POSTER: Privacy Preserving Distributed Matching for Device-to-Device IoT Communications

Eyuphan Bulut
Virginia Commonwealth University
Richmond, VA
ebulut@vcu.edu

İsmail Güvenç
North Carolina State University
Raleigh, NC
iguvenc@ncsu.edu

Kemal Akkaya
Florida International University
Miami, FL
kakkaya@fiu.edu

ABSTRACT

Device-to-device (D2D) communication enables machine-type devices (MTD) in Internet-of-Things (IoT) network communicate directly with each other and offload the cellular network. However, it may introduce interference as they share the same spectrum with the other devices that are directly connected to the base station. In this study, we look at the problem of assigning D2D communicating IoT pairs to the IoT devices that are directly connected to the base station such that the overall system throughput is not only maximized but also a stable matching is obtained. Different than previous work, we study many-to-one matching and propose a distributed privacy preserving stable matching process for efficient resource allocation without releasing location information.

CCS CONCEPTS

• **Security and privacy → Mobile and wireless security**; • **Networks → Mobile networks**.

KEYWORDS

Internet-of-Things (IoT), device-to-device (D2D) communication, matching theory, privacy.

ACM Reference Format:
Eyuphan Bulut, İsmail Güvenç, and Kemal Akkaya. 2019. POSTER: Privacy Preserving Distributed Matching for Device-to-Device IoT Communications. In *WiSec '19: ACM Conference on Security and Privacy in Wireless and Mobile Networks, May 15–17, 2019, Miami, FL, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3317549.3326309

1 INTRODUCTION

As the number of applications in the era of Internet of Things (IoT) has been growing, we face new challenges in the wireless communication. Since the current cellular infrastructure has been designed for mobile communication coming from human users, the different traffic characteristics of massive machine-type devices (MTD) have resulted in problems such as allocation of sufficient channel resources to these devices operating in the same spectrum.

Adoption of Device-to-device (D2D) communication among IoT devices has been considered as a potential solution for scalable cellular communication infrastructure for massive IoT networks [1]. This enables autonomous communication opportunity between devices without having a centralized controller. It brings several advantages including offloading of the network, and improving the energy efficiency and system throughput. Based on the traffic characteristics of nearby IoT devices, an efficient pairing could be achieved (e.g., considering their mutual communication needs) [3]. On the other hand, as IoT devices communicating through D2D communication will use the same spectrum with IoT devices that are directly communicating with base station, an interference issue will emerge, potentially degrading the expected performance. In the literature, several solutions based on power management [8], multiple-input multiple- output (MIMO) techniques [9] and matching theory [10] have been offered but these mostly study a one time setting of D2D network topology, and under the same network management authority. However, to provide a scalable D2D network architecture among IoT devices, devices from different owners as well as dynamic changes in the network have to be considered. This then requires continuous and autonomous matching of D2D communicating IoT device pairs with directly connected IoT devices that use the same spectrum with them in a privacy preserving manner as shown in Fig. 1.

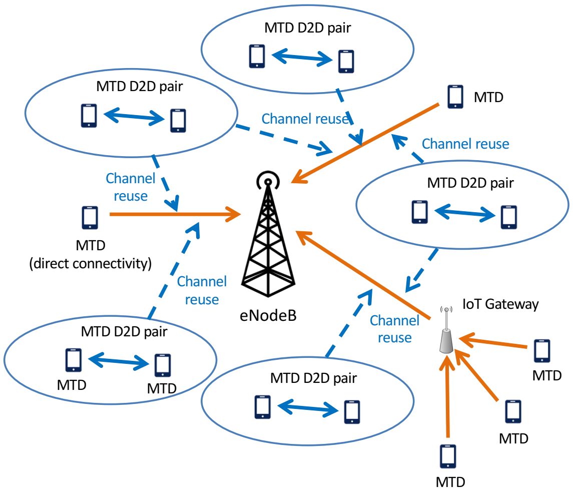

Figure 1: Device-to-device communicating IoT device pairs and IoT devices with direct cellular connectivity.

Contributions. This paper presents our ongoing effort to integrate device-to-device communication among IoT devices. Our goal is to develop a scalable system architecture by matching the device-to-device communicating IoT device pairs with the directly communicating IoT devices in the most efficient (with minimum interference) while also preserving their location privacy.

WiSec '19, May 15–17, 2019, Miami, FL, USA
© 2019 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-6726-4/19/05.
https://doi.org/10.1145/3317549.3326309

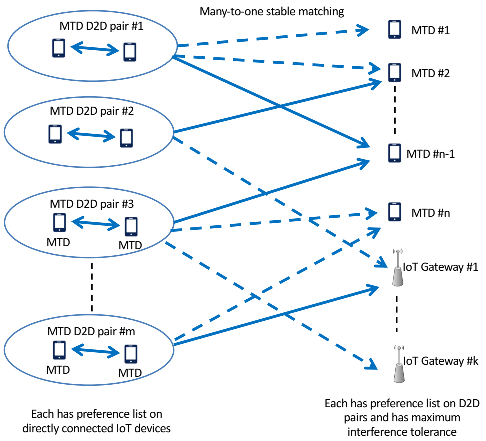
Many-to-one stable matching
MTD D2D pair #1
MTD D2D pair #2
MTD D2D pair #3
MTD
MTD
MTD D2D pair #m
MTD
MTD
MTD #1
MTD #2
MTD #n-1
MTD #n
IoT Gateway #1
IoT Gateway #k
Each has preference list on directly connected IoT devices
Each has preference list on D2D pairs and has maximum interference tolerance

Figure 2: Many-to-one matching between D2D IoT device pairs and directly connected IoT devices and gateways.

