Privacy-Preserving V2V Charge Sharing Coordination using the Hungarian Algorithm

Ahmed Bakr[1], Mahmoud Srewa[1], Eyuphan Bulut[2], Kemal Akkaya[3], Mizanur Rahman[4], and Ahmad Alsharif[1,5]

[1]Department of Computer Science, University of Alabama, AL, USA
[2]Department of Computer Science, Virginia Commonwealth University, Richmond, VA, USA
[3]Department of Electrical and Computer Engineering, Florida International University, FL, USA
[4]Department of Civil, Construction, and Environmental Engineering, University of Alabama, Tuscaloosa, AL USA
[5]Department of Electrical Engineering, Faculty of Engineering at Shoubra, Benha University, Cairo, Egypt

2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring) | 979-8-3503-1114-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/VTC2023-Spring57618.2023.10199243

***Abstract*—Electric Vehicles (EVs) are being widely adopted as a green alternative to fossil-based vehicles. However, the current charging infrastructure for EVs is inadequate to meet the growing charge demand. Vehicle-to-Vehicle (V2V) charging offers a promising solution that enables a charge supplier EV to provide charging services to a charge demander EV in a distributed manner. Nevertheless, V2V matching and charge scheduling can disclose sensitive location information about the drivers, such as their whereabouts and driving patterns. In this paper, we propose a privacy-preserving scheme for centralized optimal matching of demander EVs with supplier EVs, while protecting their sensitive information. In our scheme, charge demanders report to a matching server their encrypted location information and the requested energy quantities, whereas charge suppliers report encrypted charge costs such that the matching server can learn only the cost to match each demander to each supplier without revealing any location information or the exchanged charge amount. Then, the Hungarian algorithm is used to match demanders to suppliers while minimizing the total cost. The security analysis and simulation results show that our scheme can achieve optimal V2V matching while preserving drivers' privacy with negligible computation overhead. Overall, our proposed scheme provides an effective solution for V2V charging, while maintaining privacy and confidentiality of sensitive drivers' information.**

I. Introduction

Due to the negative environmental impact of gas-powered or internal combustion engine vehicles, Electric Vehicles (EVs) have become a major focus for governments, the automotive industry, and consumers. Several countries are not only embracing EVs as a means of achieving zero-emission and all-electric transportation systems [1], [2], but also implementing strict regulations to mandate that all newly manufactured vehicles be electric [3], [4]. A recent study predicts that EVs will make up 60% of all vehicles sold worldwide by 2030, indicating the widespread adoption of EVs [5].

One of the biggest obstacles hindering the widespread adoption of EVs is the insufficient charging infrastructure, particularly in suburban and rural areas [6]. Additionally, long charging times and the need for frequent charging are additional barriers faced by EV owners. As per a recent study, there are approximately 16.5 million EVs globally, whereas only about 1.8 million charging points are available publicly [7]. With the current EV to Charging Stations (CS) ratio standing at 11%, there is a pressing need for new and innovative solutions that do not rely solely on public CS.

The limited availability of charging infrastructure has led to an increased interest in Vehicle-to-Vehicle (V2V) charging as a flexible and distributed alternative to traditional CS [8]. In V2V charging, an EV with excess charge (the charge supplier) can provide charging services to another EV in need of a charge (the charge demander), regardless of location or time. To effectively address the issue of inadequate CS, it is crucial to develop optimal V2V charge coordination and scheduling mechanisms [9].

However, to achieve optimal V2V charge coordination, charge demanders and suppliers must disclose sensitive information, such as their location and the amount of energy to be exchanged, to a scheduling server or other entity that can compute the optimal demander-supplier match. Disclosing such information raises serious privacy concerns that may discourage both demanders and suppliers from participating in the system [9]. As a result, it is essential to devise a way to perform optimal demander-supplier matching while safeguarding the privacy of all involved entities.

In this paper, we propose a novel privacy-preserving scheme to achieve optimal V2V charge coordination. In our scheme, each charge demander EV sends an encrypted charge request containing encrypted location information and the requested energy quantities to a matching server. Each charge supplier EV, on the other hand, sends an encrypted charge offer that includes the charging costs. By using these encrypted requests and offers, the matching server can determine the cost to match each demander to each supplier, without revealing any sensitive information. The Hungarian algorithm [10] is then used to obtain the optimal demander-supplier match that minimizes the total cost.

The remaining sections of this paper are organized as follows. Section II reviews related work in this research area. Section III describes the system model and design goals. The proposed scheme is presented in Section IV. The security analysis and performance evaluation are discussed in Section V. Finally, Section VI concludes our work.

