

STABLE-MATCHING BASED RESOURCE ALLOCATION METHODS IN  
WIRELESS COMMUNICATION SYSTEMS

by

Yağmur Sabucu Sandal

Ph.D., Electrical and Electronics Engineering, Boğaziçi University, 2019

Submitted to the Institute for Graduate Studies in  
Science and Engineering in partial fulfillment of  
the requirements for the degree of  
Doctor of Philosophy

Graduate Program in Electrical and Electronics Engineering  
Boğaziçi University

2019

STABLE-MATCHING BASED RESOURCE ALLOCATION METHODS IN  
WIRELESS COMMUNICATION SYSTEMS

APPROVED BY:

Assoc. Prof. Ali Emre Pusane (Thesis Supervisor)	.....
Prof. Gunes Karabulut Kurt (ITU) (Thesis Co-supervisor)	.....
Prof. Tuna Tugcu	.....
Assoc. Prof. Serhat Erkucuk (Kadir Has University)	.....
Assist. Prof. Eylem Erdogan (Medeniyet University)	.....
Assist. Prof. Sema Dumanli Oktar	.....

DATE OF APPROVAL: 19.08.2019

## ACKNOWLEDGEMENTS

Firstly, I would like to express my sincere gratitude to my advisors Assoc. Prof. Ali Emre Pusane and Prof. Gunes Karabulut Kurt for their continuous support, patience, and motivation from the first day of my Ph.D. education to the end of my Ph.D. thesis. Their valuable guidance and positive criticism were invaluable for me throughout my Ph.D. study.

Besides my advisors, I would like to thank the rest of my thesis committee: Assoc. Prof. Serhat Erkucuk and Prof. Tuna Tugcu for their insightful comments and suggestions, which incited me to widen my research from various perspectives. My special thanks for Assoc. Prof. Serhat Erkucuk, who was also my M.Sc. advisor, for his support and encouragement during my graduate studies. Additionally, I am very grateful to have an opportunity to collaborate with Dr. Francesco Benedetto, who kindly helped me through my research.

I thank my fellows in Istanbul Technical University for their continuous moral support. During these 6 years, we had many precious memories together.

I am deeply thankful to my mother, Gulay Sabucu, my father Harun Sabucu, and my brother H. Abdul Sabucu, for their love, support, and sacrifices. Without them, this thesis would never have been written. Last but not the least, I would like to thank my lovely husband Unal Sandal, for his endless love, patience and support during my Ph.D. studies.

I would like to also acknowledge The Scientific and Technological Research Council of Turkey (TUBITAK) for financial support during the Ph.D. study through the direct National Scholarship Program (2211E).

## ABSTRACT

# STABLE-MATCHING BASED RESOURCE ALLOCATION METHODS IN WIRELESS COMMUNICATION SYSTEMS

As the number of smart devices increases day by day, the need for new resource allocation techniques also increases. 5G technologies such as Long-Term Evolution Advanced (LTE-A), carrier aggregated heterogeneous networks (HetNets), or Internet of things (IoT) networks with mobile edge computing (MEC) features require high data rates and ultra low latency with the restricted resources. Resource allocation and secure communication are two of the most important challenges in wireless communication. Graph-based algorithms are proposed in order to achieve resource allocation with a low computational complexity. The primary objective of this thesis is to address the resource allocation challenges, e.g., fairness and stability, by using stable matching (SM)-based approaches. SM algorithm requires channel state information (CSI) before starting allocation. However, CSI transmission may cause an overload of the up-link channel. The problem is extensively elaborated in many aspects for different wireless communication systems such as HetNets and IoT networks. The overload on the uplink channel, through CSI transmission, is decreased significantly by the proposed partial feedback matching (PFM) algorithm. Finally, IoT networks are very fragile against attackers in physical layer as the number of connected smart devices increases. A three state SM-based attacker identification and punishment policy, is proposed in order to increase the robustness of the network. Both analytical and simulation results are presented to demonstrate that the proposed SM-based approaches have better performance than the algorithms that exist in the literature.

## ÖZET

### KABLOSUZ HABERLEŞME SİSTEMLERİNDE KARARLI EŞLEME ALGORİTMASI İLE KAYNAK DAĞITIMI

Kablosuz haberleşme ağlarında etkin olan akıllı mobil cihazların sayılarının her geçen gün artması, kısıtlı kaynakların dağıtım için yeni yaklaşımları gerektirmiştir. İleri düzeyde uzun süreli evrim (LTE-A), taşıyıcı birleştirmeli (CA) heterojen ağlar (HetNet) ya da nesnelerin Interneti (IoT) ve mobil sınır hesaplama (MEC) gibi 5G sistemlerde kullanılması beklenen teknolojiler, yüksek hızlar ve çok düşük gecikmeleri gerektirirler. Kaynak dağıtımı ve güvenli iletişim konuları, bu teknolojiler için araştırılması gereken en önemli sorunlar arasında yer almaktadır. Graf tabanlı algoritmalar bu tarz işlemler için düşük karmaşıklığından çok tercih edilmektedir. Bu tezin asıl amacı, graf tabanlı kararlı eşleme (SM) algoritması kullanarak olabildiğince adil ve kararlı bir şekilde kısıtlı kaynakların dağıtımını sağlamaktır. Kararlı eşleme algoritması kaynak dağıtımına başlamadan önce kanal durum bilgisine (CSI) ihtiyaç duymaktadır. Bu kanal durum bilgileri ne yazık ki kanalda aşırı yüklenmeye sebep olabilir. Bu sebeple kısmi geri bildirim algoritması (PFM) önerilmiştir. PFM ile sadece çok az miktarda kanal bilgisi ile bile tam sayıda kanal bilgisine yakın sonuçlar elde edilmiştir. Kablosuz haberleşme sistemlerindeki bir başka önemli zorluk ise fiziksel katman güvenliğidir. Kablosuz ağlar yapıları gereği bir çok saldırıya maruz kalabilirler. Ağa bağlı akıllı mobil cihaz sayısı arttıkça güvenlik zafiyeti de büyümeye başlar. Bu probleme çözüm olarak da yine SM tabanlı saldırgan tespit etme ve cezalandırma yaklaşımı sunulmuştur. Teorik ve nümerik sonuçlar, SM tabanlı yaklaşımların performanslarının literatürde varolan yaklaşımlardan daha iyi sonuç verdiğini ispatlamıştır.

## TABLE OF CONTENTS

ACKNOWLEDGEMENTS . . . . .	iii
ABSTRACT . . . . .	iv
ÖZET . . . . .	v
LIST OF FIGURES . . . . .	viii
LIST OF TABLES . . . . .	xii
LIST OF SYMBOLS . . . . .	xiii
LIST OF ACRONYMS/ABBREVIATIONS . . . . .	xvii
1. INTRODUCTION . . . . .	1
1.1. Motivations . . . . .	2
1.2. Contributions . . . . .	2
1.3. Related works . . . . .	3
1.3.1. Carrier Aggregation in Heterogeneous Networks . . . . .	4
1.3.2. Secure communication in Carrier Aggregated Heterogeneous Net- works . . . . .	6
1.3.3. Mobile edge computing in Internet of Things . . . . .	8
1.4. Stable Matching Algorithm . . . . .	10
1.5. Carrier Aggregation in Heterogeneous Networks . . . . .	18
1.6. Mobile edge computing in Internet of things . . . . .	22
2. APPLICATION OF STABLE MATCHING ALGORITHM IN CARRIER AG- GREGATED HETEROGENEOUS NETWORKS . . . . .	27
2.1. Motivation . . . . .	27
2.2. System Model . . . . .	27
2.3. Variations of the stable matching based carrier aggregated resource al- location approach . . . . .	34
2.3.1. Many-to-one Stable Matching Based Carrier Aggregation . . . . .	34
2.3.2. Partial Feedback Matching based Carrier Aggregation . . . . .	36
2.4. Stability Analysis of PFM . . . . .	39
2.5. Robustness of PFM Against Channel Estimation Error . . . . .	44
2.6. Simulation results . . . . .	46

2.7. Conclusions . . . . .	54
3. SECURE STABLE MATCHING ALGORITHM IN CARRIER AGGREGATED HETEROGENEOUS NETWORKS . . . . .	56
3.1. Motivation . . . . .	56
3.2. System Model for a Secure Scenario . . . . .	56
3.2.1. Selfish User Model . . . . .	58
3.3. Trust-Based Stable Matching Approach . . . . .	59
3.4. Simulation results . . . . .	60
3.5. Conclusions . . . . .	64
4. REPUTATION-BASED ATTACKER IDENTIFICATION POLICY FOR MO- BILE EDGE COMPUTING IN INTERNET OF THINGS BY USING STABLE MATCHING ALGORITHM . . . . .	65
4.1. Motivation . . . . .	65
4.2. System Model . . . . .	66
4.2.1. Attacker Model . . . . .	67
4.3. Reputation-based Attacker Identification Policy . . . . .	68
4.3.1. SM based local attacker identification . . . . .	69
4.3.2. Reputation based identification . . . . .	72
4.3.3. Threshold analysis for identification . . . . .	73
4.4. Performance evaluation . . . . .	74
4.5. Numerical Results . . . . .	78
4.6. Conclusions . . . . .	81
5. CONCLUSION . . . . .	82
6. Future Works . . . . .	84
REFERENCES . . . . .	85

## LIST OF FIGURES

Figure 1.1.	Stable Matching Algorithm . . . . .	11
Figure 1.2.	Algorithm 1: Stable Matching Algorithm . . . . .	12
Figure 1.3.	Rogue couple illustration . . . . .	17
Figure 1.4.	General Carrier Aggregated Heterogeneous Networks . . . . .	19
Figure 1.5.	Comparison of conventional network with LTE-Advanced network, which aggregates one 20 MHz CC and two 10 MHz CCs. . . . .	20
Figure 1.6.	Carrier aggregation deployments: (a) Intraband contiguous, (b) intraband noncontiguous, and (c) interband noncontiguous . . . .	21
Figure 1.7.	Different types of services supplied from IoT network suppliers . .	23
Figure 1.8.	Cloud, Fog, and edge structures in a network. . . . .	25
Figure 2.1.	System model of carrier aggregated HetNet. Carrier aggregation enabled LTE-A users (green) are positioned in the concurrent area of SBSs and MBS while the other users (gray) are placed out of this concurrent area. . . . .	28
Figure 2.2.	Algorithm 2: Many-to-one Stable Matching Algorithm . . . . .	32
Figure 2.3.	Algorithm 3: Partial Feedback Matching Algorithm . . . . .	40



Figure 2.4.	Fairness comparisons of PFM algorithm and ORA (a) for $K=32$ UEs and $N=\{256, 512, 1024, 2048\}$ subcarriers. . . . .	47
Figure 2.5.	Fairness performances are illustrated for various number of UEs. .	48
Figure 2.6.	Rate comparison of PFM, PF, ORA for $K = 32$ UEs and $N = \{256, 512, 1024, 2048\}$ subcarriers. . . . .	48
Figure 2.7.	Rate performance of $(2/N)$ –partial CSI feedback for $K = 32$ UEs $N = 2048$ subcarriers. . . . .	49
Figure 2.8.	Fairness performance of $(2/N)$ –partial CSI feedback for $K = 32$ UEs $N = 2048$ subcarriers. . . . .	49
Figure 2.9.	Feedback gain is shown when various number of subcarrier feedbacks with $f/N$ –PFM algorithm for a CA HetNet of $K = 32$ UEs and $N = 2048$ subcarriers. . . . .	50
Figure 2.10.	Rate performances is shown when various number of subcarrier feedbacks with $f/N$ –PFM algorithm for a CA HetNet of $K = 32$ UEs and $N = 2048$ subcarriers. . . . .	51
Figure 2.11.	Rate performances with $K = 32$ UEs and $N = \{256, 512, 1024, 2048\}$ subcarriers for different $\sigma_\epsilon^2$ . . . . .	51
Figure 2.12.	Fairness performances with $K = 32$ UEs and $N = \{256, 512, 1024, 2048\}$ subcarriers for different $\sigma_\epsilon^2$ . . . . .	52
Figure 2.13.	Rate performances with $K = 32$ UEs and $N = 2048$ subcarriers for $\sigma_\epsilon^2 = 0.5$ . . . . .	53

Figure 2.14.	The average user dissatisfaction results for 32 UEs and various subcarriers considering different amount of partial feedback CSI. . . .	53
Figure 2.15.	Rate (a) and Network instability (b) results for 32 UEs and various subcarriers considering different amount of partial subcarrier feedbacks. . . . .	54
Figure 3.1.	$K$ users, including $L$ selfish users, are uniformly distributed in the coverage area $([-50, 50] \text{ m})$ , where LTE SBS and MBS are placed at the center $[0.0]$ . . . . .	57
Figure 3.2.	False detection performance for different misleading ratio thresholds when the punishment factor is 0.7. . . . .	61
Figure 3.3.	The rate of selfish users with misleading ratio threshold $\xi = 0.1$ for different punishment factors $\tau^p \in \{0.1, 0.3, 0.5, 0.7, 1\}$ for 32 users and 2048 subcarriers exist in total. . . . .	62
Figure 3.4.	The rate of selfish users with misleading ratio threshold $\xi = 0.7$ for different punishment factors $\tau^p \in \{0.1, 0.3, 0.5, 0.7, 1\}$ for 32 users and 2048 subcarriers exist in total. . . . .	62
Figure 3.5.	The misleading ratio performances are illustrated with misleading ratio threshold $\xi = 0.7$ for different punishment factors $\tau^p \in \{0.1, 0.3, 0.5, 0.7, 1\}$ for 32 users and 2048 subcarriers exist in total. . . . .	63
Figure 3.6.	Fairness performances are illustrated with misleading ratio threshold $\xi = 0.7$ for different punishment factors $\tau^p \in \{0.1, 0.3, 0.5, 0.7, 1\}$ for 32 users and 2048 subcarriers exist in total. . . . .	63

Figure 4.1.	$K$ IoT devices, including $K^m$ malicious IoT devices, are uniformly distributed in the concurrent area of two APs with edge servers. . . . .	66
Figure 4.2.	PDF of the decision variables under different conditions. . . . .	72
Figure 4.3.	Theoretical and simulation results of $P_D$ for different $PFA$ assumptions and misleading factors $\phi$ . . . . .	79
Figure 4.4.	The state transitions when the misleading factor is $\phi = 1.1$ (a) Honest users (b) Selfish users . . . . .	80
Figure 4.5.	The average number of IoT devices at each state are shown after $W$ allocation time for different probability of attackers, (a) $p = 0.1$ , (b) $p = 0.5$ , and (c) $p = 0.9$ . . . . .	80

LIST OF TABLES

Table 1.1. Man and Woman IDs in SM Algorithm . . . . . 13

Table 1.2. Stable Matchings . . . . . 15

Table 1.3. Random Matchings . . . . . 16

## LIST OF SYMBOLS

$Q_k$	Quota
$\rho_x$	The number of received proposal of woman $x$
$U_{n'}$	The man, who is matched with the woman $n'$ temporarily.
$X^{man,t}$	Proposal list of men at step $t$
$\alpha_k^{man}$	Proposal rank of the $k^{\text{th}}$ man
$\succ_k^{man}$	The preference list of the $k^{\text{th}}$ man
$\succ_n^{woman}$	The preference list of the $n^{\text{th}}$ woman
$\rho_x$	Number of proposals to $x$
$U_{n'}$	Temporary partner
$\mu_{(k,n)}$	Matching index
$\mathcal{M}$	Matching matrix
$\mathbf{K}$	User equipment
$\mathcal{N}$	The set of subcarriers
$N_c$	The number of subcarriers of each CC
$R$	Total rate of such a CA
$r_k(n)$	The marginal rate of the $k^{\text{th}}$ UE and the $n^{\text{th}}$ subcarrier
$W_b$	Bandwidth
$c_k(n)$	SNR of the $k^{\text{th}}$ UE and the $n^{\text{th}}$ subcarrier
$\sigma_k^2(n)$	The variance of the complex additive white Gaussian noise (AWGN)
$P_{k,n}$	The power of the channel gains
$P_n$	The transmit power of subcarriers
$\phi_k^T$	Rate proportionality
$\mathcal{O}(\cdot)$	Complexity operator
$(f/N)\text{--PFM}$	PFM with top- $f$ CSI feedback
$G_f$	The total feedback gain of the system
$\arg \min_k x$	Argument function, which minimizes $x$
$S_q^k$	ID of the assigned subcarrier to the $k^{\text{th}}$ UE
$\text{rank}(x, \succ_y)$	The rank of the value $x$ in the preference list of $y$ ( $\succ_y$ )

$PI$	Pairwise instability
$PB_{S_q^k, \hat{n}}^k$	Pairwise blocking
$BI_{S_q^k}^k$	Blocking index
$\beta_k$	Individual dissatisfaction ratio
$DI^k$	The dissatisfaction index of each UE
$D$	The average user dissatisfaction of a network
$NI$	Total network instability,
$RL^k$	Individual rate loss of each UE
$L$	The overall rate loss for the network
$\tilde{h}_{k,n}$	The estimated channel gain
$\tilde{p}_{k,n}$	The erroneous preference lists
$\epsilon_{k,n}$	The channel estimation error
$\tilde{\mathbf{H}}$	The erroneous channel matrix
$\mathbf{M}^{ORA}$	The matching matrix of ORA
$\mathbf{M}^{PFM}$	The matching matrix of PFM
$L$	Selfish users
$N_0$	The noise power
$L(x_1, x_2)$	Path loss
$\alpha$	The path loss exponent
$\beta$	Path loss at 1-meter distance
$\chi$	The deviation in fitting (in dB)
$MR$	Misleading ratio
$\tau_k^i$	Trust index
$\phi$	Predefined misleading factor
$R_k^{prom,i}$	The promised rate
$R_k^{obt,i}$	Obtained rate
$RE_k^i$	the rate error
$\tau^p$	punishment factor
$w$	The bandwidth per resource block
$\xi$	misleading threshold
$f^i(t)$	Jain's fairness index

$P_s$	fix transmit power of IoT devices
$\phi_k^i$	misleading factor
$i$	SM allocation round
H0	binary hypothesis, which states the absence of the intentional attackers
H1	binary hypothesis, which states the presence of the intentional attackers
$s^{\text{th}}$	mobile edge resource
$Z_k^i$	The decision variable of each IoT device
$P^{FA}$	Probability of false alarm
$P^D$	probability of attacker detection
$M_2$	the second-order moment of the received signal
$M_4$	the fourth-order moment of the received signal
$E[.]$	denotes the expectation operator
$ \cdot $	the absolute value
$Re(\cdot)$	the real part of the complex number.
$p$	attacking probability
$\hat{P}_{h,1,2}$	estimated test variable for $h$
$\hat{P}_{\epsilon,1,2}$	estimated test variable for $\epsilon$
$W$	number of observations with a number
$T_k$	The reputation index
$P_{M,S}^M$	probability of transition of malicious device from malicious to suspicious
$P_{S,H}^M$	probability of transition of malicious device from suspicious to honest
$P_{S,M}^M$	probability of transition of malicious device from suspicious to malicious
$P_{H,S}^M$	probability of transition of malicious device from honest to suspicious
$P_{M,S}^H$	probability of transition of honest device from malicious to suspicious
$P_{S,H}^H$	probability of transition of honest device from suspicious to honest

$P_{S,M}^H$	probability of transition of honest device from suspicious to malicious
$P_{H,S}^H$	probability of transition of honest device from honest to suspicious
$N_H^H$	number of honest users at honest state
$N_M^H$	number of honest users at malicious state
$N_H^M$	number of malicious users at honest state
$N_M^M$	number of malicious users at malicious state
$\lambda_1$	state transition threshold from malicious to suspicious
$\lambda_2$	state transition threshold from honest to suspicious
$\lambda_3$	state transition threshold from suspicious to honest
$\lambda_4$	state transition threshold from suspicious to malicious



## LIST OF ACRONYMS/ABBREVIATIONS

HetNet	Heterogeneous Network
CA	Carrier Aggregation
3GPP	The 3 <sup>rd</sup> Generation Partnership Project
LTE-A	Long Term Evolution- Advanced
QoS	Quality of Service
4G	The 4 <sup>th</sup> Generation
5G	The 5 <sup>th</sup> Generation
CSI	Channel State Information
PF	Proportional Fair
UE	User Equipment
GA	Greedy Algorithm
CC	Carrier Component
CQI	Channel Quality Indicator
RI	Rank Indicator
PMI	Pre-coding Matrix Indicator
MIMO	Multiple Input Multiple Output
AWGN	Additive White Gaussian Noise
SM	Stable Matching
ORA	Optimal Rate Algorithm
OFDM	Orthogonal Frequency Division Multiplexing
IoT	Internet of Things
DDoS	Distributed denial-of-service
MEC	Mobile edge computing
MSM	Many-to-one Stable Matching
PFM	Partial Feedback Matching
RB	Resource block
EE	Energy Efficient
GA	Greedy Algorithm

CQI	Channel Quality Indicator
D2D	Device-to-device
Wi-Fi	Wireless Fidelity
BS	Base station
ETSI	European Telecommunications Standard Institute
AP	Access Points
SMOP	Smart mobile device offloading payoff
RF	Radio Frequency
IaaS	Infrastructure as a service
SaaS	Software as a service
PaaS	Platform as a service
RAN	Radio Access Network
MBS	Macro Base Station
SBS	Small Base Station
ABS	Almost blank subframes
ICIC	Inter-Cell Interference Coordination
PF	Proportional Fair
MD	Mobile Devices

## 1. INTRODUCTION

In order to address the increasing demands for high data rates in wireless communication systems, new technologies, such as heterogeneous networks (HetNets), carrier aggregation (CA), and Internet of things (IoT), have been introduced in the last decade. HetNets include not only one type of cell (i.e., macro-cell), but also various low power nodes, such as pico-cells and femto-cells, different from the homogeneous networks. With the ability of providing transmission from various cells inside the concurrent area, long term evolution-advanced (LTE-A) nodes, which are able to use more than one carriers belonging to different cells (i.e., CA), are developed in the 3GPP specifications of Release-10 for HetNets in order to achieve the desired data rate. The significant increase on the number of smart devices opened a new era and required new technologies beyond these 4G technologies. In this new era, billions of devices connect to the Internet in a smart form according to the statistics in [1]. All the connections of this new family of smart devices are named as “Internet of things”. Thus, there is an essential need for the management of a great amount of data of IoT applications of these heterogeneous devices. Initially, cloud services are proposed to handle this huge amount of data; however, these services cannot meet the demand for low latency and high reliability for new real time applications, such as real time games, virtual reality, medical, and military services. Correspondingly, computation and storage tasks migrated towards the mobile edge, which has not only relaxed the data traffic on the cloud, but also decreased the latency significantly.

One of the common challenges in these technologies is to find an efficient resource allocation algorithm, which may adapt to different scenarios and meet different requirements. At this point, low-complexity graph-based algorithms, e.g., SM algorithms, are proposed as a popular solution to resource allocation problems [2–4]. Although SM based studies have already increased the efficiency of resource allocation in many aspects, new complex network structures, e.g., IoT networks with billion devices, force us to search for new facilities in this area.

The other significant challenge is to provide safe communication to the participants. Significant amount of connecting devices makes wireless network fragile against any threats, e.g., DDoS, confidentiality, eavesdropping, etc. In order to achieve the real potential of mobile edge computing (MEC), secure communication is crucial. Although Sun *et al.* [5] consider these significant problems together with rate efficiency and fair allocation, secure transmission is not elaborated extensively. Hence, none of the previous studies proposes joint solutions for rate efficiency, fairness, and security concerns. In this thesis, extended and adaptable versions of SM algorithm are proposed in order to solve the resource allocation problem, while it aims to guarantee secure and fair communication.

### 1.1. Motivations

The main objectives of this thesis are:

- (i) to provide an efficient resource allocation process for carrier aggregated HetNets by considering many various aspects such as fairness, stability, robustness, computational complexity, and transmission rate,
- (ii) to decrease the overload on the feedback channels, while uploading the channel state information (CSI) that is required by the algorithm before starting resource allocation ,
- (iii) to meet the various requirements from different types of users in the wireless communication networks with adaptable and flexible matching algorithm,
- (iv) to increase the robustness of networks, e.g., IoT networks, which are very fragile against possible attacks, as a natural result of HetNet structure.

### 1.2. Contributions

The main contributions of this study are:

- (i) many-to-one SM (MSM) algorithm uses the ideal CSI values (via feedback channel) in order to obtain the preference lists instead of using deterministic prefer-

ences (as in the original SM algorithm). The overload on the uplink channel, through CSI transmission, is decreased significantly by the proposed PFM algorithm. Specifically, PFM based CA uses partial feedback CSI instead of ideal full CSI for each UE in a CA HetNet.

- (ii) 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 investigated for the proposed variation of the MSM 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.
- (iii) As a more realistic approach, impact of channel estimation errors on feedback channels are considered by using MSM and PFM approaches for full CSI and reduced feedback CSI scenarios, respectively.
- (iv) Data rate and fairness performances are investigated for all proposed variations of SM algorithm, simultaneously, by considering the rate requirements of UEs with the feedback CSI.
- (v) The resource allocation problem, which is one the most significant challenges of the IoT MEC infrastructure, is addressed by applying a graph-based low complexity resource allocation policy, SM.
- (vi) Finally, IoT networks are very fragile against attackers in the physical layer as a nature of wireless communication systems. A three state reputation based attacker identification and punishment policy, is proposed in order to increase the robustness of the network.

### 1.3. Related works

Wide range of applications of the modern life have inspired growing interests in high speed wireless communications in the last decade. The main aim is to provide a robust technology with a high enough capacity to meet the increasing demand. As the homogeneous networks cannot meet the current demand for data traffic, an intelligent network strategy, HetNet, is proposed [6], as a mixed network structure including

macro-cells and low-power nodes, such as pico-cells and femto-cells [7]. The main idea behind a HetNet is to bring the network closer to the users by using multiple low-power base stations in order to decrease the cost by offloading the central macro-cells and to boost the spectral efficiency by potentially sharing the same spectrum [8,9]. In order to achieve higher data rates, CA is proposed in 3GPP LTE-A specifications of Release-10 standard [10]. Unlike the 3GPP specifications of Release-8 LTE-A standard [11], CA in Release-10 enables each user to communicate by using up to five carriers rather than one carrier. This new feature allows each user to reach a maximum bandwidth of 100 MHz [12].

CA is very useful to lessen the load on the network and maximize the energy efficiency by enabling the use of a carrier outside the traditional cellular frequency band [13]. Additional carriers per user would allow users to communicate without a loss of quality of service (QoS) even under unfavorable conditions [14,15]. However, CA in LTE still requires modification on resource allocation approaches. One of the main requirement is to achieve higher data rates while providing a pleasant QoS and/or fairness for each user in a network [16–18]. Correspondingly, the other requirement is a reliable channel information, which is obtained by channel estimation or feedback transmission for an efficient resource allocation. The channel information requirements substantially increase the complexity of the system or the overhead on the feedback channel.

