Verify	40	Eq.(1)	Signature	16	Eq.(4, 9)
Verify	12.8	Eq.(6)			

EV n deposits its bill value γ_n for its random number R_{nt2}. After 24 hours, the bank notifies the CSP the set of random numbers that did not pay the requested bills. The CSP sends the charging requests that includes the random numbers that did not pay the bill to the CA, which can reveal their identities using the Identity Reveal function in the unlinkable K-time group signature. Hence, the functionality (F4) is fulfilled.

V. PERFORMANCE EVALUATION AND DISCUSSIONS

In this section, the implementation details and the scalability and security analysis of the proposed strategy are presented.

A. Implementation Details

Since the existing blockchain platforms do not support the adoption of K-times group signature, the proposed strategy is implemented and tested from scratch using Python. An Ubuntu operating system on a virtual machine with 7 GB RAM and 1.8 GHZ processor is used in the simulation. All the cryptographic materials are developed using the Charm library [16].

B. Scalability Analysis

The scalability of the proposed strategy is measured by calculating the communication and computation overheads at the EV's side and the CSP's side and the authentication time.

1) Computation Overheads: The computation overheads are measured by calculating the time taken to perform the cryptographic operations described in the proposed strategy.

(I) At the EV side: According to Table I, the EV takes 35.5 ms to send a message and 19.15 ms to process a block.

(II) At the CSP side: According to Table II, the total time to process a charging request is 55.6 ms and the time to send a scheduling transaction is 19.5 ms.

The computation overheads showed that the proposed strategy has a close performance to the strategy in [11] (i.e., unlinkable K-times group signature takes around 5 ms more than the group signature per a signature or a verification operation). Hence, the proposed strategy still can serve 1400 EVs in 30 mins, as shown in Fig. 2.

2) Communication Overheads: The communication overheads are measured by calculating the sizes of the messages and blocks generated throughout the proposed phases.

TABLE III
TOTAL SIZE OF DIFFERENT DATA SENT IN THE MESSAGES

Data	Size	Data	Size	Data	Size
R_{nt}	24 B	GPS location	6 B	B_n	2 B
Group Sign	408 B	Energy value	2 B	T_n	2 B
Timestamp	13 B	Encrypted Msg.	128 B	P_n	1 B

(I) At the EV side: The size of each component of the generated data is listed in Table III. Accordingly, the size of the messages generated by the EV owner are 549 B for the encrypted data, a timestamp, and k-times signature (i.e., Eq.(1)) and 128 B for encrypted R_{nt2} (i.e., Eq.(5)).

(I)) At the CSP side: The communication overheads at the CSP side include all the messages and blocks generated by the CSP throughout a time slot. The messages generated by the CSP (Eq. $(4, 9)$) include encrypted data, a timestamp, and a signature. Hence, the total size of any one of these messages is (269 B). The sizes of a block are calculated while changing the number of charging EVs as shown in Fig. 3.

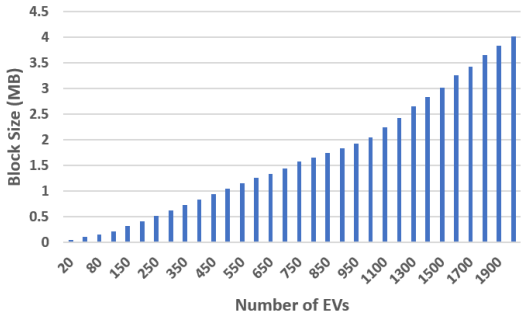

Fig. 3. Illustration of the storage requirements for a single block of data.

3) Authentication Time: The time the CS takes to decrypt Λ_{nt} (Eq.(5)) and search for R_{nt2} in Σ_{st} received from the CSP (Eq.(4)). The decryption takes 2.8 ms and searching for R_{nt2} in a list of 100 numbers takes 0.6 ms. Hence, the authentication time is 3.4 ms, which is less than the required 20 ms [12] for DWC authentication. Charging 100 EVs per CS captures a scenario in which all passing EVs require charge [11].