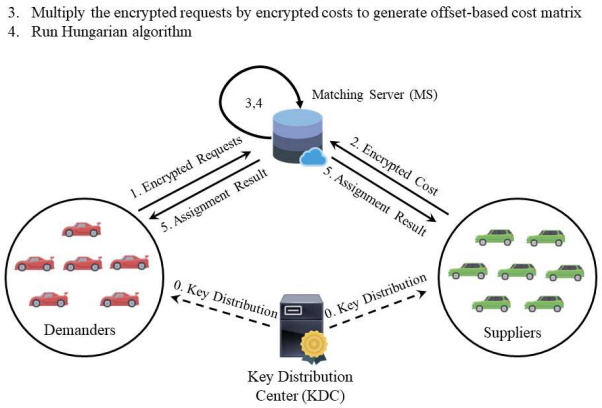


Figure 1: System model

II. Related Works

Several V2V matching algorithms have been proposed in [11]–[13]. In [11], [12] demanders and suppliers cooperatively provide a centralized matching server with sensitive information such as location information and requested energy amount. The server uses this information to build a demander-supplier cost matrix and uses the Hungarian algorithm to find the optimal demander-supplier match. Moreover, a comprehensive framework that considers cost optimization, system energy efficiency, and user satisfaction is proposed in [13]. However, none of these works consider privacy protection of sensitive information.

The authors in [14], [15] addressed the location privacy concerns by proposing Bichromatic Mutual Nearest Neighbor (BMNN) assignments using partially homomorphic encryption-based techniques in a decentralized network. The Euclidean distance between a demander and a neighbor supplier can be computed using the encrypted location information and a distributed stable matching can be achieved in several matching rounds. However, the assignment in [14], [15] is determined based on the Euclidean distance between supplier and demander only while neglecting other cost parameters such as charge cost and amount of charge. Furthermore, the coverage area for such a decentralized solution is limited to neighboring suppliers. Extending the coverage area and offering optimal V2V matching necessitate having a centralized server that should find the optimum demander-supplier match.

Different from the existing literature, this paper proposes a privacy-preserving centralized optimal demander-supplier matching using realistic cost value while preventing any entity, including the matching server, from learning any sensitive information.

III. System Models and Design Goals

A. Network Model

As shown in Figure 1, the network model consists of a Key Distribution Center (KDC), a Matching Server (MS), a group of demanders, and a group of suppliers. The main notations used in the paper are given in Table I. We use bold lowercase notation, e.g. $\mathbf{d}$, for vectors and bold uppercase notation, e.g. $\mathbf{M}$, for matrices. The entities' roles are described as follows:

Table I: Main notations

Notation	Description
k	No. of demanders = No. for suppliers = k
$\mathbb{DS}$	Set of demander $\mathbb{DS} = \{D_i, 1 \leq i \leq k\}$
$\mathbb{SS}$	Set of suppliers $\mathbb{SS} = \{S_j, 1 \leq j \leq k\}$
$\mathcal{MK}$	Set of master keys $\mathcal{MK} = \{\mathbf{M}_1, \mathbf{M}_2, \mathbf{N}_1, \ldots, \mathbf{N}_8\}$
$\mathcal{DK}_i$	Secret key set for demander D_i
$\mathcal{SK}_j$	Secret key set for supplier S_j
$cost_{i,j}$	Cost to match D_i to S_j
Q_i	The quantity in KW that D_i requests to charge
$\mathbf{ed}_i$	Encrypted charge request vector of demander D_i
$\mathbf{ec}_j$	Encrypted charge offer vector of supplier S_j
P_j	A supplier S_j selling price per KW
m, n	Number of rows and columns in the map, respectively
v	Flattened map size=$(n \times m) + 1$
$\mathbf{d}_i$	Charge request vector of demander D_i
loc_i	The location of D_i
$\mathbf{c}_j$	Charge offer vector of supplier S_j
$cost_j^{loc_i}$	Cost for S_j to travel to the location of D_i
$\mathbf{X}, \mathbf{Y}$	Components of the server's key
$\mathbf{sp}$	Splitting vector used during the encryption

- **Demanders**: A set of demanders $\mathbb{DS} = \{D_i, 1 \leq i \leq k\}$ represents EV owners who demand some energy quantity for their EVs to be charged at a specific location.
- **Suppliers**: A set of suppliers $\mathbb{SS} = \{S_j, 1 \leq j \leq k\}$ consists of electric vehicles that offer charging as a service.
- **Key Distribution Center (KDC)**: The KDC is responsible for generating the master secret key set $\mathcal{MK}$, a unique demander secret key $\mathcal{DK}_i$ for each demander D_i, and a unique supplier secret key $\mathcal{SK}_j$ for each supplier S_j. The KDC is needed only for system setup and will not be involved in the demander-supplier matching process.
- **Matching Server (MS)**: The MS collects the demanders' encrypted charging requests and the suppliers' encrypted charging offers. Using the encrypted collected data and without leaking any sensitive information, the server can derive a cost matrix where each value in the cost matrix $cost_{i,j}$ represents the cost to match supplier S_j's offer to demander D_i's request. Then, the MS runs the Hungarian algorithm to find the optimal V2V matching result while minimizing the total cost.

