Ad Hoc Networks 90 (2019) 101730

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Efficient and privacy preserving supplier matching for electric vehicle charging

Fatih Yucel[a], Kemal Akkaya[b], Eyuphan Bulut[a,*]

[a] Dept. of Comp. Science, Virginia Commonwealth University, Richmond, VA 23284, United States
[b] Dept. of Elec. and Comp. Eng., Florida International University, Miami, FL 33174, United States

ARTICLE INFO

Article history:
Received 6 May 2018
Revised 26 June 2018
Accepted 27 July 2018
Available online 29 July 2018

Keywords:
Electric vehicle charging
Scheduling
Privacy
Paillier homomorphic encryption
Distributed stable matching
Vehicular network

ABSTRACT

Electric Vehicle (EV) charging takes longer time and happens more frequently compared to refueling of fossil-based vehicles. This requires in-advance scheduling on charging stations depending on the route of the demander EVs for efficient resource allocation. However, such scheduling and frequent charging may leak sensitive information about the users which may expose their driving patterns, whereabouts, schedules, etc. The situation is compounded with the proliferation of EV chargers such as V2V charging where any two EVs can charge each other through a charging cable. In such cases, the matching of these EVs is typically done in a centralized manner which exposes private information to third parties which do the matching. To address this issue, in this paper, we propose an efficient and privacy-preserving distributed matching of demander EVs with charge suppliers (i.e., public/private stations, V2V chargers) using bichromatic mutual nearest neighbor (BMNN) assignments. To this end, we use partially homomorphic encryption-based BMNN computation through local communication (e.g., DSRC or LTE-direct) between users while hiding their locations. The proposed matching algorithm provides not only a satisfactory assignment for all parties but also achieves an efficient matching in dynamic environments where new demanders and suppliers show up and some leave. The simulation results indicate that the proposed matching of suppliers and demanders can be achieved in a distributed fashion within reasonable computation and convergence times while preserving privacy of users. Moreover, due to the nature of its design, it provides a more efficient matching process for dynamic environments compared to standard stable matching algorithm, reducing the average waiting time for users until matching.

1. Introduction

Due to the potential of electric vehicles (EVs) for providing sustainable and eco-friendly transportation systems, many auto companies have recently launched several new EV models. While this may result in a mass penetration of EVs in the market, the current charging infrastructure is not sufficient to supply the needs of masses. Thus, there is an ongoing effort to expand the charging options for the users. Recently, several different companies have built their own charging networks (e.g., ChargePoint [1]). They coordinate access to charging stations owned by them and provide maintenance services to keep charging stations running. While each charging network website provides the map of their own charging stations, there exist web sites (such as PlugShare [2]) that provide a complete view of all charging stations from different charging networks as well as the residential stations in an area on the map. This helps EV drivers locate available charging stations, and monitor their availability.

In order to provide more options for charging, there are also EV owners who open their residential charging stations to other EV owners and share through the charging network web sites. Similarly, Vehicle-to-Vehicle (V2V) charge sharing based solutions [3–5] are proposed recently to encourage EV owners with excessive charge share/sell their charge with other EV owners in need. There are V2V charging products (e.g., Orca Inceptive [6] by Andromeda Power) in market today which are used by EV owners for charge sharing.

While all these efforts for expanding the charging options help address the frequent and long-period charging needs of EVs, to minimize the waiting times and increase the travel efficiency and driver comfort for the EV users, in-advance scheduling of charging is needed. Obviously, this scheduling needs to consider the spatial distribution of the EVs, the availability of charge suppliers (i.e., public/private charging stations, V2V chargers) and EV owners. An

* Corresponding author.
E-mail addresses: yucelf@vcu.edu (F. Yucel), kakkaya@fiu.edu (K. Akkaya), ebulut@vcu.edu (E. Bulut).

https://doi.org/10.1016/j.adhoc.2018.07.029
1570-8705/

optimum matching could be obtained at a centralized server, once locations of both suppliers and demanders as well as other parameters (e.g., energy needs of demanders, maximum supply amounts of V2V suppliers) are received. While this can yield an optimal matching (e.g., minimum travel distance), it will have the following deficiencies:

- Some private information about the users (both demanders and V2V suppliers) including their locations during this process could be leaked, and with a proper analysis of schedule and charging information (time, location) user's driving patterns and whereabouts may be exposed.
- In practice, users may prefer not to sacrifice individual convenience for the overall benefit of all users. Thus, assigning the closest available charge provider to a demander (to get the service as quickly as possible), as well as the closest demander to a V2V supplier or station may be preferred (to make profit as quickly as possible).
- The cost of running a centralized algorithm could be high (e.g., Hungarian algorithm ($O(N^3)$)) and the algorithm cannot be adjusted to dynamic environments, where new users join and some leave, quickly.

While a number of approaches have been proposed recently to address privacy issues in EV charging[7–12], they are geared mostly for charging on the power grid and within a single charging provider. However, as the number of EVs increases and different options (e.g., mobile V2V and residential) for charge suppliers emerge, there is a need for many-to-many matching for efficient resource utilization, better customer satisfaction in terms of costs and driving, and increased social welfare in the network. There are some recent works [13–15] that study this matching problem. However, they have the potential privacy and security pitfalls of centralized matching at a server and they can not adapt to dynamic environments (which can potentially generate long waiting durations for new arriving demanders). In this paper, we address these issues and present an efficient and privacy-preserving local online matching algorithm between demander EVs and all kinds of suppliers. The proposed algorithm counts on the local communication (e.g., DSRC or LTE-direct) between demander EVs and suppliers. The specific contributions of this work can be summarized as follows:

- We propose a privacy preserving bichromatic mutual nearest neighbor (BMNN) computation using Paillier based partially homomorphic scheme without knowing the actual locations of users.
- We propose a distributed online matching algorithm which not only preserves the privacy of the users but also satisfies each user with their assignment similar to standard stable matching (i.e., Gale-Shapley algorithm [16]) but with less overhead.
- The proposed algorithm works in rounds and proceeds with immediate satisfactory assignments at each round while allowing users join and leave between rounds, thus it adapts to dynamic environments very quickly.
- We provide analytical and extensive simulation results showing the computation and convergence analysis of the proposed algorithm with different parameters and dynamic environments.

The rest of the paper is organized as follows. We discuss the related work in Section 2. In Section 3, we discuss the problem and present the preliminaries about our solution. In Section 4, we discuss the proposed bichromatic mutual nearest neighbor (BMNN) based matching in detail. We also provide an analysis on its convergence. In Section 5, we present our evaluation of the proposed solution. Finally, we end up with conclusion in Section 6.

2. Related work

2.1. EV charging

EV charging has been studied extensively in the context of charging coordination with the power grid. Current literature on scheduling of EV charging mostly focus on minimizing charging waiting time [17] considering the spatio-temporal characteristics [18], and decreasing the impacts on grid load through delayed charging activities. However, during the arrangement of charging, privacy leakages can occur as presented in many works. For example, the impact of the location of EV charging is analyzed in [19] and it has been shown that charging at foreign stations would lead to breach of privacy much more than the charging at home.

To address the privacy concerns during charging, several approaches have been proposed [7–12,20]. For example, in [20], an efficient privacy preserving reservation system is proposed for EVs. The identity of the user who has reserved the station is hidden from the station, thus, a location privacy is achieved. There are also some works [4,21,22] that offer privacy-preserving payment systems for EV charging. For example, in [4], a localized P2P electricity trading system among EVs is proposed using consortium blockchains. An iterative double auction based mechanism is used to optimize electricity pricing and the amount of traded electricity among vehicles, with a goal of maximizing social welfare while protecting privacy of EVs.