### **1.3.1. Carrier Aggregation in Heterogeneous Networks**

CA approaches can be placed in three main categories as intraband contiguous, intraband non-contiguous, and interband non-contiguous CA [19]. In contiguous CA, component carriers (CCs) are adjacent to each other and belong to the same frequency band (intraband). However, in non-contiguous CA, the combined CCs can belong to the same frequency band with a frequency gap (or multiple frequency gaps) or they can belong to different frequency bands (interbands). CA in LTE still requires modification on CC selection and resource block (RB) allocation approaches [16]. In [20–22], a modified carrier specific proportional fair (PF) metric is maximized by using the CC

selection criteria for a CA system in HetNets. In [23], a CC selection algorithm that assigns a CC to each newly-arriving user equipment (UE) is proposed on the basis of the average channel quality; however, fairness of the system is not considered. The study in [24] focused on energy efficiency (EE) balancing between downlink and uplink by formulating an optimization problem in order to maximize the weighted sum of EEs, while the authors in [13] proposed to use the bisection method to balance the energy minimization and rate maximization.

Graph based algorithms are widely used for resource allocation purpose in wireless networks [25]. In [26], a greedy algorithm (GA) is proposed as a radio resource allocation algorithm by considering unrealistic assumptions as a constraint, such as the backlogged traffic model and the perfect channel information from channel quality indicators (CQIs). The proposed resource allocation method in [16] performs better, achieving a proportional fair throughput and higher fairness index than GA. However, it has a higher complexity than GA. In [27], a suboptimal solution is proposed based on the many-to-many two-sided matching game with externalities for device-to-device (D2D) communications. To this end, MSM algorithm is proposed as a robust solution for subcarrier allocation problems of such CA HetNets in this study. Our stability results allow to make finer assignments in terms of individual and/or social rate satisfaction on the HetNets.

There are several approaches to multiple carrier scheduling initially explored in its application to CA such as round robin scheduling and resource allocation on a user grouping [28, 29]. The round robin approach is channel unaware and the network as a whole may be inefficient in terms of throughput and bandwidth. User grouping scheduling algorithm aims to maximize the ratio of achievable instantaneous data rate of the network by using the criteria that are based on each user's equipment capability and the number of users within each carrier's coverage area [30]. In order to schedule multiple carriers, the modified Frank Kelly algorithm is proposed to maximize their individual utility functions by taking into account the primary and the secondary carriers present in the LTE 3GPP standard [28]. In [31, 32], a CC selection algorithm that assigns a CC to each newly-arriving UE is proposed on the basis of the average

channel quality, however, fairness of the system is not considered.

In [33], the Gale-Shapley and the random path to stability algorithms are proposed for coexistence between LTE and Wi-Fi systems. Although there are some studies that propose the SM algorithm as a scheduling scheme for CA systems as above, fairness and stability performances have not been considered for CA HetNets, so far. There is only one study that investigates low complexity and low feedback rate approaches in order to reduce the feedback overhead in a CA MIMO systems without considering the fairness [34]. The authors in [34] propose a novel scheme to reduce the computational complexity of the requiring rank indicator (RI), pre-coding matrix indicator (PMI), and CQI indices, and investigate a low feedback rate channel allocation approach for CA MIMO systems in [34]. However, the stability of the CA was not considered.

The complexity of resource allocation and the need for feedback information will be exponentially increased as the number of users and CCs increase. Moreover, the great interest to the complexity and feedback overhead of resource allocation in CA HetNets are getting increased with the 3GPP specifications of Release-13 LTE-A standard, which already introduces a CA of up to 32 CCs in order to achieve higher data rates ( $> 100$  MHz) for 5G systems [35]. Although there are some studies that propose variants of the SM algorithm as a scheduling scheme for CA systems, throughput and fairness performances have not been considered for the CA HetNets so far. Low complexity and low feedback rate approaches are presented in [34] in order to reduce the feedback overhead in a CA MIMO systems without considering the fairness.

### **1.3.2. Secure communication in Carrier Aggregated Heterogeneous Networks**

Physical layer security is a crucial topic for wireless communication networks as the complexity of the transmission methods are increasing tremendously. Thus, physical layer security is investigated widely for especially cooperative communication and cognitive radio networks in the literature. In [36], a trust game model is proposed



by considering the penalty of the faulty secondary users for the cooperative sensing spectrum to cope with malicious users. In [37], the effects of the inaccuracy of the trust degree on the secrecy rate is investigated under the assumption of a potential eavesdropper in the cooperative network. In [38], delivery-based attacker identification and punishment policies are proposed as a solution for data falsification of cooperative spectrum sensing in cognitive radio networks. In [39], an evolutionary game algorithm is proposed as a solution for cooperative behavior of selfish nodes for OFDM wireless communication systems in order to achieve higher secrecy rate. In [40], a capacity- and trust-aware base station cooperation strategy has been proposed for the non-uniform HetNets by considering the limited capacity and trustworthiness of BSs. This study investigates the optimal BS densities in terms of spectral efficiency results. However, fairness is not considered.

There are also a few other studies that investigate malicious users in wireless communications other than cooperative communications; however, existing studies are not enough for providing both reliable and fair communication. In [41], a modified neighbor-weight trust determination algorithm based on the reputation results is proposed by aiming to detect and isolate the malicious nodes from mobile ad hoc networks. In [42,43], a novel trust based network security method is proposed as an integration of the trust values in the optimization framework in a multi-hop wireless network. Trust values are obtained from an history. In [44], a trust evaluation method based on the use of probabilistic functions, called confidence interval calculation, is proposed as a solution for denial-of-service and Sybil attacks in wireless sensor networks. In [45], both selfish and malicious behavior of the agents are investigated with the deployment of trust/reputation management systems by designing cost-effective intrusion detection system by using a trust update mechanism based on partial monitoring of the agents. However, the effects of the trust value on the data rates or fairness are not included. In [46], a smart mode selection and bearer split-scheduling strategy is proposed to achieve fair and efficient bandwidth aggregation of LTE and Wi-Fi links. In [47], a resource allocation optimization problem with joint carrier aggregation in cellular networks is studied by considering real-time and delay-tolerant applications of mobile users. Although the proposed algorithms achieve high data rates and proportional

fairness, the potential security threats are not investigated in these studies. In [48], a reputation based method is proposed for misbehavior detection in uplink data offloading between Wi-Fi access and LTE access. Although the impact of energy efficiency and throughput is examined, fairness is not considered.

In this thesis, a trust-based SM approach is proposed for resource allocation under a selfish user threat in a CA HetNet. Stable matching algorithm has not been considered for the security threats in a CA HetNet before. The main aim is to preserve fair transmission by detecting selfish users with a low-complexity SM algorithm with some extensions. In the identification step of the proposed trust-based SM approach, the selfish user detection threshold has a significant role in order to avoid detecting honest users as selfish users as a result of bad channel estimation and decrease the misleading performances. Additionally, the punishment factor, which affects the trust index of each user in the network, has an essential role on the rate efficiency as well. The appropriate detection threshold and punishment indices are investigated in this study in terms of both misleading ratio and fairness.

### **1.3.3. Mobile edge computing in Internet of Things**

As the number of smart devices increases day by day, the need for new technologies, which may provide high security, high speed, and low complexity [49], increases, too. New applications of smart devices, such as real-time games, emergency applications, or significant medical applications, have very high data rate and low latency requirements, which cannot be addressed with cloud or fog networks directly. Thus, all the computing capabilities are offloaded to the mobile edge devices in order to decrease the latency significantly. MEC is defined and standardized by ETSI in [76, 77]. The MEC paradigm was proposed to address this issue by offloading the tasks to the edge devices corresponding to the nearest access points (APs). Resource allocation of available resources in edge devices to the IoT devices, is one of the main concerns in MEC.

Game theory is widely used in order to address the resource allocation problem

in wireless communication networks. In [33], the Gale-Shapley [50] and random paths to stability algorithms are proposed for coexistence between LTE and Wi-Fi systems. Although the stability issue is touched on slightly, fairness is again not considered. As an extension to [50], in [2, 51], many-to-one SM algorithm is used instead of one-to-one SM algorithm for the non-orthogonal spectrum assignment and for over-the-top applications in 5G networks, respectively. However, security aspects are not included. [52] focuses on energy consumption and time delay of the mobile terminal and also includes the stability analysis with a joint wireless and cloud resource allocation solution. [53] develops a novel online small-cell base station peer offloading framework, by leveraging the Lyapunov technique. This study mainly focuses on energy consumption problem.

In [54], Wang *et al.*, propose a fair policy based on non-cooperative strategic game, including three different offloading policies: executing tasks in local devices, offloading tasks to local servers, and nearby offloading in order to decrease overall system costs. In [55], hierarchical game for joint wireless and cloud resource allocation is proposed in order to minimize the cost of mobile terminals and delays. Another joint computation offloading problem is addressed with a low complexity algorithm different from the previous algorithms [56]. In [57], joint resource allocation and offloading optimization is proposed in order to decrease both cost and latency. Cost and latency trade off in MEC resource allocation is included in a scenario of one macro base station equipped with multiple MEC servers by using resource block allocation in [58]. Feng *et al.* propose a game theoretic Stackelberg game approach in order to address the pricing problem of cyber insurance security through fog computing platform [59].

In [60], successive convex optimization approach is proposed as a solution to resource allocation problem, which associates mobile users to the mm-wave access points with MEC hosts with the objective of minimizing power and latency. In [61], decentralized game based offloading and resource allocation approach is proposed in the case of multiple MEC active servers in the network. However, security issues are not included in this study. A multiuser offloading problem is addressed by proposing maximizing smart mobile device offloading payoff (SMOP) algorithm based on a game model in [62]. In [63], a Nash bargaining based resource allocation method is proposed

by considering users' individual demands in order to maximize the system throughput and minimize the delay. This study focused on effectiveness, fairness, and throughput; however, it does not consider security issues.

In [64], a Bayesian game theoretic framework is proposed for resource allocation in a MEC network. The analyses demonstrate that rationality (selfish behavior) does not lead to a more efficient allocation and incomplete information leads to a socially better outcome. In [65], Bayesian game based power allocation are proposed for MEC network, which includes selfish users and greedy users together. This study offers a power allocation algorithm, which considers the user's Bayesian probabilistic behaviors to calculate the utility.

Although there have been already many studies about MEC, as above, there are still open problems to be addressed, such as resource management and secure communication in order to meet various demands on IoT networks. In this thesis, SM algorithm is extended and proposed as a robust and low complexity solution for MEC offloading problems. Our stability results allow to make finer assignments in terms of individual and/or social rate satisfaction in IoT networks.

#### 1.4. Stable Matching Algorithm

Stable matching algorithm (also known as stable marriage algorithm) is initially presented in [50]. The main aim is to find the perfect match for everyone in both groups. The stable marriage process is illustrated in Figure 1.1. Men and women are defined as two distinct groups. Each woman and man has a deterministic preference list that reflects the desired levels to be matched with one of the opposite group members, in descending order. Thus, the first element of any preference list is the most desired man/woman. The preference list does not change through the SM algorithm.

SM algorithm is presented in detail in Figure 1.2. The preference list of each man and woman is represented by  $\succ_k^{man}$ : and  $\succ_n^{woman}$ ., respectively. There is a one-to-one matching, which means that each man can be matched with at a single ( $Q_k = 1$ )

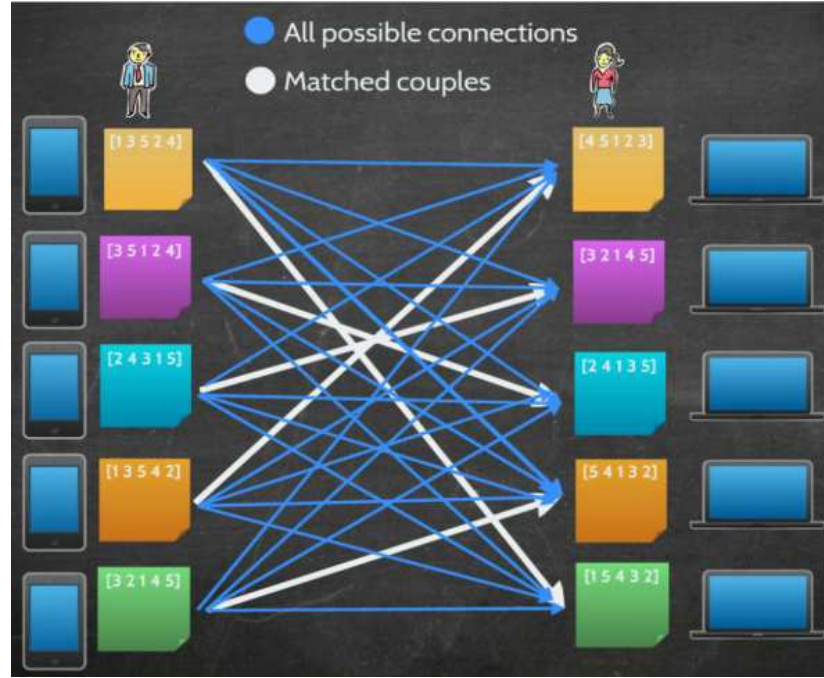


Figure 1.1. Stable Matching Algorithm

woman.  $\rho_x$  refers to the number of received proposals of woman  $x$ . A man can make only one proposal at a time, while a woman can have more than one proposals, at the same time.  $U_{n'}$  refers to the man, who is matched with the woman  $n'$  temporarily.

As a starting point, each man proposes to the woman, who is ranked first in his preference list, simultaneously. In the case of receiving only one proposal, the corresponding woman directly accepts the only proposal. In the case of receiving more than one proposals, the corresponding woman selects the one ranked highest among the proposals. When a woman accepts any proposal, she is temporarily matched with that man (engagement). Through the end of SM algorithm, women continue receiving and considering the new proposals. In the following steps, if an engaged woman receives a proposal from the man, who is ranked better than the man, whom she is already engaged, then she breaks off the engagement and accepts the new proposal. Thus, all the engagements may change until everyone is matched with one another. After the broken off engagement, the abandoned man continues to make proposals to the next woman in his preference list until getting a positive response (accepted). Hence, the process goes on until everyone is matched.

**Initialization:**  $\{r, k\} \in \mathcal{K}$ ,  $n \in \mathcal{N}$ ,  
 $K = N$ ,  $\forall Q_k = 1$ ,  $t = 0$   
 $X^{man,t}$ : proposal list of men at step  $t$ .  
 $\alpha_k^{man}$ : proposal rank of the  $k^{\text{th}}$  man ( $\alpha_k^{man} = 1$  at  $t = 0$ )  
 $\succ_n^{woman}$ : preference list of the  $n^{\text{th}}$  woman.  
 $\succ_k^{man}$ : preference list of the  $k^{\text{th}}$  man  
 $\rho_x$ : number of proposals to  $x \in \mathcal{N}$ .  
 $U_{n'}$ : temporary partner  $x \in \mathcal{N}$ .  
**while**  $\forall Q_k \neq 0$  **do**  
    Each man,  $k \in K$  ( $Q_k \neq 0$ ), makes proposal to  $X^{man,t}$ .  
    **for**  $n' \in X^{man,t}$  **do**  
        **if**  $\rho_{n'} > 1$  **then**  
            **if**  $\mu_{U_{n'},n'} = 1$  **then**  
                 $n'$  is assigned to the most desired man  
                **if** any new proposer,  $k$ ,  $\succ_{n'}^{woman} U_{n'}$  **then**  
                     $\mu_{U_{n'},n'} = 0$ ,  $\mu_{k,n'} = 1$   
                     $Q_{U_{n'}} = 1$ ,  $Q_k = 0$ .  
                **end if**  
            **else**  
                 $n'$  is assigned to the most desired man  
                 $\mu_{k,n'} = 1$ ,  $Q_k = 0$ .  
            **end if**  
             $\alpha_k^u = \alpha_k^u + 1$ , where  $k \in K$   
        **else**  
            **if**  $\mu_{U_{n'},n'} = 1$  **then**  
                 $n'$  is assigned to the most desired man  
                **if** the new proposer,  $k$ ,  $\succ_{n'}^{woman} U_{n'}$  **then**  
                     $\mu_{U_{n'},n'} = 0$ ,  $\mu_{k,n'} = 1$   
                     $Q_{U_{n'}} = Q_{U_{n'}} + 1$ ,  $Q_k = 0$ .  
                **end if**  
            **else**  
                 $n'$  is assigned to the proposer man (i.e.,  $k$ ).  
                 $\mu_{k,n'} = 1$ ,  $Q_k = 0$ .  
            **end if**  
             $\alpha_k^u = \alpha_k^u + 1$ , where  $k \in K$   
        **end if**  
    **end for**  
     $t = t + 1$   
**end while**

Figure 1.2. SM Algorithm

Since SM algorithm is a one-to-one matching algorithm, the number of men,  $K$ , is equal to the number of women,  $N$ . For simplicity, a matching can be illustrated using an  $K \times N$  binary matching matrix,  $\mathbf{M}$ , given as

$$\mathbf{M} = \begin{bmatrix} \mu_{1,1} & \mu_{1,2} & \cdots & \mu_{1,N} \\ \mu_{2,1} & \mu_{2,2} & \cdots & \mu_{2,N} \\ \cdots & \cdots & \cdots & \cdots \\ \mu_{K,1} & \cdots & \cdots & \mu_{K,N} \end{bmatrix}, \quad (1.1)$$

where  $\mu_{(k,n)}$  is the matching index, defined as

$$\mu_{(k,n)} = \begin{cases} 1, & \text{if the } k^{\text{th}} \text{ man \& } n^{\text{th}} \text{ woman is matched,} \\ 0, & \text{otherwise.} \end{cases} \quad (1.2)$$

As an explanatory example, SM algorithm is utilized for 5 men and 5 women in Example 1 simply.

**Example 1.** *Let  $K = 5$  men and  $N = 5$  women participate in a matching. For the sake of simplicity, let's give an ID number to each man and woman. Let the IDs of Bob, Joey, Jake, Adam, and Sheldon be 1, 2, 3, 4, and 5, respectively. Similarly, let the IDs of Alice, Monica, Sophie, Rachel, and Amy be 1, 2, 3, 4, and 5, respectively, as in Table 1.1.*

Table 1.1. Man and Woman IDs in SM Algorithm

ID (k or n)	Man	Woman
1	Bob	Alice
2	Joey	Monica
3	Jake	Sophie
4	Adam	Rachel
5	Sheldon	Amy

Let the preference lists of men be given as

$$\begin{aligned}
 \succ_1^{man} &= \{1, 2, 4, 3, 5\}, \\
 \succ_2^{man} &= \{2, 1, 3, 4, 5\}, \\
 \succ_3^{man} &= \{4, 1, 3, 2, 5\}, \\
 \succ_4^{man} &= \{2, 4, 1, 3, 5\}, \\
 \succ_5^{man} &= \{5, 2, 4, 1, 3\},
 \end{aligned} \tag{1.3}$$

According to preference lists of man, it is seen that Bob desires to match with Alice the most and Sophie the least. Preference lists of women are also given as

$$\begin{aligned}
 \succ_1^{woman} &= \{4, 2, 1, 3, 5\}, \\
 \succ_2^{woman} &= \{3, 2, 4, 1, 5\}, \\
 \succ_3^{woman} &= \{1, 2, 4, 3, 5\}, \\
 \succ_4^{woman} &= \{3, 4, 2, 1, 5\}, \\
 \succ_5^{woman} &= \{5, 4, 1, 3, 2\},
 \end{aligned} \tag{1.4}$$

At the beginning of SM algorithm, Bob proposes to Alice, Joey and Adam proposes to the same woman, Monica, and Jake proposes to Rachel. In this case Alice, Rachel, and Amy have only one proposal for each, thus they accept and get engaged with Bob, Jake, and Sheldon, respectively. The matching indices of Bob-Alice, Jake-Rachel, and Sheldon-Amy couples are  $\mu_{1,1} = 1$ ,  $\mu_{3,4} = 1$ , and  $\mu_{5,5} = 1$ , respectively. In the mean time, Monica ( $n = 2$ ) has two proposals from Joey ( $k = 2$ ) and Adam ( $k = 4$ ). According to Monica's preference list  $\succ_2^{woman}$ , she desires to match with Joey more than Adam. Thus, Monica accepts Joey's proposal and get engaged with him ( $\mu_{2,2} = 1$ ).

The rejected man, Adam, proposes to the second placed woman in his preference list  $\succ_4^{man}$ . Rachel is already engaged, but nevertheless she considers the new proposal.



According to Rachel's preference list  $\succ_4^{woman}$ , she still desires to match with Jake more than Adam. Thus, Adam is rejected again. Next, Adam proposes to Alice according to his preference list. This time, Alice prefers Adam rather than Bob. Thus, she breaks off the engagement ( $\mu_{1,1} = 0$ ) and get re-engaged with Adam, ( $\mu_{4,1} = 1$ ).

Now, Bob makes proposals again until he gets a positive response. Eventually, Bob is matched with Sophie ( $\mu_{1,3} = 1$ ). Hence, at the end of the matching process, the matching matrix is obtained as

$$\mathbf{M} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \quad (1.5)$$

The final matchings are illustrated as in Table 1.2.

Table 1.2. Final Stable Matchings

	<b>Man</b>	<b>Woman</b>
Couple	Bob (1)	Sophie (3)
Couple	Joey (2)	Monica (2)
Couple	Jake (3)	Rachel (4)
Couple	Adam (4)	Alice (1)
Couple	Sheldon (5)	Amy (5)

SM algorithm possesses several nice properties that contribute to the fairness of the results such as completeness and stability.

**Definition 1.** A matching is complete if and only if all men and women are assigned at the end of the algorithm.

As in Example 1, the algorithm is finalized after everyone is matched. Thus, SM algorithm achieves a complete matching. SM algorithm guarantees that all women and men are matched.

**Definition 2.** For any two man-woman matching such as  $\mu_{(k,n)} = 1$  and  $\mu_{\hat{k},\hat{n}} = 1$ , if the  $k^{th}$  man would prefer the  $\hat{n}^{th}$  woman over the  $n^{th}$  woman and the  $\hat{n}^{th}$  woman would prefer the  $k^{th}$  man over the  $\hat{k}^{th}$  man, then the  $k^{th}$  man and the  $\hat{n}^{th}$  woman couple is called rogue couple in the SM algorithm.

Rogue couples means that there are at least two unhappy people in the network. An explanatory example is given in Example 2.

**Example 2.** Considering the same variables in Example 1. Assume that the people in Example 1 are randomly matched. The final matching matrix is obtained as

$$\mathbf{M} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \quad (1.6)$$

Hence, the final matchings are recorded as in Table 1.3.

Table 1.3. Random Matchings

	Man	Woman
Couple	Bob (1)	Rachel (4)
Couple	Joey (2)	Monica (2)
Couple	Jake (3)	Sophie (3)
Couple	Adam (4)	Alice (1)
Couple	Sheldon (5)	Amy (5)

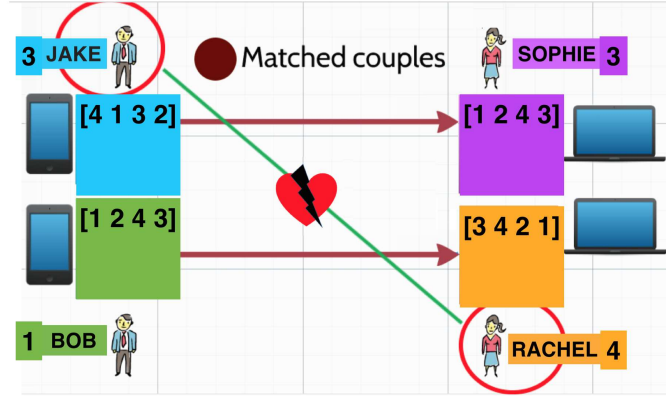


Figure 1.3. Rogue couple illustration

As seen in Figure 1.3, Bob is matched with Rachel, and Jake is matched with Sophie. By considering the preference lists of these people, it is noticed that Rachel prefers Jake rather than Bob, and similarly, Jake prefer Rachel rather than his final match, Sophie. Here, Jake - Rachel couple is called rogue couple as defined in Definition 2.

SM algorithm also guarantees perfect and stable matchings by using the preference lists as in Theorem 1. If there are no rogue couples at the end of the matching process, the matching is referred as perfect and stable matching.

**Theorem 1.** *SM algorithm always gives perfect and stable matchings as results.*

*Proof.* Let us consider a matching  $\mathcal{M}(k, n) = 1$ . Assume that  $k$  had a preference,  $\hat{n}$ , that ranked higher than  $n$  in its preference list. This would either mean that  $k$  proposed to  $\hat{n}$  in an earlier round of the algorithm and  $\hat{n}$  rejected the proposal or  $\hat{n}$  is matched with another applicant that is ranked better than  $k$  in the  $\hat{n}$ 's preference list. Hence, any  $(k, \hat{n})$  cannot be a rogue couple.  $\square$

With all these good features, SM algorithm is very appropriate for resource allocation problems in wireless communication systems such as CA HetNets, and IoT networks. In addition to stability and completeness of SM algorithm, the low complexity structure is another reason for being preferred for resource allocation in CA HetNet.

### 1.5. Carrier Aggregation in Heterogeneous Networks

As new applications on mobile devices are developed, the existing technologies in wireless communications cannot meet the tremendous demands. New applications expect higher data rates and lower latency as much as possible. Thus, services compete each other for limited resources. The existing features of homogeneous networks are far from meeting expectations. In order to meet these challenges, more efficient modulation and coding techniques, multi-antenna features, and cognitive radio technologies are extensively studied in the literature. Nevertheless, these features alone are not enough to serve these applications properly, especially in the cell edges, where the data rate performance decreases fatally. Additionally, system fails when the network is significantly crowded. In this manner, small-cells are introduced in the 3GPP specifications of Release-9 (R9) in [66] in order to lessen the density of macro-network. One of the greatest benefits of small-cell deployments is to provide great performances to the users even placed at the cell edges. Additionally, small-cell deployments cost significantly less than macro-networks, and it is easier to construct [67].