B. Threat models and Design Goals

We consider a semi-honest model in which the server, demanders, and suppliers are considered "honest but curious", i.e., they do not disrupt the proposed scheme's proper operation, but any entity is curious to learn sensitive location information of the users. Based on the network and threat models, the following goals should be met.

1) **Optimal and realistic demander-supplier matching**: The matching server should be able to compute an optimal demander-supplier matching result considering a realistic cost that includes not only the cost to service

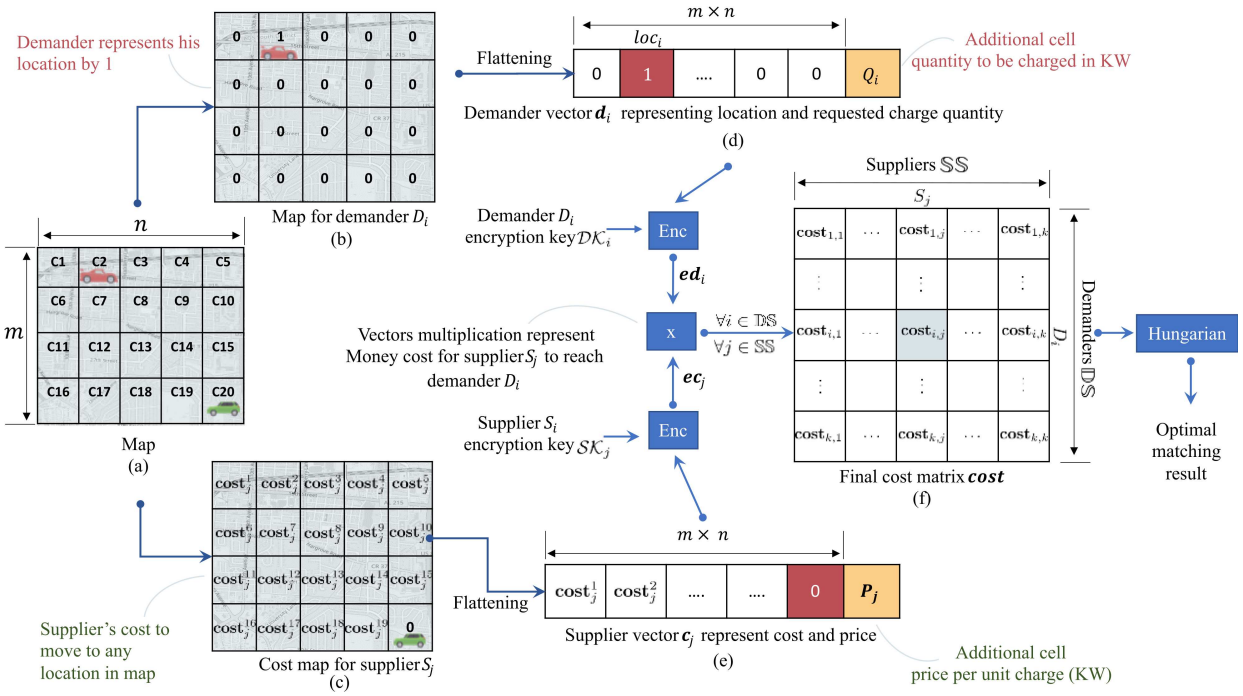


Figure 2: Overview of the data representation and information flow with a sample representation for 5×4 map

the requested energy quantity, but also the additional cost needed for the supplier to travel to the demander's location.

2) **Privacy protection of sensitive information**: No entity in the system should be able to extract the following sensitive information: the demander's location, the supplier's location, and the requested amount of energy.

Note that, during the V2V charging process, the demander and supplier are physically located at the same location. With the knowledge of the average V2V charge rate, revealing the requested amount of energy would reveal not only the location of the demander and supplier, but also the time period during which both are physically located.