The aforementioned works consider the privacy of EVs during their individual charging reservation or scheduling. That is, they do not address the privacy exposure during matching of multiple charge suppliers and demander EVs. However, with the proliferation of enhanced charge supplier options including residential and V2V charge suppliers, a need for hiding the location of charge suppliers (until they are matched) has emerged. Note that this is not needed with public charging stations as their locations are known even before matching.

2.2. Matching

In some recent work [3,5,13–15], the matching of supplier and demander EVs have been studied using different matching algorithms. The impact of commuting patterns of EV drivers, city (transportation and charging) infrastructure and pricing is studied on the spatio-temporal matching of charge requesting EVs with both charging stations and V2V suppliers. However, the main focus in these works is the optimization of the matching in terms of the traveling distances, user preferences or price. In these multi-supplier multi-demander matching systems, EV owners communicate with the scheduler at the server to request for charging and send their location and other related information. Knowing the location of available suppliers and demanders, the scheduler then matches them using various criteria (e.g., total minimum traveling distance [13,15], maximized preference [14]). However, both the demanders and some suppliers (e.g., V2V charge supplier EV) may not want to share their location information with the server in order not to expose their living patterns. Moreover, these works are not designed to work distributively and cannot adapt to the node joins and leaves in dynamic environments quickly while satisfying the users with assignments. To the best of our knowledge, this is the first study that addresses these issues together in the matching of demander EVs to suppliers.

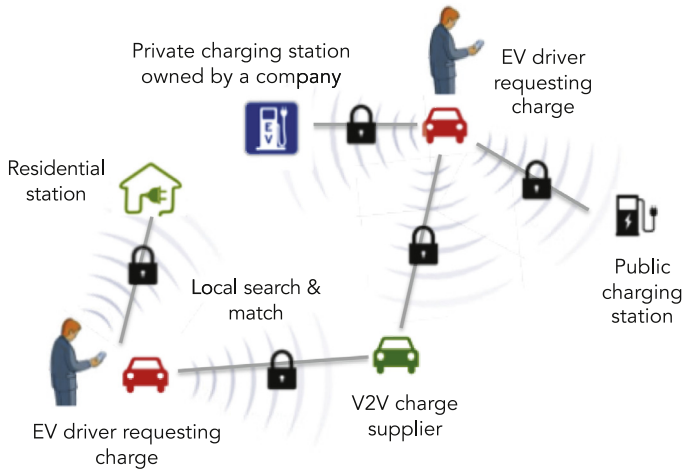

Fig. 1. Overview of the local search and match system.

3. Preliminaries

3.1. System overview and definitions

We assume a system model, as shown in Fig. 1, with two sets of user groups: (i) EV owners requesting for charge, and (ii) charge suppliers (i.e., public/private charging stations, residential stations and V2V chargers). Note that there is no centralized scheduler (i.e., server) assumed in the system. We assume that requester EVs initiate a local query using a local communication technology, as will be detailed shortly, to check if there is available suppliers in their vicinity. The suppliers will collect these requests, and reply back within a reasonable decision time frame to be matched with the requester EVs based on their needs in a distributed manner.

The proposed system counts on the computation of bichromatic mutual nearest neighbors (BMNN) for both demanders and suppliers. Given the set of demanders, $\mathcal{D} = \{D_1, D_2, \ldots, D_N\}$, and suppliers, $\mathcal{S} = \{S_1, S_2, \ldots, S_M\}$, the bichromatic nearest neighbor (BNN) of a demander, D_i $i \in 1 \ldots N$ and a supplier S_j $j \in 1 \ldots M$ is defined as:

$$BNN(D_i) = S_j \text{ s.t. } dist(D_i, S_j) < dist(D_i, S_k)\ \forall k \in \{1 \ldots M\} - j \quad (1)$$

$$BNN(S_j) = D_i \text{ s.t. } dist(S_j, D_i) < dist(S_j, D_k)\ \forall k \in \{1 \ldots N\} - i \quad (2)$$

Here, $dist(.)$ is defined as the Euclidean distance. Then, bichromatic mutual nearest neighbor of a user is defined as:

$$BMNN(D_i) = \begin{cases} S_j, & \text{if } BNN(D_i) = S_j \ \&\ BNN(S_j) = D_i \\ None, & \text{otherwise} \end{cases} \quad (3)$$

In order to preserve the location privacy of users, this computation, however, needs to be made without revealing the actual locations of users to each other. To this end, we use partially homomorphic encryption involving multiple parties. Once each demander computes its own BMNN, then a matching is done if there exists one. Then, the matched pairs exchange the actual locations to meet and perform the charging (after a possible authentication [23]). Note that if a demander is matched to a V2V supplier, either the supplier may drive to the demander's location to provide service or the demander may drive to the supplier's location depending on the arrangement between the parties.

3.2. Background

3.2.1. Local communication options

Local communication between the demanders and suppliers could be achieved via two different technologies: (i) Long-Term Evolution (LTE) Direct and (ii) Dedicated Short-Range Communications (DSRC). LTE Direct is the long-distance peer-to-peer (P2P) protocol introduced in 3GPP Release 12 specification [24]. This communication protocol will exploit direct communication between nearby LTE devices (e.g., smartphones of users) and will enable P2P location based applications and services. In theory, LTE Direct is designed to support communication with up to 1000 devices in a proximity range of 500 m. So, through the app, EV owners can find out local stations or V2V chargers in their surrounding with a broadcast of their desired criteria for charging. The second technology is DSRC (or IEEE 802.11p) standard, which has been developed for vehicular communications to be used in intelligent transportation systems and increase safety at roads. DSRC-based communication can reach up to 900 m transmission ranges with varying data rates. Installment of mandatory DSRC devices on vehicles in the US by 2020 has been planned but not yet finalized [25]. Many vehicle vendors (e.g., Toyota [26], Lexus [27], Volkswagen [28]) have already released their plans to make their new vehicles equipped with DSRC units. Indeed, there are already more than 100,000 DSRC-equipped Toyota and Lexus vehicles on Japan roads (as of March 2018) [27]. With its adoption in the vehicles of other manufacturers and in other countries, this number will increase and a free of charge communication opportunity as opposed to using cellular networks will be established between vehicles. Similar to the LTE Direct, DSRC can help enable building a charging network without a server while increasing privacy. EV owners can do local queries in their vicinity to check if there exists a mobile V2V charger. In the same manner, once the charging stations or other residential stations are equipped with on-board-units (OBU), they can be found with local queries.

Note that there is still a discussion on which of these technologies will be adopted in vehicles as a standard. There are some studies [29–31] comparing the performance evaluation of DSRC and LTE for vehicular networks in detail. In general, LTE can provide more reliable communication especially in dense vehicle scenarios and achieve better communication at longer ranges than DSRC. However, there could be other concerns for LTE-based vehicular communication such as privacy and accessibility issues [31]. The proposed system can potentially work with both options under the provided range among users.

