Winter 2018

Coexistence and Secure Communication in Wireless Networks

Saygin Bakşi
Old Dominion University, sayginb@gmail.com

COEXISTENCE AND SECURE COMMUNICATION IN WIRELESS NETWORKS

by

Saygın Bakşi
B.Sc. January 2010, Işık University
M.Sc. June 2013, Işık University

A Dissertation Submitted to the Faculty of
Old Dominion University in Partial Fulfillment of the
Requirements for the Degree of

DOCTOR OF PHILOSOPHY

ELECTRICAL & COMPUTER ENGINEERING

OLD DOMINION UNIVERSITY
December 2018

Approved by:

Dimitrie C. Popescu (Director)

Chunsheng Xin (Member)

Jiang Li (Member)

Otilia Popescu (Member)

ABSTRACT

COEXISTENCE AND SECURE COMMUNICATION IN WIRELESS NETWORKS

Saygın Bakşi
Old Dominion University, 2018
Director: Dr. Dimitrie C. Popescu

In a wireless system, transmitted electromagnetic waves can propagate in all directions and can be received by other users in the system. The signals received by unintended receivers pose two problems; increased interference causing lower system throughput or successful decoding of the information which removes secrecy of the communication. Radio frequency spectrum is a scarce resource and it is allocated by technologies already in use. As a result, many communication systems use the spectrum opportunistically whenever it is available in cognitive radio setting or use unlicensed bands. Hence, efficient use of spectrum by sharing users is crucial to increase maximize system throughput. In addition, secrecy of a wireless communication system is traditionally provided by computational complexity of cryptography techniques employed. However, cryptography systems depend on either a random secret key generation mechanism or a trusted key distribution system. Recent developments in the wireless communication area provided a solution to both key generation and distribution problem via exploiting randomness of the wireless channel unconditional to the computational complexity.

In this dissertation, we propose solutions to the problems discussed. For spectrum sharing, we present a detailed analysis of challenges of efficient spectrum sharing without a central enforcing mechanism, provide insight to already existing power control algorithms and propose a novel non-greedy power allocation algorithm. Numerical simulations show that the proposed algorithm increases system throughput more than greedy algorithms and can use available spectrum to the fullest, yet it is robust to the presence of greedy users. For secrecy, we propose a practical and fast system for random secret key generation and reconciliation. We extend the proposed system to multiple-input-multiple-output systems and increase security via role reversal of the nodes while making it quicker by pre-encoding procedure. Information theory calculation and numerical simulations demonstrates that the proposed system provides a secure channel for legitimate users in the presence of a passive eavesdropper.

ACKNOWLEDGMENTS

There are many people whom I would like to thank for their help and support throughout my long journey at Old Dominion University.

First and foremost, I would like to thank my advisor Dr. Dimitrie C. Popescu for his endless support, both academic and personal. He graciously gave me the freedom to find and study the topics I am interested in, yet, provided guidance whenever needed to make sure I was never lost. His help reached beyond academics and I was very lucky to feel his constant support during recovery from my unexpected injury. Words cannot describe how grateful I am to have him as my advisor.

I have immense gratitude for my committee members, (in no particular order) Dr. Otilia Popescu, Dr. Jiang Li and Dr. Chunsheng Xin. Their support, feedback and genuine interest in my dissertation led to this great accomplishment and the improvement of my dissertation.

Throughout my journey at Old Dominion University, I was lucky to be supported by an assistantship from the Electrical and Computer Engineering Department. I have learned a great amount from both faculty and staff which led me to improve both as an engineer and a person. I would especially like to thank Dr. Lee Belfore and Dr. Vishnukumar Lakdawala for taking extra time to provide feedback, to guide and support me during my assistantship.

I would like to thank John Snoap for his help with my research. It was a pleasure to work with John and I appreciate all the time we spent on valuable discussions as we explored physical layer security together. My lab mates Prosanta Paul and Peng Jiang were always friendly, reliable and ready to help however they could. They contributed to my experience at ODU in many ways, and thanks to them, long days at the lab felt enjoyable.

I am grateful to have Dr. Onur Kaya as my master's advisor, whose guidance and encouragement led me to pursue my Ph.D. degree. Without him, I would not be here today.

Thanks to my friends, I was able to have fun without talking about research, which kept me sane. During my hardest times, Alex Salas was there to help me and this dissertation would not be possible without his support and friendship.

I would like to thank Mercedes Hunt for her neverending support and encouragement, even when I felt down. She has made my life more beautiful everyday and her existence in my life has made me a better person.

Finally, I would like to thank my family for believing in me without hesitation and for their endless support in every way imaginable. My parents and my brother always had a vast, positive impact on my life and I appreciate them a bit more every single day.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

Figure Page

CHAPTER 1

INTRODUCTION

Wireless communication systems along with the services they provide have become an essential component of the modern society. The number of new devices that employ wireless communication is constantly growing. As a result, services we use via these devices get more complex everyday and require more resources. Two of the main components of these services are transmission rate and security as we would like to access to a service quickly and securely. Due to the nature of wireless systems, the electromagnetic waves propagate in all directions and can be received by any device within proximity, which makes achieving both goals very challenging.

The main physical resource used by wireless systems, the frequency spectrum, is limited by the capabilities of the electronic devices and many frequency bands of interest are already licensed to specific wireless systems. Therefore, there is not enough spectrum available to new systems and applications which in turn forces new systems to use unlicensed or ISM bands. In addition, these systems may have many users, especially in crowded environments and the interference created by users can degrade the transmission rate for everyone. Due to these challenges, a smart way of sharing the available spectrum is needed to maintain the service quality and innovation for new services.

The services used via a wireless device store critical data about the users, and this information is exchanged with the servers constantly. Any wireless device within proximity can receive the wireless signals and try to access critical information that is shared with the server. To overcome information leak, the data is typically sent and received encrypted; thus, a malicious person without the encryption key cannot access the data. Traditionally, encryption is implemented in the application layer. With recent developments, new techniques that exploit the random nature of the wireless channel have been developed as an additional security layer on top of the existing ones to further improve security.

In this dissertation, we will discuss and try to solve both problems.

1.1 CO-EXISTENCE OF WIRELESS SYSTEMS

In wireless communication systems, the information is embedded into electromagnetic waveforms by the transmitter and sent to the receiver. Due to the nature of the system, electromagnetic waves propagate in all directions and can be received by all receivers that are listening on the same frequency channel. In a scenario where multiple users are trying to use the same set of frequencies, each transmitter creates interference to the other receivers, thus forcing other transmitters to increase transmission power to compensate for the interference. In the end, the total interference increases, reducing the transmission rates of individual users and system throughput.

Another problem with wireless communication systems is that the usable spectrum is already licensed and many new systems are designed to use limited unlicensed bands or ISM bands. However, these licensed bands may not be used at all times; thus, the spectrum becomes underutilized. To use the spectrum more efficiently, cognitive radio was proposed. In cognitive radio, the unlicensed users may use the licensed bands as long as they do not create interference to the licensed users. This approach increases spectrum efficiency but creates another problem between unlicensed users. Unlike licensed users, unlicensed users are not controlled by a central authority; therefore, they all have to choose the frequencies they would like to use. As there is no priority between unlicensed users, they can freely use the available spectrum to maximize their transmission rates without considering the interference created to the other users. If the spectrum is not shared wisely, the amount of interference can be out of control and limit the system throughput. In addition, there is no enforcement mechanism for a user to control the interference she creates, which can further damage the transmission rates of the users who limit their created interference.

In this dissertation, we will introduce several power control mechanisms and their performance in terms of system throughput in a distributed system. We will also consider the case where only some of the users are employing the proposed algorithm and the rest of the users are greedy and do not try to control their interference to the other users. In the end, we will propose a new heuristic algorithm that is both robust to the existence of greedy users and ensures high system throughput.

1.2 SECURE COMMUNICATION

Due to the shared nature of the transmission medium used – the radio frequency (RF) spectrum, wireless communications are inherently insecure and prone to eavesdropping. To protect against eavesdropping and to ensure confidentiality of transmitted data, many wireless systems employ encryption using secret keys available only to the transmitter and the corresponding legitimate receiver. However, guaranteeing agreement between the secret keys at transmitter and receiver poses a formidable challenge when the key must be exchanged over an insecure channel, and the agreement must be accomplished such that legitimate users can reveal the secret key while eavesdroppers are unable to do so.

In recent years various physical layer approaches have been proposed for generating encryption keys using channel state information to avoid difficulties associated with secret key distribution and management. These approaches use the inherent randomness of wireless channels and take advantage of the reciprocity properties of the channel between a wireless transmitter and its corresponding legitimate receiver to establish secret keys which cannot be recreated by eavesdroppers overhearing the information exchanged over an uncorrelated channel.

Secret key generation at the physical layer avoids the need for key distribution or exchange since the keys become known to the transmitter and the legitimate receiver during the generation process. Furthermore, with time-varying wireless channels keys can be renewed dynamically using new measurements of the channel parameters. In this dissertation, we will propose a novel key generation technique for both SISO and MIMO systems with key reconciliation by Low-Density Parity-Check (LDPC) codes for practically fast key generation.

1.3 DISSERTATION ORGANIZATION AND CONTRIBUTIONS

This dissertation is composed of proposed solutions to two main problems for wireless communication networks.

The first problem, distributed spectrum sharing in mutually interfering wireless networks is covered in Chapters 2 and 3. In Chapter 2, the system model and problem statement is presented. Various spectrum sharing scenarios are explained and two main power allocation

algorithms from the literature is introduced. In addition to existing algorithms, DPARM algorithm is proposed as an alternative for distributed spectrum sharing that is suitable for both dense and sparse environments. The performance of the algorithms are presented with numerical simulations. In Chapter 3, the robustness of the algorithms is explained. Basically, the algorithms are divided into two groups, greedy and non-greedy. As the system in consideration does not have a central enforcing mechanism, the users in the system are assumed to be using either type of the power allocation algorithms and the performance of the power allocation algorithm in the presence of greedy users is studied. In the end, a new DPARM-inspired algorithm robust to greedy user presence is proposed. The results of this study are published in the following journal and conferences.

- S. Bakşi, D.C. Popescu, "Distributed Power Allocation for Rate Maximization in Cognitive Radio Networks with Horizontal Spectrum Sharing", *IEEE Wireless Communications and Networking Conference*, New Orleans, LA, April 2015 [1].

- S. Bakşi, D.C. Popescu, "Horizontal Spectrum Sharing and Coexistence Scenarios for Mutually Interfering Wireless Systems", *IEEE BlackSeaCom 2015*, Constanta, Romania, May 2015 [2].

- S. Bakşi, D.C. Popescu, "Distributed Power Allocation for Spectrum Sharing in Mutually Interfering Wireless Systems", *Physical Communication*, vol. 22, pp. 42–48, 2017 [3].

The second problem, secure communication, is discussed in Chapters 4 and 5. In Chapter 4, we introduce a novel secret key generation and reconciliation system that exploits the randomness of the wireless channels. The proposed system is designed to be fast and practical; therefore it does not require channel variance estimation prior to key generation process. Moreover, the calculation of the Log-Likelihood-Rates (LLR) of the channel samples are fast to calculate. The system performance is evaluated in a realistic scenario where the side information created by leader node is transmitted via a noisy channel and key mismatch rates are calculated as a result of errors in both key generation and key reconciliation processes. In Chapter 5, the secure key generation is extended to MIMO systems. A novel

pre-encoding system that scrambles the channel measurements to remove dependency on channel coherence time is proposed. Moreover, a unique role reversal system is proposed to increase security when eavesdropper is physically located near one of the legitimate nodes. The results of this study are published in conferences, and submitted to be published in journal form as noted below.

- S. Bakşi, J. Snoap, D.C. Popescu, "Secret Key Generation Using One-Bit Quantized Channel State Information", *IEEE Wireless Communications and Networking Conference (WCNC)*, San Francisco, CA, March 2017 [4].

- S. Bakşi, D.C. Popescu, "Secret Key Generation in MIMO Wireless Systems Using Precoded Channel Measurements",*IEEE PIMRC 2017*, Montreal, Canada, Oct. 2017 [5].