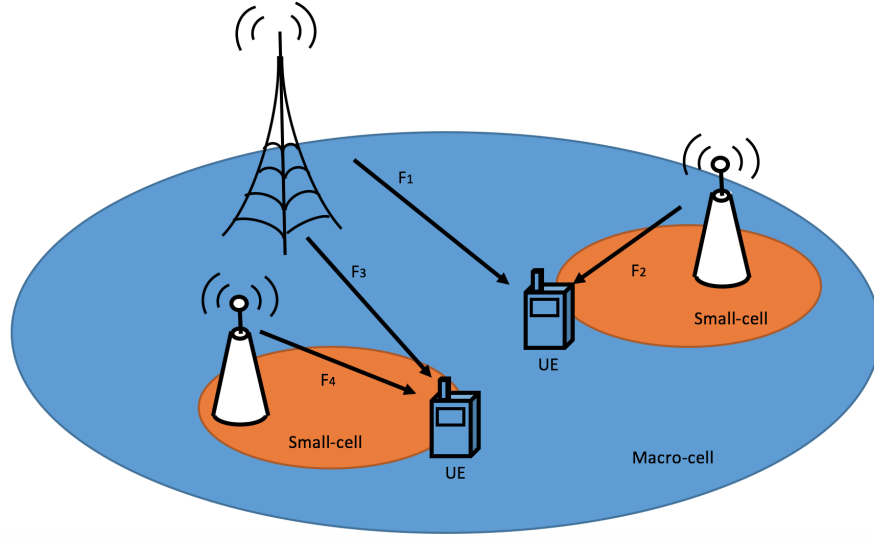


Figure 1.4. General Carrier Aggregated Heterogeneous Networks

By considering different size of small-cells and macro-cells as a mix structure is referred as HetNet, as shown in Figure 1.4. Note that, UE have to be LTE in order to use the benefits of HetNet structure. A HetNet includes at least two different types of cells among macro-, micro-, pico-, and femto-cells in decreasing base station power order. The cell size also depends on antenna properties and the environment, such as city, rural, outdoor, or indoor. Although HetNet structures relax the data traffic, significantly, there are still needs for higher data rates as well as lower latency in order to cope with the requirements of new applications. Thus, with the aim of achieving wider transmission bandwidths in HetNets, CA is introduced in the LTE-A system by giving an opportunity to efficiently utilize the fragmented spectrum of multiple frequency resources [10, 68]. After carrier aggregation, each carrier is called carrier component. There are two categories:

- (i) **Primary component carrier:** In each aggregation, one of the CC is the main carrier of that group. Primary CC is a must for both downlink and uplink transmissions.
- (ii) **Secondary component carrier:** All the CCs, other than primary component carriers, are called secondary component carriers. In the initial CA settlement the number of aggregated CCs is restricted by 5 CCs in the 3GPP specifications of Release-10 [10], whereas after a while new technologies force to get more CCs

and the maximum CCs for an aggregation is increased to 32 CCs in the 3GPP specifications of Release-14 [35].

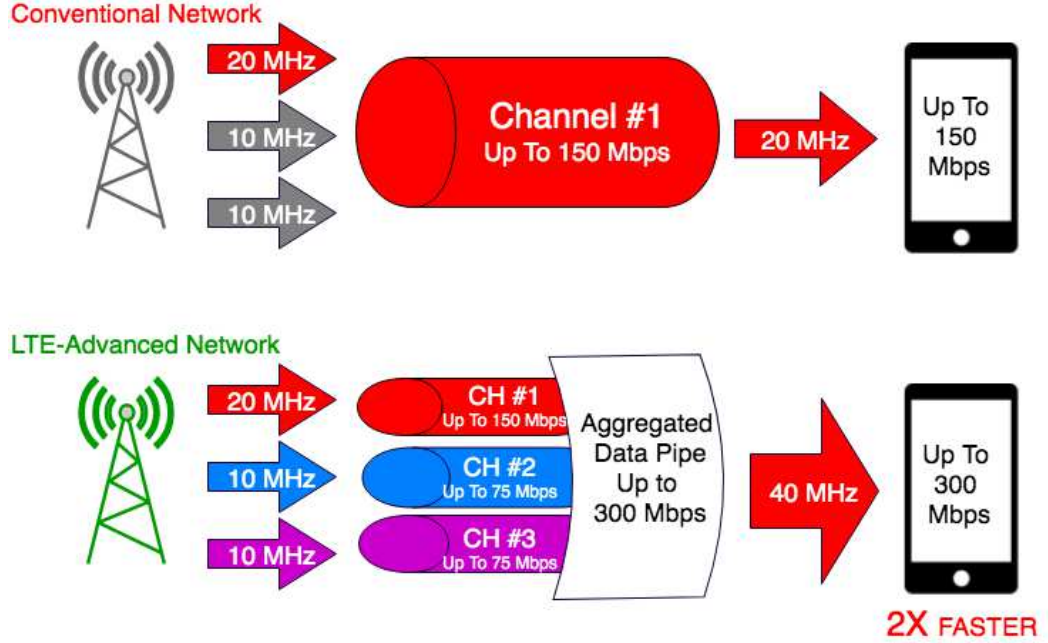


Figure 1.5. Comparison of conventional network with LTE-Advanced network, which aggregates one 20 MHz CC and two 10 MHz CCs.

According to [10], each UE can have at most 5 CCs with the same or different bandwidths as 1.4, 3, 5, 10, 15, or 20 MHz. Therefore, each UE can achieve 100 MHz at maximum. An illustrative example is given in Figure 1.5. In the conventional LTE networks (defined in R9), LTE users are not capable of aggregating carriers. Thus, the two of the three CCs are idle in the network. Fortunately, carrier aggregation enabled LTE-Advanced users are introduced in the 3GPP specifications of Release-10 [10]. Thus, all CCs can be used to increase the data rate in LTE-Advanced networks, as seen in Figure 1.5. As a result of aggregating three different available CCs, one can reach two times faster data rates.

Subcarriers can be aggregated from the same or different CCs [69]. The different deployments of CA can be defined in three main categories as intraband contiguous, intraband non-contiguous, and interband non-contiguous CA:

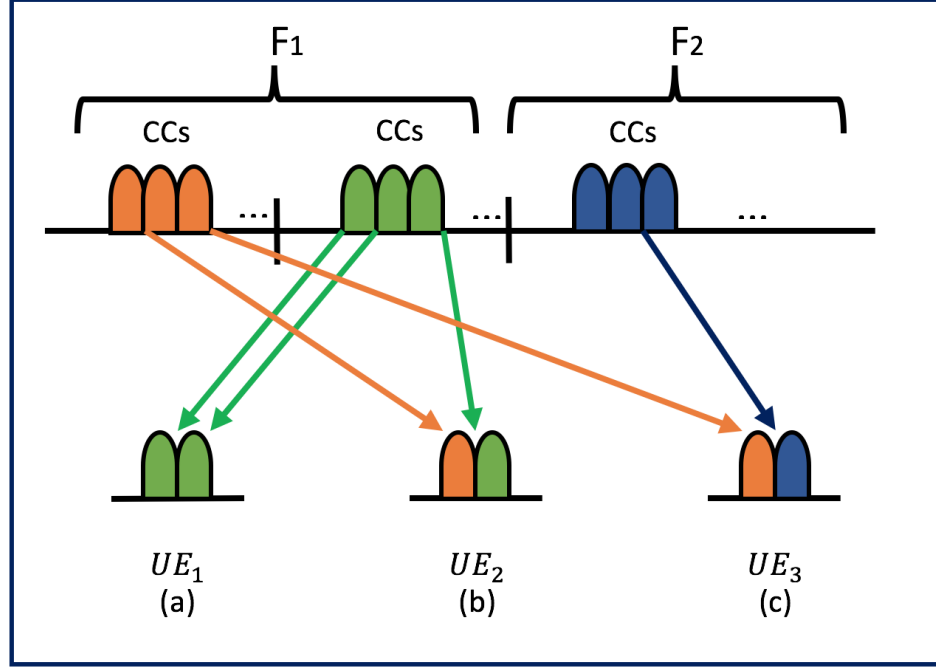


Figure 1.6. Carrier aggregation deployments: (a) Intraband contiguous, (b) intraband noncontiguous, and (c) interband noncontiguous

- (i) **Intraband contiguous:** In contiguous CA, CCs are adjacent to each other and belong to the same frequency band as in Figure 1.6 (a). RF views this type of aggregated channels as one enlarged channel. Only one transceiver is enough as a result of adjacent structure. Note that, it is crucial to ensure that UE has an ability of using the wider bandwidth without any loss on performance. This extension can be adapted easily to the existing RF elements in the base station.
- (ii) **Intraband non-contiguous:** In non-contiguous CA, combined CCs can belong to the same frequency band with a frequency gap or frequency gaps. Now, this multi-carrier signal cannot be treated as single channel, thus more than one transceivers are required. The number of transceivers depends on the number of channels, from the view of RF. As the number of transceivers increases, the complexity increases as well. This complexity affects the UE more than base station in terms of power and cost.
- (iii) **Interband non-contiguous:** In non-contiguous CA, the combined CCs can belong to different frequency bands (interbands) as in Figure 1.6 (c). This type of carrier aggregation uses the component carriers belonging to different bands. Component carriers are not adjacent. Thus, multiple receivers are required.

Moreover, there are additional challenges, including reducing cross modulation from the two transceivers. Hence, this type of carrier aggregation is the most complicated one.

One of the major challenges in CA HetNets is to find an appropriate resource allocation algorithm for various nodes with different data rate requirements. In this study, SM algorithm is proposed to achieve stable subcarrier allocation by considering QoS requirements in a CA HetNet. Another significant challenge of CA HetNets is the complexity of the resource allocations, which increases with each additional CC. In order to reduce the computational complexity of resource allocation, SM algorithm is preferred for its simple structure to allocate subcarriers belonging to the same/different CCs to the UEs in different CA HetNet scenarios. In previous studies, it is shown that SM algorithm achieves also a very good performance even when the preference lists are incomplete [70, 71]. This property is also very useful to reduce the CSI overhead on the feedback channel. To this end, in Chapter 2, SM algorithm is applied to the CA HetNets.

### **1.6. Mobile edge computing in Internet of things**

Computation-intensive applications like virtual reality, and interactive gaming are required to support ultra low latency and ultra high rate computing. For instance, transformation vehicles may generate Tera bytes in minutes [72]. However, mobile devices have limited battery and storage capabilities. In order to run the applications, that require high energy consumption in a limited-battery mobile handsets, mobile devices offload their most energy-consuming tasks to the nearby servers. Cloud computing promises to relax the data storage capability of mobile devices and enable to access higher rates by offloading their computation-intensive tasks [73]. The main objectives of cloud computing are to increase data rate while relaxing network bandwidth, and decreasing the power consumption in IoT devices.

Reliability is very significant for time-sensitive decisions of emerging applications. Low latency is another vital requirement for some critical applications such as electrical



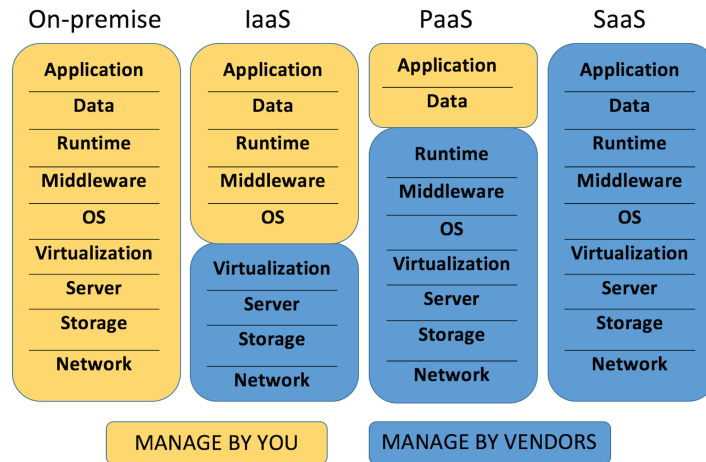


Figure 1.7. Different types of services supplied from IoT network suppliers

shutdowns, fire or disaster averting systems, military, and remote surgery. Moreover, IoT data belonging to this kind of emerging applications has to be protected against any possible attack. Cloud servers provide their services in three main categories as shown in Figure 1.7. In Figure 1.7, there is an additional on-premises category, which is actually no cloud computing. All categories are explained clearly as:

- (i) **On-premise services:** This is the case, where no cloud computing occurs. In this service, company has to purchase servers, computers, and software. Companies have the maximum control in the system. As an advantage, only one payment is enough for user licenses. On-premises hosting has a large initial installation, which can take time to get everything proper. The other issue is security. In on-premises hosting, one has to ensure the security.
- (ii) **Infrastructure as a service (IaaS):** Infrastructure as a Service provides network structure, server computation with a storage, and an additional virtualization layer. With all these services, a company can create virtual machines, install operating systems and required software. There is a mid-level control in this service. A company can manage the operating systems and perform maintenance; however, it is not permitted to make any changes in the network infrastructure or server. IaaS makes sure that companies do not need to concern about purchas-

ing and maintaining the hardware. IaaS has a flexible structure that allows any company to require any additional storage or computing power. On the other hand, the cost depends on consumption. Moreover, server is fully independent from the company. Thus, reliability might be little concern. This service is a great option for startups or small companies in order to save time and money. IaaS is also useful in case of there is an uncertainty about the requirements of new applications.

- (iii) **Platforms as a service (PaaS):** Platform as a service offers more services than IaaS. PaaS provides not only network infrastructure, server, and system software, but also, database software and development runtimes. PaaS is very useful for companies, that desire to develop or host their own applications in the cloud. Additionally, companies are free from purchasing and long installation processes. PaaS delivers a framework for developers that they can develop and deploy software applications. Service availability might be a great concern, i.e., any changes in the provided environment could effect the applications served by the corresponding networks. PaaS is very beneficial in order to speed up the process in case of multiple developers working on the same project. PaaS can also simplify some challenges, if the company has a request in order to develop the application rapidly.
- (iv) **Software as a service (SaaS):** Software as a service provides to companies all the service layers so that they do not have to concern any physical installation. SaaS is also called as 'on-demand service'. Companies do not need to worry about server space or any software licensing fee. SaaS has a great flexibility in terms of quick deployment. Many SaaS applications are run in the web browser instead of requiring download or installation. Beyond these features, when there is any disruption or error in the system, service provider treats immediately. SaaS might cause synchronization problems in case of multiple SaaS applications being used in the same company. As a solution, a digital assistant is proposed. Digital assistant can integrate with over 50 applications. Security is a great concern in SaaS. SaaS is also useful for startups get involved to the business, quickly.

All these beneficial services served through only centralized cloud at first. However, cloud computing does not meet the low latency requirement of many critical applications. Thus, this technology is moving to a closer point to the mobile devices by introducing fog computing and edge computing technologies [74].

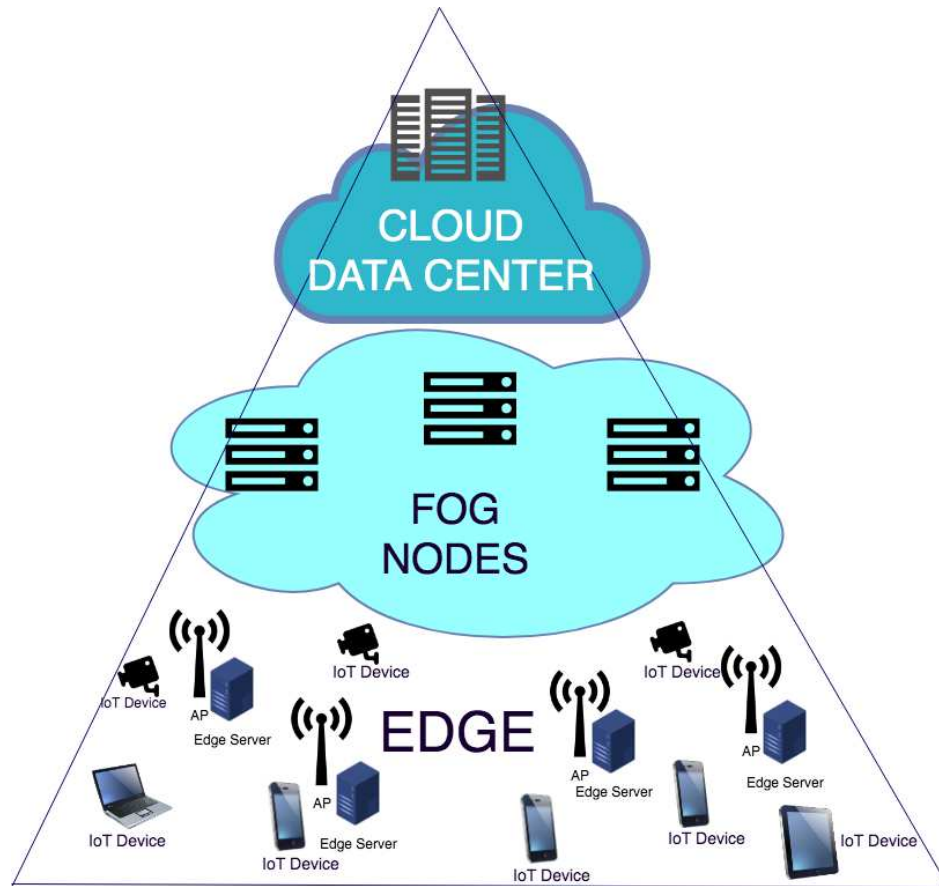


Figure 1.8. Cloud, Fog, and edge structures in a network.

Cisco defined the fog computing as an extension to cloud computing to realize the full potential of IoT [75]. The fog is a layer between the edge and the cloud as shown in Figure 1.8, which extends the cloud closer to the IoT devices. Any device with computing (necessary processing power), storage capability, and network connectivity can be a fog node, i.e., switches, routers, embedded servers, industrial gateways, industrial controllers. The data is first transmitted to the fog nodes, then it is transmitted for processing to the sources in a fog structure. In this structure, system interacts with both gateways and embedded computer systems at the same time.

Fog computing has many additional features compared to the cloud structure. Fog nodes may receive feeds by using any protocol in real-time, while cloud system receives data summaries. Fog nodes are able to run IoT applications for real-time control and transmit the analytics in milliseconds. Moreover, fog nodes can provide transient storage. Fog nodes send data summaries to the cloud, while the cloud sends new application rules to the fog nodes.

With edge computing, services are much closer to the user than they are in cloud a fog services. Edge computing relax the load on embedded computing platforms, significantly. Cloud computing servers produce always-on shared pools for computing resources such as storage, processors. IoT devices use these external resources through RANs and the Internet. Edge nodes directly interface to sensors by interfacing to sensors and controllers. Although the reliability decreases as the computing processes moved to the end users, both, computing capability and data rate are extensively increases. In addition, ultra low latency required applications are mostly satisfied with edge computing.

## 2. APPLICATION OF STABLE MATCHING ALGORITHM IN CARRIER AGGREGATED HETEROGENEOUS NETWORKS

In order to address the increasing demands for high data rates in wireless communications, CA is introduced in the 3GPP LTE-A specifications of Release-10 for HetNets, a platform for the implementation of features with new functionalities. In this study, resource allocation problem is addressed. Stable matching algorithm is extended and adapted to the CA HetNets. Subcarriers are matched with UEs instead of women matched with men, respectively.

### 2.1. Motivation

One of the major challenges in CA HetNets is to find an appropriate resource allocation algorithm for various nodes with different data rate requirements. SM algorithm is one of the most popular allocation algorithms introduced in the last decade. In this study, an important variation of the MSM algorithm is proposed as PFM algorithm, to achieve fair and stable subcarrier allocation by considering rate requirements in a HetNet. The stability concerns for CA HetNets are investigated for the proposed variation of the MSM algorithm in order to determine the rate satisfaction of both user equipments and the entire HetNet. The rate and fairness performances of the proposed algorithm are also compared with the optimal rate algorithm (ORA), which achieves the maximum rate, and with PF algorithm, which is widely used for fair resource allocation problems. Computer simulations show that the proposed variations of SM algorithms are very robust even with partial CSI in terms of rate and fairness.

### 2.2. System Model

The system under consideration is a CA HetNet with multiple UEs and subcarriers corresponding to the same band or different bands. An LTE-A macrocell base

station (MBS) and a number of smallcell base stations (SBSs), i.e., micro-, pico-, or femto-cells, interacting with each other.  $K$  UEs are uniformly distributed on a concurrent area of LTE-A MBS and SBSs as depicted in Figure 2.1. At this stage, SBS and MBS are assumed to communicate with each other by using almost blank subframes (ABS) in order to neglect the co-channel interference [11] and OFDMA is used in order to avoid inter-user interference. Without loss of generality, we neglect the inter-cell interference by considering the related studies of inter-cell interference coordinations (ICICs) in the literature [78, 79].

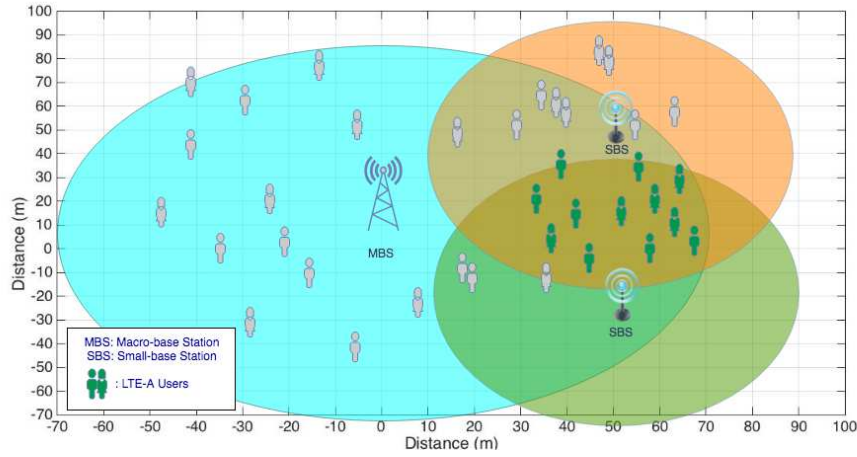


Figure 2.1. System model of carrier aggregated HetNet. Carrier aggregation enabled LTE-A users (green) are positioned in the concurrent area of SBSs and MBS while the other users (gray) are placed out of this concurrent area.

Assume that each UE and each subcarrier has an ID number as  $k \in \mathcal{K}$  and  $n \in \mathcal{N}$ , respectively.  $\mathcal{K}$  refers the set of UEs and  $\mathcal{N}$  refers the set of subcarriers in the HetNet. CCs can belong to the same band or different bands. The number of subcarriers of each CC,  $N_c$ , where  $c \in \{1, 2, \dots, M\}$ , can differ from one CC to another. The number of CCs in each frequency band can also differ from band to band. The total number of subcarriers,  $N$ , belonging to all contiguous/non-contiguous CCs of such a CA HetNet is  $N = \sum_{c=1}^M N_c$ . Unless otherwise stated, perfect CSI is assumed at both the UEs and the subcarriers. Total rate of such a CA HetNet is obtained as

$$R = \sum_{k=1}^K \sum_{n=1}^N \mu_{(k,n)} r_k(n) \text{ [bps]}, \quad (2.1)$$

where  $\mu_{(k,n)} \in \{0, 1\}$  is the assignment index that takes on the value 1 if the  $k^{\text{th}}$  UE and the  $n^{\text{th}}$  subcarrier is matched, and 0, otherwise. The marginal rate of the  $k^{\text{th}}$  UE and the  $n^{\text{th}}$  subcarrier,  $r_k(n)$ , can be calculated using the Shannon's rate formula [80] as

$$r_k(n) = W_b \log_2(1 + c_k(n)) \quad [bps], \quad (2.2)$$

where  $W_b$  refers to the bandwidth, and  $c_k(n)$  is the SNR of the  $k^{\text{th}}$  UE and the  $n^{\text{th}}$  subcarrier and it can be written as

$$c_k(n) = \frac{P_{k,n}}{\sigma_k^2(n)}, \quad (2.3)$$

where  $\sigma_k^2(n)$  is the variance of the complex additive white Gaussian noise (AWGN) component of the  $n^{\text{th}}$  subcarrier and  $P_{k,n}$  is the power of the channel gains, calculated as

$$P_{k,n} = P_n |h_{k,n}|^2, \quad (2.4)$$

where  $P_n$  is the transmit power of subcarriers. The channel coefficients,  $h_{k,n}$ ,  $k = \{1, \dots, K\}$ ,  $n = \{1, \dots, N\}$ , are assumed to have complex Gaussian distributions with zero mean and unit variance.

Assuming perfect phase synchronization at receiver, in this model, we can assume a Rayleigh distributed amplitude fading. Our rate optimization problem for CA HetNets is then formulated as

$$\begin{aligned}
& \underset{\mu, \forall k, n}{\text{maximize}} && R = \sum_{k=1}^K \sum_{n=1}^N \mu_{(k,n)} r_k(n) \\
& \text{s.t.} && \text{(a) } \sum_{k=1}^K \mu_{(k,n)} \leq 1, \quad \forall n, \\
& && \text{(b) } \sum_{n=1}^N \mu_{(k,n)} \leq Q_k, \quad \forall k,
\end{aligned} \tag{2.5}$$

where (a) dictates that each subcarrier is allowed to be assigned to at most one UE and (b) indicates that each UE is allowed to use at most  $Q_k$  subcarriers.  $Q_k$  is a predetermined quota value for each UE depending on the rate requirements.

In order to reach the maximum achievable rate for such subcarrier assignment problems, it has been accepted as an optimal solution that each subcarrier is allocated to the UEs with the best channel condition [81]. This assignment rule is referred as optimal rate algorithm (ORA) throughout this thesis. There is no quota for subcarrier assignments of each UE in ORA, i.e., all subcarriers can be assigned to the same UE if it is the most preferred UE for each subcarrier. Thus, ORA achieves the maximum rate for such a CA HetNet system; however, the fairness is not considered. PF algorithm compares the ratio of the feasible rate for each UE to its average throughput. The subcarriers are assigned to the UE with the maximum preference metric. Although PF has significant enhancement on fairness, it is not robust for partial feedback cases. Thus, our simulation results are compared with ORA and PF for the same scenarios.