3.2.2. Homomorphic encryption

Homomorphic Encryption (HE) allows computation (e.g., addition, multiplication) on ciphertexts such that when the generated encrypted result is decrypted, it matches the result of the operations as if they had been performed on the plaintext. Such preservation of decryptability allows working on ciphertexts without knowing the actual values and offers opportunity for preservation of privacy in various applications. HE methods could be classified into two, namely, Partially Homomorphic Encryption (PHE) and Fully Homomorphic Encryption (FHE). While PHE supports either addition or multiplication, FHE supports both addition and multiplication. However, FHE is much slower than PHE and its decryption time is too high for a real application [32]. Thus, we use a simpler and efficient PHE system called Palliers cryptosystem [33]. In Paillier's system to have one homomorphic addition, only one multiplication is used, and to have one homomorphic multiplication only one exponentiation is required. That is, the following equations are satisfied:

$$\mathbb{E}(a).\mathbb{E}(b) = \mathbb{E}(a + b) \quad (4)$$

$$\mathbb{E}(a)^b = \mathbb{E}(ab) \tag{5}$$

where, $\mathbb{E}(a)$ stands for ciphertext of a.

In Paillier's system, there are three operations defined: key generation, encryption and decryption. In key generation, after selecting two large prime numbers p and q with same bit length, first $n = pq$ and $\lambda = (p-1)(q-1)$ are computed. Then, $g = (n+1)$ and $\mu = (\lambda \bmod n^2)^{-1}$ mod n are found. The encryption key is defined as (n, g) and the decryption is defined as (λ, μ). While encrypting a plaintext (e.g., $\mathbb{E}(a)$), a random integer, $r \in (Z)_n$, is selected and ciphertext is computed as:

$$\mathbb{E}(a) = g^a r^n \pmod{n^2}$$

During the decryption, the decryption keys, (λ, μ), are used to compute the decryption as follows:

$$\mathbb{D}(a) = L((\mathbb{E}(a))^\lambda \bmod n^2).\mu (\bmod\ n)$$

where $L(u) = (u-1)/n$. Note that with given encryption and decryption computation above, both (4) and (5) are satisfied.

3.3. Adversary model

In the proposed system, we assume an honest-but-curious (HBC) adversary model, which is one of the standard models commonly used while studying privacy-preserving profile matching [34,35] or proximity testing [36–38]. In this model, the users honestly follow the distributed matching protocol while having great curiosity about the others' spatiotemporal profile. That is, they will not report wrong bichromatic nearest neighbor results and will response to the others properly. However, they will try to learn others' locations even though they are not matched and try to understand the bichromatic nearest neighbors of others to favor themselves for being selected as either service providers or receivers.

4. Privacy preserving BMNN-based distributed matching

In this section, we discuss the details of the proposed privacy preserving distributed matching of demander EVs and charge suppliers using the bichromatic mutual nearest neighbor based assignments in rounds.

The proposed algorithm is inspired by the stable matching or marriage problem, which aims to match a group of men and women to each other based on their preferences and satisfies everybody with their assigned partners. That is, there does not exist a blocking pair (m, w) such that m prefers w to his current partner, and w prefers m to her current partner. This problem is initially introduced by Gale and Shapley [16] in an economic context (e.g. market matching), and has been studied in several other domains (e.g., matching schools/residents to schools/hospitals [39,40], wireless sensor networks [41]). Some studies [42,43] have also looked at the problem of making it private and secure. However, these studies do not address the limitations and issues that arise from the real time distributed running of the stable matching. The communication overhead between the parties is ignored and most of the time it is assumed that the preference lists are formed randomly. However, due to the nature of our problem (similar to other location based service provider matching problems), the preferences of users are determined based on Euclidean distances. This brings the opportunity to simplify the matching process and revokes the need to form complete preference lists for each user. This is because the problem of stable matching in our context reduces to finding the bichromatic mutual nearest neighbor [44] for users. This also further makes the algorithm easily adapt to the dynamic environments with user joins and leaves.

The general structure of the proposed algorithm is presented in Algorithm 1 . When a demander needs a charging service, it

Algorithm 1: Generic-matching($\mathcal{D}$, $\mathcal{S}$).

```
while ∃D_i not matched do
    Find BMNN(D_i) in a privacy preserving manner
    if BMNN(D_i) ≠ None then
        Match D_i with BMNN(D_i)
    else
        Wait for the next round
```

first checks if there exists a BMNN for itself. If that is the case, it matches with that supplier; otherwise waits for the next round to be matched.

In order to run this algorithm in a privacy preserving manner, each user needs to compute its bichromatic mutual nearest neighbor without knowing others' location information. To this end, we use Paillier cryptosystem [33] based homomorphic operations between multiple parties in the vicinity.

Note that as the communication between demander EVs and suppliers is achieved through aforementioned local communication technologies, there is always a limited communication range, R, thus each user can only communicate with others within R. This may result in a situation where even though there exists a BMNN for a demander, it may not be reached at all.

4.1. Privacy preserving bichromatic mutual nearest neighbor calculation

In order to compute the bichromatic mutual nearest neighbor, the demander needs to know its closest supplier and also make sure if that supplier's nearest demander is itself (vice versa for the supplier). However, we do not want the demander to calculate its distance to all suppliers and pick the minimum as it could still reveal some information about suppliers' whereabout (i.e., on the circle with range set to distance). Thus, an indicator of the distance should be calculated to be used in the minimum finding process rather than the actual distance. To this end, we use some randomization to the distances without changing the order of the user distances.

Let's denote the ciphertext generated by the Pailier cryptosytem for m with $\mathbb{E}(m)$. The encrypted squared distance computation between a demander D_i at location $\text{loc}_{D_i} = (x_i, y_i)$ and a supplier S_j at location $\text{loc}_{S_j} = (x_j, y_j)$ could be achieved by (see (4) and (5) for description of Paillier operations used):

$$\begin{aligned} dist(i,j) &= |loc_{D_i} - loc_{S_j}| = (x_i - x_j)^2 + (y_i - y_j)^2 \\ \mathbb{E}(dist(i,j)) &= \mathbb{E}(x_i^2 - 2x_i x_j + x_j^2 + y_i^2 - 2y_i y_j + y_j^2) \\ &= \mathbb{E}(x_i^2).(\mathbb{E}(x_i))^{-2x_j}.\mathbb{E}(x_j^2).\mathbb{E}(y_i^2). \\ &\quad (\mathbb{E}(y_i))^{-2y_j}.\mathbb{E}(y_j^2) \end{aligned} \tag{6}$$

However, in order to add additional obfuscation to the distance, we add the following two random numbers to this calculation:

$$\mathbb{E}(R_1 dist(i,j) + R_2) = \mathbb{E}(dist(i,j))^{R_1} + \mathbb{E}(R_2) \tag{7}$$

In the proposed distributed system, however, each user (demander/supplier) will have own PHE keys. But this calculation has to be managed using one single key of one of the users in the vicinity. To this end, we designed a communication and computation procedure among the users, which is summarized in Algorithm 2 .

When a demander EV needs to be charged, it sends a broadcast message to the suppliers in the vicinity (step 1). Each supplier then generates its encrypted location information (i.e., $\mathbb{E}(2x_j)$, $\mathbb{E}(x_j^2)$,

Algorithm 2: Privacy preserving bichromatic nearest neighbor (BNN) calculation.

0 The user application generates encryption and decryption key pairfor each demander and supplier: $E_{D_i} = (n, g)$, $D_{D_i} = (\lambda, \mu)$.