- S. Bakşi, D.C. Popescu, "Secret Key Generation with Precoding and Role Reversal in MIMO Wireless Systems", *Submitted to IEEE Transactions on Wireless Communications*, July 2018 [6].

Finally, in Chapter 6, the dissertation concludes with a summary of dissertation contributions and discussions of future work that can further improve the results presented in the dissertation or change the direction of it.

Table 1. Organization of the Dissertation

Chapter 1	Introduction
Chapter 2	Distributed Spectrum Sharing in Mutually Interfering Wireless Networks
Chapter 3	Distributed Spectrum Sharing Robust to Greedy User Presence
Chapter 4	Secret Key Generation and Reconciliation in Wireless Communication
Chapter 5	Secret Key Generation and Reconciliation with MIMO Pre-coding and Role Reversal
Chapter 6	Conclusion and Future Work

CHAPTER 2

COEXISTENCE WITH DISTRIBUTED POWER ALLOCATION

Constant increase in demand to high speed wireless connection forces communication systems to use more and more power over multiple channels in order to match the transmission rate to the requested speeds. As we increase transmission power and the number of frequency bands used for a communication system, other communication systems see increased interference and fewer available frequency channels. This forces them to increase their transmission power and the number of frequency channels used to maintain their transmission speed as spectrum is a shared resource. As a result, a vicious cycle occurs and total interference in the system increases while reducing the system throughput. In this chapter, we introduce distributed spectrum sharing and define various distributed spectrum sharing techniques. We propose a new distributed power allocation algorithm that is suitable for both dense and sparse environments for spectrum sharing. The algorithm is tested with numerical simulations and compared to iterative water-filling and GADIA.

The chapter is organized as follows: in Section 2.1, we give the background information from the literature on horizontal spectrum sharing. In Section 2.2, we introduce the system model and discuss potential spectrum utilization scenarios,. In Section 2.3, we introduce several power allocation strategies in the literature, and the following Section 2.4 introduces our proposed distributed power allocation for rate maximization algorithm. We conclude the chapter with numerical simulations in Section 2.5, followed by the chapter summary in Section 2.6.

2.1 BACKGROUND ON HORIZONTAL SPECTRUM SHARING

The spectrum sharing problem occurs in any communication scenario with mutually interfering links [7], and applying approaches based on water filling procedures such as iterative

water filling [8] does not lead to efficient spectrum use [9]. As discussed in [9, 10] multiple equilibrium points are possible for iterative waterfilling, and these may result in suboptimal spectrum use. Spectrum sharing was studied in the literature in various contexts such as wireless communications in unlicensed bands [11], power control via pricing [12,13] or digital subscriber line (DSL) networks [14, 15].

In [11] an interference avoidance algorithm is proposed by using a game theoretic approach. The algorithm depends on channel state information between all users and measurement of channel state is open to misinformation attacks by malicious users. We note that, while protocols to overcome misleading attacks are proposed in [11], these along with the required channel state measurements, increase the complexity of the proposed algorithm, which becomes impractical as the number of users sharing the spectrum increases.

In DSL networks, bundling cables creates crosstalk (electromagnetic interference) between individual cables in the bundle, resulting in lower transmission rate for users. Although the system is not wireless, the same spectrum is used by all users and the effect of crosstalk is similar to that of interference in a wireless communication system. However, there are fundamental differences between DSL and wireless networks. In DSL systems, the loops are frequency selective, while in wireless communication, a flat fading assumption can usually be made. In addition, the channel gains in DSL loops are not changing over time; therefore, perfect knowledge of the channel for all times is possible, which is usually not the case for wireless channels. Thus, although the results for DSL systems are not directly applicable to wireless systems, they give important insight into the problem of spectrum sharing in wireless systems.

Mutually interfering wireless systems are also studied in [16,17], where several algorithms to reduce interference in shared spectrum are proposed. These are based on allocating transmission powers and frequency bands by using feedback from users in the system. We note that, even though ideally, user feedback should increase the performance of the system, it also creates potential security problems.

More recently, GADIA [18] was proposed for wireless communication systems that share available spectrum. GADIA tries to minimize the interference in the system while maximizing the net utilization of the system resources, and is applicable to dense environments

where the number of users in the system is much larger than the number of available channels (frequency bands). However, with the main goal of GADIA being interference minimization rather than maximization of user transmission rates, the algorithm may result in low system throughput in sparse environments.

2.2 SYSTEM MODEL AND SPECTRUM SHARING SCENARIOS

In this chapter, we consider a cognitive radio (CR) network consisting of secondary users (SU) accessing spectrum not allocated (or actively used) by primary users (PU)[1]. For simplicity, we assume all the SU links consist of a transmitter (TX) and a receiver (RX), and we will use the term user to represent a secondary transmitter and receiver pair throughout the dissertation. In the system, there are N number of users located randomly on a disk of radius r with uniform random distribution. The system has F number of orthogonal frequency bands available for SU access. The total transmit power of each user i is $P_i = \bar{P}$, where $i \in \{1, 2, \ldots, N\}$, and channel gains on all wireless links are denoted as h_{ij} which represents the channel gain from SU i TX to SU j RX. We assume that channel gains are a function of the corresponding distance between TX and RX, denoted d_{ij}, and that the signal attenuation exponent is η. For illustration, a three user system is shown schematically in Fig. 1.

In this context, we assume that there are no priorities associated with users, such that horizontal sharing of the frequencies available to SUs is accomplished with no central control or coordination among users, and we study a distributed approach for spectrum sharing by which each user attempts to maximize its transmission rate, while trying not to increases the total interference in the system. Unlike greedy approaches where users attempt to use all available channels, in our proposed approach users gradually increase the number of frequencies over which they transmit, provided that this does not interfere with other users in the system.

In a horizontal spectrum sharing scenario where we have N mutually interfering users

[1]The frequency bands that are allocated (or actively used) by PUs are detected by all SUs in the system and not included into the set of available frequency bands.

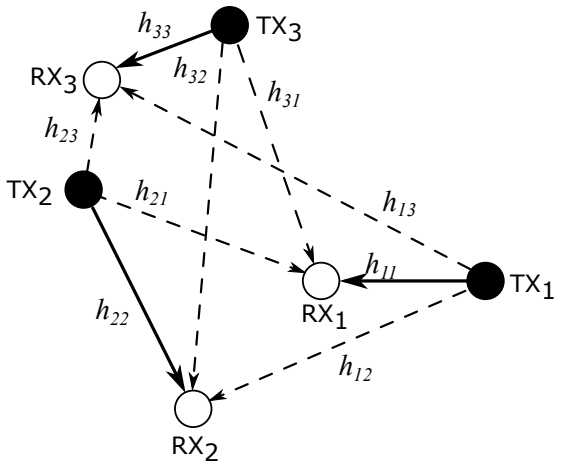


Figure 1. Representation of a system with three secondary users

sharing a set of F channels (implied by non-overlapping frequency bands) with no coordination mechanism assigning priorities to users or enforcing specific rules established for accessing the spectrum. Each user is associated with a link consisting of a transmitter and receiver pair, with transmitters having a power constraint denoted by $P_i = \bar{P}$, where $i \in \{1, 2, \ldots, N\}$. We assume all channels are available to all users at all times, and since there are no priorities defined for users, they may distribute their transmit power over the entire spectrum by using different strategies, leading to three main types of spectrum sharing scenarios:

- **Complete Overlap**: All the users distribute their available power over the entire spectrum, such that all channels are actively employed by all users, resulting in mutual interference in all the channels. This scenario is illustrated in Fig. 2 where a set of 9 channels is shared by 3 users, with each user allocating the same amount of power to each channel.
- **Separation**: Users allocate their power in orthogonal channels, and thus they do not interfere with each other. This scenario, which is illustrated in Fig. 3, is possible only when the number of active users less than or equal to the number of available channels.
- **Partial Overlap**: Users allocate their powers such that they may overlap in one or more channels but not in all channels, creating different levels of mutual interference in different frequency bands. This scenario is illustrated in Fig. 4.

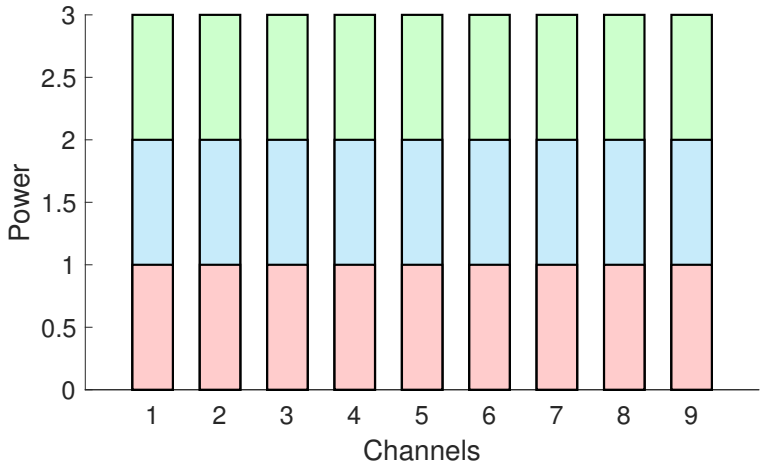


Figure 2. Complete overlap scenario for 3 users sharing 9 channels.

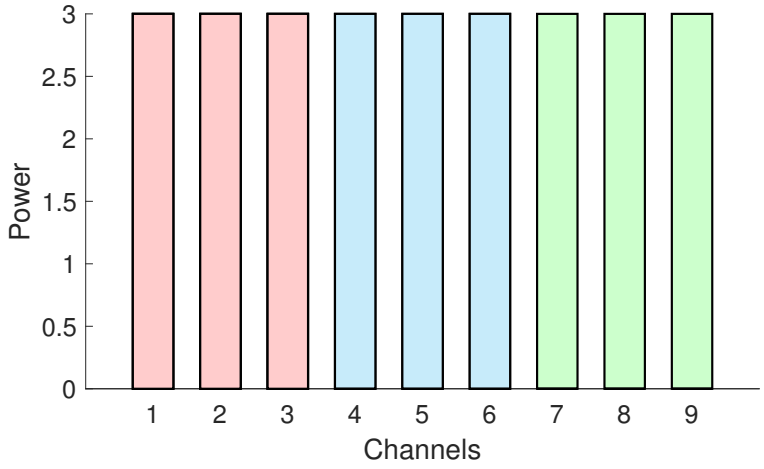


Figure 3. Separation scenario for 3 users and 9 channels.

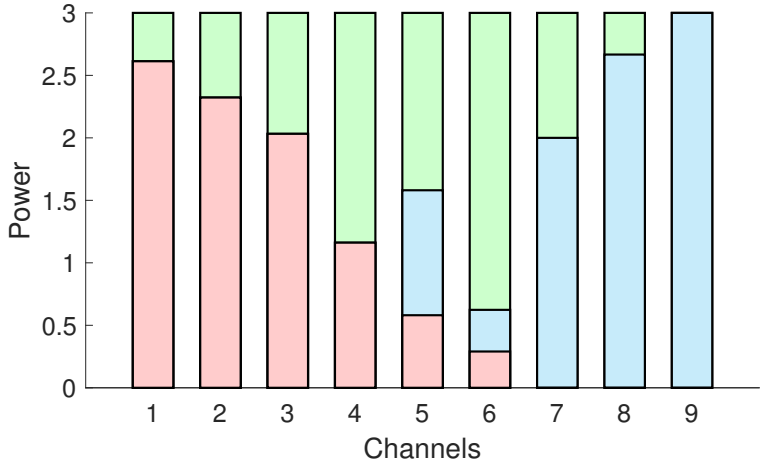


Figure 4. Partial overlap scenario for 3 users and 9 channels.

2.3 POWER ALLOCATION STRATEGIES

The power allocation strategies considered in our study are: the iterative water filling procedure [8], the GADIA algorithm [18], and the recently proposed algorithm for distributed power allocation and rate maximization [1].

2.3.1 ITERATIVE WATER-FILLING

When multiple channels with different noise levels are available for transmission, an individual user may apply the water filling procedure to distribute its transmitted power over all channels in order to maximize its transmission rate. In a multiuser setting, users apply the water filling procedure iteratively by assimilating interference with noise [8]. Iterative water filling is a greedy procedure which allows users to allocate power on all channels according to the respective levels of interference+noise experienced, and converges to a simultaneous water filling distribution of power for all users. Depending on the actual interference level, the resulting spectrum sharing scenario implied by iterative rate filling involves partial or complete overlap of users and can result in poor utilization of the shared spectrum as indicated by the total system throughput [9].

