Secure, Resilient and Stable Resource Allocation for D2D-based V2X Communication

Fatih Yucel*, Arupjyoti Bhuyan†, and Eyuphan Bulut*
*Department of Computer Science, Virginia Commonwealth University, Richmond, VA 23284
†Idaho National Labs, Idaho Falls, ID
Email: {yucelf, ebulut}@vcu.edu, arupjyoti.bhuyan@inl.gov

***Abstract*—Device-to-device (D2D) communication has been utilized in Vehicle-to-Everything (V2X) communication in order to reuse the cellular network resources and increase spectrum efficiency. Existing works however focus on the maximization of throughput solely without considering the security of channels as well as the resilience of the D2D communication. To address that, in this paper, we study the resource allocation problem between the D2D communicating pairs and regular cellular users in a vehicular network. We consider assignment of D2D pairs to both more secure cellular user channels and more than one channel for resilience. We model the problem as a resource allocation problem between competing parties with their own preferences and leverage *Stable Matching Theory* to obtain a satisfying matching for all involved parties. As existing algorithms that find stable matching do not work for such quota-based systems with multiple level preferences (e.g., secure channel first), we first develop an Integer Linear Programming (ILP) based optimal solution and propose a heuristic based polynomial algorithm that runs much faster than ILP solution. Through simulations, we show that the heuristic based algorithm provides close to optimal results with a much lower complexity and outperforms the existing solutions.**

***Index Terms*—V2X Communication, Device-to-device (D2D), stable matching, 5G network.**

I. Introduction

Device-to-device (D2D) communication is a promising technology in 5G communications that lets nearby user equipments (UEs) communicate with each other without the involvement of a cellular base station (BS). D2D communication in cellular networks can provide significant performance improvement by several means including offloading of the traffic from cellular base stations, reusing the cellular resources and increasing spectrum efficiency, and increasing the coverage of cellular networks by connecting more users [1], [2].

On the other side, as vehicles have become ubiquitous and intelligent with different types of sensors, new paradigms such as connected vehicles and social Internet of Vehicles (IoV) have emerged within the context of Intelligent Transportation Systems (ITS). Vehicles now have been considered one of the fastest growing connected devices after smartphones and tablets [3]. With connected vehicles, the goal is to enable various applications including road safety improvement, traffic efficiency optimization and infotainment services [4], [5]. To this end, D2D communication has been integrated into V2X (e.g., Vehicle to Infrastructure (V2I) with Road Side Units (RSU), Vehicle to Vehicle (V2V)) communication [6], [7].

While initial efforts for V2X communication have focused on adopting ad hoc technologies such as IEEE 802.11p standard and Dedicated Short Range Communications (DSRC), due to the performance related issues and to maintain the quality of service (QoS) especially in massive access, recently Third Generation Partnership Project (3GPP) based communication models (starting with Release 14 [8]) have been developed. The goal is to benefit from the global and widespread deployment and coverage of cellular systems and reuse the same resources for V2X communication without affecting the performance of cellular users. Adopting this idea and 3GPP standards, many research studies have been conducted recently to investigate the feasibility and performance of such D2D-based V2X communications. However, most of the existing work [9]–[11] have focused on development of efficient admission control (e.g., with minimum interference) and radio resource allocation strategies for the purpose of maximizing the throughput for D2D pairs or the sum rate of the entire network. While such efforts will be crucial for high bandwidth requiring V2X communication applications, there are other parameters that will be significant especially within the context of vehicular communication used for exchanging safety messages between vehicles. Such messages are usually small size but they require low delay as well as reliable and secure communication between vehicles. Thus, D2D communication in such V2X systems requires resilience to these metrics more than the maximum data rate.

The resilience of a system is usually defined as its ability to cope with unexpected failures or resource-insufficient situations and to recover from their effects promptly. Within the context of D2D-based V2X communication, where cellular user equipment (CUE) resources are reused by D2D communicating vehicular user equipments (VUE), one way to increase the resilience is to allow alternative channels to D2D communicating pairs. For example, in case of a failure in one channel, transmission of critical packets (e.g., safety messages) could be achieved successfully in alternative channels, and reliability and resilience of the communication could be increased. On the other hand, such a system will increase the competition among D2D users to allocate the existing channels and make the resource allocation problem more challenging.