IV. The Proposed Scheme

A. Proposed Data Representation and Information flow

Figure 2 shows an overview of the proposed data representation and secure information flow. First, a charge-as-a-service area is divided into $m \times n$ cells where each cell has a unique identifier, as shown in Figure 2a. All the demanders and suppliers should represent their sensitive information in the form of a vector of size $v = m \times n + 1$, where the first $m \times n$ elements in the vector represent the map cells.

As shown in Figure 2b,d, a demander D_i builds a charge request vector $\mathbf{d}_i$ that represents his sensitive location information by setting the element corresponding to his location loc_i to 1 and fill all the other elements by zeros. Additionally, D_i represents the requested charge amount Q_i in the last element in the $\mathbf{d}_i$ vector.

On the other hand, a supplier S_j builds his charge offer vector $\mathbf{c_j}$ by reporting the price per unit charge P_j at the last element in $\mathbf{c_j}$, as shown in Figure 2e. Additionally, Figure 2c depicts an additional cost that the supplier S_j incurs to reach every location in the map. For instance, $cost_j^1$ represents an additional cost by S_j to reach cell $(C1)$ in the service area.

The dot product between $\mathbf{d}_i$ and $\mathbf{c}_j$ would result in a realistic cost value $cost_{i,j} = Q_i P_j + cost_j^{loc_i}$, where $cost_{i,j}$ includes the cost on D_i to charge a quantity Q_i from S_j plus the cost required by S_j to travel to D_i's location loc_i.

Note that, the vectors $\mathbf{d}_i$ and $\mathbf{c}_j$ leak sensitive information including the demander's location, the supplier's location, and the requested charge quantity, which can reveal the charging time during which both demander and supplier EVs will be at the same location that violates users' privacy. Therefore, both D_i and S_j encrypt $\mathbf{d}_i$ and $\mathbf{c}_j$, respectively before sending them to the MS as shown in Figure 2f. In this way, the MS can use the encrypted vectors to generate the cost matrix to match each demander to each supplier while preventing the leakage of sensitive information. The final step by the server is to run the Hungarian Algorithm to generate the optimal demander-supplier matching result and return the result to demanders and suppliers.

B. System Setup

The KDC generates two invertible matrices of random numbers, $\mathbf{X}$ and $\mathbf{Y}$, and sets the server's key as $\mathbf{X}^{-1}\mathbf{Y}^{-1}$. In addition, the KDC generates a master key set $\mathcal{MK} = \{\mathbf{M}_1, \mathbf{M}_2, \mathbf{N}_1, \ldots, \mathbf{N}_8\}$, where $\mathbf{X}$, $\mathbf{Y}$, and each element in $\mathcal{MK}$ is $v \times v$ invertible matrix of random numbers. The KDC also generates a splitting vector $\mathbf{sp}$ of size $1 \times v$ that is shared with all the demanders and suppliers.

The KDC uses $\mathcal{MK}$, $\mathbf{X}$, and $\mathbf{Y}$ to generate unique secret keys for each demander/supplier in the system. For a demander D_i, the KDC generates $\mathcal{DK}_i$ as:

$$\mathcal{DK}_i = \begin{Bmatrix} \mathbf{A}_i\mathbf{N}_1\mathbf{X} \ , \ \mathbf{A}_i\mathbf{N}_2\mathbf{X} \ , \ \mathbf{B}_i\mathbf{N}_3\mathbf{X} \ , \ \mathbf{B}_i\mathbf{N}_4\mathbf{X} \ , \\ \mathbf{C}_i\mathbf{N}_5\mathbf{X} \ , \ \mathbf{C}_i\mathbf{N}_6\mathbf{X} \ , \ \mathbf{D}_i\mathbf{N}_7\mathbf{X} \ , \ \mathbf{D}_i\mathbf{N}_8\mathbf{X} \end{Bmatrix}$$

, where $\mathbf{A}_i, \mathbf{B}_i, \mathbf{C}_i$, and $\mathbf{D}_i$ are $v \times v$ matrices of random numbers such that $\mathbf{A}_i + \mathbf{B}_i = \mathbf{M}_1$ and $\mathbf{C}_i + \mathbf{D}_i = \mathbf{M}_2$. Similarly, for each supplier S_j, the KDC generates $\mathcal{SK}_j$ as:

$$\mathcal{SK}_j = \begin{Bmatrix} \mathbf{Y}\mathbf{N}_1^{-1}\mathbf{E}_j \ , \ \mathbf{Y}\mathbf{N}_2^{-1}\mathbf{F}_j \ , \ \mathbf{Y}\mathbf{N}_3^{-1}\mathbf{E}_j \ , \ \mathbf{Y}\mathbf{N}_4^{-1}\mathbf{F}_j \ , \\ \mathbf{Y}\mathbf{N}_5^{-1}\mathbf{G}_j \ , \ \mathbf{Y}\mathbf{N}_6^{-1}\mathbf{H}_j \ , \ \mathbf{Y}\mathbf{N}_7^{-1}\mathbf{G}_j \ , \ \mathbf{Y}\mathbf{N}_8^{-1}\mathbf{H}_j \end{Bmatrix}$$