2.3.2 THE GADIA ALGORITHM

The GADIA algorithm [18] aims to mitigate mutual interference among users sharing the spectrum by limiting the number of channels over which users can allocate their power to a single one. Unlike iterative water filling where power is allocated to maximize individual user rates, the GADIA algorithm focuses on maximizing a different metric dubbed network utilization, and user rates or system throughput are not considered in the power allocation procedure. Moreover, limiting users to a single channel makes GADIA suited for dense environments where the number of users is larger than the number of channels to be shared, and where assigning single channels to users makes practical sense. However, as it will be seen in our study, in sparse environments where the number of users is less than the number of available frequency bands, assigning each user only one channel is strictly inefficient in terms of system throughput. We note that, in spite of its name, the GADIA algorithm is a

non-greedy approach to spectrum sharing since it tries to avoid creating mutual interference.

GADIA [18] solves the mutual interference problem by limiting the number of bands over which users can allocate their power to a single frequency, and power allocation implied by GADIA maximizes the network utilization function defined as

$$U = -\sum_{i} I_i P_i \tag{1}$$

where I_i is interference received by user i and P_i is power of user i. However, GADIA mainly focuses on dense environments where the number of users is much larger than the number of available frequency bands, and where assigning single frequencies to users makes practical sense.

We note that, limiting the number of frequency bands over which a given user can allocate its power can be detrimental in sparse environments, where assigning more frequencies to users is a more practical approach, and we conclude this section by noting that our proposed approach, presented in detail in the following section, enables more efficient use of available frequencies in a sparse environment, while preserving the benefits of GADIA in dense environments.

2.4 DISTRIBUTED POWER ALLOCATION FOR RATE MAXIMIZATION

Our proposed approach is based on allowing users to dynamically update the number of frequencies over which they can allocate their transmitted power. Specifically, users gradually increase the number of frequencies over time using an individual decision metric in terms of bits/hertz/transmission defined as:

$$G_i = \sum_{m=1}^{L_i} \log_2 \left[1 + \frac{h_{ii}^{(m)} P_i^{(m)}}{\sigma^2 + \sum_j h_{ji}^{(m)} P_j^{(m)}} \right] + \sum_{m=1}^{M} \log_2 \left[1 + \frac{\sum_j h_{ji}^{(m)} P_j^{(m)}}{\sigma^2 + h_{ii}^{(m)} P_i^{(m)}} \right], \tag{2}$$

where $m \in \{1, 2, \ldots, F\}$, $i, j \in \{1, 2, \ldots, N\}$, $i \neq j$, $h_{ij} = d_{ij}^{-\eta}$ and L is limit of number of frequency bands that user i is allowed to use. The decision metric function is designed to make users polite to each other, such that instead of greedy maximization of its own

transmission rate, a given user treats interference as if it is the received power of a virtual user, and tries to maximize the sum rate taking the virtual user into account. Therefore, by applying this strategy, the other users' transmission rates are affected less than when greedy water filling is applied. Since the power allocations of all users are mutually dependent, users will be compelled to vacate some spectrum to avoid interference, instead of allocating its power over all the available frequency bands.

At a given iteration, user i is allowed to use a maximum number of L_i frequency bands, and will attempt to maximize their own transmission rate

$$\max_{P_i} R_i(L_i), \tag{3}$$

where the transmission rate for user i is defined as

$$R_i(L_i) = \sum_{m=1}^{L_i} \log_2 \left(1 + \frac{h_{ii}^{(m)} P_i^{(m)}}{\sum_{j=1, j\neq i}^{N} h_{ji}^{(m)} P_j^{(m)} + \sigma^2} \right), \quad i, j = 1, \ldots N. \tag{4}$$

We note that the limit L_i on how many frequency bands a given user i can employ for power allocation is dynamic and is increased by one after each iteration. Since there is no limit on maximum value of L_i, users may use all the available spectrum if no other users are seeking to use the spectrum, which ensures spectrum ends up being used efficiently. We also note that, for maximizing the transmission rate water-filling must be applied, but, each user will apply water-filling within their limited number of frequency bands.

After water filling application, the decision function (2) is used to assess the efficiency of the power allocation, and then the process is repeated iteratively as outlined in Fig. 5.

2.5 SIMULATIONS

In this section we present simulation results that illustrate the total rate performance of the proposed algorithm, and compare it with that of alternative algorithms for power allocation which include GADIA, iterative water filling, and uniform power distribution over

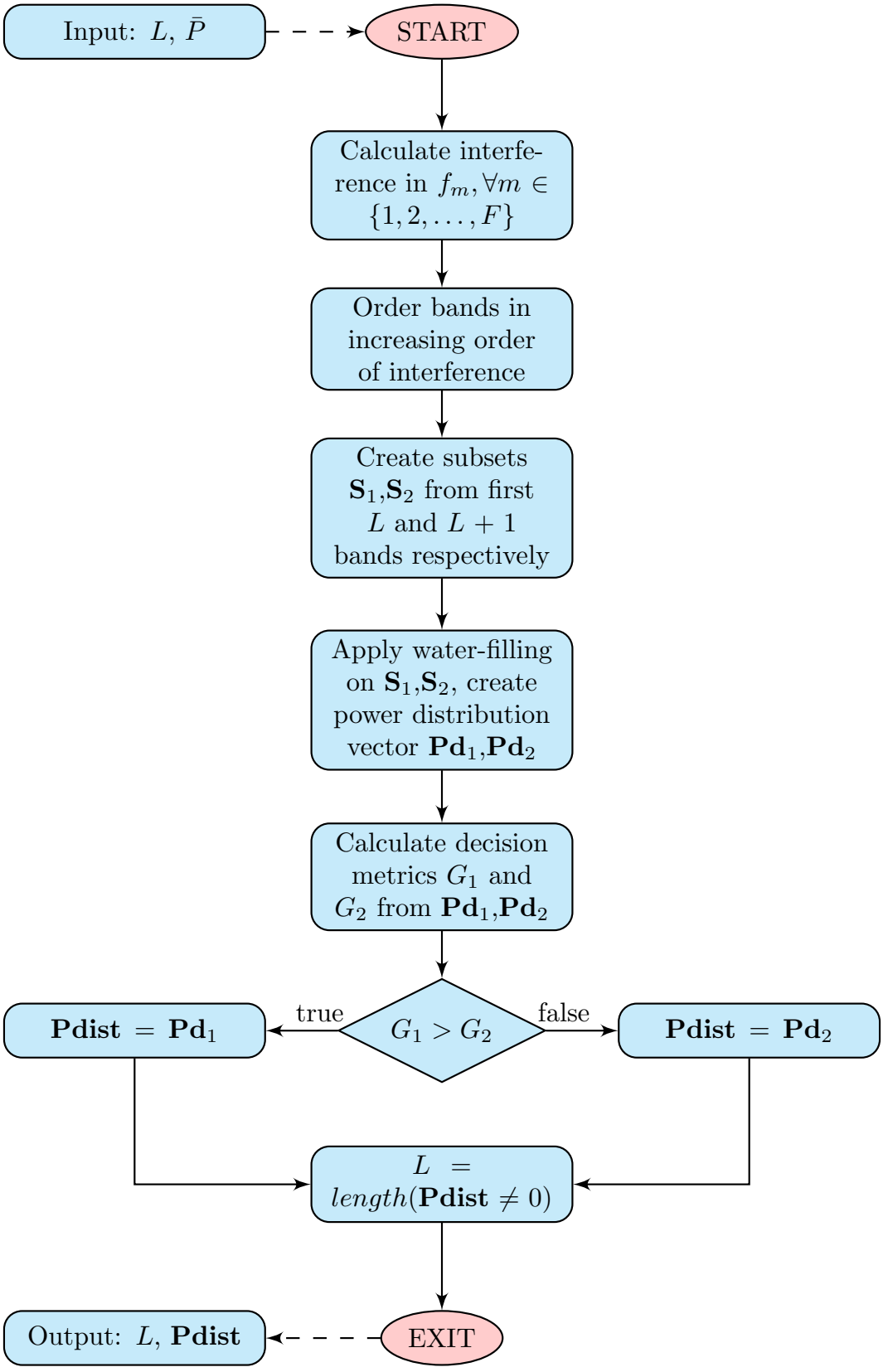


Figure 5. Proposed algorithm for distributed power allocation

all frequencies (complete overlap scenario).

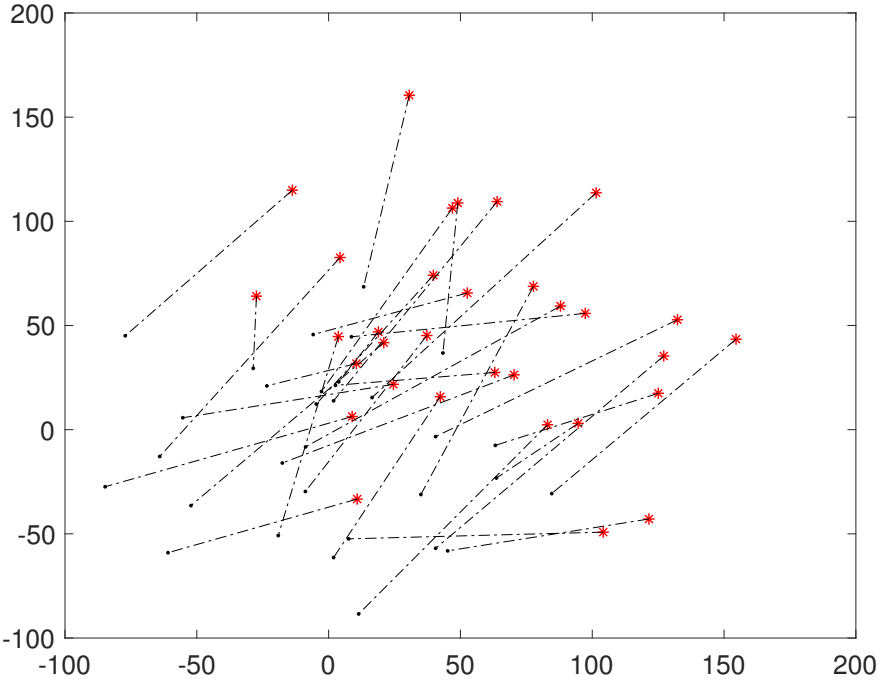
The simulation setup consists of N SU links with TX and RX at random locations uniformly distributed inside a circular region with radius $r = 100$. A free-space propagation environment was considered for which the path loss exponent $\eta = 2$. For each different constellation of users, the simulation was run for 5 times and the corresponding plot was obtained by taking the average of total transmission rates normalized by the number of available channels. The power spectral density of the noise at all RX is $\sigma^2 = 10^{-8}$, and user powers are equal and normalized to one, that is, $\bar{P}_i = 1$, for $i \in \{1, 2, \ldots, N\}$. The plotted rates are normalized by calculating the total rate per user per channel.