1 EV_{D_i} broadcasts a message for its charging need to all suppliers in the vicinity (i.e., communication range).

2 After receiving this request, each EV_{S_j} generates the following ciphertexts using their own public keys and broadcasts to the demander D_i.

$$\mathbb{E}_{S_j}(2x_j),\ \mathbb{E}_{S_j}(x_j^2),\ \mathbb{E}_{S_j}(2y_j),\ \mathbb{E}_{S_j}(y_j^2),\ \mathbb{E}_{S_j}(1)$$

3 After collecting these ciphertexts from suppliers, the demander EV_{D_i} generates two random numbers R_1 and R_2, then executes the following homomorphic operations for each supplier, EV_{S_j}:

$$\mathbb{E}_{S_j}(1)^{R_1 x_i^2} = \mathbb{E}_{S_j}(R_1 x_i^2),$$
$$\mathbb{E}_{S_j}(1)^{R_2} = \mathbb{E}_{S_j}(R_2),$$
$$\mathbb{E}_{S_j}(2x_j)^{-R_1 x_i} = \mathbb{E}_{S_j}(-2R_1 x_i x_j),$$
$$\mathbb{E}_{S_j}(2y_j)^{-R_1 y_i} = \mathbb{E}_{S_j}(-2R_1 y_i y_j),$$
$$\mathbb{E}_{S_j}(-2R_1 x_i x_j).\mathbb{E}_{S_j}(R_1 x_i^2).\mathbb{E}_{S_j}(R_1 x_j^2) = \mathbb{E}_{S_j}(R_1 (x_i - x_j)^2)$$
$$\mathbb{E}_{S_j}(-2R_1 y_i y_j).\mathbb{E}_{S_j}(R_1 y_i^2).\mathbb{E}_{S_j}(R_1 y_j^2) = \mathbb{E}_{S_j}(R_1 (y_i - y_j)^2)$$
$$\mathbb{E}_{S_j}(R_1 (x_i - x_j)^2).\mathbb{E}_{S_j}(R_1 (y_i - y_j)^2).\mathbb{E}_{S_j}(R_2) =$$
$$\mathbb{E}_{\mathbf{S_j}}(\mathbf{R_1}[\mathbf{dist}(\mathbf{i}, \mathbf{j})]^2 + \mathbf{R_2})$$

4 EV_{D_i} sends the encrypted distance indicator (**bold term above**) to each supplier together with $\mathbb{E}_{S*}(1)$ of a randomly selected supplier (S_*) that responded. The response to S_* does not include $\mathbb{E}_{S*}(1)$, so that it knows that it is selected (for minimum computation) and skips step 5.

5 Each EV_{S_j}, except S_*, receiving the distance indicator performs the following operations and sends it back to the demander, which then forwards all responses to S_* in an array.

$$d = \mathbb{D}_{S_j}(\mathbb{E}_{\mathbf{S_j}}(\mathbf{R_1}[\mathbf{dist}(\mathbf{i}, \mathbf{j})]^2 + \mathbf{R_2}))$$
$$\mathbb{E}_{S*}(R_1[dist(i, j)]^2 + R_2) = \mathbb{E}_{S*}(1)^d$$

6 EV_{S*}, after receiving the ciphertexts, decrypts them and finds the minimum of distance indicators and notifies the demander about the index of the minimum in the array and its plaintext.

$\mathbb{E}(2y_j)$, $\mathbb{E}(y_j^2)$) and $\mathbb{E}(1)$ using its PHE public key and sends it to the demander (step 2). The demander then randomly selects two numbers and performs the necessary homomorphic operations to obtain the *distance indicator* in (7) for each supplier (step 3). However, as each of these distance indicators are computed by different keys. To be able to make a comparison and find their minimum, the demander selects a random supplier (S_*) among the responders and sends $\mathbb{E}_{S*}(1)$ to the other suppliers. S_* itself does not receive it, thus knows that it is selected for minimum computation (step 4). Other suppliers then decrypt this distance indicator and perform the necessary homomorphic operation (step 5) to get the distance indicator encrypted by the selected supplier's key. This information is then shared with the demander, which is further forwarded to the selected supplier. S_* then decrypts all information and finds the minimum of the distance indicators and notify the demander about it (step 6). Note that after S_* finds the minimum, it will not be able to understand the supplier with that minimum. Only the demander will be able to determine it as it knows R_1 and R_2. The communication aspect of this procedure among a demander and three suppliers is also illustrated in Fig. 2. Note that if the supplier is a public station it may not be necessary to follow this

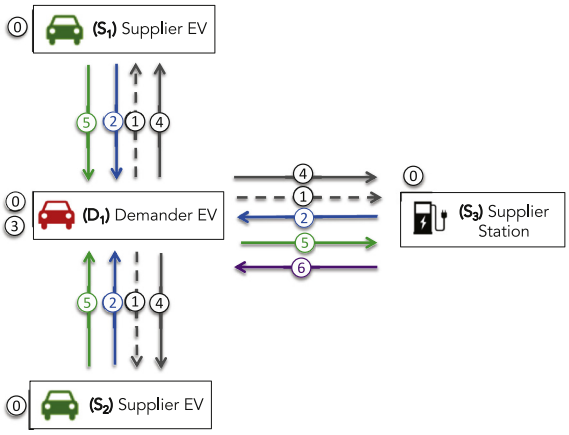

Fig. 2. The communication between the demander EV and suppliers during the privacy preserving bichromatic nearest neighbor calculation.

procedure however, for private and residential stations as well as V2V suppliers it will be needed.

Once the demander learns its BNN among suppliers, it asks that supplier to check if there exists a BMNN situation. Then, the same process with demander/supplier roles reversed is initiated by that supplier and if it ends up that BNN of that supplier is also this demander, the demander is notified about it.

4.2. Efficient distributed matching

In this part, we describe the detailed procedures followed by the demanders and suppliers for the matching in rounds. When a demander needs to be charged, it broadcasts this need and waits for the responses from suppliers. If the demander receives only one response from a single supplier, it skips the BNN calculation and proposes to the only supplier it has for matching. The supplier who receives a propose message then initiates the BNN procedure for itself. If it ends up that the demander proposed to the supplier is BNN for the supplier then it accepts the matching. This is also naturally followed by the encrypted raw location exchange between each other using their public keys. If the demander, however, receives responses from multiple suppliers, it starts the procedure to find its own BNN first using Algorithm 2. After that, the nearest supplier is proposed and the rest is followed as in previous case. Algorithms 3 and 4 show these procedures run by demanders

Algorithm 3: DemanderEV().

```
notMatched ← true
while notMatched do
    Broadcast the need for matching
    if only one supplier, s1, responded then
        s ← s1
    else
        s ← BichromaticNearestNeighbor() in Algorithm 2
    sendMessage(propose, d, s)
    msg ← getMessage()
    if msg.type is accept then
        notMatched ← false
```

and suppliers.

Note that there may not be the same number of demanders and suppliers available, thus the matching can end up with some suppliers or demanders not matched. It is also possible that due to the range of the communication technology used, the users will have

Algorithm 4: Supplier().

```
1  notMatched ← true
2  while notMatched do
3      msg ← getMessage()
4      switch msg.type do
5          case broadcast
6              respond with encrypted distances
7          case propose
8              d ← msg.sender
9              d_n ← BichromaticNearestNeighbor() in Algorithm 2
10             if d == d_n then
11                 sendMessage(accept, s, d)
12                 notMatched ← false
13             else
14                 sendMessage(reject, s, d)
```

a partial view of the network. Therefore, a demander cannot be matched even though there exists a supplier at some far distance. However, such cases may not be preferred either in reality as an EV requesting charge may not have enough range to drive to such far suppliers.