, where $\mathbf{E}_j, \mathbf{F}_j, \mathbf{G}_j$, and $\mathbf{H}_j$ are $v \times v$ matrices of random numbers, such that $\mathbf{E}_j + \mathbf{F}_j = \mathbf{M}_1^{-1}$ and $\mathbf{G}_j + \mathbf{H}_j = \mathbf{M}_2^{-1}$. Note that, an EV owner who joins the system as a demander and supplier receives a demander key $\mathcal{DK}$ and a supplier key $\mathcal{SK}$.

C. Demanders: Encrypted Charging Requests

A demander D_i, requesting to charge his/her EV during an assignment round r, should send the matching server a V2V charging request that includes his encrypted location vector $\mathbf{ed}_i$. D_i can generate $\mathbf{ed}_i$ as follows:

1) D_i builds $\mathbf{d}_i$, as shown in Figure 2.
2) D_i splits $\mathbf{d}_i$ into two random vectors $\mathbf{d}'_i$ and $\mathbf{d}''_i$ using the splitting indicator $\mathbf{sp}$. For the k-th element in $\mathbf{d}_i$, splitting is done as follows:

$$\mathbf{d}'_i(k) = \mathbf{d}''_i(k) = \mathbf{d}_i(k) \quad \text{if} \quad \mathbf{sp}(k) = 1$$
$$\mathbf{d}'_i(k) = w_k \ , \ \mathbf{d}''_i(k) = \mathbf{d}_i(k) - \mathbf{d}'_i(k) \quad \text{if} \quad \mathbf{sp}(k) = 0$$

, where w_k is a random number.
3) D_i uses $\mathbf{d}'_i$, $\mathbf{d}''_i$ and his/her demander's key $\mathcal{DK}_i$ to generate his/her encrypted location vector $\mathbf{ed}_i$ as:

$$\mathbf{ed}_i = \begin{bmatrix} \mathbf{d}'_i\mathbf{A}_i\mathbf{N}_1\mathbf{X} \ , \ \mathbf{d}'_i\mathbf{A}_i\mathbf{N}_2\mathbf{X} \ , \ \mathbf{d}'_i\mathbf{B}_i\mathbf{N}_3\mathbf{X} \ , \\ \mathbf{d}'_i\mathbf{B}_i\mathbf{N}_4\mathbf{X} \ , \ \mathbf{d}''_i\mathbf{C}_i\mathbf{N}_5\mathbf{X} \ , \ \mathbf{d}''_i\mathbf{C}_i\mathbf{N}_6\mathbf{X} \ , \\ \mathbf{d}''_i\mathbf{D}_i\mathbf{N}_7\mathbf{X} \ , \ \mathbf{d}''_i\mathbf{D}_i\mathbf{N}_8\mathbf{X} \end{bmatrix}$$

, where $\mathbf{ed}_i$ is a row vector of size $1 \times (8v)$.
4) D_i sends $\mathbf{ed}_i$ to the MS.

D. Suppliers: Encrypted Charging Offers

A supplier S_j, joining the same assignment round r should send MS a V2V charge-sharing offer that includes the encrypted cost vector $\mathbf{ec}_j$. S_j can generate $\mathbf{ec}_j$ as follows:

1) S_j builds the cost vector $\mathbf{c}_j$, as shown in Figure 2.
2) S_j splits $\mathbf{c}_j$ into two random vectors $\mathbf{c}'_j$ and $\mathbf{c}''_j$ using the splitting indicator $\mathbf{sp}$. For the k-th element in $\mathbf{c}_j$, splitting is done as follows:

$$\mathbf{c}'_j(k) = \mathbf{c}''_j(k) = \mathbf{c}_j(k) \quad \text{if} \quad \mathbf{sp}(k) = 0$$
$$\mathbf{c}'_j(k) = z_k \ , \ \mathbf{c}''_j(k) = \mathbf{c}_j(k) - \mathbf{c}'_j(k) \quad \text{if} \quad \mathbf{sp}(k) = 1$$