2.5.1 SPARSE ENVIRONMENT

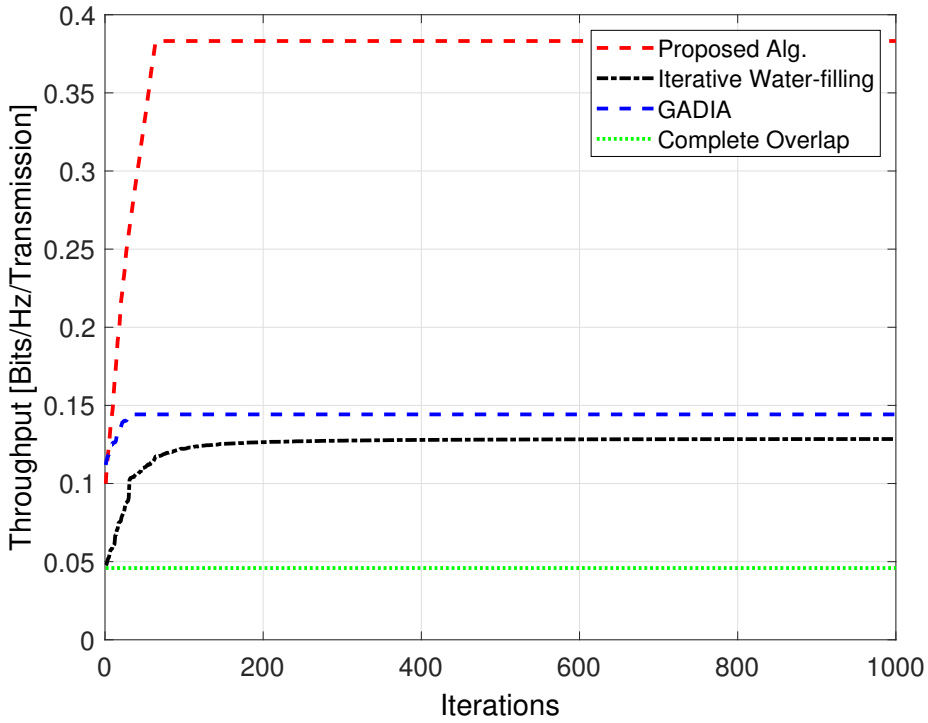
For this scenario, the number of users is $N = 32$ and number of available frequency bands is $F = 96$, and Figure 6 shows a sample simulation with typical user constellations and the variation of the total rate during the algorithm. In this case, the proposed algorithm outperforms all the other algorithms since users are allocating power over most frequency bands while trying to avoid creating interference to other users. Almost all users use the same number of distinct frequency bands for power allocation (which is equal to 3 for the considered example) and the total interference experienced by users is very small, leading to very high rate values. For GADIA, users allocated power only on one frequency band which ensures no interference is generated. However not all of the frequency bands are allocated, and the system throughput is lower than that corresponding to our proposed algorithm. For the water-filling case, most users use more frequency bands than used with GADIA or our proposed approach. Because of this, the resulting rates are larger than those obtained with GADIA, but lower than with our proposed algorithm, since interference among users is higher.

2.5.2 DENSE ENVIRONMENT

For this scenario, the number of users is $N = 100$ and the number of available frequency bands is $F = 4$, and Figure 7 shows a sample simulation with typical user constellations and the variation of the total rate during the algorithm. Since all the frequency bands have high

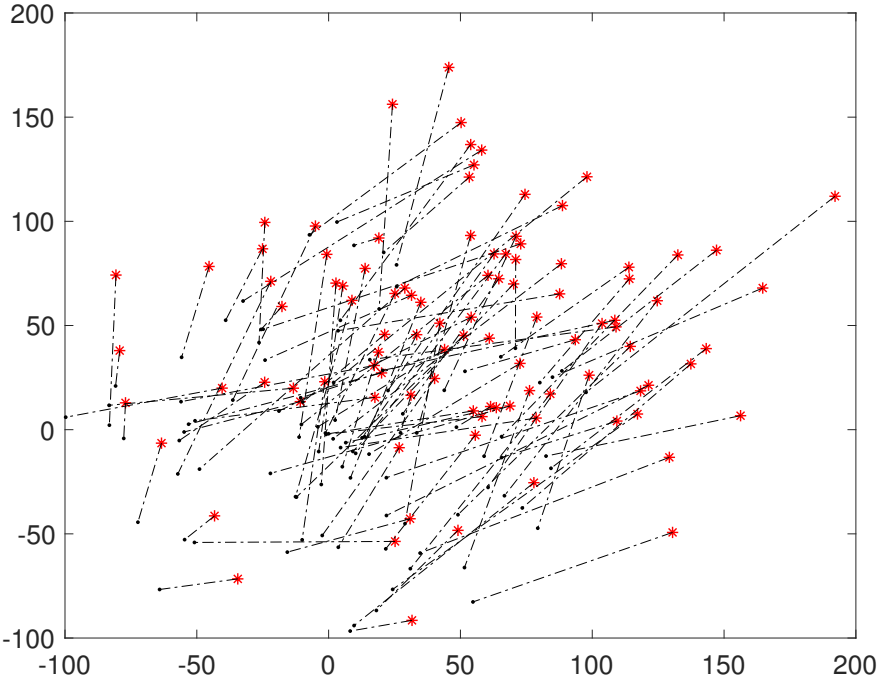


(a) User constellation

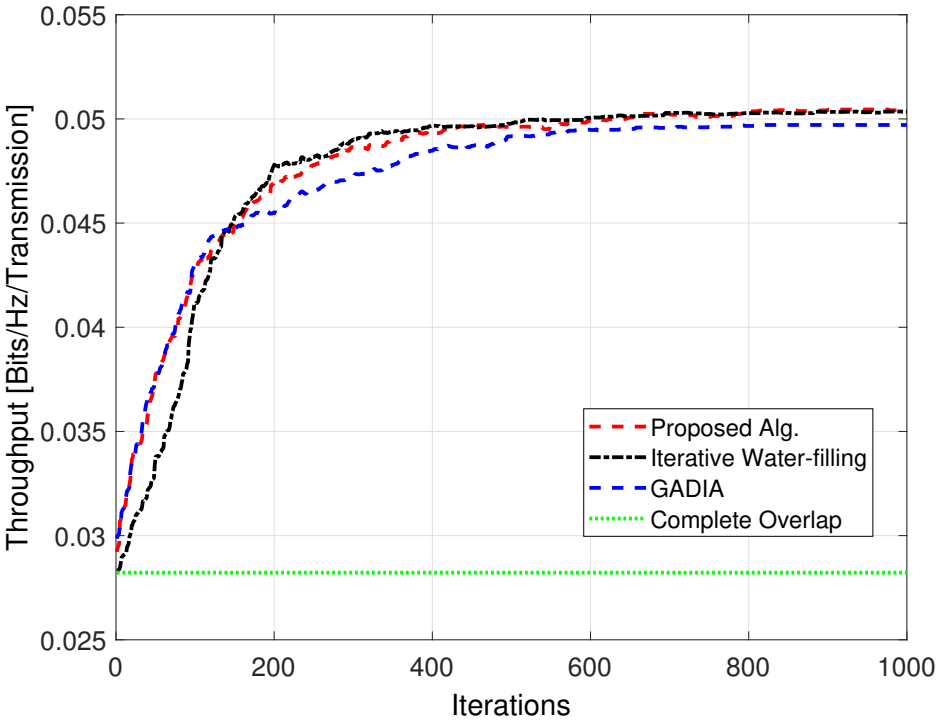


(b) Total transmission rate

Figure 6. Sample simulation results for sparse environment



(a) User constellation



(b) Total transmission rate

Figure 7. Sample simulation results for dense environment

interference levels in dense environments, the proposed algorithm behaves similar to GADIA and avoids creating interference by allocating only one frequency to most users. Thus, the total transmission rate is very close to the one obtained applying GADIA. It is also worth noting that, in the dense user scenario, power allocation obtained by applying water filling converges to a total transmission rate that is similar, although the actual power allocations of users are not similar.

2.6 CHAPTER SUMMARY

In this chapter, we outlined the problem of horizontal spectrum sharing in cognitive radio networks and proposed a new algorithm for distributed power allocation that maximizes a given user's rate while avoiding interference to the other users in the system. The proposed algorithm is based on a new metric which enables users to decide if their power allocation over the available spectrum leaves enough room for other users, so that the total interference in the system is reduced and the system throughput is increased.

The proposed algorithm is illustrated with numerical results obtained from simulations, which compare the total transmission rate achieved with the proposed algorithm to that achieved by GADIA and by the iterative water filling procedures. Results indicate that the proposed algorithm outperforms GADIA and iterative water-filling algorithms in sparse environments, while having similar performance in dense environments, thus offering a meaningful alternative for solving horizontal spectrum sharing problem in cognitive radio networks.

CHAPTER 3

POWER ALLOCATION WITH INTERFERENCE CONTROL

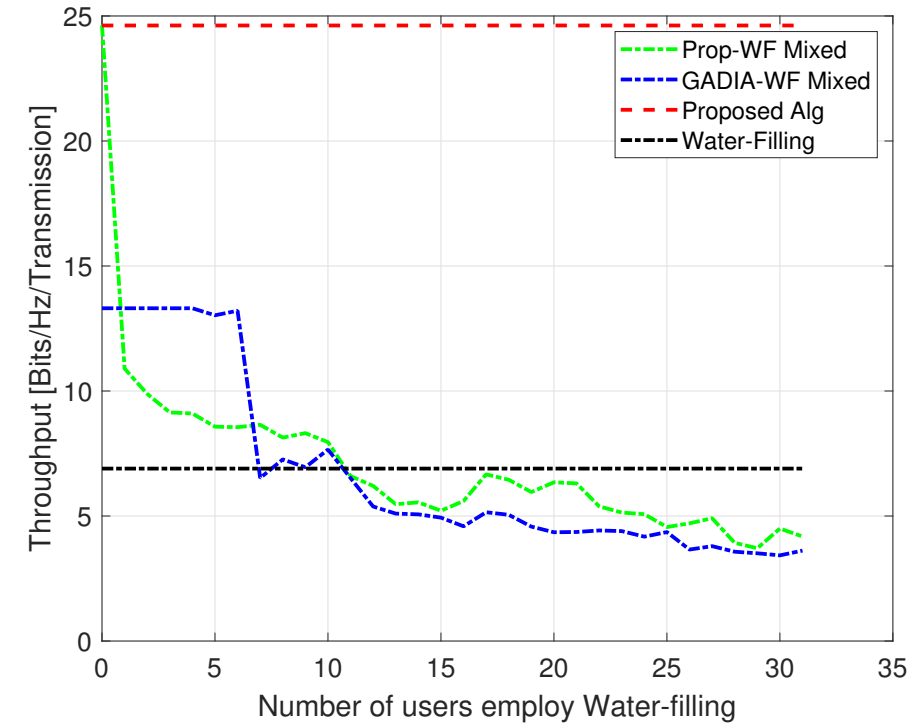
Although approaches like GADIA and DPARM (as introduced in Chapter 2) are desirable from both spectrum utilization and system throughput perspectives, without a coordinating mechanism to enforce their application by all users, greedy transmitters cannot be prevented from using all available frequency bands and distribute their power according to the water filling algorithm. Moreover, as the number of greedy users increases, the total system rate declines rapidly [2]. This motivates the work presented in this chapter, in which a new non-greedy algorithm for power allocation is presented. The proposed algorithm requires no central control or coordination and allows transmitters to gradually use more frequencies to allocate transmit power as long as the desired signal dominates interference, which requires that the signal-to-interference ratio (SIR) in the chosen frequencies be larger than one.

The chapter is organized as follows: the effect of presence of greedy users in the network is studied in Section 3.1. Based on the findings, a new algorithm for rate maximization with interference control is presented in Section 3.2. The performance of the new algorithm is illustrated with numerical results obtained from simulations for both sparse and dense wireless scenarios in Section 3.3. The chapter is concluded with final remarks in Section 3.4.