The advantage of the proposed matching over the standard preference list based stable matching algorithm [16] is, it adapts to the changes in the network very quickly. That is, once a round of matching is performed, in the next round new demanders/suppliers may show up or some suppliers indicate that they are not available any more. As the proposed algorithm proceeds in rounds, the matching with the updated list of demanders and suppliers can immediately be effective even before the existing demanders are not matched yet.

Fig. 3 shows an example scenario, where initially five different demander EVs ask for charge from the stations and V2V chargers in their vicinity. In the first round, only ($D1$, $S1$) and (D_3, S_3) are matched as they are the only ones that they see each other as their BMNN. In the second round, a new demander, D_6, shows up and makes a request and a new supplier, S_7, becomes available to serve the demanders. The BMNNs are updated for all the users and this time ($D5$, $S2$) and ($D4$, $S7$) are matched. Finally, at the third round, ($D2$, $S5$) and ($D6$, $S6$) are matched.

4.3. Analysis

In this section, we first analyze the convergence of the algorithm in terms of the number of rounds needed. Then, we provide its privacy analysis under the assumed HBC model.

4.3.1. Algorithm's convergence

As each demander is assigned to its nearest supplier which also considers the demander as its nearest demander (i.e., mutual bichromatic nearest neighborhood relationship), we first analyze the probability that such cases will occur. Assume that there are N demanders and M suppliers randomly distributed in an area with a population density ρ_d and ρ_s, respectively. Consider a demander D_1 and a supplier S_1 with distance to each other r (see Fig. 4). In order to have S_1 as the bichromatic nearest neighbor of D_1, there should not be any other supplier within the circle centered at D_1 with radius r. The probability that such a situation will occur is:

$$P(S_1 = BNN(D_1)) = 2\pi r \rho_s e^{-\pi r^2 \rho_s} dr \tag{8}$$

Then, given the fact that S_1 is the bichromatic nearest neighbor of D_1, the probability that D_1 is the bichromatic nearest neighbor of S_1 can be calculated as:

$$P(D_1 = BNN(S_1) \mid S_1 = BNN(D_1)) = e^{-\pi r^2 \rho_d} \tag{9}$$

The probability that D_1 and S_1 will then be bichromatic mutual nearest neighbors (BMNN) is the product of these two probabilities above. With the integral from $r = 0$ to $r = \infty$, the ratio of the demanders having a BMNN can be found:

$$\begin{aligned} \chi &= \int_{r=0}^{\infty} 2\pi r \rho_s e^{-\pi r^2(\rho_s+\rho_d)} dr \\ &= -\frac{\rho_s}{\rho_s+\rho_d} e^{-\pi r^2(\rho_s+\rho_d)} \Big|_0^{\infty} \\ &= \frac{\rho_s}{\rho_s+\rho_d} \end{aligned} \tag{10}$$

So, if there are the same number of demanders and suppliers (regardless of the count), it is expected that 50% of the demanders will find a BMNN for them and match in the first round. In the next round, the count for both becomes half (i.e., D/2), and again half finds a BMNN to match. At the end, this yields a log(D) rounds until all match. However, due to the range of the local communication technology used, some demanders may not be matched as they may not see other available suppliers. This then results in earlier termination of the entire matching process. Moreover, if there are more suppliers this also reduces the number of rounds. For example, with x demanders and $2x$ suppliers, 66% of the demanders are expected to find a BMNN for themselves in the first round. Subsequent rounds also yield more matchings for the demanders (as long as there is a demander in the range) and a quick convergence is achieved.

4.3.2. Privacy analysis

The proposed matching process preserves the privacy of the demanders and suppliers until they are matched under the HBC model. In the HBC model, users do not deviate from the protocol but try to learn as much information as possible from legitimate messages. All suppliers except the selected one for minimum computation (i.e., S_*) will only receive messages encrypted by others' keys. Thus, they will not be able to obtain the plaintexts containing the location information of others at any step. S_* will receive all the distance indicators (step 5 in Algorithm 2) and decrypt them to find the minimum. However, it will not be able to obtain the supplier id with that minimum and the actual location information due to the randomization of distances by the demander (step 3) with R_1 and R_2, which are only known by the demander. The demander will also not be able to obtain the location information of suppliers other than the one matched at the end. It will not be able to decrypt the responses (received at step 3) with location information that are encrypted by each supplier's own key. It will only reach the plaintext distance indicator once S_* notifies it, after which it will be able derive the actual location information of the matched supplier.

5. Simulation results

5.1. Experiment setup

In this section, we present several simulation results regarding the performance of the proposed privacy preserving matching algorithm. We have generated a network topology of 100 demanders and 100 suppliers in a region of size 1km by 1km. The location of the demander and suppliers are assigned with uniform distribution. Then, by changing the range, R, of the local communication technology used, we obtain different scenarios. For the PHE calculations, in general, we use 512-bit primes for p and q defined in Paillier cryptosystem. For the simulations, we use a computer with Intel core i7 processor with speed 2.5 GHz and a 16GB of memory.

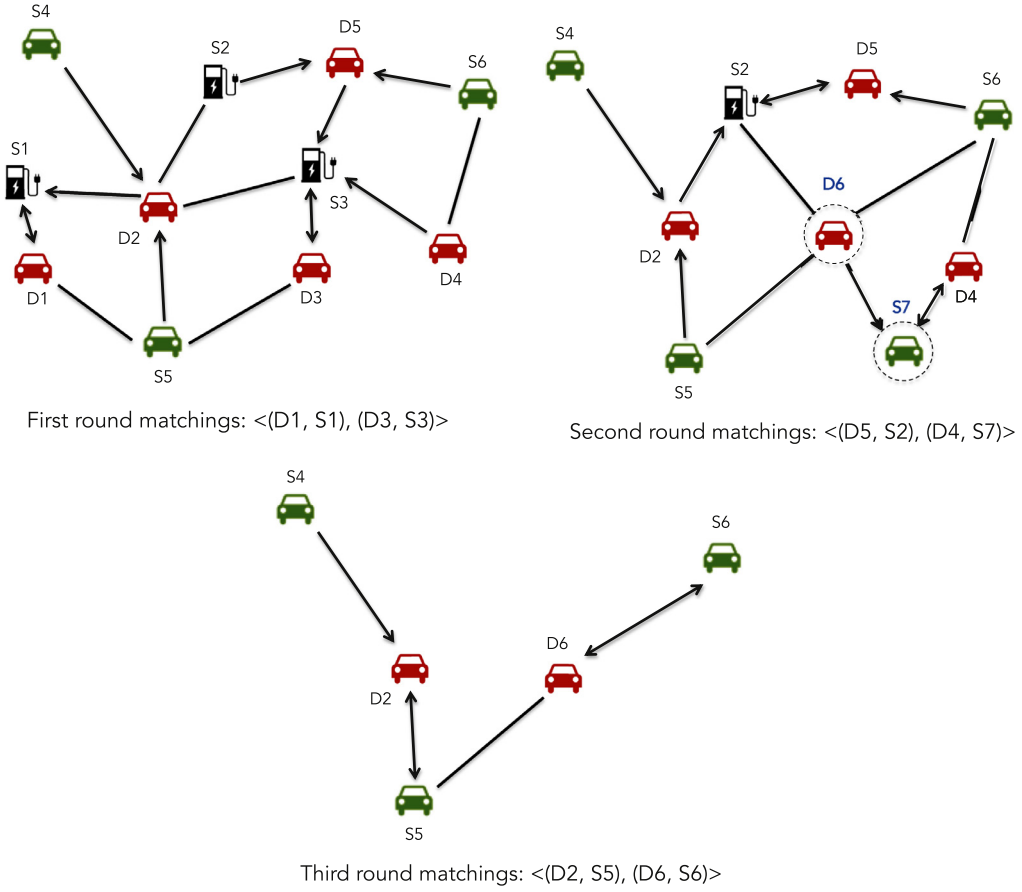

Fig. 3. Bichromatic mutual nearest neighbor (BMNN) based supplier demander assignments in each round. Arrows point to the bichromatic nearest neighbors of each node in the network. Circled users are the new ones that join to the network in the current round.