Moreover, in a V2X communication network with both VUEs and CUEs, some of the channels can be detected

978-1-7281-8693-1/20/$31.00 ©2020 IEEE

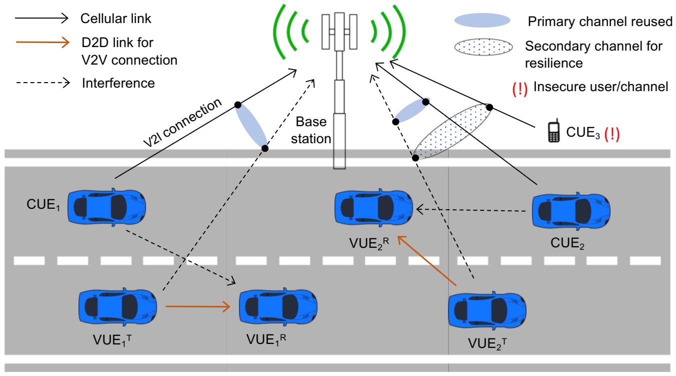


Fig. 1: Overview of vehicular communication network with V2I and V2V links, with multiple CUE assignments to VUEs for resilience and with preference given to reuse of secure CUEs.

as insecure due to the previous user behavior as well as other operations performed by channel administrator such as mobile network operators (MNO). Therefore, providing a secure system will be very significant for VUEs. In case of multiple channel assignments to VUEs to increase resilience, security of the channels has to be considered and more secure channels should be preferred initially for communication.

Fig. 1 shows an example scenario with three CUEs that are directly connected to the base station and two D2D communicating vehicle pairs, each with a transmitting VUE (denoted by VUE^T) and a receiving VUE (denoted by VUE^R). Note that CUEs can be in several forms. That is, cellular mobile phone users inside or outside (e.g., CUE_3) of the vehicles as well as vehicles themselves (e.g., CUE_1) can serve as CUEs. We assume that a separate channel is allocated to each of these CUEs, and VUEs (i.e., each VUE consists of a VUE^T and VUE^R) are assigned to one or multiple of these channels used by CUEs. In this example, VUE_1 is reusing the channel of CUE_1 and VUE_2 is reusing the channels of CUE_2 and CUE_3. We assume that reusing of channels happens for uplink communication (from VUE^T to VUE^R, and from CUE to base station (BS)), thus there will be interference from VUE^T to BS and from CUE to VUE^R. As there are multiple channels assigned to VUE_2, it uses the first one as the primary channel and the second one as secondary channel for resilience. Since CUE_3 is considered as a less secure channel compared to CUE_2, it is considered as secondary channel for VUE_2.

In this paper, our goal is two fold. We first want to increase the resilience of D2D-based V2X communication by letting them reuse the available spectrum resources of multiple CUEs. Second, we want VUEs to reuse the secure channels first in this process. We consider a one-to-many matching scenario in which each VUE can get access to the resources of multiple CUEs based on their quota allowed while each CUE allows only one VUE to share its resource. In order to take into account the preferences of both CUEs and VUEs and provide a satisfactory matching, we model the assignment problem using *Stable Matching Theory*. As this assignment problem is probably NP-complete due to its resemblance to maximum cardinality with minimum instability matching problem [12] and not solvable by a polynomial algorithm, we first model the problem using Integer Linear Programming (ILP) and then develop a heuristic based approach that runs much faster. Our results show that the proposed heuristic approach can provide much secure and stable matching between VUEs and CUEs under this resilience promoting quota-based matching scenario.

The rest of the paper is organized as follows. In Section II, we provide an overview of the related work. In Section III, we provide the system model and our assumptions. In Section IV, we discuss the details of the ILP solution and heuristic approach. In Section V, we present an evaluation of the proposed approach through simulations. Finally, we end up with conclusion in Section VI.

II. Related Work

D2D communication has been studied in various mobile network applications (e.g., mobile social networks [13], vehicular networks) for various purposes such as post-disaster emergency [14], public safety [15] and resilience [16], and using different technologies (licensed e.g., LTE, or unlicensed Bluetooth, WiFi). In V2X communication, it has also been utilized for spectrum efficiency and for coverage increase [9]–[11].

Stable Matching Theory has been introduced by Gale and Shapley initially [17] to address college admission problems and since then it has been applied in several other domains including mobile crowdsensing [18], controller assignment in SDN based networks [19] and supply demand matching in V2V charging [20]. Recently it has been also utilized in wireless communication [21], [22] especially for interference management between D2D users, femtocells and BS [23]. All these works adapt the *deferred acceptance* approach within the context of studied problem and aim to provide a stable matching between all entities in the system. Stability in the context of D2D communication has also been studied to achieve energy efficient resource allocation [24], secure relay selection [25] and to maximize the sum ergodic capacity of D2D pairs [26]. For example, in [25], social ties between D2D communication pairs and relay nodes is used to decide the best relay nodes and to obtain more secure D2D communication.

Security in the context of D2D communications has been mostly considered as physical layer security [27]–[30] with the goal of secrecy rate maximization, however these studies do not consider the user preferences, resilience and security at the same time as we do in this study. In this paper, we focus on these metrics in D2D based V2X communication specifically, and considering the preferences of VUEs and CUEs determined based on the interference induced by each to one another as well as the security of CUE channels, we aim to develop a stable matching between VUEs and CUEs. For resilience we allow multiple CUE assignment to VUEs and for preferences we consider the data rates achievable at each potential assignment between CUEs and VUEs. We also consider the security as a system level objective and aim to assign secure CUEs first to the VUEs. Moreover, as this system level objective is prioritized over user preferences to achieve higher data rates, we aim to find the most secure assignment possible with minimum instability in the system.

