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.

CSC 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:


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 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].

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

WSec ’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

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.
We follow a similar approach as in [7] to determine the potential resource allocation problem between D2D IoT pairs and directly connected IoT devices. Here, as SINR calculations need distance information, we are currently looking at solutions to speed up this process.

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-Munkres 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 \( \Gamma^c_i \) and \( \Gamma^d_j \) denote the SINR of \( c_i \) and \( d_j \), respectively. The throughput of \( c_i \) over \( d_j \) is defined as \( W_i \log (1 + \Gamma^c_i) \) and the throughput of \( d_j \) over \( c_i \) is defined as \( W_i \log (1 + \Gamma^d_j). \) Then, if \( W_i \log (1 + \Gamma^c_i) > W_i \log (1 + \Gamma^d_j) \), \( c_i \) prefers \( d_j \) to \( d_j \). A similar preference list is also formed by D2D pairs on the directly connected IoT device and let \( \Gamma^d_i \) denote the bandwidth allocated to \( i^{th} \) directly connected IoT device and let \( \Gamma^d_i \) denote the SINR of \( d_i \) and \( d_j \), respectively. The throughput of \( d_i \) over \( d_j \) is defined as \( W_i \log (1 + \Gamma^d_i) \) and the throughput of \( d_j \) over \( d_i \) is defined as \( W_i \log (1 + \Gamma^d_j). \) Then, if \( W_i \log (1 + \Gamma^d_i) > W_i \log (1 + \Gamma^d_j), c_i \) 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 converges, 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-1815665, CNS-1814727.

REFERENCES