2 PROPOSED APPROACH

The resource allocation problem between D2D IoT pairs and directly connected IoT devices could be modeled using a weighted bipartite graph and solved by Kuhn-Munkers algorithm [5]. However, a more stable solution considering individual preferences of both sides can be achieved via stable matching based solutions [7]. Such a system can benefit both the directly connected IoT devices who own the resources and the D2D communicating IoT device pairs. In [7], a one-to-one matching has been studied among cellular users and D2D pairs. However, especially in IoT domain, it is possible to provide a many-to-one matching in which multiple D2D IoT device pairs are matched with the same resource owner (directly communicating IoT device) without hurting their performance.

2.1 Preference List Formation

We follow a similar approach as in [7] to determine the potential edges in the bipartite graph between a D2D pair, d and a directly connected IoT device, c. If both c and d's transmission powers can be adjusted to satisfy the minimum SINR requirement and maximum interference tolerated, an assignment between them is considered possible. However, different than [7], we propose a many-to-one matching as shown in Fig.2. To this end, we define an interference tolerance level for each node in the bipartite graph. That is direct IoT devices form a preference list of D2D pairs in the increasing order of interference they cause to it. The direct IoT device can be matched with as many D2D pairs as possible as long as their total interference is less than the tolerance of the direct IoT device.

Let W_i denote the bandwidth allocated to i^{th} directly connected IoT device and let Γ_i^c and Γ_j^d denote the SINR of c_i and d_j, respectively. The throughput of c_i over d_j is defined as $W_i log(1 + \Gamma_i^c)$ and the throughput of d_j over c_i is defined as $W_i log(1 + \Gamma_j^d)$. Then, if $W_i log(1 + \Gamma_j^d) > W_i log(1 + \Gamma_{j'}^d)$, c_i prefers d_j to $d_{j'}$. A similar preference list is also formed by D2D pairs on the directly connected IoT devices. Here, as SINR calculations need distance information between the users, we propose to use an homomorphic encryption based distance calculation without providing actual location information [11].

2.2 Distributed Privacy Preserving Many-to-One Matching

Once the preference lists of each node in the bipartite graph is formed, we follow the deferred acceptance mechanism proposed by Gale-Shapley [6] for matching. However, this can not be applied directly to many-to-one matching. In [4] a many-to-one stable matching is proposed between tasks and workers in a crowdsourcing system within task budgets. We plan to adjust this approach to our model here utilizing the maximum tolerable interference as the budget of the resource of the directly connected IoT devices. However, the algorithm has to be updated to be able to run in a distributed privacy preserving manner, without causing nodes release their preference lists. To this end, we will use distributed implementation of classical deferred acceptance mechanism [2], but we will adjust it to many-to-one matching. This will require a multi-step communication period until matching coverges, thus we are currently looking at solutions to speed up this process.

3 CONCLUSION

In this paper, we provide the details of our initial design on integrating device-to-device communication among the devices in an IoT network. Our goal is to achieve a distributed many-to-one matching among D2D IoT pairs and direct IoT devices without releasing their location information benefiting from homomorphic encryption based distance calculation.

4 ACKNOWLEDGMENTS

This work was supported in part by National Science Foundation awards CNS-1815603, CNS-1814727.

REFERENCES

[1] Oladayo Bello and Sherali Zeadally. 2016. Intelligent device-to-device communication in the internet of things. *IEEE Systems Journal* 10, 3 (2016), 1172–1182.

[2] Ismel Brito and Pedro Meseguer. 2005. Distributed stable matching problems. In *CP*. Springer, 152–166.

[3] Eyuphan Bulut and Ismail Güvenç. 2018. Dynamically Shared Wide-Area Cellular Communication for Hyper-dense IoT Devices. In *2018 IEEE 43rd Conference on Local Computer Networks Workshops (LCN Workshops)*. IEEE, 64–69.

[4] Yanjiao Chen and Xiaoyan Yin. 2017. Stable Job Assignment for Crowdsourcing. In *GLOBECOM 2017-2017 IEEE Global Communications Conference*. IEEE, 1–6.

[5] Daquan Feng, Lu Lu, Yi Yuan-Wu, Geoffrey Ye Li, Gang Feng, and Shaoqian Li. 2013. Device-to-device communications underlaying cellular networks. *IEEE Transactions on Communications* 61, 8 (2013), 3541–3551.

[6] D Gale and L Shapley. 1962. College Admissions and Stability of Marriage. American Mathematicas Monthly, 69, 9-15.

[7] Yunan Gu, Yanru Zhang, Miao Pan, and Zhu Han. 2015. Matching and cheating in device to device communications underlying cellular networks. *IEEE Journal on Selected Areas in Communications* 33, 10 (2015), 2156–2166.

[8] Yanxiang Jiang, Qiang Liu, Fuchun Zheng, Xiqi Gao, and Xiaohu You. 2016. Energy-efficient joint resource allocation and power control for D2D communications. *IEEE Transactions on Vehicular Technology* 65, 8 (2016), 6119–6127.

[9] Xingqin Lin, Robert W Heath, and Jeffrey G Andrews. 2015. The interplay between massive MIMO and underlaid D2D networking. *IEEE Transactions on Wireless Communications* 14, 6 (2015), 3337–3351.

[10] Lingyang Song, Dusit Niyato, Zhu Han, and Ekram Hossain. 2014. Game-theoretic resource allocation methods for device-to-device communication. *IEEE Wireless Communications* 21, 3 (2014), 136–144.

[11] Fatih Yucel, Kemal Akkaya, and Eyuphan Bulut. 2018. Efficient and Privacy Preserving Supplier Matching for Electric Vehicle Charging. *Ad Hoc Networks* (2018).