III. System Model

Without loss of generality, we consider a system with a single base station (BS) having a circular coverage area. We assume there are n cellular user equipments (CUE) denoted by set $\mathcal{C} = \{CUE_1, CUE_2, \ldots, CUE_n\}$ and m D2D communicating vehicular user equipments (VUE) denoted by set $\mathcal{D} = \{VUE_1, VUE_2, \ldots, VUE_m\}$. Note that each VUE consists of a transmitter (e.g., VUE_1^T) and a receiver (e.g., VUE_1^R) vehicle but considered as a single entity for simplicity. Each CUE is allocated a unique orthogonal channel thus it does not create interference with other CUEs. On the other hand, VUEs reuse the resources of CUEs for spectrum efficiency. While each CUE allows one VUE to use its resources, in order to increase the resilience and reliability of the D2D communication for VUEs we do allow assignment of multiple CUE resources to each VUE. Note that since each CUE uses a different channel, the communication of a VUE with multiple CUEs does not interfere with each other. We also assume that spectrum reuse is only performed for uplink traffic similar to previous work [26]. In order to promote resilience, we assume that each $VUE_j \in \mathcal{D}$ has a quota defining the number of CUEs that can be assigned to it and denoted by q_j. We also assume a binary security indicator for each channel i (used by CUE_i) and denote it by s_i. Note that if a channel is certainly known to be insecure, it will not even be considered in the system. An insecure channel in our system model is either one that is new in the system, so whether it is secure or not is presently unknown, or one whose security score, which is estimated by the degree of similarity to the previously detected insecure channels, is lower than a certain threshold. More complex (e.g., non-binary) security models will be investigated in future work.

As both CUEs and VUEs prefer to have higher signal to interference noise ratio (SINR) for a higher bandwidth, we first define these similar to previous work and form their preferences accordingly. Let Γ_i^j and Γ_j^i denote the SINR of $CUE_i \in \mathcal{C}$ and $VUE_j \in \mathcal{D}$ with respect to each other's interference, respectively. We define

$$\Gamma_i^j = \frac{P_i^c g_{i,B}}{\sigma^2 + \rho_{i,j} P_j^d h_{j,B}} \text{ and } \Gamma_j^i = \frac{P_j^v g_j}{\sigma^2 + \rho_{i,j} P_i^c h_{i,j}} \tag{1}$$

where, P_i^c and P_j^v denote the transmission power of CUE_i and VUE_j^T, respectively; $g_{i,B}$ denotes the channel gain between CUE_i and BS; g_j denotes the channel gain between VUE_j^T and VUE_j^R; $h_{j,B}$ denotes the channel gain of interference link between VUE_j^T and BS; and $h_{i,j}$ denotes the channel gain of interference link between CUE_i and VUE_j^R. We also define

$$\rho_{i,j} = \begin{cases} 1, & \text{if } VUE_j \text{ reuses the channel of } CUE_i \\ 0, & \text{otherwise.} \end{cases}$$

Here, the channel gains are usually defined by taking into account both the slow and fast fading factors and the distance between the transmitter and receiver. That is, for example [22], $g_{i,B} = K\beta_{i,B}\zeta_{i,B}d_{i,B}^{-\alpha}$, where K is a constant value, $\beta_{i,B}$ and $\zeta_{i,B}$ are fast and slow fading gains, $d_{i,B}$ is the distance between CUE_i and BS, and α is path loss exponent. We assume a model with low/moderate mobility (e.g., city center), so Doppler effect on channel state information is ignored. For highly mobile systems, however, formulations should be modified as in [26].

Utility (i.e., data rate) of CUE_i and VUE_j can then be computed by $W_i log(1+\Gamma_i^j)$ and $W_i log(1+\Gamma_j^i)$, respectively, where W_i denotes the bandwidth allocated to the channel i. Then, just in terms of data rate, we consider a preference relation for each CUE such that CUE_i prefers VUE_j over $VUE_{j'}$ if $W_i log(1+\Gamma_i^j) > W_i log(1+\Gamma_i^{j'})$. Similarly, we form a preference relation for each VUE such that VUE_j prefers $CUE_i \in \mathcal{C}$ over $CUE_{i'} \in \mathcal{C}$ if $W_i log(1+\Gamma_j^i) > W_{i'} log(1+\Gamma_j^{i'})$. As our goal in this paper is not to maximize the system throughput, for simplicity, we assume that the transmission power of both CUEs and VUEs are optimized once and do not change, and also the channel gains are mostly defined by the distance between the transmitter and receivers in an inversely proportional manner (i.e., the further a VUE located from BS the less interference it can cause to CUE so the gain would be higher). Note that this then simply defines the preference order of a CUE in the descending order of distances from VUE^Ts to the BS and the preference order of a VUE in the descending order of distances from CUEs to the VUE^Rs.