In order to achieve both high throughput and rate based fair allocation, some variations of the SM algorithm are proposed for subcarrier assignment in a CA HetNet. SM algorithm was originally presented as a solution to college admissions and stable marriage problem in order to achieve a perfect and stable matching between two distinct groups, colleges-applicants or men-women, respectively [50]. In this study,  $K$  UEs and



$N$  subcarriers are matched instead of matching of colleges and applicants in the college admissions problem. The preference lists of UEs and preference lists of subcarriers are obtained by using the CSI instead of deterministic and ordered preference lists of the conventional SM algorithm. The basic idea is sorting  $P_{x,y}$  in terms of  $x$  in descending order and saves the indices of each  $x$  as

$$\succ_k^u = \arg \underset{n}{\text{sort}} \{P_{k,n}\}, \quad k \in \mathcal{K}, \quad (2.6)$$

$$\succ_n^{sc} = \arg \underset{k}{\text{sort}} \{P_{k,n}\}, \quad n \in \mathcal{N}. \quad (2.7)$$

MSM algorithm starts with the proposals of each UE to the most desired subcarrier in their preference lists as presented in Figure 2.2. If there are several proposals to a subcarrier and the proposed subcarrier is unassigned, this subcarrier is assigned to the most preferred proposer in the subcarrier's preference list. Let the  $d^{\text{th}}$  UE and the  $e^{\text{th}}$  UE propose to the  $s^{\text{th}}$  subcarrier, and assume that the  $d^{\text{th}}$  UE is preferred to the  $e^{\text{th}}$  UE by the  $s^{\text{th}}$  subcarrier as,  $\succ_s^{sc} = \{\dots \succ d \succ \dots \succ e \succ \dots\}$ , where  $x \succ y$  denotes that  $x$  is preferred to  $y$ . Then, the  $s^{\text{th}}$  subcarrier is assigned to the  $d^{\text{th}}$  UE, resulting in  $\mu_{d,s} = 1$ . If there is only one proposal for an unassigned subcarrier, it is assigned to the proposer. The assignments are saved in the assignment matrix,  $\mathbf{M}$ , as

$$\mathbf{M}(k, n) = \begin{cases} 1, & \text{if } k \text{ \& } n \text{ are matched,} \\ 0, & \text{otherwise,} \end{cases} \quad (2.8)$$

where rows represent UEs while columns represent subcarriers. Each UE continues making proposals to the subcarriers in each step until it reaches its quota,  $Q_k$ . Thus, the corresponding quotas are updated after each matching decision until all UEs and subcarriers are matched.

**Initialization:**  $\{r, k\} \in \mathcal{K}$ ,  $n \in \mathcal{N}$ ,  
 $N \geq K$ ,  $Q_k \leq N$ ,  $t = 0$   
 $X^{UE,t}$ : proposal list of UEs at step  $t$ , respectively.  
 $\alpha_k^u$ : proposal rank of the  $k^{\text{th}}$  UE ( $\alpha_k^u = 1$  at  $t = 0$ )  
 $\succ_n^{sc}$ : preference list of the  $n^{\text{th}}$  subcarrier.  
 $\succ_k^u$ : preference list of the  $k^{\text{th}}$  UE  
 $\rho_x$ : number of proposals to  $x \in \mathcal{N}$ .  
**while**  $\forall Q_k \neq \emptyset$  **do**  
    Each UE,  $k \in K$  ( $Q_k \neq 0$ ), makes proposal to  $X^{UE,t}$ .  
    **for**  $n' \in X^{UE,t}$  **do**  
        **if**  $\rho_{n'} > 1$  **then**  
            **if**  $\mu_{U_{n'},n'} = 1$  **then**  
                 $n'$  is assigned to the most desired UE  
                **if** any new proposer,  $k$ ,  $\succ_{n'}^{sc} U_{n'}$  **then**  
                     $\mu_{U_{n'},n'} = 0$ ,  $\mu_{k,n'} = 1$   
                     $Q_{U_{n'}} = Q_{U_{n'}} + 1$ ,  $Q_k = Q_k - 1$ .  
                **end if**  
            **else**  
                 $n'$  is assigned to the most desired UE  
                 $\mu_{k,n'} = 1$ ,  $Q_k = Q_k - 1$ .  
            **end if**  
             $\alpha_k^u = \alpha_k^u + 1$ , where  $k \in K$   
        **else**  
            **if**  $\mu_{U_{n'},n'} = 1$  **then**  
                 $n'$  is assigned to the most desired UE  
                **if** the new proposer,  $k$ ,  $\succ_{n'}^{sc} U_{n'}$  **then**  
                     $\mu_{U_{n'},n'} = 0$ ,  $\mu_{k,n'} = 1$   
                     $Q_{U_{n'}} = Q_{U_{n'}} + 1$ ,  $Q_k = Q_k - 1$ .  
                **end if**  
            **else**  
                 $n'$  is assigned to the proposer UE (i.e.,  $k$ ).  
                 $\mu_{k,n'} = 1$ ,  $Q_k = Q_k - 1$ .  
            **end if**  
             $\alpha_k^u = \alpha_k^u + 1$ , where  $k \in K$   
        **end if**  
    **end for**  
     $t = t + 1$   
**end while**

Figure 2.2. Proposed MSM Algorithm for HetNets

One of the significant goals of using MSM based approaches in HetNets is to design an algorithm that achieves acceptable rate levels while providing higher rates to the UEs at the same time. MSM algorithm possesses several nice properties that contribute to the rate based approaches from a fairness perspective. MSM algorithm also guarantees perfect and stable matchings that ensure high QoS by using the preference lists as in Theorem 1.

**Definition 3.** *For any two UE-subcarrier assignments such as  $\mu_{(k,n)} = 1$  and  $\mu_{\hat{k},\hat{n}} = 1$ , if the  $k^{\text{th}}$  UE would prefer the  $\hat{n}^{\text{th}}$  subcarrier over the  $n^{\text{th}}$  subcarrier, and the  $\hat{n}^{\text{th}}$  subcarrier would prefer the  $k^{\text{th}}$  UE over the  $\hat{k}^{\text{th}}$  UE, then the  $k^{\text{th}}$  UE and the  $\hat{n}^{\text{th}}$  subcarrier are called a blocking assignment (also known as rogue couple in the stable marriage algorithm).*

**Definition 4.** *An assignment is perfect and stable if and only if there are no blocking assignments at the end of the matching process.*

**Theorem 2.1.** *SM algorithm always gives perfect and stable matchings [82]*

By considering these useful properties of the MSM algorithm, we are able to determine the quota of each UE,  $Q_k$ , by considering rate or to set  $Q_k = N/K$  in order to achieve a high fairness in terms of the number of subcarriers. The well-known Jain's fairness index [83] is used in order to measure the fairness of the proposed algorithms. In order to further assess the performance of the proposed algorithms in terms of instantaneous,  $\phi_k^r$ , and long-term fairness. Jain's fairness index uses the ratio of the individual rate of each UE and the total rate of the network. Fairness index,  $\Phi$ , of a HetNet can be obtained by using the fairness index of each of the  $k^{\text{th}}$  UE by using (2.1) as in [83].

$$\Phi = \frac{\left( \sum_{k=1}^K \phi_k^r \right)^2}{K \sum_{k=1}^K \phi_k^{r^2}}, \quad (2.9)$$

where  $\phi_k^r$  is defined based on rate proportionality as

$$\phi_k^r = \frac{R_k}{\sum_{k=1}^K R_k}. \quad (2.10)$$

### 2.3. Variations of the stable matching based carrier aggregated resource allocation approach

Fairness aware and practically implementable variations of SM algorithm are proposed here as a solution to resource allocation in CA HetNets. Two important variations of the SM algorithm are considered for different scenarios in this thesis. In the first variation, the original one-to-one SM algorithm is extended to many-to-one allocation by considering rate in a CA HetNet and referred to MSM resource approach. This algorithm is very similar to the many-to-one matching in college admission problem [3,84,85]. In the college admission problem, colleges put the best  $Q$  applications on their wait list, where  $Q$  is the quota of each college. However, in our MSM algorithm, each UE accepts one subcarrier (proposer) and rejects the rest, instantaneously, and is open to new proposals for the next matching process until it reaches its quota,  $Q_k$ . Unlike the previous studies, MSM algorithm uses partial preference lists that consider partial CSI from the feedback channel in order to reduce the feedback overhead in the second variation, which is referred in this thesis as PFM. To be applicable in realistic scenarios, MSM and PFM are examined under noisy feedback channel conditions as well. These approaches give opportunity to allocate subcarriers to the UEs in a CA HetNet with a high fairness despite a very small rate loss even under noisy environment.

#### 2.3.1. Many-to-one Stable Matching Based Carrier Aggregation

In order to achieve higher data rates, CA is proposed for different scenarios of HetNets in [68]. CA technology allows UEs to communicate with more than one

carriers, which may belong to the same or different frequency bands [69]. Resource allocation is another essential issue in CA in order to use the frequency bands efficiently. Thus, we propose MSM for inter-band non-contiguous CA HetNets in this subsection. In order to apply the proposed algorithms to these HetNets, we assume that each subcarrier has a unique ID,  $n$ , in the whole HetNet and the IDs of the subcarriers belonging to same CC are consecutive.

One of the main motivations of using the MSM algorithm for CA HetNets is the low computational complexity. MSM algorithm performs a linear search on the preference list of each UE and of each subcarrier; thus, the total maximum run-time of the MSM algorithm for a  $K$  UE and  $N$  subcarrier system is  $\mathcal{O}(KN)$ . The computational complexity in the sorting process for preference list preparation is  $\mathcal{O}((N-1)\log(N-1))$  for each UE. The overall computational complexity of sorting is  $\mathcal{O}(K(N-1)\log(N-1))$ . Hence, the total SM complexity can be obtained as  $\mathcal{O}(KN\log(N-1))$ .

In previous studies, it was shown that MSM algorithm achieves a very good performance even when the preference lists are incomplete [70,71]; however, to the best of our knowledge, the data overhead on the feedback channel has not been considered before. Thus, MSM algorithm is examined for a CA HetNet scenario that has reduced feedback CSI in Section 2.3.2. Furthermore, a quick analysis reveals that UEs are matched to their first or second most desired subcarriers in their preference lists by a probability of about 70%. This has the potential to allow for successful operation with partial CSI. The reliability of the preference lists is also very critical for the MSM algorithm. Unlike previous studies, the impact of channel estimation errors on the MSM algorithm is also investigated for a CA HetNet in Section 2.5. Stability and rate satisfaction of each UE and the overall HetNet is analyzed in order to determine the effect of partial feedback CSI on the HetNet. Using PFM (Figure 2.2) instead of MSM (Figure 1.2) for allocation in a HetNet that has users with partial preferences, decreases the stability concern in a network significantly. An explanatory basic example of MSM is given in Example 3.

**Example 3.** *Let  $N = 6$  subcarriers be assigned to  $K = 3$  UEs in a many-to-one stable*

matching. Let the preference lists be obtained as

$$\begin{aligned}\gamma_1^u &= \{1, 2, 4, 3, 5, 6\}, \\ \gamma_2^u &= \{2, 1, 6, 3, 4, 5\}, \\ \gamma_3^u &= \{3, 1, 6, 2, 5, 4\},\end{aligned}\tag{2.11}$$

$$\begin{aligned}\gamma_1^{sc} &= \{2, 1, 3\}, \\ \gamma_2^{sc} &= \{3, 2, 1\}, \\ \gamma_3^{sc} &= \{1, 2, 3\}, \\ \gamma_4^{sc} &= \{3, 2, 1\}, \\ \gamma_5^{sc} &= \{1, 3, 2\}, \\ \gamma_6^{sc} &= \{1, 3, 2\}.\end{aligned}\tag{2.12}$$

Eventually, the matching matrix is obtained as

$$\mathbf{M}^{MSM} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}.\tag{2.13}$$

### 2.3.2. Partial Feedback Matching based Carrier Aggregation

In MSM algorithm, the preference lists are obtained by using full CSI, which are assumed to be perfectly known by both subcarriers at BSs and UEs. As mentioned before, MSM algorithm assigns each UE to its first or second preference by a probability of 70%. Starting from this point, in PFM algorithm, it is assumed that each UE has  $(f/N)$ — partial feedback CSI including top- $f$  preferences of each UE are considered,

where  $f \leq N$ , i.e.,  $f = (N - 1)$ , corresponds to full CSI transmission<sup>1</sup>. The preference list of the  $k^{\text{th}}$  UE is obtained by the  $(f/N)$ – partial feedback CSI as

$$\succ_k^{u,f} = \{C_{k,1} \succ \dots \succ C_{k,f}\}, \quad k \in K, \quad (2.14)$$

where  $C_{k,f}$  is the  $\log_2 N$  bits long binary feedback information of the channel between the  $k^{\text{th}}$  UE and the  $f^{\text{th}}$  ranked subcarrier. In order to obtain the full preference list of each UE in a HetNet that has  $K$  UEs and  $N$  subcarriers,  $(N - 1)\log_2 N$  bits are needed. Thus, the total feedback gain of the system,  $G_f$ , when there is an  $(f/N)$ – partial feedback CSI, is calculated as

$$G_f = ((N - 1) - f)K\log_2 N \text{ [bits]}. \quad (2.15)$$

Partial feedback CSI decreases the feedback data overhead significantly. By using this motivation, we assume that full CSI corresponding to each UE is perfectly known while the CSI corresponding each subcarrier may be partially received in order to decrease the data overhead on the feedback uplink channel. Thus, PFM algorithm is proposed as a robust variation of MSM algorithm as in Figure 2.3. PFM algorithm starts with the proposals of each UE to their most preferred preferences in the corresponding lists as in the original SM algorithm. The proposals of all UEs at step  $t$  are saved in a proposal list,  $X^{UE,t}$ . Considering that each UE feedback only the best  $f$  CSI to BSs, subcarrier has a partial preference list and UEs have complete preference lists. After SM with partial CSI, the remaining subcarriers are assigned by considering the instantaneous individual fairness index. Subcarriers are assigned to the UE that

---

<sup>1</sup>The feedback information of  $(N - 1)$  subcarriers is sufficient to know the all information in a scenario with  $N$  subcarriers.

has minimum fairness index as

$$M(\arg \min_k \{\phi_k^r\}, \hat{n}) = 1, \quad k \in \mathcal{K}, \quad (2.16)$$

where  $\hat{n}$  is an unassigned subcarrier. Different from MSM, a UE is not restricted with a quota after partial stable matching. The algorithm ends when all subcarriers are assigned to a UE. An explanatory basic example of MSM is given in Example 4

**Example 4.** *Let the same parameters in Example 3 be used in this example. However, the preference lists of UEs are partially feed backed as*

$$\begin{aligned} \succ_1^u &= \{1, 2, \dots\}, \\ \succ_2^u &= \{2, 1, \dots\}, \\ \succ_3^u &= \{3, 1, \dots\}. \end{aligned} \quad (2.17)$$

*Assume that, the fairness indices after the matchings with the partial CSI are calculated as*

$$\begin{aligned} \phi_1^r &= 0.023, \\ \phi_2^r &= 0.456, \\ \phi_3^r &= 0.253. \end{aligned} \quad (2.18)$$

*The unassigned subcarriers are  $n = \{4, 5, 6\}$ . The UE  $k = 1$  has the minimum fairness index, thus one of the unassigned subcarriers,  $n = 4$  is assigned to UE  $k = 1$ . Then the fairness index is calculated as  $\phi_1^r = 0.123$ . The minimum fairness index still belongs to the UE  $k = 1$ . Then,  $n = 5$  is assigned to UE  $k = 1$ , as well. Now, the fairness index is calculated as  $\phi_1^r = 0.223$ . Then,  $n = 6$  is assigned to UE  $k = 1$ . Eventually,*



the matching matrix is obtained as

$$\mathbf{M}^{PFM} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}. \quad (2.19)$$

,the fairness index is calculated as  $\phi_1^r = 0.123$ .

## 2.4. Stability Analysis of PFM

In PFM algorithm, partial feedback information may or may not provide a fully stable matching. By considering this, a special form of stability is defined according to the partial preferences by using a degree of instability in [86].

**Definition 5.** Let  $\mu_{k,S_q^k} = 1$  (for any  $q \in \{1, 2, \dots, Q_k\}$ ), where  $S_q^k$  is the ID of the assigned subcarrier to the  $k^{th}$  UE and belongs to the set of assigned subcarriers to  $k$ ,  $\mathcal{S}^k$  ( $S_q^k \in \mathcal{S}^k$ ) and  $\hat{n} \notin \mathcal{S}^k$ . The rank difference between  $S_q^k$  and  $\hat{n}$  in the preference list of  $k$  is referred as pairwise-regret (PR) and is defined as

$$PR(k, \hat{n}, S_q^k, \succ_k^u) = \{rank(S_q^k, \succ_k^u) - rank(\hat{n}, \succ_k^u)\}, \quad (2.20)$$

where  $rank(x, \succ_y)$  is the rank of the value  $x$  in the preference list of  $y$  ( $\succ_y$ ). If  $PR(k, \hat{n}, S_q^k, \succ_k^u) < 0$ , there is no regret from the view of the  $k^{th}$  user for the assignment of  $S_q^k$  compared to unassigned subcarrier  $\hat{n}$ .

**Definition 6.** For any given assignments  $\mu_{k,S_q^k} = 1$  and  $(\hat{n}, U_{\hat{n}})$ , where  $U_{\hat{n}}$  is the ID of the assigned UE to the subcarrier  $\hat{n}$  and  $\hat{n} \notin \mathcal{S}^k$ , the pairwise instability of  $k$  and  $\hat{n}$ ,  $PI(k, \hat{n}, S_q^k, \succ_k^u, \succ_{\hat{n}}^{sc})$  is the minimum of the PR values of  $k$  and  $\hat{n}$

$$PI(k, \hat{n}, S_q^k, \succ_k^u, \succ_{\hat{n}}^{sc}) = \min\{PR(k, \hat{n}, S_q^k, \succ_k^u), PR(\hat{n}, k, U_{\hat{n}}, \succ_{\hat{n}}^{sc})\}. \quad (2.21)$$

```

1: Initialization:  $k \in \mathcal{K}$ ,  $n \in \mathcal{N}$ ,  $N \geq K$ ,  $Q_k \leq N$ ,  $t = 0$ ,  $N'$ : set of unassigned subcarriers.
2:  $X^{SC,t}$ : proposal list of subcarriers at step  $t$ , respectively.
3:  $\alpha_n^{sc}$ : proposal rank of the  $n^{\text{th}}$  subcarrier ( $\alpha_n^{sc} = 1$  at  $t = 0$ )
4:  $\alpha_k^u$ : proposal rank of the  $k^{\text{th}}$  UE ( $\alpha_k^u = 1$  at  $t = 0$ )
5:  $\succ_n^{sc}$ : preference list of the  $n^{\text{th}}$  subcarrier
6:  $\succ_k^{u,f}$  ( $f/N$ )—partial preference list of the  $k^{\text{th}}$  UE
7:  $\rho_x$ : number of proposals to  $x \in \mathcal{K} \cup \mathcal{N}$ .
8:  $k'$ : most desired UE (lowest ranked) on  $\succ_{n'}^{sc}$ .
9:  $\phi^k$ : Jain's fairness index
10: while  $\forall Q_k \neq \emptyset$  do
11:   if  $X^{SC,t} == \emptyset$  then
12:     Unassigned subcarriers,  $S^u$ , are determined
13:     while  $\{S^u \neq \emptyset\}$  do
14:       Calculate  $\phi^k$ ,  $\forall k$ 
15:        $n \in S^u$  is assigned to  $k' = \arg\min(\phi^k)$ 
16:        $\mu_{k',n} = 1$ .  $n$  is removed from  $S^u$ ,
17:        $Q_{k'} = Q_{k'} - 1$ .
18:     end while
19:   else
20:     Each  $k \in K$  ( $Q_k \neq 0$ ), makes proposal to,  $X^{UE,t}$ .
21:     for  $n' \in X^{UE,t}$  do
22:       if  $\rho_{n'} > 1$  then
23:         if  $\mu_{U_{n'},n'} = 1$  then
24:           if any new proposer,  $k'$ ,  $\succ_{n'}^{sc} U_{n'}$  then
25:              $n'$  is assigned to the UE  $k'$ 
26:              $\mu_{U_{n'},n'} = 0$ ,  $\mu_{k',n'} = 1$ 
27:              $Q_{U_{n'}} = Q_{U_{n'}} + 1$ ,  $Q_{k'} = Q_{k'} - 1$ .
28:           end if
29:         else
30:            $n'$  is assigned to the most desired UE  $k'$ 
31:            $\mu_{k',n'} = 1$ ,  $Q_{k'} = Q_{k'} - 1$ .
32:         end if
33:          $\alpha_{k'}^u = \alpha_{k'}^u + 1$ , where  $k' \in K$ 
34:       else
35:         if  $\mu_{U_{n'},n'} = 1$  then
36:           if the new proposer,  $k'$ ,  $\succ_{n'}^{sc} U_{n'}$  then
37:              $\mu_{U_{n'},n'} = 0$ ,  $\mu_{k',n'} = 1$ 
38:              $Q_{U_{n'}} = Q_{U_{n'}} + 1$ ,  $Q_{k'} = Q_{k'} - 1$ .
39:           end if
40:         else
41:            $n'$  is assigned to the proposer UE.
42:            $\mu_{k',n'} = 1$ ,  $Q_{k'} = Q_{k'} - 1$ .
43:         end if
44:          $\alpha_{k'}^u = \alpha_{k'}^u + 1$ , where  $k' \in K$ 
45:       end if
46:     end for
47:   end if
48:    $t = t + 1$ .
49: end while

```

Figure 2.3. Proposed PFM Algorithm for HetNets

**Definition 7.** According to the Definitions 3 and 6,  $\{k, S_q^k\}$  and  $\{U_{\hat{n}}, \hat{n}\}$  assignments are called “pairwise-stable”, if  $PI(k, \hat{n}, S_q^k, \succ_k^u, \succ_{\hat{n}}^{sc}) < 0$ ; otherwise, there is a blocking assignment  $(k, \hat{n})$  and accordingly an instability occurs in the network.

In order to be able to determine the stability of the whole HetNet, the existence of blocking assignment is saved as a pairwise blocking index of the  $k^{\text{th}}$  UE for an assigned subcarrier  $S_q^k$  compared to an unassigned subcarrier  $\hat{n}$ ,  $PB_{S_q^k, \hat{n}}^k$  as

$$PB_{S_q^k, \hat{n}}^k = \begin{cases} 1, & \text{if } PI(k, \hat{n}, S_q^k, \succ_k^u, \succ_{\hat{n}}^{sc}) > 0, \\ 0, & \text{otherwise.} \end{cases} \quad (2.22)$$

Note that,  $(k, S_q^k)$  is a blocking assignment if there is at least one  $PB_{S_q^k, \hat{n}}^k = 1$  for any  $\hat{n} \notin \mathcal{S}^k$ . Thus, blocking index of an assignment of  $(k, S_q^k)$  is

$$BI_{S_q^k}^k = \begin{cases} 1, & \text{if } \max_{\hat{n}} \{PB_{S_q^k, \hat{n}}^k\} = 1, \quad \hat{n} \notin \mathcal{S}^k, \\ 0, & \text{otherwise.} \end{cases} \quad (2.23)$$

Considering that a UE may be assigned more than one subcarriers, the UE may have stable and blocking assignments together. To be able to determine the stability of a UE, all assigned subcarriers of UE should be taken into account. By using blocking index of each assignment, an individual dissatisfaction ratio of a UE is obtained as

$$\beta_k = \frac{\sum_{q=1}^{Q_k} BI_{S_q^k}^k}{Q_k}. \quad (2.24)$$

Accordingly, an individual instability for the  $k^{\text{th}}$  UE can be defined by using individual rate dissatisfaction ratio as in Definition 8.

**Definition 8.** A UE  $k$  is individually stable if all of its assignments are stable ( $\beta_k = 0$ ) while a UE  $k$  is referred to as individually unstable, if all are blocking assignments ( $\beta_k = 1$ ). When a UE has both stable and blocking assignments at the end of the algorithm ( $0 < \beta_k < 1$ ), the UE is referred as individually partial stable.

A UE is assumed to be dissatisfied at the end of PFM, if the individual dissatisfaction ratio of a UE,  $\beta_k$ , is greater than zero. Then, the dissatisfaction index of each UE is obtained as

$$DI^k = \begin{cases} 1, & \text{if } \beta_k > 0, \\ 0, & \text{otherwise} \end{cases} \quad (2.25)$$

In the same manners, the average user dissatisfaction  $D$  of a network can be calculated by using the dissatisfaction indices of all UEs as  $D = \frac{\sum_{k=1}^K DI^k}{K}$ . Hence, the total network instability,  $NI$ , can be calculated by using the average of the individual instability results of all UEs as

$$NI = \frac{\sum_{k=1}^K \beta_k}{K}. \quad (2.26)$$

By considering these useful definitions, we can finally define the network stability, similarly, as in Definition 8, as

**Definition 9.** A network is stable, if and only if all UEs in the network are individually stable, while a network is unstable if all UEs are individually unstable. Finally, a network is partially stable, if some UEs in the network are individually partial stable.

Instability of a network has significant effects on the rate and accordingly QoS. Instability causes both individual rate loss and accordingly an overall network rate loss.

Individual rate loss of each UE can be obtained by using pairwise blocking indices as

$$RL^k = \sum_{q=1}^{Q_k} \max_{\hat{n}} \left\{ \log_2 \frac{1 + c_k(\hat{n})}{1 + c_k(S_q^k)} PB_{S_q^k, \hat{n}}^k \right\}. \quad (2.27)$$

The overall rate loss for the network,  $L$ , is the sum of individual rate losses for each UE of the network as

$$L = \sum_{k=1}^K RL^k. \quad (2.28)$$

PFM algorithm provides prominent decrease on the rate loss by decreasing the instability of the network in case of partial preferences. Additionally, the run-time complexity of the proposed PFM algorithm is the same as that of the classical SM algorithms. In classical SM algorithm (one-to-one assignment), each UE makes a proposal at each step until it is assigned to a subcarrier. In the worst case, there are  $K$  proposals and there is only one assignment in each step. Therefore, the algorithm ends in at most  $K$  steps with  $K$  proposals in each. Thus, the run-time complexity is  $\mathcal{O}(K^2)$  for the worst case when there are  $K$  UEs and  $K$  subcarriers in the network. Even if a UE requires multiple subcarriers, the run-time complexity can be obtained similarly as  $\mathcal{O}(KN \log(N - 1))$  when there are  $K$  UEs and  $N$  subcarriers in the network ( $K < N$ ).

For the proposed PFM algorithm,  $K$  UEs make  $K$  proposals for the first  $f$  steps and in the worst case if there is one assignment in each  $f$  step, there are  $(N - f)$  unassigned subcarriers remaining. Consequently, the run-time complexity of UE proposals is  $\mathcal{O}(Kf)$ . Note that, there is no quota for the proposed UE after partial matchings as in Figure 2.3. For the proposals of the subcarriers, there are  $(N - f)$  proposals in each step and there are at most  $K$  entries in the preference list of each subcarrier. Thus, the run-time complexity for the proposals of the subcarriers is  $\mathcal{O}((N - f)K)$ . Hence, the total run-time complexity of the PFM algorithm is the same as the many-to-one

extension of SM algorithm,  $\mathcal{O}(KN\log(N-1))$ . As a result, the robustness of MSM algorithm against instability due to the partial preferences are increased by the proposed PFM algorithm with no additional run-time complexity. The corresponding instability results for different partial feedback transmissions are shown in Section 2.6.