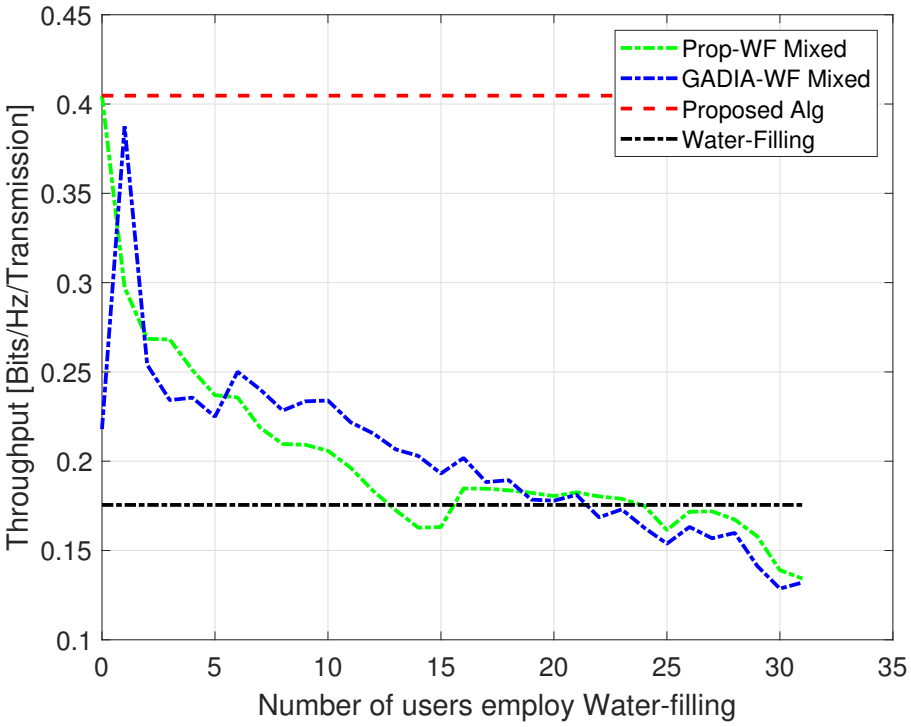
3.1 SPECTRUM SHARING WITH GREEDY AND NON-GREEDY USERS

To evaluate the presence of greedy users' effects on co-existence and spectrum sharing, we consider a case study in both sparse and dense environments, where some users perform greedy power allocation based on iterative water filling while others use the non-greedy approaches based on GADIA or DPARM algorithm outlined in the previous chapter.

To illustrate the total and individual rate performance we perform simulations with different numbers of greedy users. In each simulation, one user is observed and fixed with an algorithm, while other users apply either the observed users' non-greedy algorithm or



(a) Individual transmission rate



(b) Total transmission rate

Figure 8. Illustration of non-greedy user behavior in sparse environments.

water-filling. For comparison, we also show in the plots the rates in the system when all users are greedy and when all users are non-greedy.

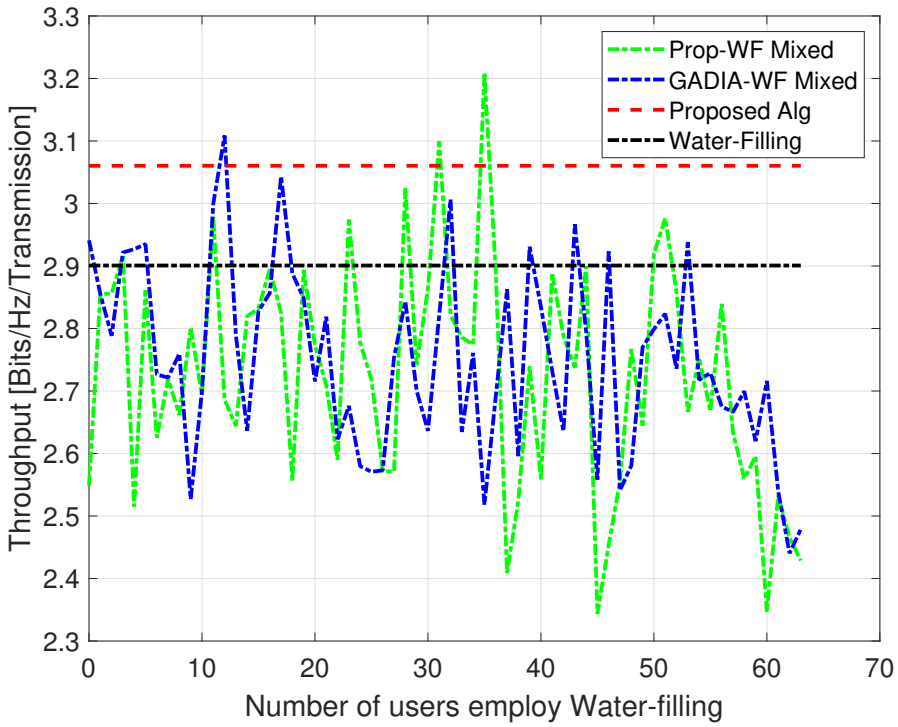
The simulation setup consists of N mutually interfering links with transmitters and receivers placed at random locations uniformly distributed inside a circular region with radius $r = 100$. A free-space propagation environment is considered, and for each user distribution, the simulation was run multiple times and the average rate values were taken and normalized by the number of available channels. The power spectral density of the noise is the same at all receivers $\sigma^2 = 10^{-8}$. All user powers are equal and normalized to one, that is, $\bar{P}_i = 1$, for $i \in \{1, 2, \ldots, N\}$. Simulations are run for sparse and dense environments where the number of users $N = 32$ and the number of channels $F = 64$ for sparse environment, $N = 64$ and $F = 16$ for dense environment.

3.1.1 NON-GREEDY USERS

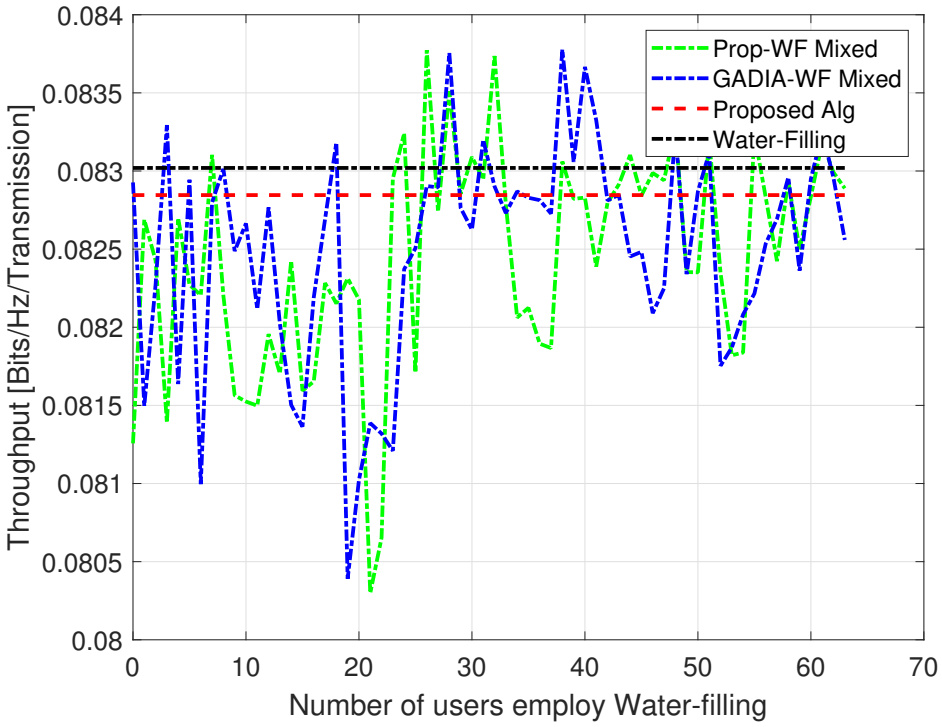
In this section we observe a user that applies either GADIA or the distributed power allocation algorithm for rate maximization in [1], while the other users apply either water-filling or the same non-greedy algorithm as the observed user. The variation of the individual and total transmission rates as the number of greedy users increases for sparse and dense environments is shown in Fig. 8 and Fig. 9, respectively.

Sparse Environment

As seen from Fig. 8, in this case the highest total rate is reached when all the users apply the distributed power allocation algorithm for rate maximization in [1]; that is, when all users apply the non-greedy approach. When users apply the alternative non-greedy approach implied by GADIA, the output is very similar, but the total and individual rate values are slightly lower. As the number of greedy users increases, the achievable total rate decreases rapidly. In addition, the individual rate of the non-greedy user also decreases, such that when more of the users are greedy and apply water filling, all users will be better off applying the greedy water filling approach for allocating transmit powers.



(a) Individual transmission rate



(b) Total transmission rate

Figure 9. Illustration of non-greedy user behavior in dense environments.

Dense Environment

In this case interference is not avoidable since there are fewer channels available than active users, and, as can be observed from Fig. 9, the total rate achieved with both greedy and non-greedy approaches are similar. In this case, as the number of greedy users in the system increases, both the total rate and the non-greedy user's rate do not change significantly. Thus, in dense environments, the greedy and non-greedy approaches for power allocation yield similar co-existence scenarios.

3.1.2 GREEDY USERS

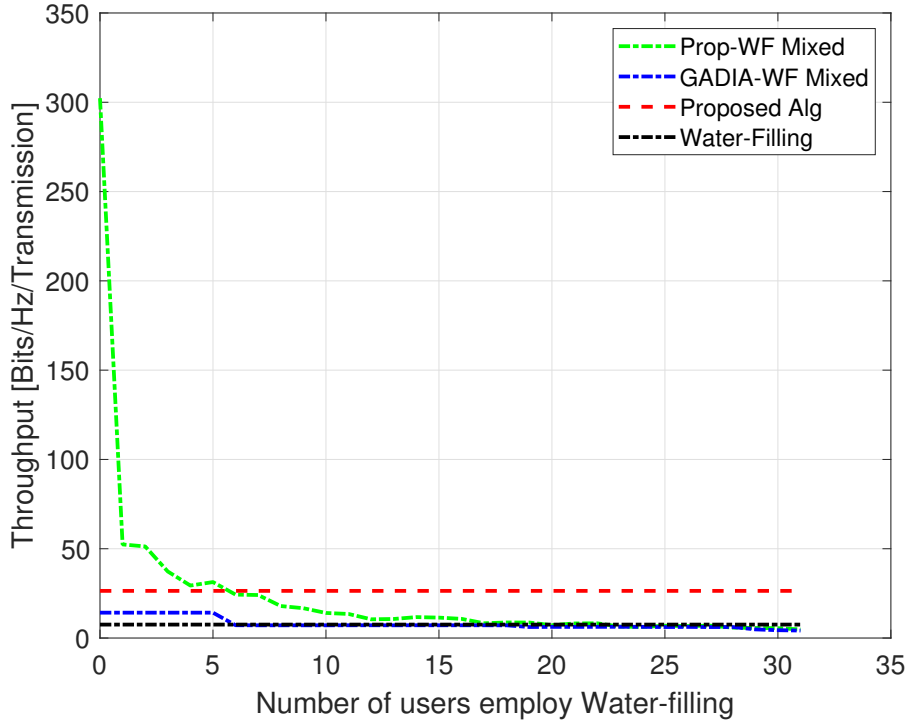
In this section we focus on a user that applies water filling to allocate its transmitted power, while the other users apply also water-filling or a non-greedy approach for power allocation. The variation of the individual and total transmission rates as the number of greedy users increases for sparse and dense environments is shown in Fig. 10 and Fig. 11, respectively.

Sparse Environment

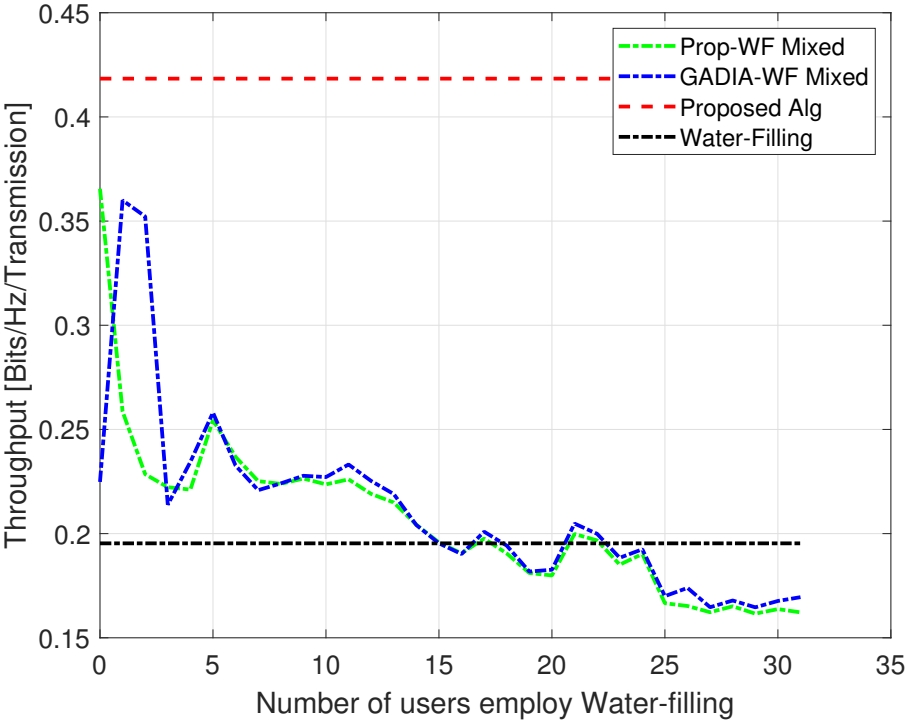
As seen from Fig. 10, since in this case the observed user is greedy and uses water filling to allocate power over all channels, it will get a large individual transmission rate, which motivates the user to continue its greedy approach in allocating power. However, the total rate of the system is lower in this case due to the large mutual interference among users.