Note that while preference of CUEs and VUEs are determined based on the data rates they can achieve, as a system level objective, we also aim to assign secure channels first to the VUEs. However, this may conflict with the preferences of users as they all consider their data rates, thus our goal is to find the most secure assignments first then minimize the instability in the assignments as much as possible.

Definition 1 (Matching). *A mapping $\mathcal{M}$ between the sets $\mathcal{C}$ and $\mathcal{D}$ is considered a feasible one-to-many matching if*

- *There is at most one VUE reusing the channel of each CUE, i.e.,*
$$\sum_{\forall j} \rho_{i,j} \leq 1, \ \forall i$$
- *There is at most q_j channels each VUE can use, i.e.,*
$$\sum_{\forall i} \rho_{i,j} \leq q_j, \ \forall j$$

Definition 2 (Unhappy pair). *Given a matching $\mathcal{M}$, a VUE v and a CUE c form an unhappy pair if:*

- *c is either unmatched or matched to a VUE that she prefers less than v due to larger interference,*
- *v either has unused quota, or he prefers c to one of the CUEs in his current assignment.*

Definition 3 (Stable matching). *A matching $\mathcal{M}$ is stable if it admits no unhappy pair.*

IV. Stable Resource Allocation

In this section, we first model the problem using Integer Linear Programming (ILP) and develop a heuristic based solution that runs fast.

A. ILP based Optimal Solution

Given the following variables:

$$\mathcal{X}_{ij} = \begin{cases} 1, & \text{if } CUE_i \text{ is assigned to } VUE_j \\ 0, & \text{otherwise} \end{cases}$$

$$\mathcal{U}_{ij} = \begin{cases} 1, & \text{if } (CUE_i, VUE_j) \text{ is an unhappy pair} \\ 0, & \text{otherwise} \end{cases}$$

and the feasibility constraints:

$$\sum_{\forall j} \mathcal{X}_{ij} \le 1 \qquad \forall i$$

$$\sum_{\forall i} \mathcal{X}_{ij} \le q_j \qquad \forall j$$

We formulate the problem of finding the maximum security assignment with minimum instability as

$$\max\left\{ P \times \sum_{i=1}^{n}\sum_{j=1}^{m}(s_i \times \mathcal{X}_{ij}) - \sum_{i=1}^{n}\sum_{j=1}^{m}\mathcal{U}_{ij} \right\} \tag{2}$$

where the first term refers to the overall security of the system while the second term refers to the instability. $P = n \times m$ denotes the problem size and makes the security the primary objective (and the stability the secondary objective).

B. Heuristic-based Solution

We present a pseudo-code description of the proposed solution in Algorithm 1. The key idea behind this algorithm is that it reserves the space for secure CUEs in the partner sets of VUEs and matches the given CUEs and VUEs purely based on their preferences as long as this reserved space allows to match as many secure CUEs as it can be matched in a feasible matching. Once it reaches the point where matching another insecure CUE for a better stability would result in a decreased number of matched secure CUEs in the final matching, it only matches the secure CUEs while still considering preferences as much as possible.

To achieve the functionality described above, Algorithm 1 maintains two variables, Q_r and S_R, which refer to the total remaining quotas of the VUEs and the number of the secure CUEs that are still unmatched, respectively. Thus, in lines 1-2, Q_r is initialized to be the sum of the quotas of VUEs in $\mathcal{D}$, and S_r to be the number of secure CUEs in $\mathcal{C}$. Then, in the for loop in lines 3-23, the algorithm iterates through the VUEs in $\mathcal{D}$ in order of their appearance in the common preference list ($P_\mathcal{C}$) of the CUEs to find their assignments. That is, in the ith iteration of this for loop, the algorithm decides which CUEs should be assigned to the ith most preferred VUE (line 4). To this end, it iterates through the preference list of this VUE (v) as long as he has unused quota (line 6), and matches him with the jth CUE (c) in his preference list (line 9) if the following conditions are satisfied.

Algorithm 1: Heuristic ($\mathcal{C}$, $\mathcal{D}$)