## 2.5. Robustness of PFM Against Channel Estimation Error

In classical approaches, preference lists employed in the SM algorithm are assumed to be fixed and channel corruptions are not included [4]. Authors in [87] focused on the energy consumption of the feedback channel; however, they did not consider any fairness or stability results under unfavorable feedback channel conditions. As a more realistic scenario, effects of channel estimation errors on the preference lists are considered in this section. Let  $\tilde{h}_{k,n}$  be the estimated channel gain of the  $n^{\text{th}}$  subcarrier as observed by the  $k^{\text{th}}$  UEs. Accordingly, the erroneous preference lists are considered using

$$\tilde{p}_{k,n} = |\tilde{h}_{k,n}|^2, \quad (2.29)$$

where  $\tilde{h}_{k,n} = h_{k,n} + \epsilon_{k,n}$  and  $\epsilon_{k,n}$  is the channel estimation error, which is assumed to be complex Gaussian distributed with zero mean and variance  $\sigma_\epsilon^2$ . An illustrative example is given in Example 5.

**Example 5.** *Let there be  $K = 2$  UEs and  $N = 4$  subcarriers in one CC in the system. Assume the preference lists of UEs and CCs,  $\succ_k^u$  and  $\succ_n^{sc}$ , respectively, to be,*

$$\begin{aligned} \succ_1^u &= \{4, 2, 3, 1\}, \\ \succ_2^u &= \{1, 4, 2, 3\}, \end{aligned} \quad (2.30)$$

$$\begin{aligned} \succ_1^{sc} &= \{2, 1\}, \\ \succ_2^{sc} &= \{1, 2\}, \\ \succ_3^{sc} &= \{1, 2\}, \\ \succ_4^{sc} &= \{2, 1\}. \end{aligned} \quad (2.31)$$

Assume that the CSI is disturbed by a complex Gaussian estimation error with zero mean and variance of  $\sigma_\epsilon^2$ , thus the erroneous channel coefficients are

$$|\tilde{h}_{k,n}| = |h_{k,n} + \epsilon_{k,n}|. \quad (2.32)$$

Preference lists of UEs and CCs,  $\succ^{u,E}$  and  $\succ^{sc}$ , can be obtained from (2.6) and (2.7) by using the erroneous channel matrix,  $\tilde{\mathbf{H}}$ , as

$$\begin{aligned} \succ_1^{u,E} &= \{3, 4, 2, 1\}, \\ \succ_2^{u,E} &= \{1, 3, 4, 2\}, \end{aligned} \quad (2.33)$$

$$\begin{aligned} \succ_1^{sc} &= \{2, 1\}, \\ \succ_2^{sc} &= \{2, 1\}, \\ \succ_3^{sc} &= \{1, 2\}, \\ \succ_4^{sc} &= \{2, 1\}. \end{aligned} \quad (2.34)$$

After PFM algorithm is applied, the matching matrix  $\tilde{\mathbf{M}}$  can be obtained as

$$\mathbf{M}^{PFM} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}, \quad (2.35)$$

If ORA is applied, the matching matrix is obtained as

$$\mathbf{M}^{ORA} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \quad (2.36)$$

PFM algorithm has still better performance than ORA in terms of fairness, since each UE has a weight 2, while, with ORA, first UE is assigned to three subcarriers, and the second UE is assigned to one subcarrier. Hence, PFM algorithm is indeed, a robust

algorithm against the corruptions or destructions on the feedback channel. According to the matching matrix, the second UE is matched with subcarriers  $S_1^2 = 1$  and  $S_2^2 = 2$ . Unfortunately, matchings  $\mu_{2,2}$  and  $\mu_{1,4}$  create a blocking assignment. According to the instability equations in Section 2.3.2, the pairwise instability of  $k$  and  $\hat{n}$  is obtained as  $PI(2, 4, 2, \succ_2^u, \succ_4^{sc}) > 0$ . Then, pairwise blocking index of the second UE for an assigned subcarrier is 2 compared to an unassigned subcarrier 4,  $PB_{2,4}^2 = 1$ . On the other hand, there is no blocking assignment between  $\mu_{2,2}$  and  $\mu_{3,1}$ , resulted as  $PI(2, 3, 2, \succ_2^u, \succ_3^{sc}) < 0$ . Accordingly, the blocking index of the 2<sup>nd</sup> UE is  $BI_2^2 = 1$ . Similarly, The blocking index of the 1<sup>st</sup> UE is calculated as  $BI_1^2 = 0$ . Thus, the 2<sup>nd</sup> UE is individually partial stable. The individual dissatisfaction ratio of the 2<sup>nd</sup> UE is calculated as  $\beta_k = 0.5$ . the network instability and dissatisfaction ratio are calculated as  $NI = 0.25$  and  $D = 0.5$ , respectively. As a results, the overall network is also partial stable.

## 2.6. Simulation results

In this section, the proposed approaches are evaluated under realistic system parameters for subcarrier allocation in a CA LTE-A HetNet. According to 3GPP standardizations, each frequency band of five CCs can have different bandwidths such as  $\{1.4, 3, 5, 10, 15, 20\}$  MHz and support different number of subcarriers,  $\{128, 256, 512, 1024, 1536, 2048\}$ , respectively [35]. Although 3GPP proposed CA of up to five CCs to reach a maximum bandwidth of 100 MHz, the specifications in Release-15 for CA scenarios consider only two CCs for dual uplink [35]. For being consistent with the state-of-the-art standardization studies, the simulation results are obtained for two CCs in uplink, unless otherwise is stated.

In this thesis, the proposed algorithm is examined for different interband noncontiguous CA scenarios. According to [88], femto and pico base stations can provide 32 users. Without loss of generality, we use the pico base station parameters and set the number of users as  $K = 32$ , which is also divisible by the number of subcarriers. The transmit power of the subcarriers is assumed to be  $P_n = 1W$ . The proposed algorithm is compared with the two algorithms, ORA and PF, which are widely used for resource



allocation problems in the literature. ORA is also widely used as the simplest resource allocation approach, which assigns each subcarrier to the UE that has the best channel. However, ORA does not consider fairness. In case of partial CSI, ORA assign subcarriers randomly to the UEs. Another popular resource allocation algorithm is PF algorithm [89]. The PF algorithm compares the ratio of the feasible rate for each UE with its average throughput, which is defined as the preference metric. The subcarriers are assigned to the UE with the maximum preference metric. Although PF has significant enhancement on fairness, it is not robust for partial feedback cases.

In the first scenario, two CCs belong to two different SBSs, which both use the frequency band 2.1 GHz. All UEs and CCs in the network have full CSI unless otherwise stated. In Figures 2.4, 2.5, and 2.6, fairness and rate performances of PFM algorithm are illustrated and compared with ORA and PF for various SNR values. Total Jain's fairness and the rate of the network are obtained by using (2.1) and (2.9). Jain's fairness index [90] is defined as  $f^i(t) = (\sum_{k=1}^K r_k^i(t))^2 / K \sum_{k=1}^K (r_k^i(t))^2$ , which is a positive fraction that takes a value of 1 only if all the  $K$  users in the cell have exactly the same instantaneous rate. In Figure 2.4, fairness of the PFM algorithm is slightly better than PF algorithm, while it has much more fair results when compares to ORA. The improvement on the fairness performance increases as the number of subcarriers decreases.

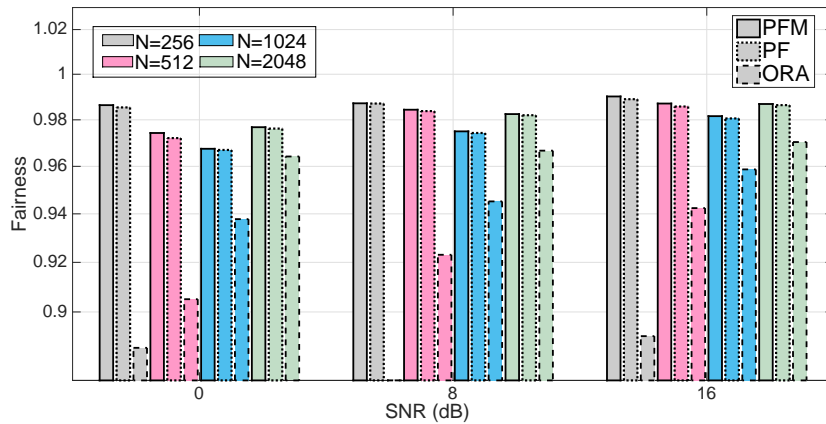


Figure 2.4. Fairness comparisons of PFM algorithm and ORA (a) for  $K=32$  UEs and  $N=\{256, 512, 1024, 2048\}$  subcarriers.

In Figure 2.5, the fairness performances of PFM, PF, ORA are illustrated for  $N = 512$  subcarriers and various number of UEs active in the network ( $K = 8, 16, 32, 64, 128, 256$ ) when SNR is 0 dB. The fairness performance gap between PFM and ORA algorithms is increased as  $K$  increases. Although rate loss increases as the number of subcarriers increases, as expected, the rate performance of PFM algorithm has a minimal loss when it is compared to the ORA. The rate performance is better than PF, as shown in Figure 2.6.

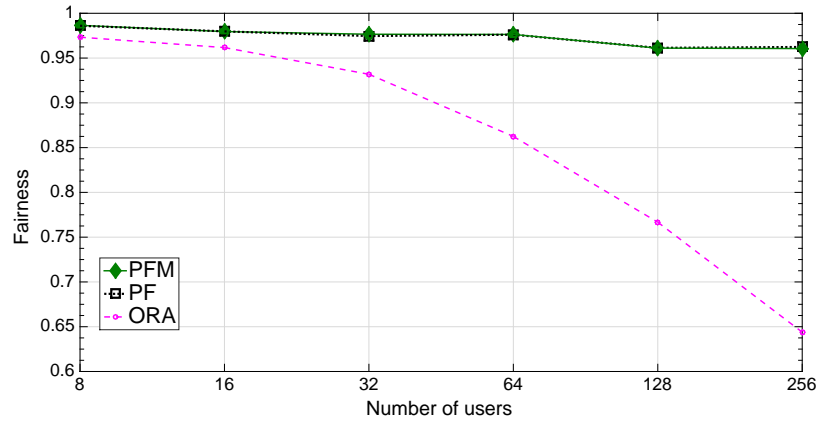


Figure 2.5. Fairness performances are illustrated for various number of UEs.

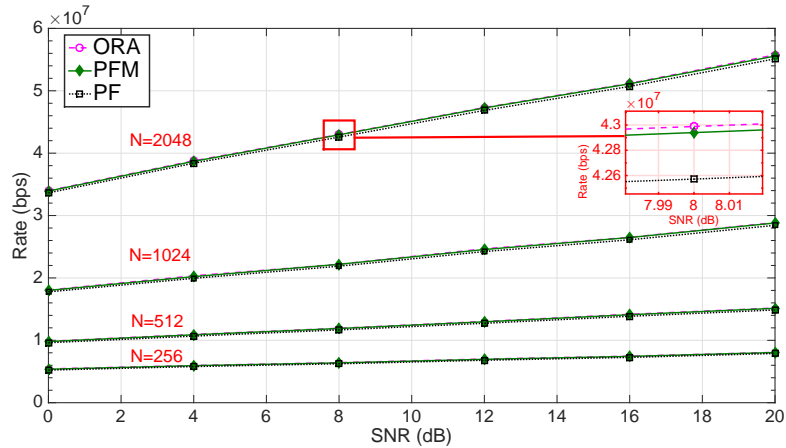


Figure 2.6. Rate comparison of PFM, PF, ORA for  $K = 32$  UEs and  $N = \{256, 512, 1024, 2048\}$  subcarriers.

Unless otherwise stated, we consider a noncontiguous CA HetNet model for our next simulation results, where all  $N$  subcarriers belong to the two CCs of each 10 MHz frequency bands on 800 MHz (MBS) and 2.1 GHz (SBS). In order to reduce the feedback overhead, the CA LTE-A system performance is examined when UEs have

partial preference lists. The rate and fairness performances of  $(2/N)$ -PFM, ORA, PF in Figure 2.7 and Figure 2.8 are obtained for  $K = 32$  UEs and  $N = 2048$  subcarriers. It is assumed that all algorithms are examined for the case, in which only the best  $f = 2$  subcarriers on the preference list of each UE are transmitted as feedback. The rate performance of the proposed PFM algorithm slightly decreases in case of partial feedback. On the other hand, the fairness performance of  $(2/N)$ -PFM algorithm is outperforming  $(N/N)$ -PFM, ORA, and PF on fairness, as expected. PF algorithm has a significant loss on fairness performance. Note that,  $(N/N)$ -PFM equals to MSM when  $f = N$ .

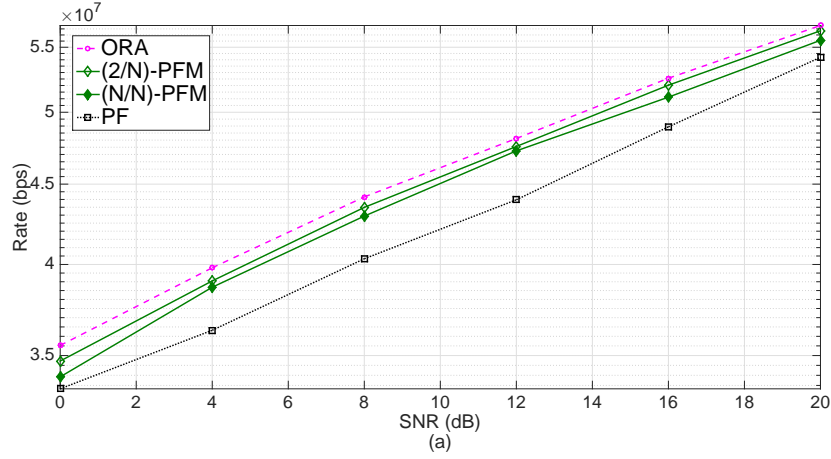


Figure 2.7. Rate performance of  $(2/N)$ -partial CSI feedback for  $K = 32$  UEs  $N = 2048$  subcarriers.

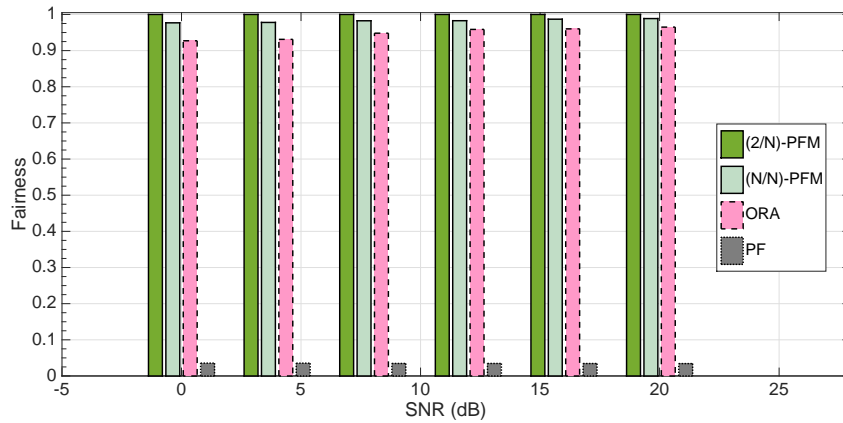


Figure 2.8. Fairness performance of  $(2/N)$ -partial CSI feedback for  $K = 32$  UEs  $N = 2048$  subcarriers.

The impact of the number of subcarrier feedbacks is illustrated in Figure 2.9 and Figure 2.10. There are  $N = 2048$  subcarriers active in the network. The data overhead

on the feedback channel is calculated by using (2.15). The data overhead on the feedback channel is decreased significantly and the total feedback gain for  $(2/N)$ -PFM as  $G_2 = ((2047) - 2) \times 32 \times \log_2 2048 = 720544$  bits. Results show that the rate performance is still above 44 Mbps if  $f = 256$  partial feedback with a feedback gain of  $G_{256} = 630432$  bits is employed. Thus, feedback data overhead decreases almost 87%. Similarly, the rate loss,  $L$ , can be acceptable when the feedback gain is significantly high. According to Figure 2.10, the rate performance of  $(256/2048)$ -PFM is still over 95% compared to  $(N/N)$ -PFM. Thus, a proper feedback data decrement by using partial preferences relaxes the data overhead significantly and also provides high data rates as well.

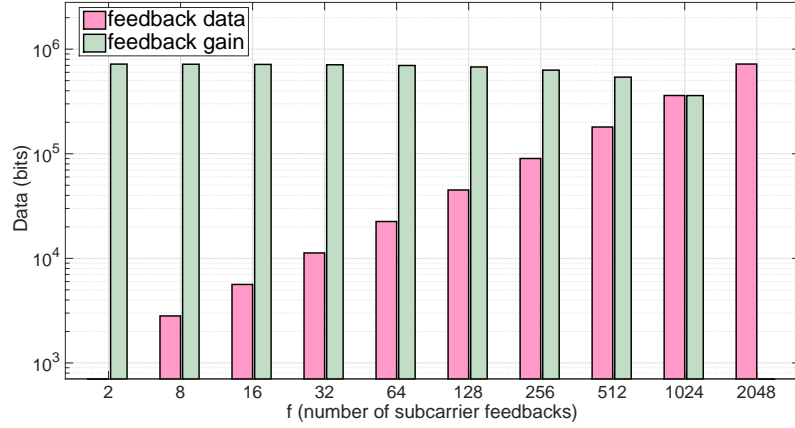


Figure 2.9. Feedback gain is shown when various number of subcarrier feedbacks with  $f/N$ -PFM algorithm for a CA HetNet of  $K = 32$  UEs and  $N = 2048$  subcarriers.

The robustness of  $(2/N)$ -PFM algorithm against the channel distortions is illustrated for a CA HetNet in Figures 2.11 and 2.12 for the systems with different number of subcarriers,  $N = \{256, 512, 1024, 2048\}$ , when SNR is 0 dB. All three algorithms are very robust to the channel distortions when only  $f = 2$  subcarrier informations received as a feedback via the erroneous channel, as seen in Figure 2.11.  $(2/N)$ -PFM algorithm outperforms PF in terms of rate, while ORA outperforms PFM and PF, as expected.

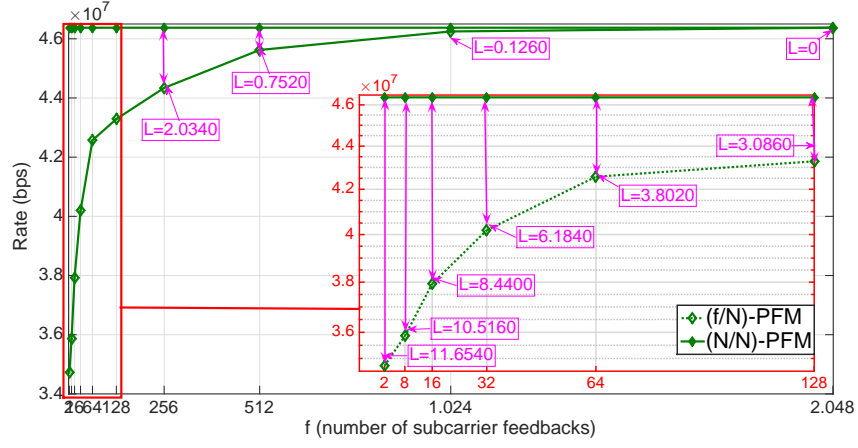


Figure 2.10. Rate performances is shown when various number of subcarrier feedbacks with  $f/N$ -PFM algorithm for a CA HetNet of  $K = 32$  UEs and  $N = 2048$  subcarriers.

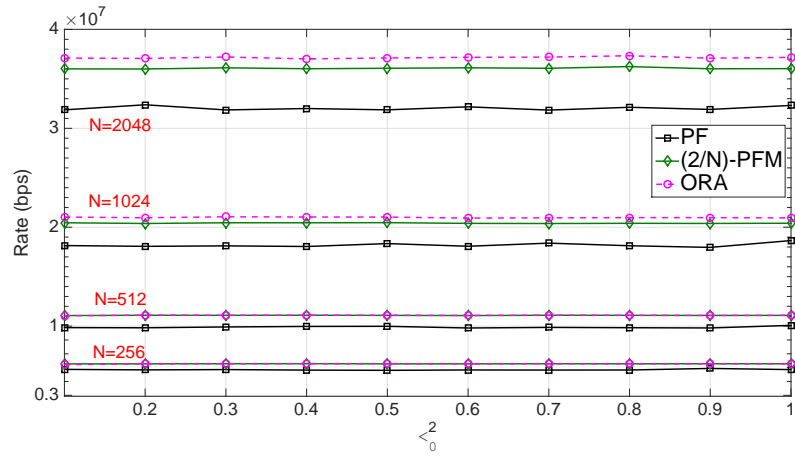


Figure 2.11. Rate performances with  $K = 32$  UEs and  $N = \{256, 512, 1024, 2048\}$  subcarriers for different  $\sigma_\epsilon^2$ .

In Figure 2.12, the fairness of the system is slightly decreased as the channel distortion increases. Note that the impact of the number of subcarrier feedbacks are much bigger than the impact of the channel distortions. Thus, rate loss is seen clearly in case of low number of subcarrier feedbacks, while it is hardly visible for noisy environment.

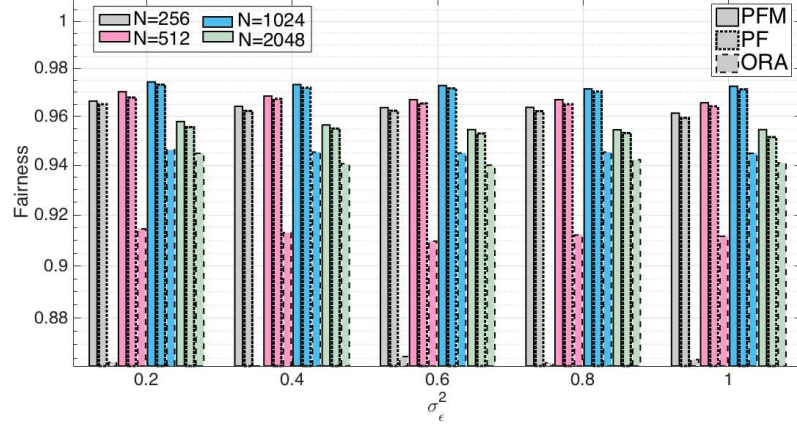


Figure 2.12. Fairness performances with  $K = 32$  UEs and  $N = \{256, 512, 1024, 2048\}$  subcarriers for different  $\sigma_\epsilon^2$ .

The performance comparisons of PFM, ORA, and PF approaches are illustrated in Figure 2.13 for a CA HetNet with  $K = 32$  UEs and  $N = 2048$  subcarriers, when  $\sigma_\epsilon^2 = 0.5$ . For  $(N/N)$ -PFM with erroneous CSI, the loss on the rate and fairness performances are acceptable for such a HetNet. As expected, the performance of the PFM algorithm with erroneous CSI is almost the same with the PFM algorithm. The effect of partial CSI is much more than the channel estimation when considering that the effect of PFM on the network.

Finally, the instability results for  $(f/N)$ -PFM, PF, and ORA are illustrated in Figure 2.14 and Figure 2.15 by considering an erroneous channel with  $\sigma_\epsilon^2 = 0.5$ . In Figure 2.14, the average user dissatisfaction (D) of  $(f/N)$ -PFM decreases as the number of subcarrier feedbacks increases, while the average user dissatisfaction of PF increases, as expected.  $(f/N)$ -PFM reduce the average number of dissatisfied UE, in the network compared to  $(N/N)$ -PFM for both low and high number of subcarriers are active in the network.

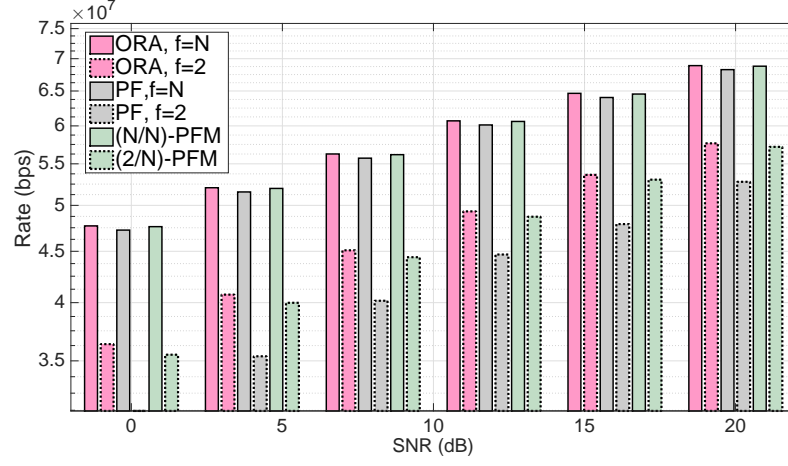


Figure 2.13. Rate performances with  $K = 32$  UEs and  $N = 2048$  subcarriers for  $\sigma_\epsilon^2 = 0.5$ .

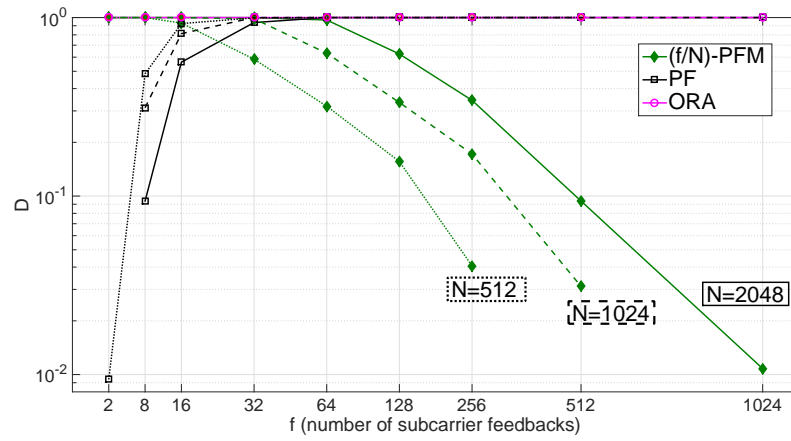


Figure 2.14. The average user dissatisfaction results for 32 UEs and various subcarriers considering different amount of partial feedback CSI.

In Figure 2.15, the rate (a) and network instability ( $NI$ ) (b) results are obtained in terms of the number of unstable assignments when different number of subcarrier feedbacks are transmitted by using (2.26). Note that  $NI = 0$ , when the number of subcarrier feedbacks is equal to  $N$  ( $(f/N)$ -PFM). The rate of all algorithms increase as the number of subcarrier feedbacks increases as expected. The proposed  $(f/N)$ -PFM algorithm explicitly outperforms the other algorithms in terms of rate and network instability when the number of subcarrier feedbacks is greater than 16, as shown in Figure 2.15 (b). Regardless of the number of active subcarriers in the network, PFM manages to reduce the instability ratio significantly.