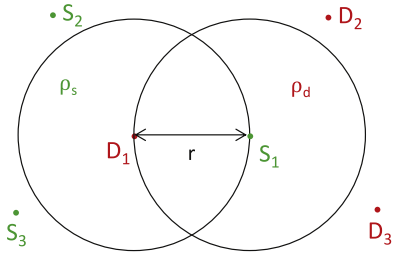

Fig. 4. A demander (D_1) and a supplier (S_1) as bichromatic mutual nearest neighbors. Population density of demanders and suppliers in the area are denoted with ρ_d and ρ_s, respectively.

For every result in this section, we took the average of 100 different runs for statistical significance.

5.2. Performance metrics

We evaluate the performance of the proposed algorithm based on the following metrics:

- **Number of rounds:** This is number of iterations performed in the proposed algorithm until all demanders are matched.
- **Coverage:** This is the ratio of demanders and suppliers matched to the total count in the network.
- **Number of messages:** This is the number of messages exchanged between the demanders and suppliers during the entire matching process.
- **Convergence duration:** This duration includes the total duration that takes for the algorithm to converge (match all possible demanders). It includes both the computation overhead due to encryption and communication overhead due to the messaging.
- **Privacy overhead:** This is the additional processing time required due to the integration of Paillier operations at nodes.
- **Average duration until matched:** This is the average duration that passes from the time demander asks for charging service until it is matched to a supplier.

5.3. Performance results

We first look at the impact of supplier/demander ratio on the number of rounds needed for the algorithm to converge. As the number of supplier options increases (i.e., $\frac{\rho_s}{\rho_s+\rho_d}$) for the demanders, they can be matched with a supplier more quickly. Fig. 5 shows the number of rounds with respect to this supplier/demander ratio changing in the range of [1–2]x. Note that after the ratio reaches 2, the number of rounds stabilizes around 5.5 rounds.

Next, in Fig. 6, we look at the impact of communication range on the number of rounds. As the communication range increases, each demander can reach out more suppliers. While this provides additional matching opportunity for the remaining demanders and increases the coverage (i.e., the number of matched demanders), it delays the convergence of the algorithm as the algorithm stops when all demanders are matched or there is no supplier in their range. Fig. 6 also shows how the coverage is affected by the communication range. Note that when the communication range is small, some of the demanders may not be matched with any supplier. This results in less coverage but it also decreases the number of rounds needed for the convergence of the algorithm.

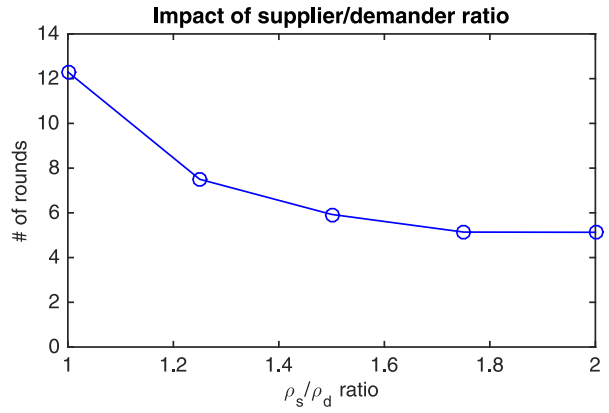

Fig. 5. The impact of supplier to demander ratio on the number of rounds.

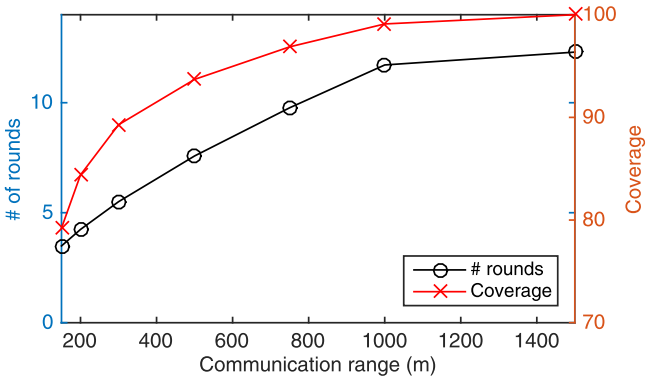

Fig. 6. The impact of communication range on the number of rounds.

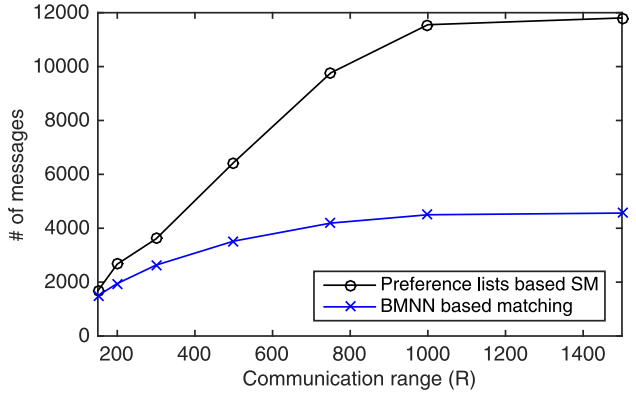

Fig. 7. The comparison of the total number of messages exchanged between users in preference list based standard stable matching and BMNN based (stable) matching.

In Fig. 7, we compare the proposed BMNN based matching process with the standard preference list based stable matching (SM) [16] in terms of messaging overhead. We use the distributed version implemented in [45]. In the proposed BMNN based matching process, the demander only needs to know the nearest neighbor while the standard stable matching algorithm requires the demander know the entire preference list. Moreover, the standard stable matching algorithm causes additional message exchanges due to the deferred acceptance concept it adopts. Due to all these reasons, the standard algorithm generates unnecessary messaging overhead. With the proposed algorithm, only immediate acceptances are allowed, thus messaging overhead is reduced significantly.

Table 1
Average preference list sizes for different R.

Range (R) - meter	100	250	500	750	1000	1500
Avg preference list size	2.8	15.5	48.4	80.3	97.5	100

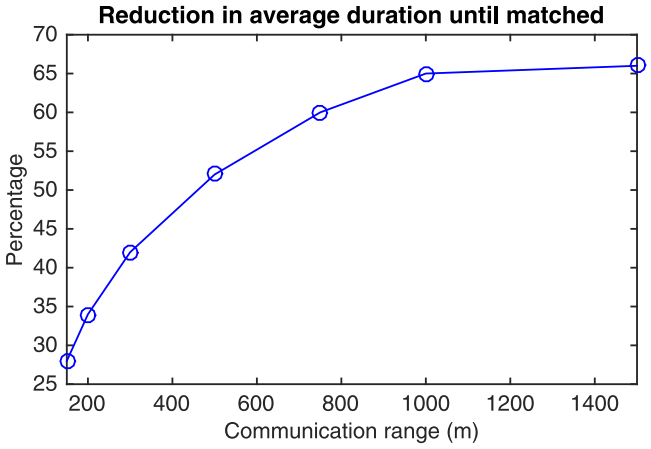

Fig. 8. The percentage of reduction obtained with the proposed BMNN based matching on the average duration a demander waits to be matched.