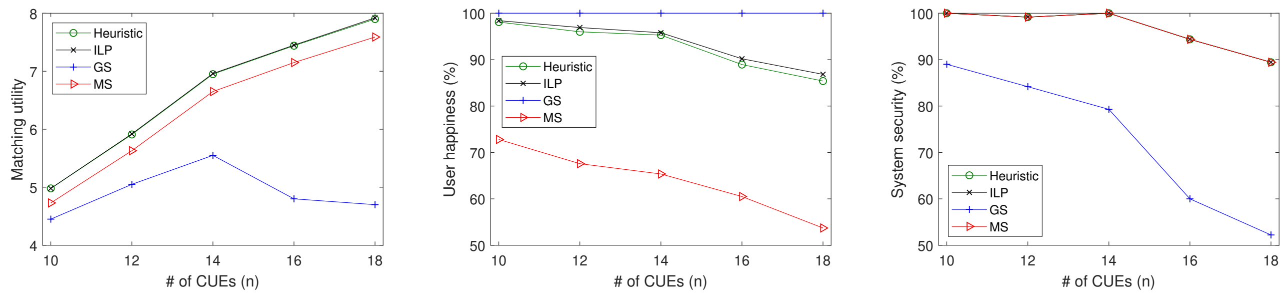
```
Input: C: The set of CUEs
       D: The set of VUEs
1  Q_r ← Σ_{d∈D} q_d
2  S_r ← Σ_{c∈C} s_c
3  for i ← 1 to m do
4      v ← P_C(i)
5      for j ← 1 to n do
6          if |M(v)| = q_v then
7              break
8          end
9          c ← P_v(j)
10         if M(c) = ∅ then
11             if s_j = 1 then
12                 M(v) ← M(v) ∪ {c}
13                 M(c) ← v
14                 Q_r ← Q_r − 1
15                 S_r ← S_r − 1
16             else if Q_r > S_r then
17                 M(v) ← M(v) ∪ {c}
18                 M(c) ← v
19                 Q_r ← Q_r − 1
20             end
21         end
22     end
23 end
24 return M
```

- CUE c should be unmatched (line 10).
- If CUE c is secure it is automatically added, otherwise Q_r should be larger than S_r (line 16) to avoid using the space reserved for secure CUEs.

Runtime analysis. It is clear from the for loops beginning in lines 3 and 5 that the time complexity of Algorithm 1 is $\mathcal{O}(mn)$. However, in the initialization step, we need to form the preference lists of all VUEs and the common preference list of CUEs, which take $\mathcal{O}(mn \log n)$ and $\mathcal{O}(m \log m)$ time, respectively, and make the overall time complexity of the proposed solution $\mathcal{O}(m \log m + mn \log n)$.

V. Simulation Results

To evaluate the performance of the proposed heuristic based solution, we perform real data based simulations using the NYC taxi data set [31]. For each instance, we first randomly select a 2-minutes long time frame in a randomly selected day in December of 2015. Then, we use the location of the passengers that requested a taxi in that time frame to set up the locations of half of our CUEs (*stationary CUEs*). We also use the locations of the taxis that dropped off their passengers within the same time frame to set up the locations of the remaining half of the CUEs (*mobile CUEs*) as well as the locations of the transmitter and receiver in each VUE (they



(a)

(b)

(c)

Fig. 3: Performance comparison of the algorithms against varying number of CUEs ($m = 5$).

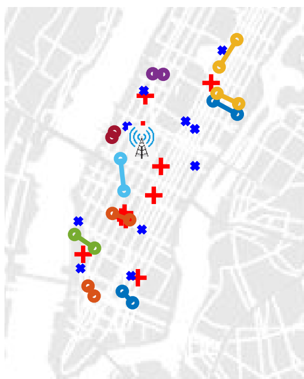


Fig. 2: An instance with 10 VUEs (connected circles), 10 mobile CUEs (x marks), and 10 stationary CUEs (plus signs).

are paired only if the distance between them is at most R). The location of the BS is assigned randomly in the Manhattan area.

Given the generated CUE set of size n, we assign a security score of 1 to the randomly selected $n \times \beta$ CUEs, and 0 to the remaining. On the other hand, the quota of each VUE is assigned randomly from $[1, q_{max}]$. The default values of R, β and q_{max} are 100 meters, 0.5, and 3, respectively, but we also present the results with different R, β and q_{max} values. Following the procedure above, we generate 100 different instances and provide the average results. The distribution of CUEs and VUEs in an instance with 20 CUEs and 10 VUEs is illustrated in Fig. 2.

In evaluation of the results, we compare the ILP solution and our algorithm with *Gale-Shapley (GS) algorithm* [17] which achieves perfectly stable matchings but does not consider security aspect of channels, and *Maximum Security (MS) algorithm* which maximizes the number of matched secure CUEs without considering preferences by finding a maximum matching between VUEs and secure CUEs first, and then randomly assigning the remaining insecure CUEs to the VUEs with unused quota. Lastly, we utilize the following metrics to evaluate the performance of the algorithms.