Dense Environment

In this case, as can be observed from Fig. 11, the observed greedy user's rate increases when other users apply the non-greedy approach, which motivates again the user to continue its greedy approach. However, as the number of greedy users increases, the individual rate of the observed user decreases. We note that, in dense environments, the total rates of the system where all the users use the same greedy or non-greedy approach for power allocation are very close to each other, and in this case, water filling application by all users increases the system throughput.

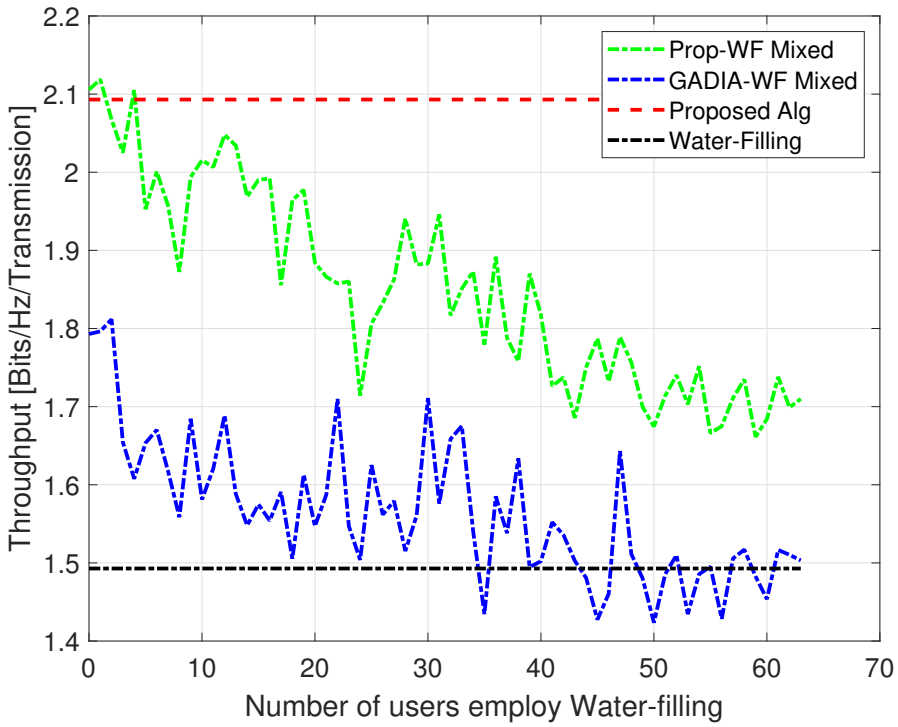


(a) Individual transmission rate

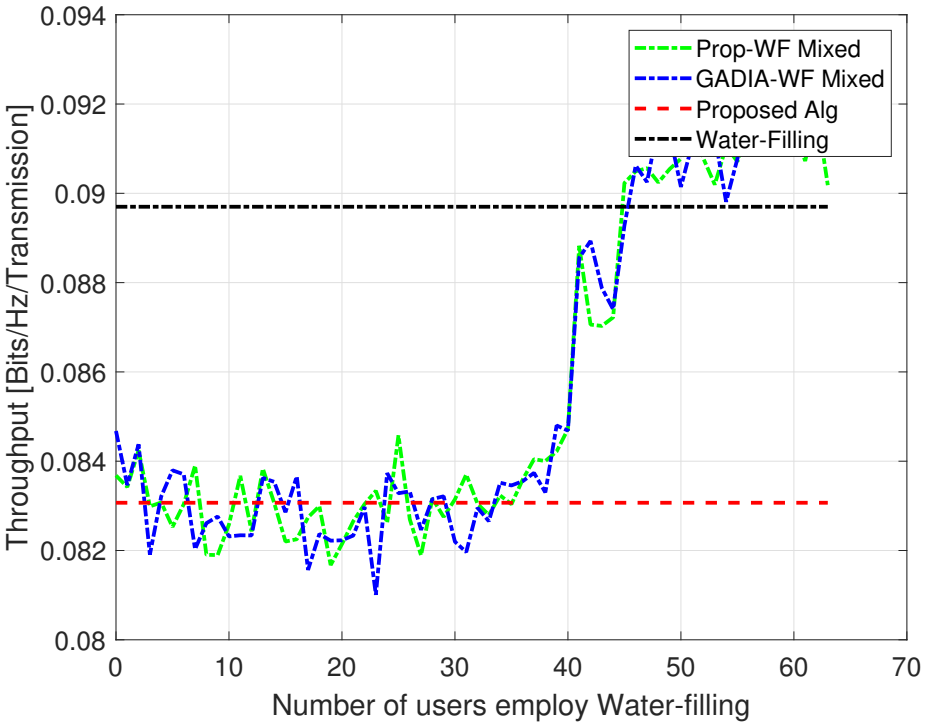


(b) Total transmission rate

Figure 10. Simulation results for observation of greedy user in sparse environment.



(a) Individual transmission rate



(b) Total transmission rate

Figure 11. Simulation results for observation of greedy user in dense environment.

In this chapter, we have considered the problem of horizontal spectrum sharing by users employing greedy and non-greedy power allocation strategies. We analyzed both the system throughput and individual user transmission rates in an environment where the number of greedy users in the system varies. Our study indicates that individual user rates depends mainly on the number of greedy users in the system, i.e., if there are many greedy users, the individual user's transmission rate is low regardless of whether specific users are greedy or not. By contrast, when all users employ non-greedy approaches, they will obtain higher transmission rates. However, with only a few greedy users in the system, their use of the greedy water filling algorithm results in high transmission rates relative to the non-greedy users, and encourages all users to be greedy in the long term. When all users switch to greedy algorithms, this will result in individual transmission rates below those possible when all users apply non-greedy approaches, and this behavior should be discouraged to enable coexistence of mutually interfering systems. In light of this observation, in the next section, we introduce a new non-greedy power allocation algorithm that is robust to greedy users's presence, yet manages to keep the system throughput maximized when all users use non-greedy algorithms.

3.2 RATE MAXIMIZATION WITH INTERFERENCE CONTROL

Let us denote the transmission rate for wireless link i by

$$R_i = \sum_{m=1}^{F} \log_2 \left(1 + \frac{h_{ii}^{(m)} P_i^{(m)}}{\sum_{j=1, j\neq i}^{N} h_{ji}^{(m)} P_j^{(m)} + \sigma^2} \right), \quad i, j = 1, \ldots N, \tag{5}$$

where $P_i^{(m)}$ denotes the power allocated by transmitter i on frequency band m and σ^2 is the power spectral density of the additive white Gaussian noise corrupting the signal.

Furthermore, let the SIR at the receiver corresponding to link i over and frequency m be

$$\gamma_i^{(m)} = \frac{h_{ii}^{(m)} P_i^{(m)}}{\sum_{j=1, j\neq i}^{N} h_{ji}^{(m)} P_j^{(m)}}. \tag{6}$$

To maximize the transmission rate for a set of mutually interfering links while also controlling interference, an iterative procedure consisting of the following main steps is performed:

- Transmitters sequentially update their power allocations by distributing available power over a subset of L frequencies with least amount of interference using a water filling procedure.
- Transmitters then calculate the SIR in each of the L frequency bands used as well as in the unused $F - L$ bands.
- If $L < F$, the transmitter will attempt to distribute its available power over a set of $L + 1$ frequency bands with least interference.
- If the SIR in all the newly chosen frequency bands used is larger than 1, the transmitter uses resulting power allocation.
- If the SIR in at least one of the newly chosen frequency bands is less than 1, then the transmitter reduces the number of frequency bands used by one and reallocates power by water filling.

The number of available frequencies is initialized to $L = 1$, and transmitters start by allocating their entire power to the frequency with minimum interference. This initial step is similar to the GADIA algorithm [18]. However, unlike GADIA, L can be incremented in subsequent iterations if additional frequencies where interference is weak are available (that is, the corresponding SIR > 1). Moreover, if incrementing L yields power allocations for which the SIR < 1 in any frequency, L is decremented and the transmit power is redistributed over fewer frequency bands until a suitable power allocation is obtained or only a single frequency is used for transmission, which ensures the convergence of the proposed algorithm to a fixed point. A flowchart of the algorithm is shown in Fig. 12.

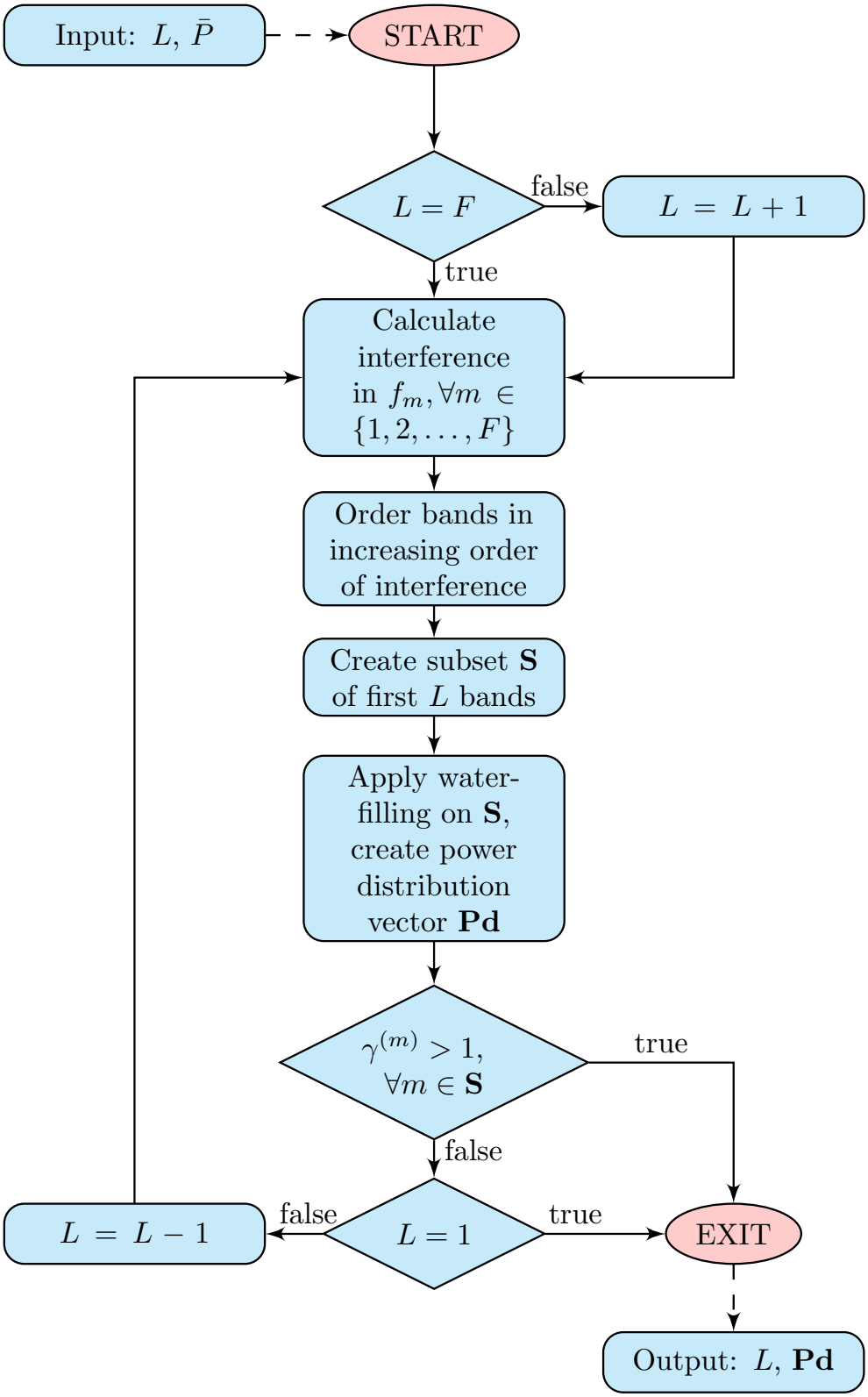


Figure 12. Flowchart for the proposed algorithm for power allocation for rate maximization with interference control.