, where z_k is a random number.
3) S_j uses $\mathbf{c}'_j$, $\mathbf{c}''_i$ and his/her supplier's key $\mathcal{SK}_j$ to generate his/her encrypted cost vector $\mathbf{ec}_j$ as

$$\mathbf{ec}_j = \begin{bmatrix} \mathbf{Y}\mathbf{N}_1^{-1}\mathbf{E}_j\mathbf{c}'_j \ , \ \mathbf{Y}\mathbf{N}_2^{-1}\mathbf{F}_j\mathbf{c}'_j \ , \ \mathbf{Y}\mathbf{N}_3^{-1}\mathbf{E}_j\mathbf{c}'_j \ , \\ \mathbf{Y}\mathbf{N}_4^{-1}\mathbf{F}_j\mathbf{c}'_j \ , \ \mathbf{Y}\mathbf{N}_5^{-1}\mathbf{G}_j\mathbf{c}''_j \ , \ \mathbf{Y}\mathbf{N}_6^{-1}\mathbf{H}_j\mathbf{c}''_j \ , \\ \mathbf{Y}\mathbf{N}_7^{-1}\mathbf{G}_j\mathbf{c}''_j \ , \ \mathbf{Y}\mathbf{N}_8^{-1}\mathbf{H}_j\mathbf{c}''_j \end{bmatrix}^T$$

, where $\mathbf{es}_j$ is a column vector of size $1 \times (8v)$.
4) S_j sends $\mathbf{ec}_j$ to the MS.

E. Server: Privacy-Preserving Assignment

The matching server performs the following steps to find the best-matched demander-supplier pairs such that the cost of the demanders' EVs is minimized while preserving the demanders' and suppliers' locations.

1) The server builds the cost matrix by computing the matching cost between each D_i and each S_j as:

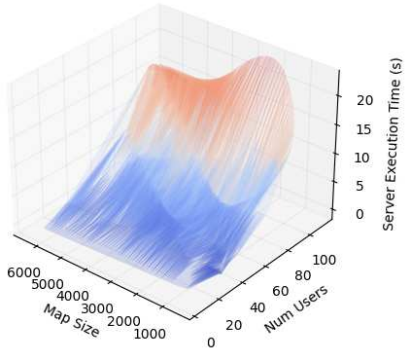
$$cost_{ij} = \mathbf{ed}_i \ \mathbf{X}^{-1} \ \mathbf{Y}^{-1} \ \mathbf{ec}_j \tag{1}$$

2) The server executes the Hungarian Algorithm, which matches demanders and suppliers so that each individual is satisfied by generating the optimal demander-supplier assignment and returning the assignment results to the demander and suppliers so that they can proceed with the energy sharing process.
Note that, the Hungarian algorithm requires the existence of the same number of charging offers and requests in order to return the optimal matching result. To overcome this limitation, we operate in a specific round r on the minimum of the number of suppliers' offers and the number of demanders' request. Let k_d represents the number of the received charging requests from the demanders and k_s represents the number of the received charging offers from the suppliers. In each assignment round, the server will use $k = min(k_d, k_s)$, and one of the following three scenarios will happen:
   a) If $k_d = k_s$, then a normal operation is achieved such that all the k_d charging requests can be served by the existing charging k_s offers.
   b) If $k_d < k_s$, then, $k = k_d$ and thus the firstly submitted k suppliers' offers will be used to serve all the submitted k_d requests and the remaining $k_s - k_d$ charging offers will not be used.
   c) If $k_d > k_s$, then $k = k_s$ which indicated that only k_s out of k_d requests can be served. In this case, the firstly submitted k request will be served by the k_s offers and the remaining $k_d - k_s$ charging requests cannot be served during this assignment round and will be considered in the next round.

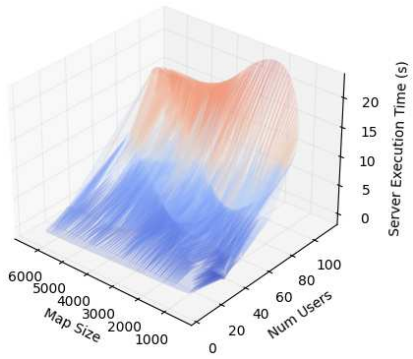
V. Discussion and Evaluations

A. Privacy Protection of Sensitive Information

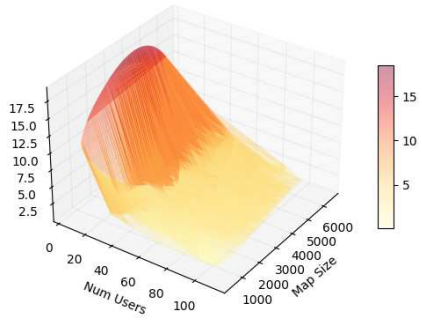
As discussed in subsection IV-A, the sensitive information represented in $\mathbf{d}_i$ and $\mathbf{c}_j$ should not be accessed by external adversaries, the server, or any other user in the system. In our scheme, we utilize a modified version of the encryption scheme presented in [16], [17]. The security of this technique has been formally proven in the known ciphertext model [16]. Therefore, without the knowledge of the master key set $\mathcal{MK}$, the sensitive information cannot be extracted from the encrypted vectors by any entity in the system. In addition, each user can join the system as a demander and supplier