- **Matching utility**: This is the value of (2) divided by the problem size ($m \times n$), and shows the utility of a matching in terms of both user happiness and security.
- **User happiness (stability)**: This metric quantifies the satisfaction of both VUEs and CUEs with the produced matching, and it is computed by:

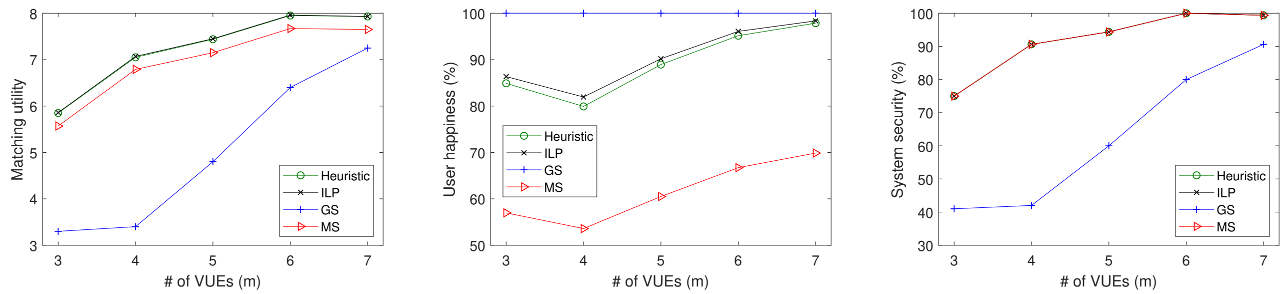
$$100 \times \left(1 - \frac{\text{\# of unhappy pairs}}{m \times n}\right).$$

- **System security**: This is the ratio of the number of matched secure CUEs to the total number of secure CUEs.
- **Running time**: Since we assume a mobile system with ever-changing conditions, the matching between the VUEs and CUEs should be updated regularly. Thus, the running time of a matching algorithm is also a critical element in its evaluation.

A. Results

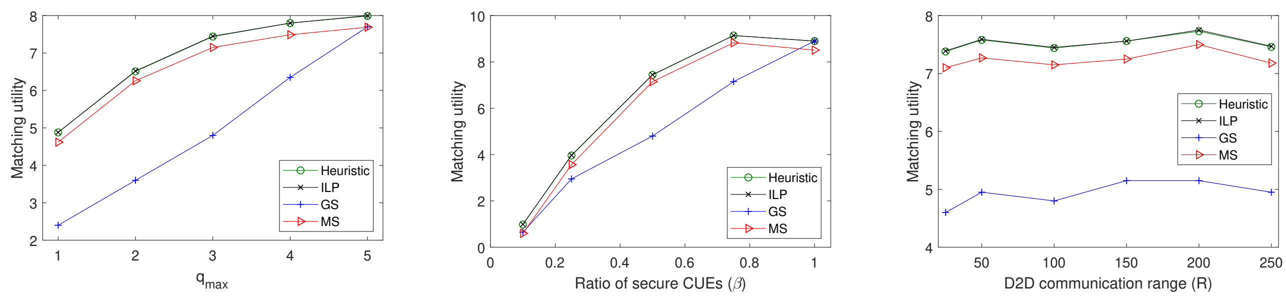
We first examine the performance of the algorithms with varying number of CUEs in Fig. 3. In Fig. 3a, we observe that the proposed solution produces very close to optimal results (ILP), and that the Gale-Shapley algorithm produces the worst matchings in terms of matching utility despite its perfect user happiness score (Fig. 3b). This is because it does not take the system security into account, which is prioritized in the system objective defined in (2). On the other hand, although the MS algorithm achieves the highest system security score possible as our algorithm and the ILP solution do, it produces the worst matchings in terms of user happiness and upsets up to 47% of all CUE-VUE pairs. We also see that the user happiness scores of our algorithm and the ILP solution reduce with increasing number of CUEs, because when there are a larger number of secure CUEs in the system, a bigger sacrifice from user happiness should be made to match as many of these CUEs as possible due to the potential discrepancies between their security and interference values (i.e., their rank in the preference lists of the VUEs).

Next, we look at the performance of the algorithms with different number of VUEs in Fig. 4. Here, we see a similar picture with Fig. 3 in terms of relative performance of the algorithms, but the impact of increasing the number of VUEs on the performance of the algorithms mostly seems to be the opposite of that of increasing the number of CUEs. That is mainly because increasing the number of VUEs (in Fig. 4)



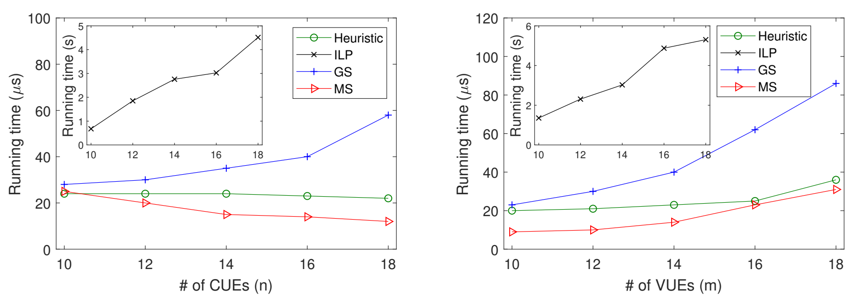
(a) (b) (c)

Fig. 4: Performance comparison of the algorithms against varying number of VUEs ($n = 16$).