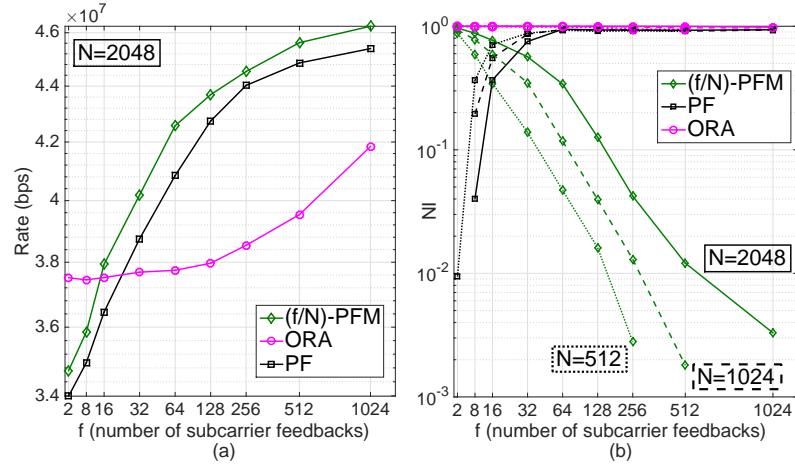


Figure 2.15. Rate (a) and Network instability (b) results for 32 UEs and various subcarriers considering different amount of partial subcarrier feedbacks.

## 2.7. Conclusions

Although CA HetNets achieve high data rates, there are still some handicaps in realistic systems such as complexity, fairness, and rate management on the resource allocation. In this thesis, an important variation of the MSM algorithm is proposed as PFM algorithm, which allows to partial preferences in order to decrease the data overhead on feedback channel in dual uplink inter band noncontiguous CA HetNet scenarios. PFM algorithm is proposed in order to achieve a fair or rate based allocation with a low complexity. The results of the rate and fairness performances of PFM algorithm are compared with those of the ORA and PF. The rate of the PFM algorithm is less than the ORA and almost the same with PF, as expected; however, it can pro-



vide fair resource allocation especially for small number of UEs and subcarriers in the system. Unlike the previous studies, PFM algorithm is examined under a noisy environment with reduced feedback CSI from realistic perspectives. Our results show that PFM algorithm is much more robust against partial CSI feedback when it compares with PF. Different from the previous studies, individual stability, partial stability, and the average network stability concerns are analyzed. The given individual stability definitions are very useful in order to obtain the average rate dissatisfaction of a network and the average network instability. Our results show that the proposed  $(f/N)$ -PFM algorithm has high performance in terms of network instability when compared with the ORA and PF, when the number of subcarrier feedbacks is greater than  $f > 16$ .

### 3. SECURE STABLE MATCHING ALGORITHM IN CARRIER AGGREGATED HETEROGENEOUS NETWORKS

#### 3.1. Motivation

CA is proposed to address the tremendous demands for high data rates in resource limited HetNets. Although the resource allocation problem for CA HetNets has been studied in the literature before, there are still many open challenges, including security threats. Thus, in this study, a trust-based SM approach is proposed as a solution for selfish user threats in a CA HetNet. The proposed approach aims to provide secure communication to honest users by using a trust index for each user to identify and gradually punish the selfish users. 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 SM 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 this study.

#### 3.2. System Model for a Secure Scenario

The system under consideration is a CA HetNet with  $K$  users that are uniformly distributed on a concurrent area of an LTE-Advanced SBS and an MBS, as seen in Figure 3.1. MBS is positioned at (0m, 0m), while SBS is positioned at (50m, 50m). All users are assumed to be LTE-Advanced users, and thus are able to communicate with multiple CCs. The possible selfish users are visualized as red, while the honest users are green. The gray users are not able to make CA, since their positions are outside of

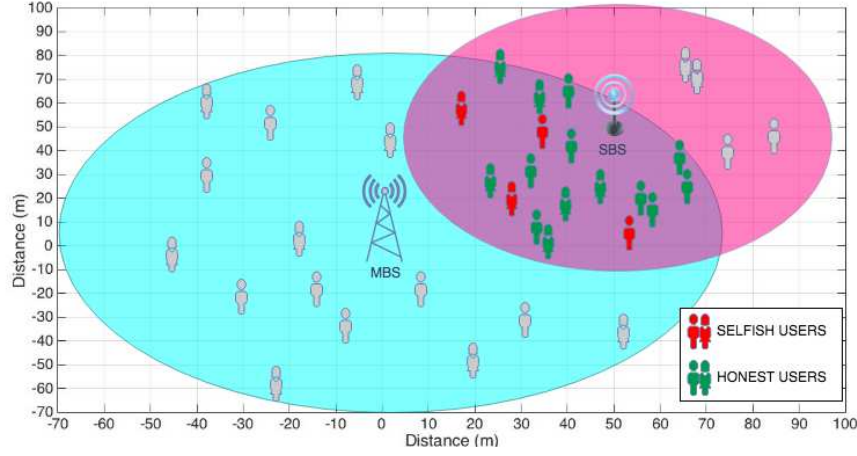


Figure 3.1.  $K$  users, including  $L$  selfish users, are uniformly distributed in the coverage area  $([-50, 50] \text{ m})$ , where LTE SBS and MBS are placed at the center  $[0.0]$ .

the concurrent area.

Let us consider that  $L$  selfish users ( $L < K$ ) are active in the network. The selfish users mislead the allocation by transmitting stronger channel information than original in order to suppress the other users and get the best channels selfishly even if it is not the best option from the view of SBS or MBS. It is assumed that the users are independent and have no information about each other. The rate of the channel between the user  $k$  and subcarrier  $n$ ,  $r_{k,n}^i$ , can be obtained as

$$r_{k,n}^i = w \log_2 \left( 1 + \frac{P_{k,n}^i 10^{\frac{-L(x_1, x_2)}{10}}}{w N_0} \right), \quad (3.1)$$

where  $P_{k,n}^i$  is the transmission power between the  $k^{\text{th}}$  user and the  $n^{\text{th}}$  subcarrier, which also includes the misleading information if  $k$  is a selfish user. The channel coefficients are complex Gaussian distributed as  $h_{k,n}^i \sim \mathcal{CN}(0, 1)$  and the channel estimation error is also assumed to be complex Gaussian distributed with zero mean and variance  $\sigma_\epsilon^2$ .  $w$  is the bandwidth of each subcarrier,  $N_0$  is the noise power and  $L(x_1, x_2)$  is the path

loss for a user located at  $(x_1, x_2) \in \mathbb{R}^2$ , stated as

$$L(x_1, x_2) = \beta + \alpha 10 \log_{10}(\sqrt{x_1^2 + x_2^2}) + \chi, \quad (3.2)$$

where  $\alpha$  is the path loss exponent,  $\beta$  is the path loss at 1-meter distance, and  $\chi$  models the deviation in fitting (in dB), which is a Gaussian random variable with zero mean and variance  $\sigma_\chi^2$ . In order to preserve fair transmission in such a HetNet, SM algorithm is proposed with some extensions by grading the honesty of all users after each allocation process. After each SM allocation process, the promised rates of users, which are obtained by using the transmitted CSI values, and the obtained rates at the end of the algorithm are compared. If the difference between the promised and obtained rates are greater than a predefined misleading threshold, the corresponding user is detected as a selfish user and punished by a predefined punishment factor of his/her grade for the next allocation process.

The number of assigned subcarriers of each user is limited to a quota,  $Q_k$ , to provide both QoS management and fairness. The algorithm ends when all the users and subcarriers are matched. Different from the previous approaches, SM algorithm is applied periodically in order to make an efficient allocation by using the latest channel information in a changing environment in the proposed SM approach. At the end of each allocation process, users are graded according to their recent misleading ratio ( $MR$ ) results. If any user has a  $MR$  that is lower than a predefined threshold, than the corresponding user is detected as a selfish user and is punished by proportionally lowering the trust index,  $\tau_k^i$ , compared to the previous one.

### 3.2.1. Selfish User Model

As in all wireless networks, HetNets are vulnerable to various security threats. One of these threats is the untruthful users that may mislead the HetNet for different reasons, such as blocking the access of other users in the network, targeting the access

of a specific user, or selfishly desiring the best sub-carriers. In this study, we focus on the selfish user's misleading on a CA HetNet. Each user has a misleading factor that is defined as

$$\phi_k^i = \begin{cases} \phi, & \text{if user } k \text{ is selfish,} \\ 1, & \text{if user } k \text{ is honest,} \end{cases} \quad (3.3)$$

where  $\phi$  is a predefined misleading factor ( $\phi > 1$ ). Selfish users transmit their CSIs as stronger than the default by using this misleading factor. Note that, the misleading factor is 1 if the user is honest.

### 3.3. Trust-Based Stable Matching Approach

In the proposed resource allocation method, each user has trust index  $\tau_k^i$ . At the end of each SM round, the promised rate,  $R_k^{prom,i}$ , which is obtained by the received channel information from users, and the obtained rate,  $R_k^{obt,i}$ , are compared to each other. The rate of the user at the end of each allocation is given by

$$R_{k,n}^i = \sum_{n=1}^N \mu_{k,n}^i r_{k,n}^i, \quad (3.4)$$

where  $\mu_{k,n}^i$  is the matching index, which is equal to 1 if subcarrier  $n$  is assigned to user  $k$ , 0 if subcarrier  $n$  is not assigned to user  $k$ . The rate of the channel between the user  $k$  and subcarrier  $n$ ,  $r_{k,n}^i$ , can be obtained by using (3.1). Correspondingly, misleading ratio of each user can be calculated as

$$MR_k^i = \frac{RE_k^i}{R_k^{prom,i}}, \quad (3.5)$$

where  $RE_k^i = R_k^{prom,i} - R_k^{obt,i}$  is the rate error of user  $k$  at the  $i^{\text{th}}$  SM process. If the difference between these rates is greater than a predefined threshold,  $\xi$ , the corresponding user is identified as a selfish user and is punished by a proportional decrease in its trust index by a punishment factor,  $0 < \tau^p < 1$ , for the next allocation

$$\tau_k^{i+1} = \begin{cases} \tau_k^i \tau^p & \text{if } MR_k^i > \xi, \\ \tau_k^i, & \text{otherwise.} \end{cases} \quad (3.6)$$

Note that, even if there are no misleading users in the network, channel estimation errors may lead to a loss on the rate efficiency. Thus, the predefined threshold has a significant role in the proposed policy. Low values of  $\xi$  may result in identifying some honest users as selfish users, whereas some selfish users cannot be identified at high values of  $\xi$ . Therefore,  $\xi$  should be carefully optimized. After the trust index calculations in each SM round,  $P_{k,n}^i$  are obtained for the next round by also including the misleading index ( $\phi$ ) and estimated channel information  $|h_{k,n}^i + \epsilon_{k,n}^i|^2$  as

$$P_{k,n}^{i+1} = \tau_k^i \phi_k^i |h_{k,n}^i + \epsilon_{k,n}^i|^2, \quad (3.7)$$

where  $\epsilon_{k,n}^i \sim \mathcal{CN}(0, \sigma_\epsilon^2)$ .

### 3.4. Simulation results

The system under consideration is a CA HetNet with  $K = 32$  users that are uniformly distributed on a concurrent area of a LTE-Advanced SBS and a MBS, which are positioned at (50m, 50m) and (0m, 0m), respectively. Our simulations are conducted for a configuration with  $2 \times 10$  MHz (10 MHz of MBS, 10 MHz of SBS) bandwidth in the downlink. Therefore, MBS and SBS have 2048 subcarriers that are assumed to be available at SBS and MBS in total (each with 1024 subcarriers) through this thesis,

unless otherwise stated. The transmit power,  $P$ , is assumed to be 1 W by default. The path loss exponent ( $\alpha$ ) values of SBS and MBS are 3 and 4, respectively. The bandwidth per resource block,  $w$ , is 180 kHz, noise power,  $N_0$ , is -174 dBm, and path loss at 1 m,  $\beta$ , is 38 dB for SBS. Determining the misleading ratio threshold has a significant role in terms of providing reliable communication for the honest users in the network. Thus, it is initially assumed that there are no selfish users in the network in order to focus only on the effect of channel estimation errors on the detection performance. The punishment factor is taken as  $\tau^p = 0.7$ . The probability of detecting any honest user as a selfish user is presented under different channel estimation error variances in Figure 3.2. From the corresponding results, the misleading ratio threshold can be determined by considering the channel estimation error variance. Even if there is severe noise in the channel, i.e.,  $\sigma_\epsilon^2 = 1$ , the probability of the occurrence of channel estimation error is minimized when the threshold is chosen as  $\xi = 0.7$ .

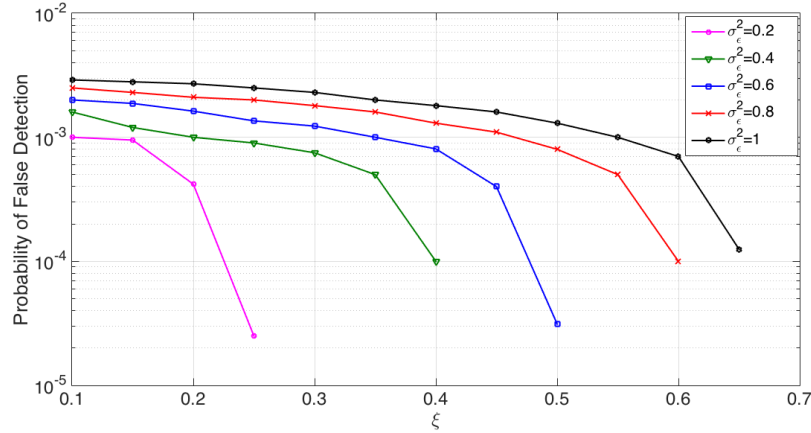


Figure 3.2. False detection performance for different misleading ratio thresholds when the punishment factor is 0.7.

From Figure 3.2, we can see that an appropriate misleading ratio could be determined as  $\xi = 0.7$  to avoid false detection under a noisy environment with  $\sigma_\epsilon^2 = 1$ . In Figure 3.3 and Figure 3.4, the average obtained rate for honest users and the average obtained rate of selfish users are shown for different misleading ratios  $\xi = 0.1$  and  $\xi = 0.7$ , respectively. There are  $L = 10$  selfish users that are always active in the network. Notice that, there is no punishment when the punishment factor is chosen as 1. At the end of the first trust-based SM round, selfish users have better transmission rates when compared to the honest users as an expected result of misleading the BSs.

At the following trust-based SM rounds, transmission rates may return to a fair level or may even result in lower transmission rates when compared to the honest users, as seen in Figure 3.3. Although selfish users are punished more effectively when the misleading ratio is chosen as  $\xi = 0.1$ , honest users have better rate recovery when the misleading ratio is chosen as  $\xi = 0.7$ . Moreover, average rate saturation is obtained faster (early SM rounds) in Figure 3.4 when compared to Figure 3.3 .

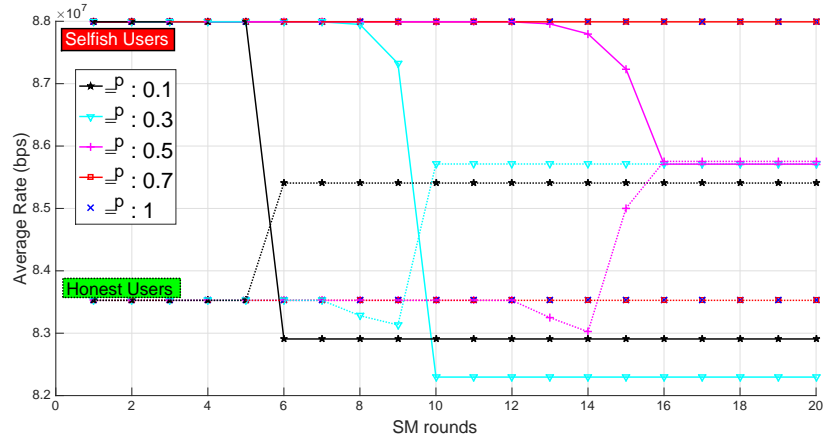


Figure 3.3. The rate of selfish users with misleading ratio threshold  $\xi = 0.1$  for different punishment factors  $\tau^p \in \{0.1, 0.3, 0.5, 0.7, 1\}$  for 32 users and 2048 subcarriers exist in total.

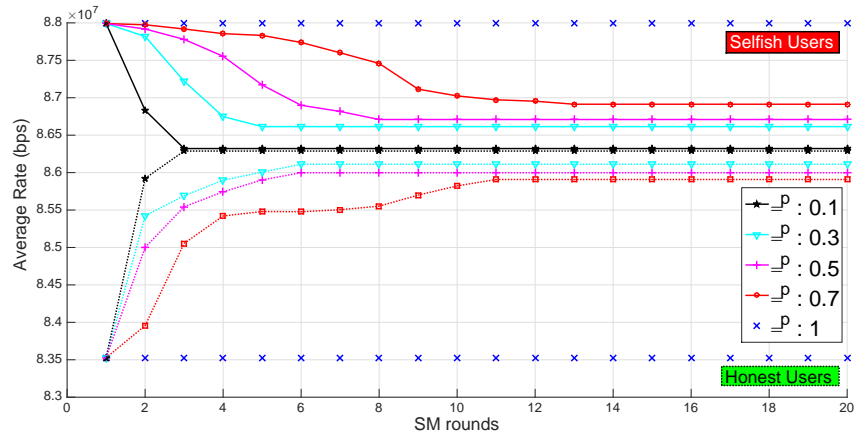


Figure 3.4. The rate of selfish users with misleading ratio threshold  $\xi = 0.7$  for different punishment factors  $\tau^p \in \{0.1, 0.3, 0.5, 0.7, 1\}$  for 32 users and 2048 subcarriers exist in total.

In Figure 3.5, misleading ratio is obtained for different punishment factors in different SM rounds when  $L = 10$  selfish users active in the network and misleading ratio threshold is chosen as  $\xi = 0.7$ . The fairness performance is obtained for different



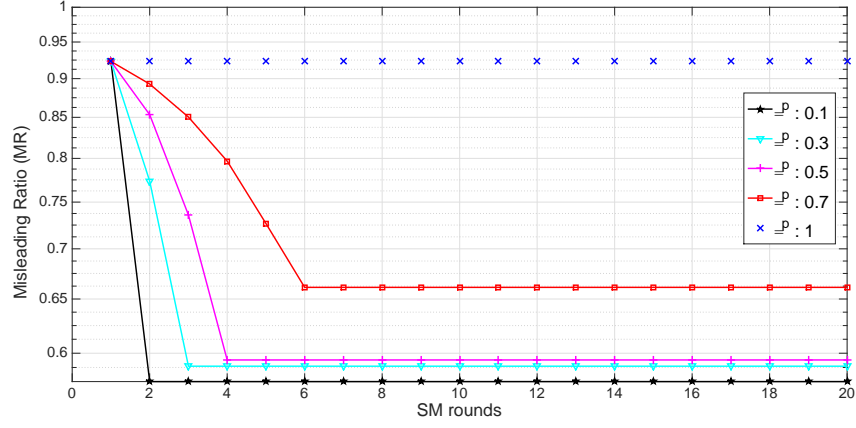


Figure 3.5. The misleading ratio performances are illustrated with misleading ratio threshold  $\xi = 0.7$  for different punishment factors  $\tau^p \in \{0.1, 0.3, 0.5, 0.7, 1\}$  for 32 users and 2048 subcarriers exist in total.

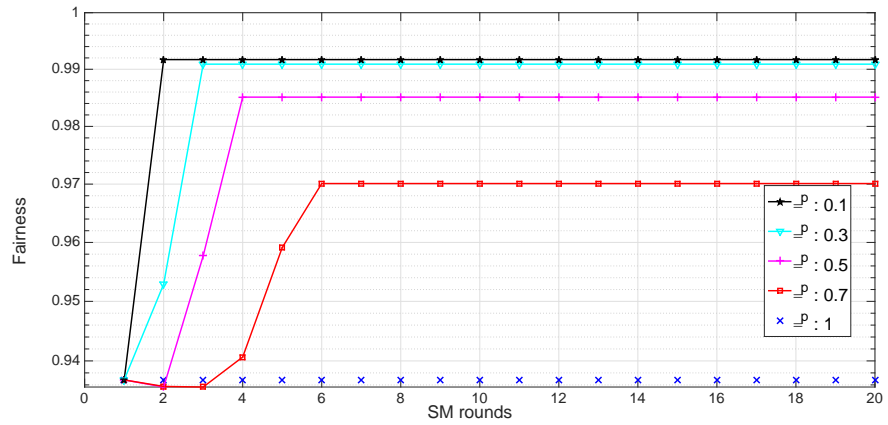


Figure 3.6. Fairness performances are illustrated with misleading ratio threshold  $\xi = 0.7$  for different punishment factors  $\tau^p \in \{0.1, 0.3, 0.5, 0.7, 1\}$  for 32 users and 2048 subcarriers exist in total.

punishment factors by using Jain's fairness index in Figure 3.6.

### 3.5. Conclusions

In trust based approach, resource allocation and security challenges are addressed by considering a specific kind of security threat (i.e., selfish users). A trust-based SM approach is proposed as a reliable resource allocation solution under selfish user threat in a CA HetNet. The problem is formulated as an SM problem aimed at minimizing the misleading rate while guaranteeing the fairness of the system. Computer simulations show that the appropriate misleading ratio threshold should be determined by considering the false detection performance. Hence, the proposed trust-based SM approach is very reliable even under severely noisy channel conditions by choosing the appropriate identification threshold specific to the channel environment, and punishment factor considering the trade-off between rate efficiency and fast recovery. This study gives an insight on the importance of identification and punishment processes for reliable communication with high data rate and fairness performances in the presence of the selfish users in the HetNet for future studies.

## 4. REPUTATION-BASED ATTACKER IDENTIFICATION POLICY FOR MOBILE EDGE COMPUTING IN INTERNET OF THINGS BY USING STABLE MATCHING ALGORITHM

### 4.1. Motivation

Smart devices with several applications, which have high computational demands and critical latency requirements, do not satisfy with the cloud networks. MEC offers lower latency and higher speed to the users by offloading the cloud computing capabilities at the nearest edge of the mobile network. In IoT MEC networks, wide range of applications with different requirements is a big challenge to cope with. Although there are some MEC deployments that are already defined and standardized by ETSI in [91], standardization is still in progress. Billions of IoT devices competes each other in order to run their applications over cloud, fog, or edge servers. The proper allocation of limited resources is one of the biggest challenges. Moreover, IoT networks are very fragile against attackers as nature of wireless networks. Security is becoming vital as the number of devices in an IoT network tends to the billions. The possible security threats and their precautions in an IoT network are elaborated in [92].

A comprehensive analysis of the security threats, challenges, and mechanisms inherent in all edge paradigms are given in [93]. According to the previous studies, even authorized edge devices may be a significant threat for IoT networks (i.e., selfish behavior) as a result of mix structure with a wide range of different requirements. Thus, the main motivation of this study is to identify attackers (selfish IoT MDs) with a reputation-based SM policy.

## 4.2. System Model

Consider an IoT network with  $K$  IoT mobile devices (MDs), and  $N$  access points (APs), which has a mobile edge server with  $S$  available resources for computational tasks, in total. As our primary aim is to achieve a secure communication, we assume, without loss of generality, that all the considered IoT devices are in the concurrent coverage area of access points and are statistically characterized by the same path loss effect. IoT edge servers provide software as a service (SaaS) to the IoT MDs for the applications related with their own specific tasks. Without loss of generality, each IoT MD has an equivalent computing-intensive tasks and desire to offload these tasks to the edge servers via  $N$  access points as illustrated in Figure 4.1. The possible malicious IoT MDs are visualized as red while the honest IoT MDs are blue. Malicious IoT MDs mislead the network by transmitting channel state information (CSI) with a relatively stronger channel than usual.

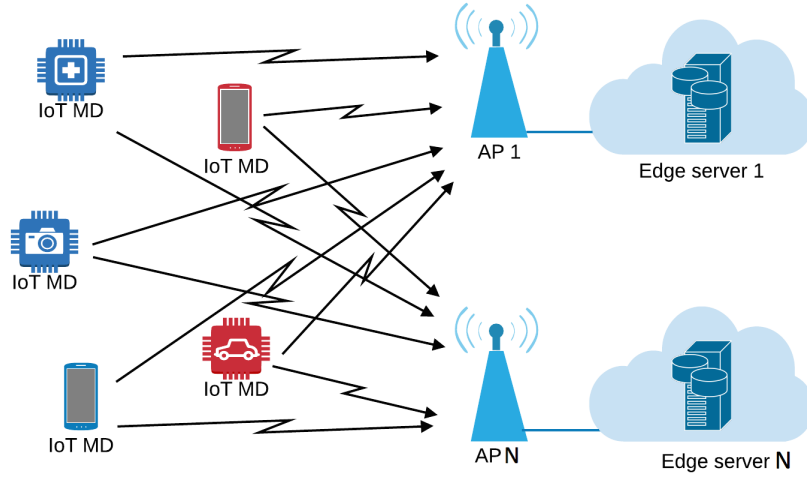


Figure 4.1.  $K$  IoT devices, including  $K^m$  malicious IoT devices, are uniformly distributed in the concurrent area of two APs with edge servers.

There are  $L$  ( $\leq K$ ) malicious IoT MDs active in the IoT network. It is assumed that all IoT devices are independent and have no information about each other. Additionally, all APs are assumed as reliable. The main aim of malicious IoT MDs is to get the best service of the IoT network and suppress all the remaining IoT MDs.

This type of attacks eventually decreases the overall performance of the network significantly. In some case, malicious IoT MDs drastically affect the network performances so that for the network it is quite impossible to provide services to any other IoT MDs (i.e., resulting in a denial of service, DoS, attack for the entire network).

The data rate between the  $k^{\text{th}}$  IoT MD and the  $s^{\text{th}}$  edge resource at the  $i^{\text{th}}$  matching slot,  $r_{k,s}^i$ , can be obtained as

$$r_{k,s}^i = w \log_2 \left( 1 + \frac{P_{k,s}^i}{w N_0} \right), \quad (4.1)$$

where  $w$  refers to the bandwidth,  $N_0$  is the noise power,  $P_{k,s}^i$  is the power of the channel gains as

$$P_{k,s}^i = P_s \phi_k^i | h_{k,s}^i + \epsilon_{k,s}^i |^2. \quad (4.2)$$

$P_s$  is the (constant) transmit power of IoT devices, while  $\phi_k^i$  is the misleading factor. The channel coefficients,  $h_{k,s}^i$ ,  $k = \{1, \dots, K\}$ ,  $s = \{1, \dots, S\}$ , and  $i = \{0, 1, \dots, W\}$ , are assumed to have complex Gaussian distributions with zero mean and unit variance.  $\epsilon_{k,s}^i$  is the channel estimation error, which is also complex Gaussian distributed with  $\epsilon \sim \mathcal{CN}(0, \sigma_\epsilon^2)$ . Assuming perfect phase synchronization at receiver, in this model, we can assume a Rayleigh distributed amplitude fading.