(a) Server execution time with privacy



(b) Server execution time without privacy



(c) Server execution time overhead percentage

Figure 3: Server execution times

Table II: Demanders and suppliers execution time in seconds with privacy scheme implemented

Map Size	400	900	1600	2500	3600	4900
Demander	0.006	0.028	0.088	0.212	0.440	0.820
Supplier	0.002	0.006	0.017	0.041	0.083	0.144

and receives a demander key $\mathcal{DK}$ and a supplier key $\mathcal{SK}$. A misbehaving user may eavesdrop a demander's encrypted vector and tries to use his supplier's key to obtain the sensitive information represented in the victim's encrypted vector. However, as shown in subsection IV-B, the mismatch between $\mathbf{X}$ in $\mathcal{DK}$ and $\mathbf{Y}$ in $\mathcal{SK}$ would thwart this attack and thus, a user cannot infer any sensitive information regarding any other user.

B. Evaluation

This subsection presents the simulation results, which demonstrate the effectiveness of our system and the negligible overhead added by implementing the privacy-preserving scheme described in Section IV. In our simulations, we considered the number of users (demanders or suppliers) ranging from 20 to 220 in a bipartite graph region divided into cells ranging from 10×10 cells to 80×80 cells. The following metrics are used in our evaluation:

1) **Demander/Supplier Execution Time**: The time it takes each demander/supplier to encrypt their messages before sending them to the server.
2) **Server Execution Time with/without Privacy**: The time it takes the server to compute the cost to match all demander-supplier pairs. This is composed of two different times: (1) the time needed to extract the cost value from the reported information, and (2) the time needed to run the Hungarian algorithm to obtain the optimal matching result. Note that with achieving privacy, our scheme adds an overhead to the first component in the server execution time.
3) **Overhead percentage**: The percentage increase in the server's execution time due to implementing the proposed privacy-preserving scheme.

Table III: System execution times in seconds

		Server Execution Time		**Overhead**	
No. Users	**Map Size**	**with Privacy**	**without Privacy**	**Time**	**Percentage**
20	100	0.019	0.017	0.002	9.5%
	1600	0.019	0.017	0.002	13.3%
	6400	0.100	0.095	0.005	5.3%
100	100	2.988	2.950	0.038	1.3%
	1600	2.135	2.082	0.053	2.6%
	6400	1.610	1.496	0.114	7.6%
220	1600	14.933	14.659	0.274	1.9%
	6400	19.049	18.468	0.581	3.1%

The experiments were carried out on a machine equipped with an Intel core I7 processor running at 2.5 GHz and 16 GB of RAM. The experiment was repeated fifty times, and average values were reported.

Table II depicts demanders' and suppliers' execution times when the privacy-preserving scheme is implemented. Without implementing our scheme, the time taken by the demanders and suppliers to prepare the messages without considering location privacy can be considered as zero. In this case, all the sensitive information is reported to the server without any processing time required for encryption. When the privacy-preserving scheme is integrated, both the demander and the supplier encrypt the sensitive information as illustrated in subsection IV-C and subsection IV-D. The execution times in Table II are in the range of milliseconds indicating that our scheme can achieve the privacy protection of sensitive information at a negligible computation overhead on the demander and supplier sides.

Figure 3a depicts the server's execution time with our privacy scheme, Figure 3b presents the execution time without privacy, and Figure 3c shows the time overhead percentage. In addition, Table III shows some sample points from the aforementioned figures. For a small number of users, although the overhead percentage seems high (e.g., 13.3%), the actual overhead to achieve privacy is extremely low (2 ms). For larger number of users, e.g. 220, the overhead to achieve privacy is around 500 ms which is negligible when compared

to the server execution time of 18s (3% overhead). In fact, the Hungarian Algorithm is the most time-consuming operation by the server with a worst case run-time complexity of $\mathcal{O}(k^3)$, where k is the number of users. This is confirmed by Figure 3c, which shows that for a large number of users, the overhead percentage is around 3% to 5%, which is an acceptable cost to achieve the privacy protection of user's sensitive information.