C. Security and Privacy analysis

The security of the unlinkable K-times group signature scheme employed in the proposed strategy is based on the Decisional Diffie–Hellman (DDH) assumption. Hence, it is computationally hard for the CSP or any curious entity to extract any information about the identity of the signer. Thus, the security requirement (S1) is satisfied in the proposed strategy. Furthermore, the deployment of the distributed random number generators ensures the uniqueness and unlinkability of the generated random numbers [11]. Hence, the proposed strategy satisfies the data unlinkability requirement (S2). The immutable blockchain ledger that can be downloaded by all EV owners adds the transparency option to the proposed strategy. Thus, the (S3) requirement is successfully satisfied. Restricting the number of signatures to one each charging coordination time slot using the unlinkable K-times group signature scheme protects the system from the DoS attacks. Hence, the security requirement (S4) is satisfied.

VI. CONCLUSION

In this paper, a secure and privacy-preserving blockchain-based networking strategy for DWC of EVs is proposed. The proposed strategy supports (a) charging coordination, (b) fast authentication for EVs, and (c) billing and payment for the charging energy. Moreover, the strategy protects the EV owner's anonymity and data unlinkability. This is made feasible by the combination of (a) unlinkable K-times group signature, which protects customer anonymity while verifying transactions, and (b) a distributed random number generation technique, which supports data unlinkability and CSP-EV interaction. In addition, the K-times group signature scheme ensures that the proposed strategy is secure against DoS attacks. Our experimental results show the scalability offered by the proposed strategy as it can support the publicly charging EVs in an urban city like Nashville, TN, USA with reasonable EVs computation and storage capabilities.

REFERENCES

[1] T. Bunsen et al., "Global EV Outlook 2018: Towards cross-modal electrification," 2018.

[2] A. N. Azad et al., "Analysis, optimization, and demonstration of a vehicular detection system intended for dynamic wireless charging applications," *IEEE Trans. Transp. Electrific.*, vol. 5, no. 1, pp. 147–161, 2018.

[3] M. Wang, M. Ismail, X. Shen, E. Serpedin, and K. Qaraqe, "Spatial and temporal online charging/discharging coordination for mobile PEVS," *IEEE Wireless Communications*, vol. 22, no. 1, pp. 112–121, 2015.

[4] H. Li, G. Dan, and K. Nahrstedt, "Portunes: Privacy-preserving fast authentication for dynamic electric vehicle charging," in *IEEE Intl. Conf on Smart Grid Communications (SmartGridComm)*, 2014, pp. 920–925.

[5] T. Zhao et al., "A secure and privacy-preserving billing scheme for online electric vehicles," in *2016 IEEE Veh. Tech. Conf. (VTC Spring)*, pp. 1–5.

[6] M. Tajmohammadi et al., "Lspp: Lightweight and secure payment protocol for dynamic wireless charging of electric vehicles in vehicular cloud," *IEEE Access*, vol. 7, pp. 148 424–148 438, 2019.

[7] D. Gabay et al., "Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs," *IEEE Trans. Veh. Technol.*, 2020.

[8] H. Li et al., "A privacy-preserving charging scheme for electric vehicles using blockchain and fog computing," *IEEE Systems Journal*, 2020.

[9] Y. Li and B. Hu, "A consortium blockchain-enabled secure and privacy-preserving optimized charging and discharging trading scheme for electric vehicles," *IEEE Transactions on Industrial Informatics*, 2020.

[10] M. Spagnuolo et al., F. Maggi, and S. Zanero, "Bitiodine: Extracting intelligence from the bitcoin network," in *International conference on financial cryptography and data security*. Springer, 2014, pp. 457–468.

[11] M. Abouyoussef and M. Ismail, "Blockchain-based privacy-preserving networking strategy for dynamic wireless charging of EVS," *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 2, pp. 1203–1215, 2022.

[12] H. Li et al., G. Dán, and K. Nahrstedt, "Portunes+: Privacy-preserving fast authentication for dynamic electric vehicle charging," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2305–2313, 2016.

[13] D. Stevenson, "Charging ahead," https://www.pwc.co.uk/industries/power-utilities/insights/electric-vehicle-infrastructure-report-april-2018.html.

[14] N. Scientists, "Preparing distribution utilities for the future - nrel." [Online]. Available: https://www.nrel.gov/docs/fy21osti/79375.pdf

[15] X. Zhao and F. Zhang, "Times limited accountable anonymous online submission control system from single-verifier k-times group signature," *Informatica*, vol. 36, no. 1, 2012.

[16] J. A. Akinyele et al., "Charm: a framework for rapidly prototyping cryptosystems," *J. of Crypto. Eng.*, vol. 3, no. 2, pp. 111–128, 2013.