Note that as the communication range changes, the size of the preference lists needed in the original stable matching algorithm also changes. In Table 1, the corresponding average list size for different R values is shown. When R=1500 m, all demanders can see all other suppliers and vice versa. Thus, the lists for demanders consist of all suppliers and the lists for suppliers consist of all demanders. As it is shown in Fig. 7, this then yields higher messaging overhead.

Next, we analyze the benefit of the proposed algorithm in terms of average duration passes for demanders until they are matched. To this end, we introduce a dynamic environment and add 5–10 new demander and supplier at every round in a random location. Fig. 8 shows the reduction in this average matching duration per demander compared to the original stable matching algorithm (with R=500m). As the communication range increases the size of the preference list gets larger as well as the communication overhead needed between users. This also results in larger waiting duration for the demanders/suppliers that join to the network while the original algorithm is still running its steps. With the proposed round based approach, the new users can be immediately be considered as part of the matching process, thus smaller waiting duration until matching is achieved. Fig. 8 shows that up to 65% reduction could be achieved and users could obtain better satisfaction.

Finally, we look at the privacy overhead introduced with the proposed location privacy preserving operations. Fig. 9 shows both the total convergence duration and the privacy overhead within it. For these simulations, we assumed that one way of communication between users take 300 ms on the average. As the communication range increases, the number of rounds to convergence increases. Thus, the total duration also increases. The privacy overhead within this duration is, however, less than 1.5 s. This result clearly shows that the proposed homomorphic calculations do not affect the overall convergence of the proposed matching process significantly. It is important to remark that it may take up to 9–10 s for the algorithm to converge when all suppliers and demanders are within the range of each other. While such a high dense connectivity may not be the case in practice most of the time, splitting of the network into subnetworks could be considered to limit the convergence delay.

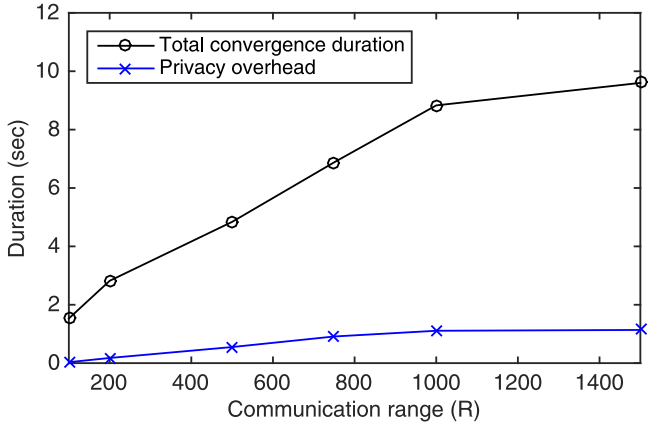

Fig. 9. Total convergence duration of proposed matching and associated privacy overhead within it.

6. Conclusion

In this paper, we study the privacy preserving matching of EVs that are in need of charge with suppliers. In the proposed system, demander EVs identify the potential suppliers in the vicinity through a local search using a P2P communication technology such as LTE-direct or DSRC and conduct a matching with their bichromatic mutual nearest neighbors (BMNN), if exists. This is achieved by using a partially homomorphic encryption-based computation between users while hiding their locations. The proposed matching algorithm provides not only a satisfactory assignment for all parties but also achieves an efficient matching in dynamic environments by its design, thus reduces the average waiting time for users until matching. It also in general avoids the potential privacy and security pitfalls of centralized matching at a server. The simulation results show that this privacy preserving matching process can converge in a reasonable time and the computation overheads for Paillier based calculations do not affect the convergence delay profoundly. Moreover, it provides low messaging overhead and short convergence duration compared to the original stable matching algorithm.