VI. Conclusions

In this paper, we proposed a novel privacy-preserving V2V charging scheme for EVs that utilizes a centralized server to match charge requests and offers while protecting users' sensitive information. The proposed scheme employs the Hungarian algorithm based on a realistic cost function to ensure efficient and secure matching, which can encourage wider participation from EV owners and support the existing charging infrastructure. Our security analysis demonstrates that the proposed scheme can effectively protect users' privacy, requests, and offers, even in cases of repeated requests or assignments. Furthermore, our experiments show that the computational overhead of the proposed scheme is negligible compared to its benefits in preserving users' privacy. Overall, our proposed scheme provides an effective solution to the challenge of V2V charging while safeguarding users' privacy.

Acknowledgment

This work is supported by US National Science Foundation under the grant number 2244371. The statements made herein are solely the responsibility of the authors.

References

[1] F. Lambert, "Countries and automakers agree to go all-electric by 2040." [Online]. Available: https://electrek.co/2021/11/10/countries-automakers-agree-go-all-electric-by-2040-weak-new-goal-cop26/

[2] The California Air Resources Board (CARB), "California moves to accelerate to 100% new zero-emission vehicle sales by 2035." [Online]. Available: https://ww2.arb.ca.gov/news/california-moves-accelerate-100-new-zero-emission-vehicle-sales-2035

[3] Norwegian Electric Vehicle Association, "Norway is leading the way for a transition to zero emission in transport." [Online]. Available: https://elbil.no/english/norwegian-ev-policy/

[4] F. Lambert, "The dutch government confirms plan to ban new petrol and diesel cars by 2030." [Online]. Available: https://electrek.co/2017/10/10/netherlands-dutch-ban-petrol-diesel-cars-2030-electric-cars/

[5] IEA, "By 2030 EVs represent more than 60% of vehicles sold globally." [Online]. Available: https://www.iea.org/reports/by-2030-evs-represent-more-than-60-of-vehicles-sold-globally-and-/require-an-adequate-surge-in-chargers-installed-in-buildings

[6] J. Kester, B. K. Sovacool, L. Noel, and G. Zarazua de Rubens, "Rethinking the spatiality of nordic electric vehicles and their popularity in urban environments: Moving beyond the city?" *Journal of Transport Geography*, vol. 82, p. 102557, 2020.

[7] IEA, "Global EV Outlook 2022: Trends in Charging Infrastructure." [Online]. Available: https://www.iea.org/reports/global-ev-outlook-2022/trends-in-charging-infrastructure

[8] H. S. Das, M. M. Rahman, S. Li, and C. Tan, "Electric vehicles standards, charging infrastructure, and impact on grid integration: A technological review," *Renewable and Sustainable Energy Reviews*, vol. 120, p. 109618, 2020.

[9] E. Bulut, M. C. Kisacikoglu, and K. Akkaya, "Spatio-Temporal non-Intrusive Direct V2V Charge Sharing Coordination," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 10, pp. 9385–9398, 2019.

[10] G. A. Mills-Tettey, A. Stentz, and M. B. Dias, "The Dynamic Hungarian Algorithm for the Assignment Problem with Changing Costs," *Robotics Institute, Pittsburgh, PA, Tech. Rep. CMU-RI-TR-07-27*, 2007.

[11] S. Hosseini and A. Yassine, "A Novel V2V Charging Scheme to Optimize Cost and Alleviate Range Anxiety," in *2022 IEEE Electrical Power and Energy Conference (EPEC)*, 2022, pp. 354–359.

[12] R. Zhang, X. Cheng, and L. Yang, "Flexible Energy Management Protocol for Cooperative EV-to-EV Charging," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 1, pp. 172–184, 2019.

[13] M. Shurrab, S. Singh, H. Otrok, R. Mizouni, V. Khadkikar, and H. Zeineldin, "A Stable Matching Game for V2V Energy Sharing–A User Satisfaction Framework," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 7601–7613, 2022.

[14] F. Yucel, E. Bulut, and K. Akkaya, "Privacy Preserving Distributed Stable Matching of Electric Vehicles and Charge Suppliers," in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, 2018.

[15] F. Yucel, K. Akkaya, and E. Bulut, "Efficient and Privacy Preserving Supplier Matching for Electric Vehicle Charging," *Ad Hoc Networks*, vol. 90, p. 101730, 2019.

[16] W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, "Secure kNN Computation on Encrypted Databases," in *Proceedings of the 2009 ACM SIGMOD International Conference on Management of data*, 2009, pp. 139–152.

[17] A. Alsharif, M. Nabil, A. Sherif, M. Mahmoud, and M. Song, "MDMS: Efficient and Privacy-Preserving Multidimension and Multisubset Data Collection for AMI Networks," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10 363–10 374, 2019.