#### 4.2.1. Attacker Model

As in all wireless networks, IoT networks are fragile against security threats. Although there are many studies examining the ways to cope with attackers [94–96], there are still open problems for specific scenarios in IoT networks. In the following of this paper, we focus on malicious IoT MDs with selfish behavior. Selfish attackers in IoT networks follow a smart strategy to mislead the resource allocation process as

Byzantine attackers [97]. This smart strategy is based on inverting the actual local sensing result in a selective manner. Specifically, an attacker decides in each SM allocation round,  $i$ , to attack, or not, with a probability, which is denoted with  $p$ . If the attacker decides to attack in a specific round, it simply transmits its CSI as a stronger channel than usual by using a misleading factor defined as:

$$\phi_k^i = \begin{cases} \phi, & \text{if IoT device } k \text{ is malicious,} \\ 1, & \text{if IoT device } k \text{ is honest,} \end{cases} \quad (4.3)$$

where  $\phi$  is a predefined misleading factor ( $\phi > 1$ ). Selfish IoT devices transmit their CSIs, stronger than the real one by using this misleading factor. Note that misleading factor is 1 if the IoT device is honest. Additionally, there may be some unintentional attackers, who are actually honest, but detected as attackers due to severe channel estimation propagation conditions. The ability to distinguish unintentional attackers (honest IoT MDs) from intentional ones (selfish IoT MDs), has a great significance especially in terms of providing fairness.

#### 4.3. Reputation-based Attacker Identification Policy

The two-fold reputation-based attacker identification policy is proposed as a robust solution against selfish IoT MDs in the network. In the first stage of this policy, available resources at the edge servers are allocated to the IoT devices by using SM algorithm. After each SM allocation, the rate performances are compared with the promised rates in order to determine whether they are malicious or not. After reputations are obtained, devices are categorized into three stages; honest, suspicious, or malicious, in the second stage.

#### 4.3.1. SM based local attacker identification

The primary aim is to detect intentional attackers while avoiding to detect honest users as attackers (unintentional attackers caused by channel estimation error). In order to discriminate between intentional and unintentional attackers, the status of each IoT MD is formulated as two alternate hypotheses: H1 hypothesis, which states the presence of the intentional attackers and H0 hypothesis, which conversely states the absence of the intentional attackers but may have state the presence of unintentional attackers.

$$\begin{aligned} H_0 : \hat{z}_{k,s}^i &= h_{k,s}^i + \epsilon_{k,s}^i, \\ H_1 : \hat{z}_{k,s}^i &= \sqrt{\phi_k^i} (h_{k,s}^i + \epsilon_{k,s}^i), \end{aligned}$$

where  $\hat{z}_{k,s}^i$  is the channel information signal between the  $k^{\text{th}}$  IoT device and the  $s^{\text{th}}$  mobile edge resource. The channel coefficients  $h_{k,s}^i$  are assumed to have complex Gaussian distributions with zero mean and unit variance. Assuming perfect phase synchronization at receiver, in this model, we can assume a Rayleigh distributed amplitude fading and  $\epsilon_{k,s}^i$  is the channel estimation error, which is assumed to be complex Gaussian distributed with zero mean and variance  $\sigma_\epsilon^2$ .  $\phi_k^i$  is the misleading factor, which is  $\phi_k^i > 1$  if the  $k^{\text{th}}$  IoT device is intentional attacker and  $\phi_k^i = 1$  otherwise. At the end of each the  $i^{\text{th}}$  SM round, each IoT device is matched with  $Q_k$  mobile edge resources.

$$Q_k = \sum_{s=1}^S \mu_{k,s}^i, \quad (4.4)$$

where  $\mu_{k,s}^i$  is the matching index. In order to provide fairness in terms of assigned mobile edge resources,  $Q_k$  is generally chosen as  $Q_k = \frac{S}{K}$  providing that  $K$  must be divisible by  $N$ . The decision variable of each IoT device,  $Z_k^i$  is compared with a

predefined threshold,  $\xi$ , to identify the intentional attackers, as follows:

$$\left( Z_k^i = \frac{1}{Q_k} \sum_{s=1}^S \mu_{k,s}^i \phi_k^i P_s | \hat{z}_{k,s}^i |^2 \right) \underset{H1}{\overset{H0}{\leq}} \xi. \quad (4.5)$$

The probability of detecting an honest IoT device as an attacker is called Probability of false alarm,  $P^{FA}$ , while the probability of attacker detection is  $P^D$ .

$$\begin{aligned} P^{FA} &= \Pr[Z_k^i > \xi | H0] \\ P^D &= \Pr[Z_k^i > \xi | H1]. \end{aligned} \quad (4.6)$$

Thus, the threshold optimization problem is

$$\max_{\xi} \{P^D - P^{FA}\}. \quad (4.7)$$

According to central limit theorem (CLT), the testing variable  $Z_k^i$  is asymptotically ( $Q_k \rightarrow \infty$ ) Gaussian [98]. The distribution of test variable  $Z_k^i$  under null hypothesis is

$$Z_k^{i,E} \sim \mathcal{N}(Q_k(1 + \sigma_\epsilon^2), Q_k^2(1 + \sigma_\epsilon^2)^2). \quad (4.8)$$

An explanatory simplified example is given in Example 6.

**Example 6.** *Let consider, there are  $K = 2$  IoT MDs and  $S = 8$  available resources at*



the edge servers. The final matching matrix is obtained as

$$\mathbf{M} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}. \quad (4.9)$$

For simplicity we assume  $i = 0$  and ignored through this example. Note that, matching matrix includes  $\mu_{k,s}$  as 0 or 1 for each relation.  $Q_k$  can be calculated from  $\frac{S}{K}$  as 4.  $P_s$  is assumed as 1W. Hence the decision variables of IoT MDs are

$$Z_k^E = \frac{1}{4} \sum_{s=1}^8 \mu_{k,s} | (h_{k,s} + \epsilon_{k,s}) |^2. \quad (4.10)$$

$$Z_1^E = \frac{1}{4} [ | (h_{1,1} + \epsilon_{1,1}) |^2 + | (h_{1,4} + \epsilon_{1,4}) |^2 + | (h_{1,6} + \epsilon_{1,6}) |^2 + | (h_{1,7} + \epsilon_{1,7}) |^2 ]. \quad (4.11)$$

$$Z_2^E = \frac{1}{4} [ | (h_{2,2} + \epsilon_{2,2}) |^2 + | (h_{2,3} + \epsilon_{2,3}) |^2 + | (h_{2,5} + \epsilon_{2,5}) |^2 + | (h_{2,8} + \epsilon_{2,8}) |^2 ]. \quad (4.12)$$

The theoretical and empirical results are matched as shown in Figure 4.2, in terms of probability density function (PDF).

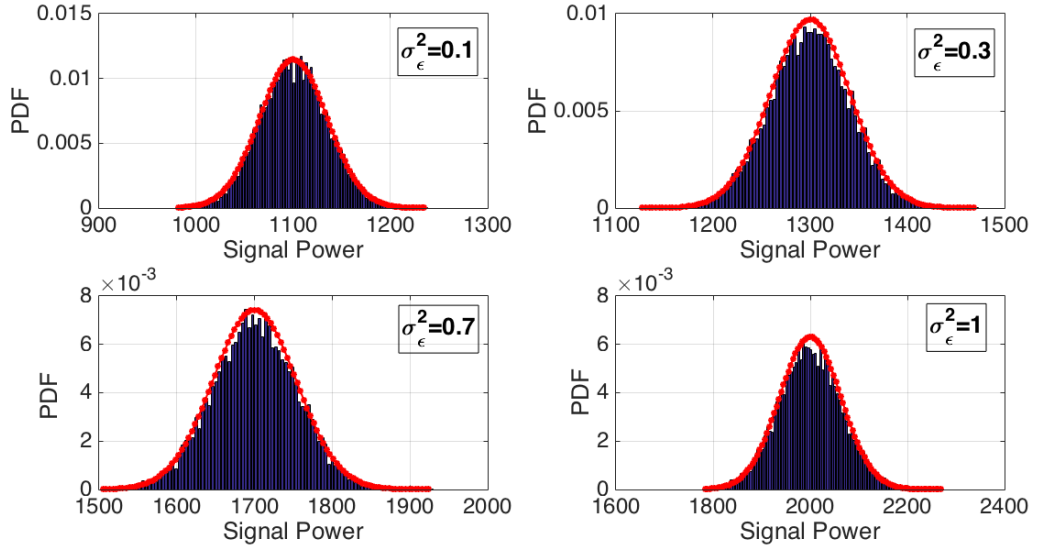


Figure 4.2. PDF of the decision variables under different conditions.

The detailed calculations are given in Section 4.4.

#### 4.3.2. Reputation based identification

All IoT devices are placed in one of the three different states, honest (H), suspicious (S), malicious (M) according to their reputations. All IoT devices are tested after each SM allocation. Each IoT device has a trust index,  $\tau_k$ , which is initially zero for all IoT devices,  $\tau_k^{i=0} = 0$ , and is defined as

$$\tau_k^{i+1} = \begin{cases} 1 & \text{if } Z_k^i > \xi, \\ 0, & \text{otherwise.} \end{cases} \quad (4.13)$$

In order to give a reward chance to any unintentional malicious IoT devices, we restrict our number of observations with a number  $W$ . Since the  $(W + 1)^{\text{th}}$  SM allocation, the oldest reputation is forgot and new reputation is included. In order to get faster results about honest of IoT devices, the proposed identification algorithm is applied even after first SM allocation (i.e., we applied state transitions by considering

the results that we get at the first allocation,  $i=1$ ) instead of waiting  $W$  times of SM allocation. The reputation index,  $T_k$ , for each IoT device  $k$  is calculated as

$$T_k = \begin{cases} \sum_{t=1}^i \tau_k^t & \text{if } i \leq W, \\ \sum_{t=i}^{W+i-1} \tau_k^t & \text{if } i > W. \end{cases} \quad (4.14)$$

The main aim is to determine the optimal thresholds that maximize the number of intentional malicious IoT devices in the malicious state while minimizing at the same time the number of honest IoT devices at malicious state. In [99], authors proposed four different thresholds to optimize the attacker detection in a cognitive radio network. In this study, we use these thresholds to optimize our secure offloading IoT network.

$$\text{State Transitions} = \begin{cases} M \rightarrow S & \text{if } T_k < \lambda_1, \\ S \rightarrow H, & \text{if } T_k < \lambda_3. \\ H \rightarrow S, & \text{if } T_k > \lambda_2. \\ S \rightarrow M, & \text{if } T_k > \lambda_4. \\ \text{No transition,} & \text{otherwise.} \end{cases} \quad (4.15)$$

#### 4.3.3. Threshold analysis for identification

Let the attacking probability of a malicious user be  $p$ . The transition probabilities of malicious IoT devices can be calculated as in [99]

$$P_{M,S}^M = \sum_{i=1}^{\lambda_1} \binom{W}{i} p^{(i)} (1-p)^{W-i}, \quad (4.16)$$

$$P_{S,H}^M = \sum_{i=1}^{\lambda_3} \binom{W}{i} p^i (1-p)^{(W-i)}, \quad (4.17)$$

$$P_{H,S}^M = \sum_{i=\lambda_2}^W \binom{W}{i} p^i (1-p)^{(W-i)}, \quad (4.18)$$

$$P_{S,M}^M = \sum_{i=\lambda_4}^W \binom{W}{i} p^i (1-p)^{(W-i)}. \quad (4.19)$$

The transition probabilities of unintentional malicious users who unintentionally attacks as a result of channel estimation error ( $p_e$ ) are obtained similarly. Let  $N_H^H$ ,  $N_M^H$  represents the number of honest users at state H and at state M, respectively. Let  $N_H^M$ ,  $N_M^M$  represents the number of malicious users at state H and at state M, respectively. The optimal thresholds can be calculated as

$$\max_{\lambda_1, \lambda_2, \lambda_3, \lambda_4} \{N_H^H + N_M^M - N_M^H - N_H^M\}. \quad (4.20)$$

#### 4.4. Performance evaluation

In order to obtain the optimal threshold, let define the second- and fourth-order moments of the received signal are evaluated. For the sake of compactness, the channel coefficient,  $h_{k,s}^i$ , the estimation error factor,  $\epsilon_{k,s}^i$ , are represented as  $h$  and  $\epsilon$ , respectively. The power of the channel coefficient,  $h$ , the estimation error,  $\epsilon$ , and the misleading factor are derived as functions of the higher order moments. Let  $M_2$  be the second-

order moment of the received signal,  $z$  and be expressed as follows:

$$\begin{aligned} M_2 &= E[\phi | (h + \epsilon)|^2] \\ &= \phi E[|h|^2] + \phi E[|\epsilon|^2] + E[Re(h\epsilon^*)] + E[Re(h^*\epsilon)], \end{aligned} \quad (4.21)$$

where  $E[.]$  denotes the expectation operator,  $|\cdot|$  is the absolute value, and  $Re(\cdot)$  denotes the real part of the complex number. Note that, the misleading factor is constant through the same SM allocation slot ( $i$ ), but may changed in another SM process with probability  $p$ . The channel coefficients, estimation errors are zero-mean and mutually independent random processes. Thus,

$$\begin{aligned} E[h] &= 0, & E[\epsilon] &= 0, \\ E[Re(h^*\epsilon)] &= 0, & E[Re(h\epsilon^*)] &= 0. \end{aligned} \quad (4.22)$$

Then, 4.21 can be rewritten as follows:

$$\begin{aligned} M_2 &= \phi E[|h|^2] + \phi E[|\epsilon|^2] \\ &= \phi(P_h + P_\epsilon) \end{aligned} \quad (4.23)$$

where  $P_\epsilon = 2\sigma_\epsilon^2$  is the noise variance, and  $P_h$  is the power level of the channel coefficients, respectively. Similarly, let  $M_4$  be the fourth-order moment of  $z$ , which are expressed as follows:

$$\begin{aligned} M_4 &= E[\phi^2 | (h + \epsilon)|^4] \\ &= \phi^2 [E[|h|^4] + E[|\epsilon|^4] + 2E[|h|^2 |\epsilon|^2] + 4E[Re(h\epsilon^*)^2]] \\ &= \phi^2 [P_h^2 + P_\epsilon^2 + 4P_h P_\epsilon].0 \end{aligned} \quad (4.24)$$

$P_h$  is rewritten in terms of  $P_\epsilon$  and  $M_2$  from (4.23) as follows:

$$P_h = \frac{M_2 - \phi P_\epsilon}{\phi}. \quad (4.25)$$

In order to obtain a second order expression of  $P_\epsilon$ , (4.25) is take place in (4.24) as in 4.26.

$$M_4 = \phi^2 \left[ \left( \frac{M_2 - \phi P_\epsilon}{\phi} \right)^2 + P_\epsilon^2 + 4 \left( \frac{M_2 - \phi P_\epsilon}{\phi} \right) P_\epsilon \right]. \quad (4.26)$$

$P_{\epsilon,1,2}$  can be found as roots of (4.26) from

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \quad (4.27)$$

where  $x$  is the roots of the second order equation

$$y = ax^2 + bx + c$$

. Thus  $P_{\epsilon,1,2}$  is obtained as follows:

$$\hat{P}_{\epsilon,1,2} = \frac{\hat{M}_2}{2\phi} \pm \frac{1}{2\phi} \sqrt{3\hat{M}_2^2 - 2\hat{M}_4}, \quad (4.28)$$

Hence, the estimated variables from equation ( 4.23) and (4.24) are shown,

$$\hat{P}_{h,1,2} = \frac{\hat{M}_2}{\phi} - \hat{P}_{\epsilon,1,2} \quad (4.29)$$

where the estimation of second- and fourth-order moments are

$$\hat{M}_2 = \frac{1}{Q} \sum_{i=1}^Q |z_i|^2 \quad \hat{M}_4 = \frac{1}{Q} \sum_{i=1}^Q |z_i|^4 \quad (4.30)$$

Hence, the desired expressions of mean  $E[\hat{Z}]$  and variance  $\hat{\sigma}^2$  can be obtained in terms of functions of the actual values  $\hat{P}_h$ ,  $\hat{P}_\epsilon$ , and  $\phi$ . The mean  $E[Z_k^i|H0]$  and the variance  $\text{var}[Z_k^i|H0]$  are evaluated under the null hypothesis to compute the threshold  $\xi$ , while the mean  $E[Z_k^i|H1]$  and the variance  $\text{var}[Z_k^i|H1]$  conversely determine the asymptotic testing power.

$$E[Z_k^i|H0] = \frac{\partial^2 \hat{P}_\epsilon}{\partial \hat{M}_2^2} \text{var}[\hat{M}_2] + \frac{\partial^2 \hat{P}_\epsilon}{\partial \hat{M}_4^2} \text{var}[\hat{M}_4] + \frac{\partial^2 \hat{P}_\epsilon}{\partial \hat{M}_2 \partial \hat{M}_4} \text{cov}[\hat{M}_2 \hat{M}_4]. \quad (4.31)$$

$$\text{var}[Z_k^i|H0] = \left( \frac{\partial \hat{P}_\epsilon}{\partial \hat{M}_2} \right)^2 \text{var}[\hat{M}_2] + \left( \frac{\partial \hat{P}_\epsilon}{\partial \hat{M}_4} \right)^2 \text{var}[\hat{M}_4] + \frac{\partial \hat{P}_\epsilon}{\partial \hat{M}_2} \frac{\partial \hat{P}_\epsilon}{\partial \hat{M}_4} \text{cov}[\hat{M}_2 \hat{M}_4]. \quad (4.32)$$

The probability of false alarm in (4.6) can be obtained by considering the Gaussian integrals as

$$P^{FA} = \Pr[Z_k^i > \xi | H0] = \text{erfc} \left( \frac{\xi - E[Z_k^i|H0]}{\sqrt{\text{var}([Z_k^i|H0])}} \right), \quad (4.33)$$

where  $\text{erfc}(\cdot)$  is the complementary error function. The test threshold,  $\xi$ , can be now evaluated from a straightforward evaluation of the Gaussian integral for a fixed prob-

ability of false alarm. Under the null hypothesis ( $H_0$ ), the test threshold as follows:

$$\xi = E[Z|H_0] + \frac{1}{\sqrt{\hat{\sigma}_{Z|H_0}^2}} \text{erfc}^{-1}(P^{FA}), \quad (4.34)$$

where  $\text{erfc}^{-1}(\cdot)$  is the (inverse of the) complementary error function. The probability of detection can also be evaluated under  $H_1$  hypothesis as

$$P^D = \text{erfc} \left( \frac{\xi - E[Z|H_1]}{\sqrt{\hat{\sigma}_{Z|H_1}^2}} \right). \quad (4.35)$$

#### 4.5. Numerical Results

Considering an IoT network deployment with  $K = 50$  IoT devices offload computing-intensive tasks to edge servers for SaaS with  $S = 100$  available resources, in total, via APs. MEC is defined and standardized by ETSI in [76, 77]. Although MEC of IoT device deployments are in progress of standardization, we consider our IoT MEC network according to ETSI specifications [91]. Unless otherwise stated, there are  $K^s = 20$  malicious (selfish) IoT devices out of 50 IoT devices. In Figure 4.3, attackers are detected by using the threshold in (4.34). The probability of detection results obtained by simulations are compared with the theoretical results in (4.35). Simulation results are obtained for attacking probability of  $p = 1$  and channel estimation error variance  $\sigma_\epsilon^2 = 0.5$ . The misleading factors are  $\phi = \{1.01, 1.1, 1.6, 2\}$ . According to Figure 4.3, the probability of detection is over 0.9, if the misleading ratio is greater than 1.5,  $\phi > 1.5$ . When the misleading ratio is less than 1.1,  $\phi < 1.1$ , the performance of the probability of detection decreases significantly.

After  $W$  rounds of SM attacker identification, each IoT device has a reputation index. According to these reputation indices, each IoT device is placed in one of the



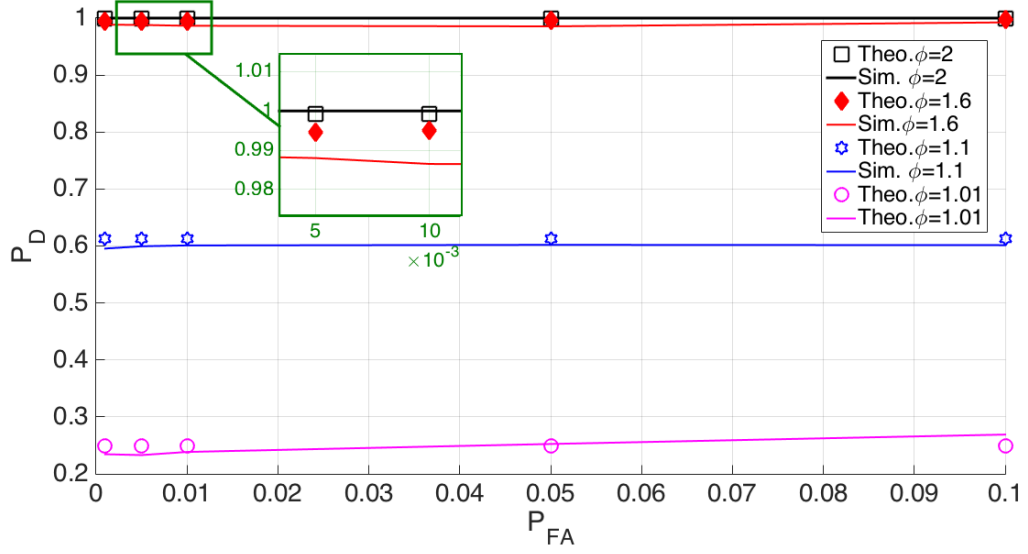


Figure 4.3. Theoretical and simulation results of  $P_D$  for different  $P_{FA}$  assumptions and misleading factors  $\phi$ .

three trust states; malicious, suspicious, or honest. In Figure 4.4, state transitions of 100 honest users and 100 selfish users are illustrated for the misleading ratios  $\phi = 1.1$ , respectively. The simulation results of the proposed approach are compared with the well known Auction approach [5]. Numerical results show that the proposed reputation based PFM method is able to identify more selfish users than the conventional (Auction) one, even if the proposed approach fails in moving some honest users in the honest state. In Figure 4.4, the available resource in edge server is 1000. The estimation error variance is 0.5 and the preliminary threshold is determined under the assumption of a fixed probability of false alarm,  $P_{FA} = 0.1$ .  $N$  refers to the average number of IoT devices in the corresponding state. The green lines represents malicious state, the pink lines refers honest state, and the red lines represents the suspicious states. The number of IoT devices are the average numbers as a result of at least  $10^6$  Monte Carlo simulations.

Finally, in Figure 4.5, identification results after  $W$  allocation time are obtained in case of different attacking probabilities. Although honest users are perfectly placed at honest state, selfish IoT devices are placed at suspicious state as seen in Figure 4.5 (a).

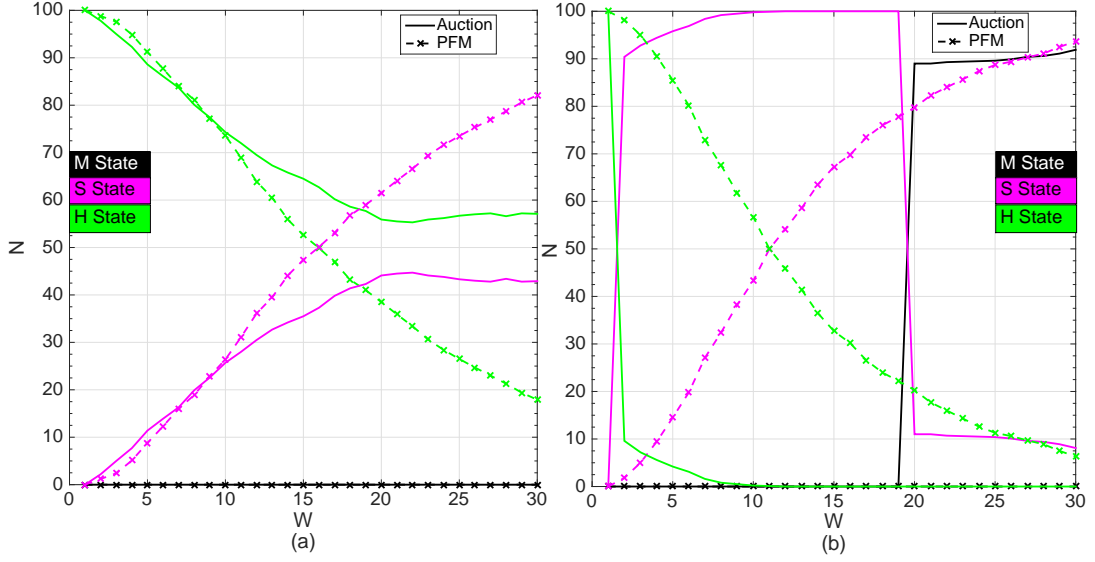


Figure 4.4. The state transitions when the misleading factor is  $\phi = 1.1$  (a) Honest users (b) Selfish users .

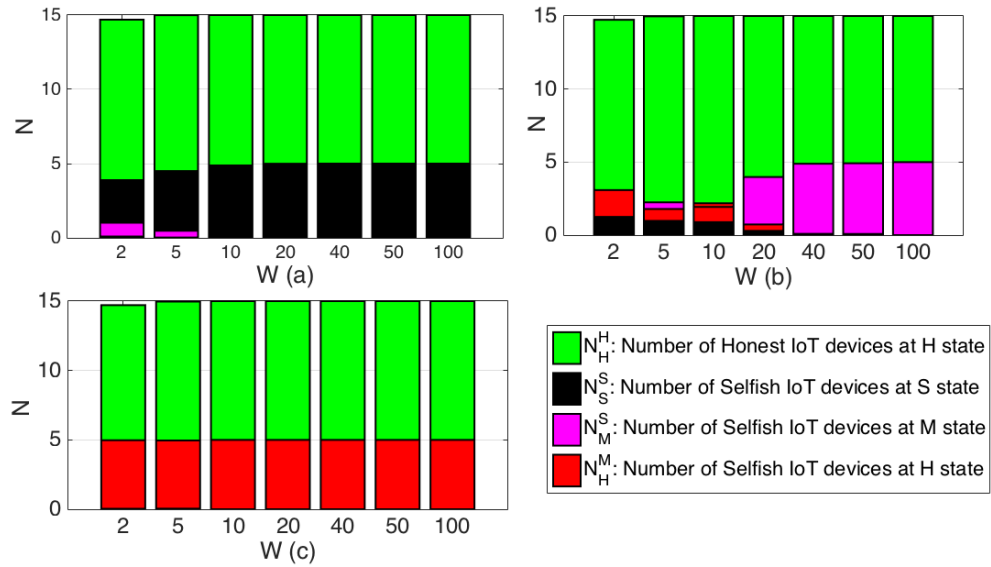


Figure 4.5. The average number of IoT devices at each state are shown after  $W$  allocation time for different probability of attackers, (a)  $p = 0.1$ , (b)  $p = 0.5$ , and (c)  $p = 0.9$ .

