

Thesis Evaluation Report

“Stable-matching Based Resource Allocation Methods In Wireless Communication Systems”

Yağmur Sabucu

Thesis committee:

Assoc. Prof. Ali Emre Pusane (Supervisor)

Assoc. Prof. Güneş Karabulut Kurt (Co-Supervisor)
(Istanbul Technical University)

Prof. Tuna Tuğcu

Assoc. Prof. Serhat Erküçük (Kadir Has University)

Assist. Prof. Eylem Erdoğan (Medeniyet University)

Assist. Prof. Sema Dumanlı Otkar

Yağmur Sabucu's Ph.D. dissertation titled "Stable-matching Based Resource Allocation Methods In Wireless Communication Systems" consists of a total of 5 chapters (including introduction and conclusion).

The main focus of this research is to develop stable matching (SM) based resource allocation approaches (namely partial feedback stable matching algorithm) in order to meet the requirements of the wireless communication systems, such as stability, fairness, high data rates, low computational complexity, and robustness against attackers.

The first chapter mainly reviews the basics and preliminaries of the SM. Chapter 2 focuses on decreasing the overload on the feedback channel and provide individual stability by using the variations of SM algorithm, and to this end, first partial feedback matching algorithm is detailed, and later their performance efficiency is proven by comparing with the existing algorithms. The proposed variations of SM algorithms are very robust even with partial channel state information (CSI) in terms of rate and fairness. Furthermore, the stability concerns for CA HetNets are reviewed and discussed. for the proposed variation of the SM algorithm in order to determine the rate satisfaction of both user equipments and the entire HetNet.

The third chapter presents the trust-based SM approach is proposed as a solution for selfish user threats in a carrier aggregated heterogeneous networks. The proposed approach aims to provide secure communication to honest users by using a trust index to identify and punish the selfish users gradually. The selfish user identification process in the proposed approach is based on a comparison between the difference of the promised rate and the obtained rate with a predefined threshold after each stable matching round. The identification threshold has a significant role in terms of avoiding false detection of honest users as selfish users as a result of bad channel estimation performances. Additionally, determining an appropriate punishment factor is another essential issue in order to achieve high rate and fairness performances. Thus, appropriate values of the threshold and the punishment factor are investigated in order to achieve a high fairness and low misleading ratio.

In Chapter 4, novel two-fold reputation based attacker identification approach is proposed as a robust solution against selfish Internet of things mobile devices in the network. Threshold is optimized for the first identification process. The optimized threshold is used in the SM based identification process. The performance efficiency is corroborated via extensive computer simulations. In the second fold, IoT devices are examined according to their reputation indexes. Final attacker identifications determines the states of the IoT devices. Three-state identification process is very important in order to give a chance to the unintentional attackers, who suffered from the channel estimation error. Finally, Chapter 5 concludes the dissertation.

The main contributions of this work can be divided into four categories:

- The overload on the uplink channel, through CSI transmission, is decreased significantly by the proposed PFM algorithm by also providing high data rates
- Stability performances of the proposed algorithm, PFM, and the user satisfaction analyses are investigated for various amounts of partial feedback CSI transmission. Stability concerns for CA HetNets are discussed for the proposed PFM algorithm in order to determine the rate satisfaction of both user equipment and the entire HetNet. Individual rate dissatisfaction of UEs and network instability results are obtained.
- As a more realistic approach, impact of channel estimation errors on feedback channels are considered by using many-to-one SM and PFM approaches for full CSI and reduced feedback CSI scenarios.
- Novel SM based approaches are proposed in order to detect selfish users in the wireless communication networks such as carrier aggregation heterogeneous networks and mobile edge computing Internet of things networks. A two-fold reputation based attacker identification and punishment policy, is proposed in order to increase the robustness of the network. Threshold, used for attacker identification, is optimized for a fixed probability of false alarm. The analytical results are supported via extensive computer simulations.

List of corresponding publications

- Journal articles

1. Y. Sabucu and A. E. Pusane, G. K. Kurt, “Robust matching algorithms for carrier aggregated heterogeneous networks”, *Physical Communication*, Vol. 33, pp. 123–134, January 2019.
2. Y. Sabucu and A. E. Pusane, G. K. Kurt, F. Benedetto, “Reputation based attacker identification in mobile edge computing in Internet of Things by using stable matching algorithm”, *In progress*, June 2019.

- International conference papers

1. Y. Sabucu, A.E. Pusane, G.K. Kurt, “Trust-Based Stable Matching Approach for Carrier Aggregated Heterogeneous Networks”, 2018 41st International Conference on Telecommunications and Signal Processing, TSP 2018, 2018.

- National conference papers

1. Y. Sabucu, A. E. Pusane and G. Karabulut Kurt, “Applications of stable matching algorithm in wireless communication systems,” 2015 23rd Signal Processing and Communications Applications Conference (SIU), Malatya, 2015, pp. 1509-1512.

- Poster presentations

1. Y. Sabucu, A.E. Pusane, G. Karabulut Kurt, Resource Allocation Using Stable Matching over Channels with Nonideal CSI, European School of Information Theory (ESIT), Gothenburg, Sweden, April 48, 2016 .
2. Y. Sabucu, A.E. Pusane, G. Karabulut Kurt, Robust Extended Matching Algorithm for Multicarrier Communications, European School of Information Theory (ESIT), Zandvoort, The Netherlands, 20-24 April, 2015.