(a) (b) (c)

Fig. 5: Performance comparison of the algorithms against varying values of (a) q_{max}; (b) β, and (c) R ($m = 5$, $n = 16$).



(a) (b)

Fig. 6: Running time of the algorithms against varying values of (a) n ($m = 5$) and (b) m ($n = 16$).

makes it easier to match secure CUEs as the sum of the quotas of VUEs gets larger, while increasing the number of CUEs (in Fig. 3) leads to a higher number of secure CUEs, hence makes finding a partner for each one less likely due to the limited quotas of VUEs. This is why we see growing system security scores for all algorithms in Fig. 4c. Besides, since it gets easier to match secure CUEs when the number of VUEs increases, the need for sacrificing from stability to match them lessens. Thus, we also see mostly increasing user happiness scores for all algorithms in Fig. 4b.

Fig. 5 demonstrates the performance comparison of the algorithms with varying values of q_{max}, β, and R. We first note that regardless of the changes in the values of these parameters, our algorithm continuously achieves almost optimal matching utility and outperforms the Gale-Shapley and MS algorithms. In Fig. 5a & 5b, we see that the matching utility scores of all algorithms mostly get higher with increasing q_{max} and β values, respectively, because in both cases the number of matched secure CUEs increases. On the other hand, Fig. 5c shows that the D2D communication range does not have a clear-cut impact on the matching utility scores of the algorithms.

Finally, in Fig. 6, we present the running times of the algorithms with different n and m values on an Intel core i7 processor that has 16 GB memory and 2.5 GHz speed. It should be noted that although the proposed algorithm produces matchings that are only marginally less efficient than the optimal matchings found via ILP as can be seen in Fig. 3, 4, & 5, its running time is about 5 orders of magnitude shorter than the running time of the ILP solution. Besides, in terms of running time, our algorithm also outperforms the Gale-Shapley algorithm, yet it is slightly outperformed by the MS algorithm. A remarkable point in Fig. 6a is decreasing running times of our algorithm and the MS algorithm despite the growing problem size. This is due to the fact that both algorithms prioritize matching secure CUEs, hence when there are a larger number of secure CUEs in the system, the limited quotas of the VUEs will be filled quicker.

VI. Conclusion

We study the utilization of D2D based V2X communication considering several objectives simultaneously. That is, for resilience we allow D2D communicating vehicle pairs (i.e., VUEs) to reuse multiple cellular resources (i.e., channels of cellular users (CUEs)); for fairness and stable assignment, we consider the preferences of each VUE and CUE based on the data rates they can achieve in potential assignments; and for security, we adopt a system level objective that prioritizes matching the secure CUEs over insecure ones. We develop a heuristic based algorithm to achieve the most secure assignment with minimum instability between CUEs and VUEs. Through simulations, we show that the proposed algorithm achieves almost the same matching quality as the optimal ILP solution which has a significantly longer running time. Moreover, we show that the proposed algorithm significantly outperforms the other matching algorithms which fail to consider the aforementioned objectives jointly in terms of most of the performance metrics considered.

Acknowledgement

This material is supported in part by Idaho National Labs (INL) under contract #236228.

References

[1] S. A. Kazmi, N. H. Tran, W. Saad, Z. Han, T. M. Ho, T. Z. Oo, and C. S. Hong, "Mode selection and resource allocation in device-to-device communications: A matching game approach," *IEEE Transactions on Mobile Computing*, vol. 16, no. 11, pp. 3126–3141, 2017.

[2] G. Araniti, A. Raschellà, A. Orsino, L. Militano, and M. Condoluci, "Device-to-device communications over 5g systems: Standardization, challenges and open issues," in *5G mobile communications*. Springer, 2017, pp. 337–360.

[3] W. Sun, D. Yuan, E. G. Ström, and F. Brännström, "Cluster-based radio resource management for d2d-supported safety-critical v2x communications," *IEEE Transactions on Wireless Communications*, vol. 15, no. 4, pp. 2756–2769, 2015.

[4] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of DSRC and cellular network technologies for V2X communications: A survey," *IEEE Trans. on Vehicular Tech.*, vol. 65, no. 12, pp. 9457–9470, 2016.

[5] L. Liang, J. Kim, S. C. Jha, K. Sivanesan, and G. Y. Li, "Spectrum and power allocation for vehicular communications with delayed CSI feedback," *IEEE Wireless Communications Letters*, vol. 6, no. 4, pp. 458–461, 2017.

[6] L. Liang, H. Peng, G. Y. Li, and X. Shen, "Vehicular communications: A physical layer perspective," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 10 647–10 659, 2017.

[7] H. Peng, L. Liang, X. Shen, and G. Y. Li, "Vehicular communications: A network layer perspective," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1064–1078, 2018.

[8] 3GPP, "Third generation partnership project (3gpp), technical specification group radio access network, study on lte-based v2x services v0.5.0, release 14," Sophia Antipolis, France, Feb 2016.