In Figure 4.5 (b), malicious IoT devices are successfully detected for  $W \geq 20$  when malicious IoT devices attacks with a probability of 0.5, while malicious IoT devices cannot be detected as malicious even if  $W$  is chosen too high as a result of low misleading detection threshold in Figure 4.5 (c).

#### 4.6. Conclusions

The two-fold reputation based attacker identification approach is proposed as a robust solution against selfish IoT MDs in the network. In the first stage of the approach, available resources at the edge servers are allocated to the IoT devices by using SM algorithm. After each SM allocation, IoT devices are checked whether they are malicious or not. The threshold is optimized for the first identification process. Optimized thresholds are used in the SM based identification process. The simulation results confirm the theoretical analyses. In the second fold, IoT devices are examined according to their reputation indices, finally identifying attackers and determining the states of the IoT devices. As demonstrated by theoretical and simulation results, our three-states identification process is very effective in identifying malicious devices. At the same time our approach also rehabilitates unintentional attackers, who suffered from bad channel propagation conditions, by moving these devices between the three proposed states (up to the honest state when the channel estimation errors decrease).

## 5. CONCLUSION

In this thesis, SM-based resource allocation methods are proposed in order to address the tremendous demands for high data rates in resource limited in 5G technologies. PFM is proposed in order to cope with many-to-one resource allocation. SM-based approaches have to meet with various requirements from different types of users in the wireless communication networks with adaptable and flexible matching algorithm. The problem is extensively elaborated in many aspects for different wireless communication systems such as HetNets and IoT networks. In order to increase the robustness of networks, e.g., IoT networks, which are very fragile against possible attacks, as a natural result of HetNet structure, trust based approaches are proposed. MSM algorithm uses the ideal CSI values (via feedback channel) in order to obtain the preference lists instead of using deterministic preferences as in the original SM algorithm. The overload on the uplink channel, through CSI transmission, is decreased significantly by the proposed partial feedback matching algorithm.

Specifically, PFM based CA uses partial feedback CSI instead of ideal full CSI for each UE in a CA HetNet. Stability performances of the proposed algorithm, PFM, and the user satisfaction analyses are investigated for various amounts of partial feedback CSI transmission. The stability concerns for CA HetNets are investigated for the proposed variation of the MSM 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 MSM and PFM approaches for full CSI and reduced feedback CSI scenarios, respectively. Data rate and fairness performances are investigated for all proposed variations of SM algorithm, simultaneously, by considering the rate requirements of UEs with the feedback CSI. The resource allocation problem, which is one the most significant challenges of IoT MEC infrastructure, are addressed by applying a graph-based low complexity resource allocation policy, SM algorithm. Finally, IoT networks are very fragile against attackers in physical layer as a natural result of wireless communication systems. A three state

reputation based attacker identification and punishment policy, is proposed in order to increase the robustness of the network. The results show that the proposed approach is able to identify more selfish users than the conventional (Auction) one, even if it fail in moving some honest users in the honest state.

## 6. Future Works

With new technologies, which provides higher transmission rates, the number of active and smart devices in wireless networks are increasing tremendously. Secure and efficient resource allocation is a significant concern, while millions of devices are active in a network. As a future work, the proposed SM based algorithms should be examined under different security scenarios, which has various types of attackers.

## REFERENCES

1. Statistica, C. E., “Internet of Things - number of connected devices worldwide 2015-2025”, *Statistica*, 2019.
2. Sanguanpuak, T., S. Guruacharya, N. Rajatheva, M. Bennis and M. Latva-Aho, “Multi-Operator Spectrum Sharing for Small Cell Networks: A Matching Game Perspective”, *IEEE Transactions on Wireless Communications*, Vol. 16, No. 6, pp. 3761–3774, June 2017.
3. Wang, G., P. Liu, Z. Yang and R. Xue, “Joint College Admissions Game and Auction Theory for Data Offloading in Heterogeneous Networks”, *Chinese Journal of Electronics*, Vol. 27, No. 1, pp. 168–174, 2018.
4. Gu, Y., Y. Zhang, L. Cai, M. Pan, L. Song and Z. Han, “LTE-Unlicensed Coexistence Mechanism: A Matching Game Framework”, *IEEE Wireless Communications*, Vol. 23, No. 6, pp. 54–60, December 2016.
5. Sun, W., J. Liu, Y. Yue and H. Zhang, “Double Auction-Based Resource Allocation for Mobile Edge Computing in Industrial Internet of Things”, *IEEE Transactions on Industrial Informatics*, Vol. 14, No. 10, pp. 4692–4701, Oct 2018.
6. Khandekar, A., N. Bhushan, J. Tingfang and V. Vanghi, “LTE-Advanced: Heterogeneous networks”, *European Proc. Wireless Conference (EW)*, pp. 978–982, April 2010.
7. Chu, X., D. Lopez-Perez, Y. Yang and F. Gunnarsson, *Heterogeneous Cellular Networks: Theory, Simulation and Deployment*, Cambridge University Press, 2013.
8. Saleh, N. and N. Patel, “Enhancing spectrum efficiently and energy efficiently via offloading mechanism in heterogeneous networks (in context of Wi-Fi and LTE-Advanced)”, *International Conf.on Innovations in Electronics, Signal Processing*

- and Communication (IESC)*, pp. 171–177, April 2017.
9. Lopez-Perez, D., I. Guvenc, G. de la Roche, M. Kountouris, T. Quek and J. Zhang, “Enhanced intercell interference coordination challenges in heterogeneous networks”, *IEEE Wireless Communications*, Vol. 18, No. 3, pp. 22–30, June 2011.
  10. 3GPP, TR and 36.808, “E-UTRA; Carrier Aggregation; base station radio transmission and reception”, *3GPP Technical Specification Group Radio Access Network*, Vol. Release 10, 2010.
  11. 3GPP, TS and 36.211, “Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation”, *3GPP Technical Specification Group Radio Access Network*, Vol. Release 8, 2008.
  12. Ratasuk, R., D. Tolli and A. Ghosh, “Carrier Aggregation in LTE-Advanced”, *Proc. IEEE Vehicular Technology Conference*, pp. 1–5, May 2010.
  13. Chavarria-Reyes, E., I. Akyildiz and E. Fadel, “Energy-Efficient Multi-Stream Carrier Aggregation for Heterogeneous Networks in 5G Wireless Systems”, *IEEE Trans. on Wireless Communications*, Vol. 15, No. 11, pp. 7432–7443, Nov 2016.
  14. Dahlman, E., S. Parkvall and J. Skold, *4G: LTE/LTE-Advanced for Mobile Broadband*, Academic Press, 2011.
  15. Wang, Q., Q. Zhang, Y. Sun, Z. Wei and Z. Feng, “A QoS-guaranteed radio resource scheduling in multi-user multi-service LTE-A systems with carrier aggregation”, *IEEE International Conf. on Computer and Communications (ICCC)*, pp. 2927–2932, Oct 2016.
  16. Rostami, S., K. Arshad and P. Rapajic, “A joint resource allocation and link adaptation algorithm with carrier aggregation for 5G LTE-Advanced network”, *Proc. Intl. Conf. on Telecommunications (ICT)*, pp. 102–106, April 2015.



17. Zhang, L., Y. Wang, L. Huang, H. Wang, and W. Wang, "QoS performance analysis on carrier aggregation based LTE-A systems", Proc. IET International Comm.Conf.on Wireless Mobile and Computing (CCWMC) , pp. 253–256, Dec 2009.
18. Zhang, L., K. Zheng, W. Wang and L. Huang, "Performance analysis on carrier scheduling schemes in the long-term evolution-advanced system with carrier aggregation", *IET Communications*, Vol. 5, No. 5, pp. 612–619, March 2011.
19. Kiwoli, L., A. Sam and E. Manasseh, "Performance analysis of carrier aggregation for various mobile network implementations scenario based on spectrum allocated", *CoRR*, Vol. 1711.02287, 2017.
20. Sun, C., J. Jiang, L. Huang and G. Lu, "Component carrier selection and interference coordination for carrier aggregation system in heterogeneous networks", IEEE International Conf. on Communication Technology (ICCT), pp. 402–407, Nov 2012.
21. Wang, Y., K. Pedersen, M. Navarro, P. Mogensen and T. Sorensen, "Uplink overhead analysis and outage protection for multi-carrier LTE-Advanced systems", IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 17–21, Sept 2009.
22. Wang, H., C. Rosa and K. Pedersen, "Uplink Component Carrier Selection for LTE-Advanced Systems with Carrier Aggregation", Proc. IEEE International Conf. on Communications (ICC), pp. 1–5, June 2011.
23. Katsha, M. and H. Mohd Ramli, "Development of a novel component carrier selection algorithm in Long Term Evolution-Advanced (LTE-A) with Carrier Aggregation", *IEEE Student Conf.on Research and Development (SCOReD)*, pp. 1–5, Dec 2016.
24. Yu, G., Q. Chen, R. Yin, H. Zhang and G. Li, "Joint Downlink and Uplink Resource

- Allocation for Energy-Efficient Carrier Aggregation”, *IEEE Trans. on Wireless Communications*, Vol. 14, No. 6, pp. 3207–3218, June 2015.
25. Gu, Y., 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. 51–59, 2015.
  26. Liao, H., P. Chen and W. Chen, “An Efficient Downlink Radio Resource Allocation with Carrier Aggregation in LTE-Advanced Networks”, *IEEE Trans. on Mobile Computing*, Vol. 13, No. 10, pp. 2229–2239, Oct 2014.
  27. Zhao, J., Y. Liu, K. Chai, Y. Chen and M. Elkashlan, “Many-to-Many Matching With Externalities for Device-to-Device Communications”, *IEEE Wireless Communications Letters*, Vol. 6, No. 1, pp. 138–141, Feb 2017.
  28. Kurrle, R., *Resource Allocation for Smart Phones in 4G LTE-Advanced Carrier Aggregation*, Master’s Thesis, Virginia Polytechnic Institute and State University, Arlington, VA, 2012.
  29. Wang, Y., K. Pedersen, P. Mogensen and T. Sorensen, “Resource allocation considerations for multi-carrier LTE-Advanced systems operating in backward compatible mode”, *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 370–374, Sept 2009.
  30. Shi, S., C. Feng and C. Guo, “A Resource Scheduling Algorithm Based on User Grouping for LTE-Advanced System with Carrier Aggregation”, *International Symposium on Computer Network and Multimedia Technology*, pp. 1–4, Jan 2009.
  31. Tian, H., S. Gao, J. Zhu and L. Chen, “Improved Component Carrier Selection Method for Non-Continuous Carrier Aggregation in LTE-Advanced Systems”, pp. 1–5, Sept 2011.
  32. Wu, F., Y. Mao, S. Leng and X. Huang, “A Carrier Aggregation Based Resource

- Allocation Scheme for Pervasive Wireless Networks”, pp. 196–201, Dec 2011.
33. Gu, Y., C. Jiang, L. Cai, M. Pan, L. Song and Z. Han, “Dynamic Path To Stability in LTE-Unlicensed With User Mobility: A Matching Framework”, *IEEE Trans. on Wireless Communications*, Vol. 16, No. 7, pp. 4547–4561, July 2017.
  34. Galanopoulos, A., C. Tsinos and F. Foukalas, “Low-complexity and low-feedback-rate channel allocation for carrier aggregation in heterogeneous networks”, *IEEE Wireless Communications and Networking Conference*, pp. 1–6, April 2016.
  35. 3GPP, TR and 36.715-02-02, “LTE Advanced Dual Uplink Interband Carrier Aggregation”, *3GPP Technical Specification Group Radio Access Network*, Vol. Release 15, 2017.
  36. Bennaceur, J., H. Idoudi and L. Saidane, “A trust game model for the cognitive radio networks”, *International Conf. on Performance Evaluation and Modeling in Wired and Wireless Networks*, pp. 1– 5, Nov 2016.
  37. Ryu, J. Y., J. Lee and T. Q. S. Quek, “Confidential Cooperative Comm. With Trust Degree of Potential Eavesdroppers”, *IEEE Trans.on Wireless Comm.*, Vol. 15, No. 6, pp. 3823–3836, June 2016.
  38. Althunibat, S., B. Denise and F. Granelli, “Identification and Punishment Policies for Spectrum Sensing Data Falsification Attackers Using Delivery-Based Assessment”, *IEEE Trans. on Vehicular Technology*, Vol. 65, No. 9, pp. 7308–7321, Sept 2016.
  39. Huang, S., J. Tan and J. Xu, “Nash Bargaining Game Based Subcarrier Allocation for Physical Layer Security in Orthogonal Frequency Division Multiplexing System”, *IEEE UIC-ATC-ScalCom*, pp. 1094–1100, Aug 2015.
  40. Wu, H., N. Zhang, X. Tao, Z. Wei and X. Shen, “Capacity- and Trust-Aware BS Cooperation in Nonuniform HetNets: Spectral Efficiency and Optimal BS Den-

- sity”, *IEEE Trans. on Vehicular Technology*, Vol. 66, No. 12, pp. 11317– 11329, Dec 2017.
41. Zawaideh, F., M. Salamah and H. Al-Bahadili, “A fair trust-based malicious node detection and isolation scheme for WSNs”, *International Conf. on the Applications of Information Technology in Developing Renewable Energy Processes Systems*, pp. 1–6, Dec 2017.
  42. Paraskevas, E., T. Jiang and J. Baras, “Trust-aware network utility optimization in multihop wireless networks with delay constraints”, *Mediterranean Conf. on Control and Automation*, pp. 593–598, June 2016.
  43. Zhao, M., J. Y. Ryu, J. Lee, T. Quek and S. Feng, “Exploiting Trust Degree for Multiple-Antenna User Cooperation”, *IEEE Trans. on Wireless Comm.*, Vol. 16, No. 8, pp. 4908–4923, Aug 2017.
  44. Basan, A., E. Basan and O. Makarevich, “A Trust Evaluation Method for Active Attack Counteraction in Wireless Sensor Networks”, *International Conf. on Cyber-Enabled Distributed Computing and Knowledge Discovery*, pp. 369–372, Oct 2017.
  45. Ntemos, K., N. Kalouptsidis and N. Kolokotronis, “Trust-based strategies for wireless networks under partial monitoring”, *European Signal Processing Conference*, pp. 2591–2595, Aug 2017.
  46. Jin, B., S. Kim, D. Yun, H. Lee, W. Kim and Y. Yi, “Aggregating LTE and WI-FI: Toward Intra-Cell Fairness and High TCP Performance”, *IEEE Trans.on Wireless Comm.*, Vol. 16, No. 10, pp. 6295–6308, Oct 2017.
  47. Shajaiah, H., A. Abdelhadi and C. Clancy, “Robust Resource Allocation with Joint Carrier Aggregation in Multi-Carrier Cellular Networks”, *IEEE Trans. on Cognitive Comm. and Networking*, , No. 99, pp. 1–1, 2017.
  48. Miliotis, V., L. Alonso and C. Verikoukis, “Resource Allocation Techniques for

- Heterogeneous Networks Under User Misbehavior”, *IEEE Comm. Letters*, Vol. 20, No. 6, pp. 1179 – 1182, June 2016.
49. Abedin, S. F., M. G. R. Alam, S. M. A. Kazmi, N. H. Tran, D. Niyato and C. S. Hong, “Resource Allocation for Ultra-Reliable and Enhanced Mobile Broadband IoT Applications in Fog Network”, *IEEE Transactions on Communications*, Vol. 67, No. 1, pp. 489–502, Jan 2019.
  50. Gale, D. and L. Shapley, “College Admissions and the Stability of Marriage”, *The American Mathematical Monthly*, Vol. 69, pp. 9–15, 1962.
  51. Datsika, E., A. Antonopoulos, D. Yuan and C. Verikoukis, “Matching Theory for Over-the-Top Service Provision in 5G Networks”, *IEEE Transactions on Wireless Communications*, Vol. 17, No. 8, pp. 5452–5464, Aug 2018.
  52. Zhang, J., W. Xia, Z. Cheng, Q. Zou, B. Huang, F. Shen, F. Yan and L. Shen, “An evolutionary game for joint wireless and cloud resource allocation in mobile edge computing”, *2017 9th International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–6, Oct 2017.
  53. Chen, L., S. Zhou and J. Xu, “Computation Peer Offloading for Energy-Constrained Mobile Edge Computing in Small-Cell Networks”, *IEEE/ACM Transactions on Networking*, Vol. 26, No. 4, pp. 1619–1632, Aug 2018.
  54. Wang, C., C. Dong, J. Qin, X. Yang and W. Wen, “Energy-efficient Offloading Policy for Resource Allocation in Distributed Mobile Edge Computing”, *2018 IEEE Symposium on Computers and Communications (ISCC)*, pp. 00366–00372, June 2018.
  55. Lan, Z., W. Xia, W. Cui, F. Yan, F. Shen, X. Zuo and L. Shen, “A Hierarchical Game for Joint Wireless and Cloud Resource Allocation in Mobile Edge Computing System”, *2018 10th International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–7, Oct 2018.

56. Zhang, J., W. Xia, F. Yan and L. Shen, “Joint Computation Offloading and Resource Allocation Optimization in Heterogeneous Networks With Mobile Edge Computing”, *IEEE Access*, Vol. 6, pp. 19324–19337, 2018.
57. Zhang, J., W. Xia, F. Yan and L. Shen, “Joint Computation Offloading and Resource Allocation Optimization in Heterogeneous Networks With Mobile Edge Computing”, *IEEE Access*, Vol. 6, pp. 19324–19337, 2018.
58. Zaw, C. W., N. N. Ei, H. Y. Reum Im, Y. K. Tun and C. S. Hong, “Cost and Latency Tradeoff in Mobile Edge Computing: A Distributed Game Approach”, *2019 IEEE International Conference on Big Data and Smart Computing (BigComp)*, pp. 1–7, Feb 2019.
59. Feng, S., Z. Xiong, D. Niyato and P. Wang, “Dynamic Resource Management to Defend Against Advanced Persistent Threats in Fog Computing: A Game Theoretic Approach”, *IEEE Transactions on Cloud Computing*, pp. 1–1, 2019.
60. Sardellitti, S., M. Merluzzi and S. Barbarossa, “Optimal Association of Mobile Users to Multi-Access Edge Computing Resources”, *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, May 2018.
61. Pham, Q., T. Leanh, N. H. Tran, B. J. Park and C. S. Hong, “Decentralized Computation Offloading and Resource Allocation for Mobile-Edge Computing: A Matching Game Approach”, *IEEE Access*, Vol. 6, pp. 75868–75885, 2018.
62. Yu, H., J. Liu and S. Guo, “Multi-User Optimal Offloading: Leveraging Mobility and Allocating Resources in Mobile Edge Cloud Computing”, *2018 IEEE International Conference on Networking, Architecture and Storage (NAS)*, pp. 1–8, Oct 2018.
63. Zhu, Z., J. Peng, X. Gu, H. Li, K. Liu, Z. Zhou and W. Liu, “Fair Resource Allocation for System Throughput Maximization in Mobile Edge Computing”, *IEEE Access*, Vol. 6, pp. 5332–5340, 2018.

64. Guglielmi, A. V., M. Levorato and L. Badia, “A Bayesian Game Theoretic Approach to Task Offloading in Edge and Cloud Computing”, *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, May 2018.
65. Meng, S., Y. Wang, W. Sun, S. Guo and K. Sun, “Dynamic Bayesian Game Based Power Allocation in Mobile Edge Computing with Users’ Behaviors”, pp. 83–87, 02 2019.
66. 3GPP, TS and 32.592, “Home eNodeB (HeNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Information model for Type 1 interface HeNB to HeNB Management System (HeMS)”, *3GPP Technical Specification Group Radio Access Network*, Vol. Release 9, 2010.
67. Public, “Improving wireless connectivity through small cell deployment”, *GSMA*, 2016.
68. Rumney, M. and A. Technologies, *LTE and the Evolution to 4G Wireless: Design and Measurement Challenges*, Wiley, 2013.
69. Pedersen, K., F. Frederiksen, C. Rosa, H. Nguyen, L. Garcia and Y. Wang, “Carrier aggregation for LTE-Advanced: functionality and performance aspects”, *IEEE Communications Magazine*, Vol. 49, No. 6, pp. 89–95, June 2011.
70. Huang, C., K. Iwama, S. Miyazaki and H. Yanagisawa, “A Tight approximation bound for the Stable Marriage Problem with Restricted Ties”, Vol. 40 of *Approx/Random, Leibniz International Proceedings in Informatics (LIPIcs)*, pp. 361–380, 2015.
71. Aziz, H., B. Péter, S. Gaspers, R. de Haan, N. Mattei and R. B., *Stable Matching with Uncertain Linear Preferences*, pp. 195–206, Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.

72. Yang, C., X. Xu, K. Ramamohanarao and J. Chen, “A Scalable Multi-Data Sources based Recursive Approximation Approach for Fast Error Recovery in Big Sensing Data on Cloud”, *IEEE Transactions on Knowledge and Data Engineering*, pp. 1–1, 2019.
73. Ravandi, B. and I. Papapanagiotou, “A Self-Learning Scheduling in Cloud Software Defined Block Storage”, *International Conference on Cloud Computing (CLOUD)*, pp. 415–422, June 2017.
74. Bonomi, F., R. Milito, J. Zhu and S. Addepalli, “Fog Computing and Its Role in the Internet of Things”, *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing*, MCC '12, pp. 13–16, ACM, New York, NY, USA, 2012.
75. Althunibat, S., B. J. Denise and F. Granelli, “Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are”, *Cisco-White Paper*, 2015.
76. Hu, Y. C., M. Patel, D. Sabella, N. Sprecher and V. Young, “Mobile edge computing a key technology towards 5G”, *ETSI White Paper*, Vol. 11, 2015.
77. Patel, M., J. Joubert, C. Chan, N. Sprecher, S. Abeta and A. Neal, “White Paper, Mobile-edge Computing (MEC) industry initiative”, *ETSI White Paper*, 2014.
78. Dao, N.-N., M. Park, J. Kim, J. Paek and S. Cho, “Resource-aware relay selection for inter-cell interference avoidance in 5G heterogeneous network for Internet of Things systems”, *Future Generation Computer Systems*, 2018.
79. Shipon Ali, “An Overview on Interference Management in 3GPP LTE- Advanced Heterogeneous Networks”, *International Journal of Future Generation Communication and Networking*, Vol. 8, No. 1, pp. 55–68, 2015.
80. Shannon, C., “Communication in the Presence of Noise”, *Proc. Institute of Radio Engineers*, Vol. 37, No. 1, pp. 10–21, 1949.



81. El-Hajj, A., Z. Dawy and W. Saad, "A stable matching game for joint up-link/downlink resource allocation in OFDMA wireless networks", *IEEE International Conf. on Communications (ICC)*, pp. 5354–5359, June 2012.
82. Gusfield, D. and R. Irving, *The Stable Marriage Problem: Structure and Algorithms*, MIT Press, 1989.
83. Jain, R., D. M. Chiu and W. Hawe, "A quantitative measure of fairness and discrimination for resource allocation in shared computer systems", *Digit. Equip. Corp., Eastern Research Lab*, Vol. DEC-TR-301, 1982.
84. Roth, A. E. and M. A. O. Sotomayor, "Two-Sided matching - A study in game-theoretic modeling and analysis", *Econometric Society Monographs, Cambridge University Press*, Vol. 18, p. 265, 1990.
85. Oualhaj, O. A., E. Sabir, A. Kobbane, J. Ben-Othman and M. E. Koutbi, "A college admissions game for content caching in heterogeneous delay tolerant networks", *International Conference on Telecommunications (ICT)*, pp. 1–5, May 2016.
86. Drummond, J. and C. Boutilier, "Elicitation and Approximately Stable Matching with Partial Preferences", *Proceedings of the International Joint Conf. on Artificial Intelligence*, pp. 97–105, 2013.
87. Zappone, A., E. Jorswieck and A. Leshem, "Distributed Resource Allocation for Energy Efficiency in MIMO OFDMA Wireless Networks", *IEEE Journal on Selected Areas in Communications*, Vol. 34, No. 12, pp. 3451–3465, Dec 2016.
88. Nanan, J. C. and B. Stern, "Small Cells Call for Scalable Architecture", *Freescale White Papers*, May 2013.
89. Khan, F. and M. Portmann, "Backhaul, QoS, and channel-aware load balancing optimization in SDN-based LTE networks", *IEEE Int. Conf. on Signal Procc. and*

*Comm. Systems* , Dec 2017.

90. Jain, R. (Editor), *The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation and Modeling*, Wiley, New York, 1991.
91. ETSI, S., “Next Generation Protocols (NGP); Scenario Definitions”, *GS NGP Industry Specification Group (ISG)*, Vol. 1.3.1, 2019.
92. Zhou, J., Z. Cao, X. Dong and A. V. Vasilakos, “Security and Privacy for Cloud-Based IoT: Challenges”, *IEEE Communications Magazine*, Vol. 55, No. 1, pp. 26–33, January 2017.
93. Roman, R., J. Lopez and M. Mambo, “Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges”, *Future Generation Computer Systems*, Vol. 78, pp. 680 – 698, 2018.
94. Khan, M. A. and K. Salah, “IoT security: Review, blockchain solutions, and open challenges”, *Future Generation Computer Systems*, Vol. 82, pp. 395 – 411, 2018.
95. Airehrour, D., J. Gutierrez and S. K. Ray, “Secure routing for internet of things: A survey”, *Journal of Network and Computer Applications*, Vol. 66, pp. 198 – 213, 2016.
96. Duan, J., D. Gao, D. Yang, C. H. Foh and H. Chen, “An Energy-Aware Trust Derivation Scheme With Game Theoretic Approach in Wireless Sensor Networks for IoT Applications”, *IEEE Internet of Things Journal*, Vol. 1, No. 1, pp. 58–69, Feb 2014.
97. Wu, J., T. Song, Y. Yu, C. Wang and J. Hu, “Generalized Byzantine Attack and Defense in Cooperative Spectrum Sensing for Cognitive Radio Networks”, *IEEE Access*, Vol. 6, pp. 53272–53286, 2018.

98. Atapattu, S., C. Tellambura and H. Jiang, *Energy Detection for Spectrum Sensing in Cognitive Radio*, Springer Publishing Company, Incorporated, 2014.
99. Benedetto, F. and G. Giunta, “A Theoretical Analysis of Asymptotical Performance of Cooperative Spectrum Sensing in the Presence of Malicious Users”, *IEEE Wireless Communications Letters*, Vol. 7, No. 3, pp. 380–383, June 2018.