We conclude presentation of the proposed strategy for power allocation with interference control by noting that this assumes that all transmitters use the same update interval τ in their power allocation, such that, after allocating power over the L frequencies, each transmitter waits for a period τ before attempting a new power allocation.

3.3 SIMULATIONS

In this section, we illustrate the proposed algorithm for power allocation with numerical results obtained from simulations showing the total rate achieved by all mutually interfering links. Specifically, we look at the total rate achieved when a subset of transmitters choose to apply greedy iterative water filling for allocation of their transmit power, while the remaining transmitters apply either GADIA or the proposed algorithm for power allocation. This is compared to the total rate achieved when all transmitters apply greedy iterative water filling for power allocation as well as with the total rate achieved when all transmitters evenly distribute their available power over all available frequencies (complete overlap case).

Extensive simulations have been run for both sparse and dense scenarios, and typical examples are presented for each scenario. For each simulation, receivers are placed on a uniform square grid while transmitters are located at random positions, and the number of greedy transmitters applying water filling for power allocation is specified. Power allocation is then simulated for all transmitters and the resulting total link rate is calculated by adding the rates on all mutually interfering rates. The average total link rates over 3 simulations are plotted as a function of the number of greedy transmitters.

3.3.1 SPARSE ENVIRONMENTS

In the first set of simulation experiments we consider sparse environments where the N number of mutually interfering links is lower than the total number of available frequency bands F. This scenario is illustrated for $N = 25$ and $F = 50$. Receivers are placed on a square grid at distances $d = 10$ from each other, while for the random placement of transmitters two distinct cases are considered: one in which the distance between any transmitter and its associated receiver is set to be equal to $3d/2$, and another in which no distance requirements are set and transmitters end up at random distances from their associated receivers. The first

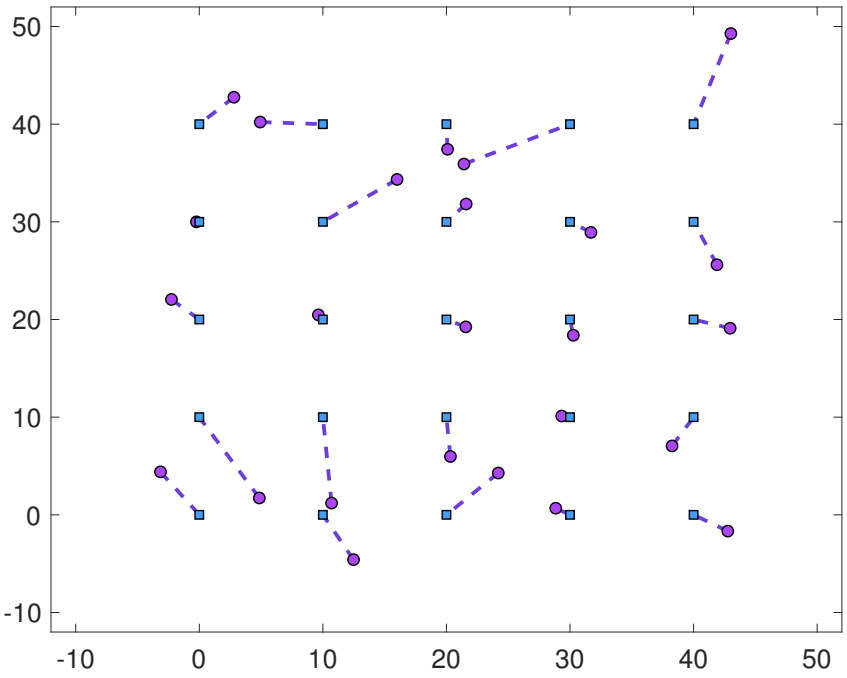
case corresponds to a low uniform SIR regime in which the signal from a given transmitter is received with low power at its associated receiver, while the second implies a mix of mutually interfering wireless links with both low and high SIRs.

We note that in sparse environments, where the number of available frequency bands is larger than the number of mutually interfering links, power allocations with no overlap in frequency among transmitters are possible. Such power allocations are desirable, especially when all links operate in the low uniform SIR regime, since they imply that all wireless links will operate with no interference. However, in the case of mixed SIRs, transmitters may be motivated to be greedy and apply water filling for power allocation to take advantage of all available frequencies rather than using just a subset of frequencies. Specifically, for high SIR links the motivation may be due to the fact that transmitters do not sense significant interference in any frequency and assume that all frequencies may be used for power allocation, while for low SIR links the transmitters are motivated to distribute their power over all frequencies in the hope of increasing their link rate. Hence, while no overlap scenarios are possible, they may be difficult to achieve in these cases.

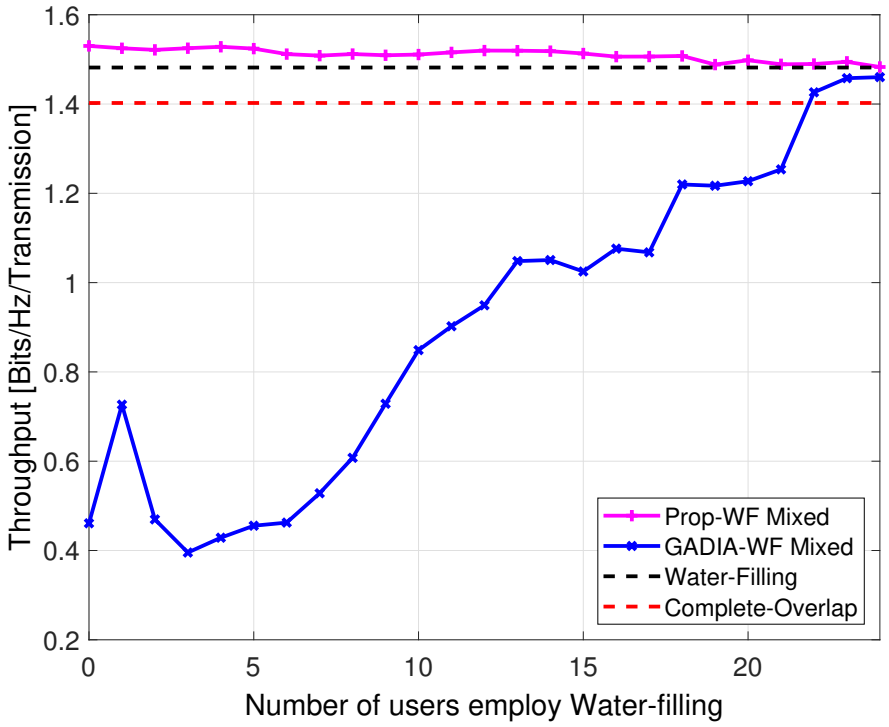
Mixed SIRs

The geographic distribution of wireless links for this scenario is shown in Fig. 13(a) with the total link rate achieved plotted in Fig. 13(b) as a function of the number of greedy transmitters.

From this figure one can see that even when 40% of transmitters (or more) are not greedy and apply the proposed algorithm for power allocation based on rate maximization with interference control, the total link rate is higher than when all transmitters would greedily apply water filling for power allocation. Also notable in this case is the fact that when the GADIA algorithm is applied by the non-greedy transmitters, total link rate achieved is below that achieved when all transmitters are greedy and apply water filling for power allocation. Furthermore, in this scenario even power allocation leading to complete overlap in all frequencies is preferable to the GADIA algorithm, since it would lead to higher total link rates, albeit lower than the total link rates obtained when the proposed algorithm or water filling is applied.

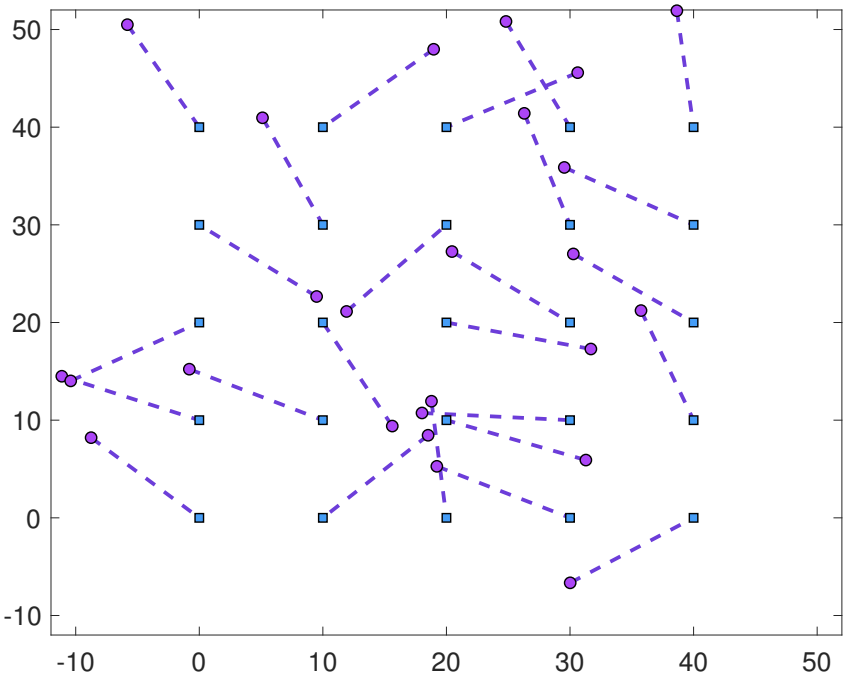


(a) Geographic distribution of links

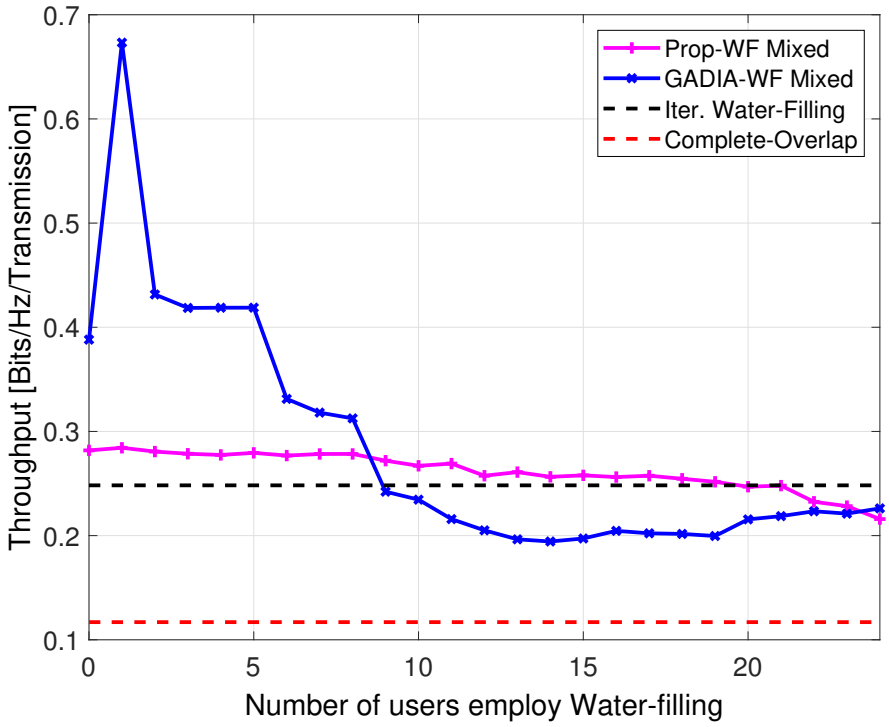


(b) Total link rate

Figure 13. Typical simulation results for sparse environments. Based on the distances between transmitters (circles) and corresponding receivers (squares), some links operate with low SIRs while others have high SIRs.



(a) Geographic distribution of links



(b) Total link rate

Figure 14. Typical simulation results for sparse environments where the distance between transmitter (circles) and receivers (squares) is equal and implies all links operate at low SIRs.