References

[1] ChargePoint, Tap. charge. go, 2017, https://www.chargepoint.com/.
[2] PlugShare, 2017, https://www.plugshare.com/.
[3] R. Alvaro-Hermana, J. Fraile-Ardanuy, P.J. Zufiria, L. Knapen, D. Janssens, Peer to peer energy trading with electric vehicles, IEEE Intell. Transp. Syst. Mag. 8 (3) (2016) 33–44.
[4] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, E. Hossain, Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains, IEEE Trans. Ind. Inf. 13 (6) (2017) 3154–3164.
[5] M. Wang, M. Ismail, R. Zhang, X. Shen, E. Serpedin, K. Qaraqe, Spatio-temporal coordinated v2v fast charging strategy for mobile gevs via price control, IEEE Trans. Smart Grid (2016).
[6] A. Power, Orca inceptive, 2018, http://www.andromedapower.com/orca-inceptive/.
[7] W. Han, Y. Xiao, Privacy preservation for v2g networks in smart grid: a survey, Comput. Commun. 91 (2016) 17–28.
[8] Z. Yang, S. Yu, W. Lou, C. Liu, Privacy-preserving communication and precise reward architecture for v2g networks in smart grid, IEEE Trans. Smart Grid 2 (4) (2011) 697–706.
[9] M. Stegelmann, D. Kesdogan, Design and evaluation of a privacy-preserving architecture for vehicle-to-grid interaction, in: European Public Key Infrastructure Workshop, Springer, 2011, pp. 75–90.
[10] Y. Cao, N. Wang, G. Kamel, Y.-J. Kim, An electric vehicle charging management scheme based on publish/subscribe communication framework, IEEE Syst. J. (2015).
[11] M. Stegelmann, D. Kesdogan, Location privacy for vehicle-to-grid interaction through battery management, in: Information Technology: New Generations (ITNG), 2012 Ninth International Conference on, IEEE, 2012, pp. 373–378.
[12] S. Han, U. Topcu, G.J. Pappas, Differentially private distributed protocol for electric vehicle charging, in: Communication, Control, and Computing (Allerton), 2014 52nd Annual Allerton Conference on, IEEE, 2014, pp. 242–249.
[13] R. Zhang, X. Cheng, L. Yang, Flexible energy management protocol for cooperative ev-to-ev charging, in: Global Communications Conference (GLOBECOM), 2016 IEEE, IEEE, 2016, pp. 1–6.
[14] R. Zhang, X. Cheng, L. Yang, Stable matching based cooperative v2v charging mechanism for electric vehicles, in: in Proceedings of Vehicular Technology Conference (VTC Fall), 2017 IEEE, IEEE, 2017, pp. 1–6.
[15] E. Bulut, M. Kisacikoglu, Mitigating range anxiety via vehicle-to-vehicle social charging system, in: Proceedings of Vehicular Technology Conference (VTC Spring), IEEE, 2017.
[16] D. Gale, L. Shapley, College admissions and stability of marriage, Am. Math. Mon. 69 (1962) 9–15.
[17] H. Qin, W. Zhang, Charging scheduling with minimal waiting in a network of electric vehicles and charging stations, in: Proceedings of the Eighth ACM international workshop on Vehicular inter-networking, ACM, 2011, pp. 51–60.
[18] N. Boysen, D. Briskorn, S. Emde, Scheduling electric vehicles and locating charging stations on a path, J. Schedul. (2017) 1–16.
[19] L. Langer, F. Skopik, G. Kienesberger, Q. Li, Privacy issues of smart e-mobility, in: Industrial Electronics Society, IECON 2013-39th Annual Conference of the IEEE, IEEE, 2013, pp. 6682–6687.
[20] J.K. Liu, W. Susilo, T.H. Yuen, M.H. Au, J. Fang, Z.L. Jiang, J. Zhou, Efficient privacy-preserving charging station reservation system for electric vehicles, Comput. J. 59 (7) (2016) 1040–1053.
[21] T. Zhao, C. Zhang, L. Wei, Y. Zhang, A secure and privacy-preserving payment system for electric vehicles, 2015.
[22] F. Knirsch, A. Unterweger, D. Engel, Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions, Comput. Sci.-Res. Dev. (2017) 1–9.
[23] B. Roberts, K. Akkaya, E. Bulut, M. Kisacikoglu, An authentication framework for electric vehicle-to-electric vehicle charging applications, MASS REU Research in Networking and Systems Workshop, IEEE, 2017.
[24] 3GPP, Mobile broadband standard, 2015, (v12) http://www.3gpp.org/specifications/releases/68-release-12.
[25] Z. Estrada, Us set to drop proposed vehicle-to-vehicle communications mandate, 2017, https://www.theverge.com/2017/11/1/16592704/vehicle-to-vehicle-communications-mandate-trump.
[26] S. Abuelsamid, Toyota has big plans to get cars talking to each other and infrastructure in the u.s., 2018, https://www.forbes.com/sites/samabuelsamid/2018/04/16/toyota-launches-aggressive-v2x-communications-roll-out-from-2021/#6d13e1d1146c.
[27] T.N. Release, Toyota and lexus to launch technology to connect vehicles and infrastructure in the u.s. in 2021., 2018, http://corporatenews.pressroom.toyota.com/releases/toyota+and+lexus+to+launch+technology+connect+vehicles+infrastructure+in+u+s+2021.htm.
[28] V.M. Services, With the aim of increasing safety in road traffic, volkswagen will enable vehicles to communicate with each other as from 2019, 2017, https://tinyurl.com/volkswagen-media-services.
[29] M. Wang, M. Winbjork, Z. Zhang, R. Blasco, H. Do, S. Sorrentino, M. Belleschi, Y. Zang, Comparison of lte and dsrc-based connectivity for intelligent transportation systems, in: Vehicular Technology Conference (VTC Spring), 2017 IEEE 85th, IEEE, 2017, pp. 1–5.
[30] Z. Xu, X. Li, X. Zhao, M.H. Zhang, Z. Wang, Dsrc versus 4g-lte for connected vehicle applications: a study on field experiments of vehicular communication performance, J. Adv. Transp. 2017 (2017).
[31] G. Americas, 5g americas white paper: Cellular v2x communications towards 5g, 2018, http://www.5gamericas.org/files/9615/2096/4441/2018_5G_Americas_White_Paper_Cellular_V2X_Communications_Towards_5G__Final_for_Distribution.pdf.
[32] M. Naehrig, K. Lauter, V. Vaikuntanathan, Can homomorphic encryption be practical? in: Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, ACM, 2011, pp. 113–124.
[33] P. Paillier, Public-key cryptosystems based on composite degree residuosity classes, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 1999, pp. 223–238.
[34] M. Li, N. Cao, S. Yu, W. Lou, Findu: privacy-preserving personal profile matching in mobile social networks, in: INFOCOM, 2011 Proceedings IEEE, IEEE, 2011, pp. 2435–2443.
[35] R. Zhang, Y. Zhang, J. Sun, G. Yan, Fine-grained private matching for proximity-based mobile social networking, in: INFOCOM, 2012 Proceedings IEEE, IEEE, 2012, pp. 1969–1977.
[36] Z. Lin, D. Foo Kune, N. Hopper, Efficient private proximity testing with gsm location sketches, in: Financial Cryptography and Data Security, 2012, pp. 73–88.
[37] J. Sun, R. Zhang, X. Jin, Y. Zhang, Securefind: secure and privacy-preserving object finding via mobile crowdsourcing, IEEE Trans. Wireless Commun. 15 (3) (2016) 1716–1728.
[38] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, D. Boneh, et al., Location privacy via private proximity testing., NDSS, 11, 2011.
[39] N.R.M. Program, 2016 main residency match, 2016, (Reuters web site) http://www.nrmp.org/wp-content/uploads/2016/04/Main-Match-Results-and-Data-2016.pdf.
[40] A. Abdulkadiroğlu, P.A. Pathak, A.E. Roth, The new york city high school match, Am. Econ. Rev. 95 (2) (2005) 364–367.
[41] B. McLaughlan, K. Akkaya, Coverage-based clustering of wireless sensor and actor networks, in: Pervasive Services, IEEE International Conference on, IEEE, 2007, pp. 45–54.
[42] P. Golle, A private stable matching algorithm, in: International Conference on Financial Cryptography and Data Security, Springer, 2006, pp. 65–80.

[43] J. Doerner, D. Evans, et al., Secure stable matching at scale, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2016, pp. 1602–1613.
[44] R.C. Wong, Y. Tao, A.W. Fu, X. Xiao, On efficient spatial matching, in: Proceedings of the 33rd International Conference on Very Large Data Bases, University of Vienna, Austria, September 23–27, 2007, 2007, pp. 579–590.
[45] I. Brito, P. Meseguer, Distributed stable matching problems, in: CP, Springer, 2005, pp. 152–166.

Fatih Yucel (M'17) received B.S. degree in Gazi University in Turkey in 2017. He is now doing Ph.D. in the Computer Science Department of Virginia Commonwealth University under the supervision of Dr. Eyuphan Bulut. He joined MoWiNG lab in Fall 2017. He is working on the development of efficient algorithms for Internet of Things (IoT) and spatial crowdsourcing. He is a member of IEEE.

Kemal Akkaya (A'08-M'08-SM'15) received the Ph.D. degree in computer science from the University of Maryland, Baltimore, MD, USA, in 2005. He is now a Professor with the Department of Electrical and Computer Engineering, Florida International University, Miami, FL, USA. His current research interests include security and privacy, energy aware routing, topology control, and quality of service issues in a variety of wireless networks. Dr. Akkaya was the recipient of the Top Cited Article Award from Elsevier in 2010. He is an Area Editor of the Elsevier Ad Hoc Network journal, and serves on the Editorial Board of the IEEE Communication Surveys and Tutorials.

Eyuphan Bulut (M'08) received the Ph.D. degree in the Computer Science department of Rensselaer Polytechnic Institute (RPI), Troy, NY, in 2011. He then worked as a senior engineer in Mobile Internet Technology Group (MITG) group of Cisco Systems in Richardson, TX for 4.5 years. He is now an Assistant Professor with the Department of Computer Science, Virginia Commonwealth University (VCU), Richmond, VA. His research interests include mobile and wireless computing, network security and privacy, mobile social networks and crowdsensing. Dr. Bulut has been in the organizing committee of the LCN and has also served on the technical program committee of several conferences. He is a member of IEEE and ACM.