[9] D. Feng, L. Lu, Y. Yuan-Wu, G. Y. Li, G. Feng, and S. Li, "Device-to-device communications underlaying cellular networks," *IEEE Transactions on communications*, vol. 61, no. 8, pp. 3541–3551, 2013.

[10] J. Hu, W. Heng, X. Li, and J. Wu, "Energy-efficient resource reuse scheme for d2d communications underlaying cellular networks," *IEEE Communications Letters*, vol. 21, no. 9, pp. 2097–2100, 2017.

[11] S. Cicalo and V. Tralli, "Qos-aware admission control and resource allocation for d2d communications underlaying cellular networks," *IEEE Trans. on Wireless Communications*, vol. 17, no. 8, pp. 5256–5269, 2018.

[12] F. Yucel and E. Bulut, "User satisfaction aware maximum utility task assignment in mobile crowdsensing," *Computer Networks*, vol. 172, p. 107156, 2020.

[13] E. Bulut and B. K. Szymanski, "Exploiting friendship relations for efficient routing in mobile social networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 12, pp. 2254–2265, 2012.

[14] G. Deepak, A. Ladas, Y. A. Sambo, H. Pervaiz, C. Politis, and M. A. Imran, "An overview of post-disaster emergency communication systems in the future networks," *IEEE Wireless Communications*, vol. 26, no. 6, pp. 132–139, 2019.

[15] G. Fodor, S. Parkvall, S. Sorrentino, P. Wallentin, Q. Lu, and N. Brahmi, "Device-to-device communications for national security and public safety," *IEEE Access*, vol. 2, pp. 1510–1520, 2014.

[16] K. Koumidis, P. Kolios, C. Panayiotou, and G. Ellinas, "Resilient device-to-device communication in emergency situations," in *18th Mediterranean Electrotechnical Conf.(MELECON)*. IEEE, 2016, pp. 1–7.

[17] D. Gale and L. S. Shapley, "College admissions and the stability of marriage," *The American Mathematical Monthly*, vol. 69, no. 1, pp. 9–15, 1962.

[18] F. Yucel, M. Yuksel, and E. Bulut, "Qos-based budget constrained stable task assignment in mobile crowdsensing," *IEEE Transactions on Mobile Computing*, 2020.

[19] T. Wang, F. Liu, J. Guo, and H. Xu, "Dynamic sdn controller assignment in data center networks: Stable matching with transfers," in *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*. IEEE, 2016, pp. 1–9.

[20] 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.

[21] Y. Gu, W. Saad, M. Bennis, M. Debbah, and Z. Han, "Matching theory for future wireless networks: Fundamentals and applications," *IEEE Communications Magazine*, vol. 53, no. 5, pp. 52–59, 2015.

[22] Y. Gu, Y. Zhang, M. Pan, and Z. Han, "Matching and cheating in device to device communications underlying cellular networks," *IEEE Journal on Selected Areas in Comm.*, vol. 33, no. 10, pp. 2156–2166, 2015.

[23] T. LeAnh, N. H. Tran, W. Saad, L. B. Le, D. Niyato, T. M. Ho, and C. S. Hong, "Matching theory for distributed user association and resource allocation in cognitive femtocell networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 9, pp. 8413–8428, 2017.

[24] Z. Zhou, K. Ota, M. Dong, and C. Xu, "Energy-efficient matching for resource allocation in d2d enabled cellular networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 6, pp. 5256–5268, 2016.

[25] B. Wang, Y. Sun, H. M. Nguyen, and T. Q. Duong, "A novel socially stable matching model for secure relay selection in d2d communications," *IEEE Wireless Communications Letters*, vol. 9, no. 2, pp. 162–165, 2019.

[26] X. Li, L. Ma, Y. Xu, and R. Shankaran, "Resource allocation for D2D-based V2X communication with imperfect CSI," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3545–3558, 2020.

[27] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Mode selection and spectrum partition for d2d inband communications: A physical layer security perspective," *IEEE Transactions on Communications*, vol. 67, no. 1, pp. 623–638, 2018.

[28] R. Zhang, X. Cheng, and L. Yang, "Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 8, pp. 5651–5663, 2016.

[29] J. Wang, Y. Huang, S. Jin, R. Schober, X. You, and C. Zhao, "Resource management for device-to-device communication: A physical layer security perspective," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 946–960, 2018.

[30] Y. Liu, W. Wang, H.-H. Chen, L. Wang, N. Cheng, W. Meng, and X. Shen, "Secrecy rate maximization via radio resource allocation in cellular underlaying V2V communications," *IEEE Transactions on Vehicular Technology*, 2020.

[31] "Taxi and limousine commission (tlc) trip record data." NYC Taxi Limousine Commission, 2019. [Online]. Available: https://www1.nyc.gov/site/tlc/about/tlc-trip-record-data.page