Uniform SIRs

The geographic distribution of wireless links for this scenario is shown in Fig. 14(a) with the total link rate achieved plotted in Fig. 14(b) as a function of the number of greedy transmitters.

From this figure one can observe results similar to the previous case when the proposed power allocation strategy based on rate maximization with interference control is applied by the non-greedy transmitters. However, if the GADIA algorithm is applied by the non-greedy transmitters in this case, higher total link rate is achieved only when the number of greedy transmitters does not exceed about 30% of the total number of transmitters, beyond which the total link rate drops below that achieved when all transmitters would act greedily and allocate power based on water filling. We note that in this case, the higher total link rates displayed in Fig. 14(b) for the mixed GADIA-water filling approach for power allocation are due to the greedy transmitters which are able to get significant increases for their link rates, while the non-greedy transmitters have lower link rates implied by the use of a single frequency for transmission according to the GADIA algorithm. We note that in this scenario power allocation with complete overlap in all frequencies implies the lowest total link rate as demonstrated by Fig. 14(b).

3.3.2 DENSE ENVIRONMENT

Next, we have simulated dense environments where the N number of mutually interfering links is larger than the total number of available frequency bands F. This scenario is illustrated for $N = 49$ and $F = 8$. Receivers are placed on a square grid at distances $d = 10$ from each other, while for the random placement of transmitters we considered the same two distinct cases: one in which the distance between any transmitter and its associated receiver is set to be equal to $3d/2$, and the other in which no distance requirements are set and transmitters end up at random distances from their associated receivers. Theses cases illustrate uniform low SIR and mixed SIR regimes, respectively, similar to the previous experiment.

We note that in dense environments, where the number of available frequency bands is smaller than the number of mutually interfering links, power allocations with no overlap

in frequency among transmitters are not realistic, especially when all wireless links operate at low SIRs. In this case we expect that all transmitters confine their signals on a single frequency, usually the one with minimum interference, which is what the GADIA algorithm dictates. However, in the case of mixed SIRs, the transmitters for links operating at high SIRs are again motivated to be greedy and apply water filling for power allocation in order to take advantage of as many frequencies as possible, thus increasing the total interference in the system.

Mixed SIRs

The geographic distribution of wireless links for this scenario is shown in Fig. 15(a) with the total link rate achieved plotted in Fig. 15(b) as a function of the number of greedy transmitters.

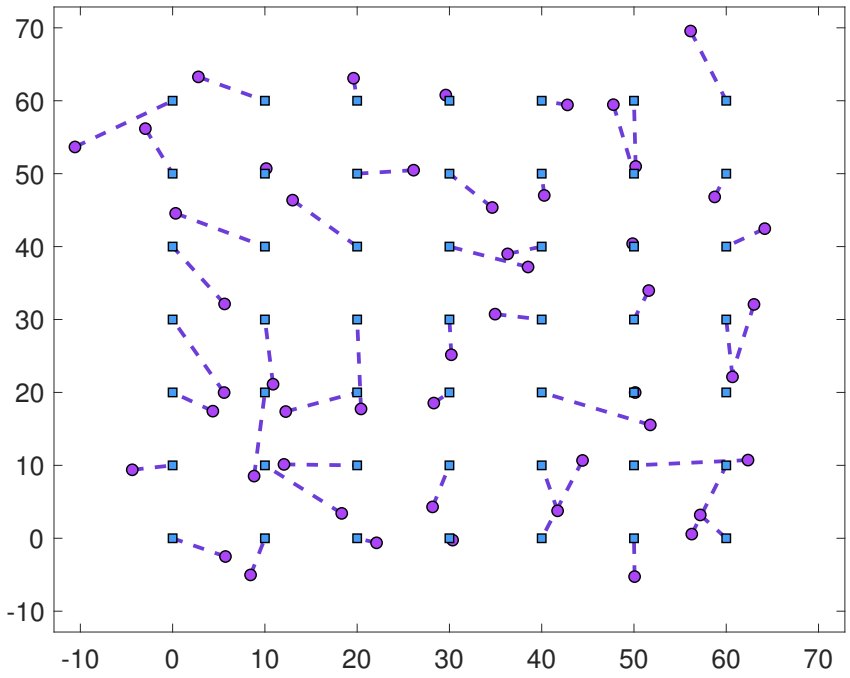
From this figure one can observe results similar to the mixed SIRs case in sparse environments: the total link rate when 40% of transmitters (or more) are not greedy is higher than when all transmitters are greedy and apply water filling for power allocation. Also notable in this case is again the fact that when the GADIA algorithm is applied by the non-greedy transmitters, total link rate achieved is below that achieved when all transmitters are greedy and apply water filling for power allocation, being significantly lower when 40% or more transmitters use GADIA.

Finally, similar to the sparse environment scenario, power allocation leading to complete overlap in all frequencies is again preferable to the GADIA algorithm since it yields higher total link rates.

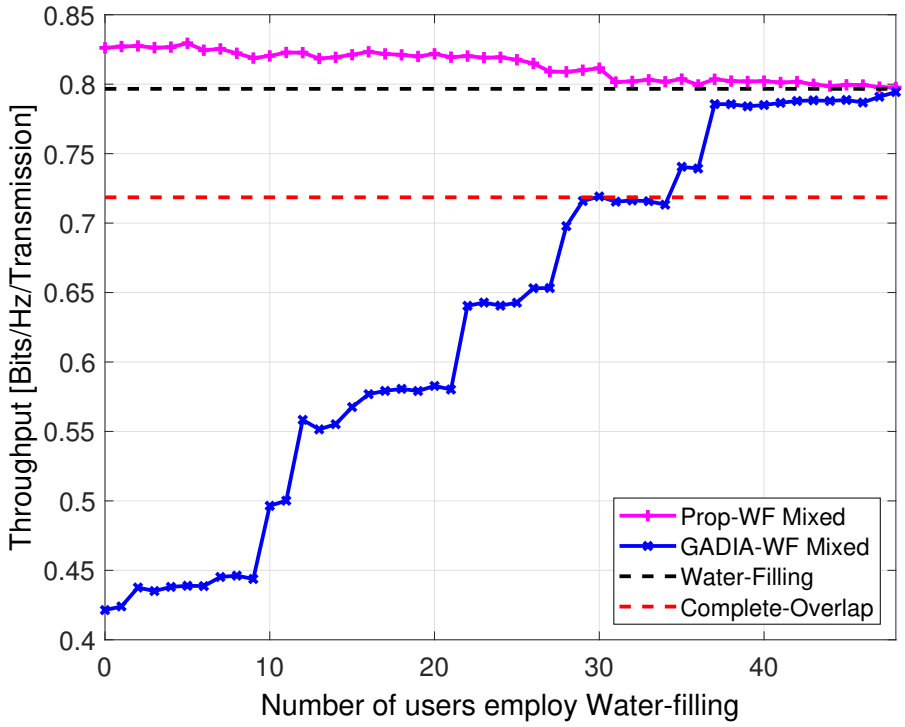
Uniform SIRs

The geographic distribution of wireless links for this scenario is shown in Fig. 16(a) with the total link rate achieved plotted in Fig. 16(b) as a function of the number of greedy transmitters.

From this figure one can observe that similar results are obtained when non-greedy transmitters apply either the proposed power allocation strategy based on rate maximization with interference control or GADIA. The corresponding total link rate achieved is also very close

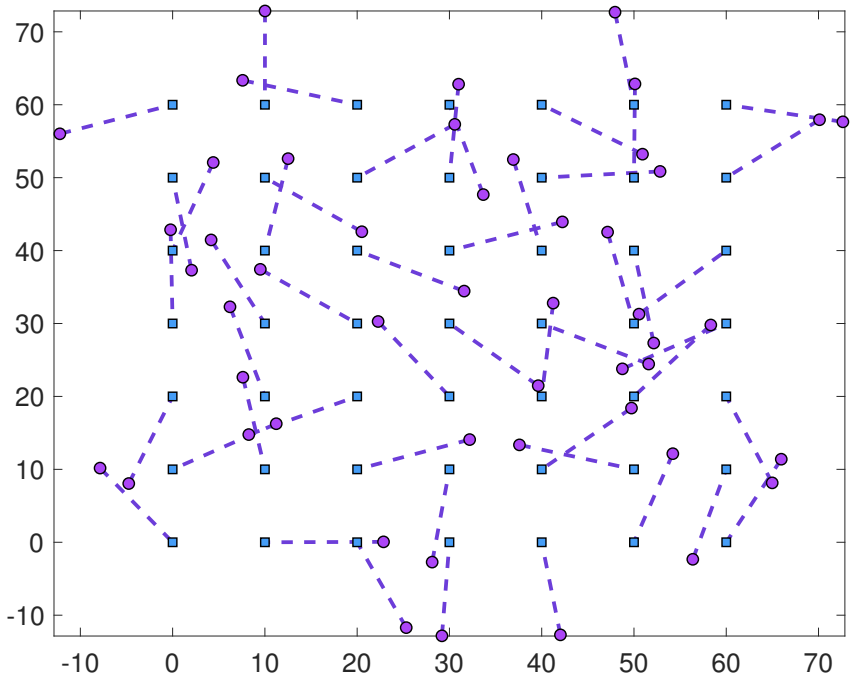


(a) Geographic distribution of links

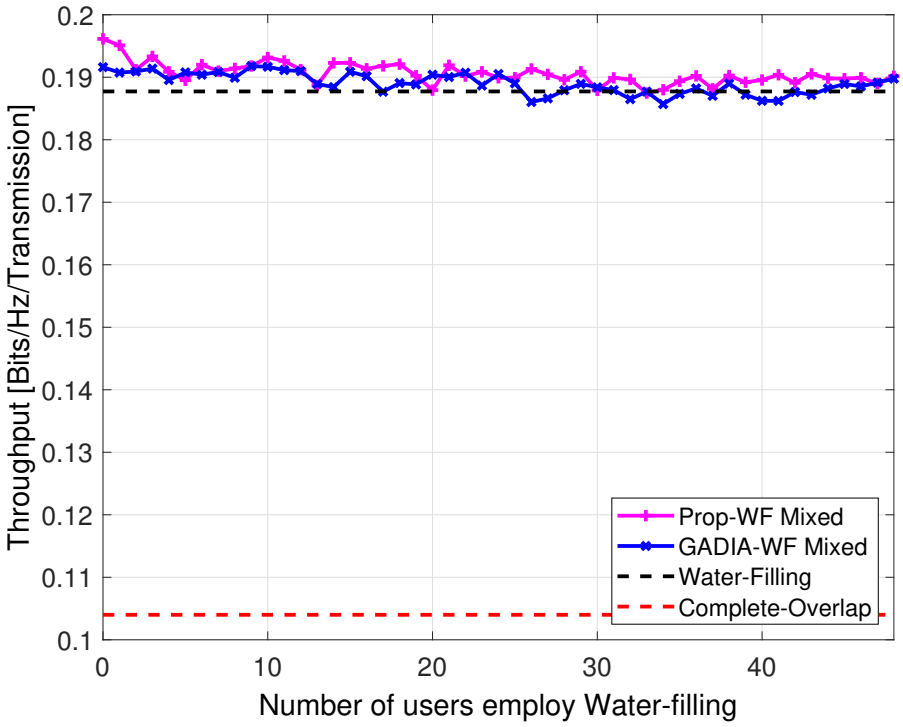


(b) Total link rate

Figure 15. Typical simulation results for dense environment. Based on the distances between transmitters (circles) and corresponding receivers (squares), some links operate with low SIRs while others have high SIRs.



(a) Geographic distribution of links ($d = 10$)



(b) Total link rate

Figure 16. Typical simulation results for dense environments where the distance between transmitter (circles) and receivers (squares) is equal and implies all links operate at low SIRs.

to that achieved when all transmitters would be greedy and allocate transmit power based on water filling. We note that this behavior should have been expected since in the case of dense environments using the frequency with minimum interference for transmission makes both practical and analytical sense. Again, as it was the case in the similar sparse environment scenario, power allocation with complete overlap in all frequencies is not desirable as it implies the lowest total link rate as Fig. 16(b) demonstrates.

3.4 CHAPTER SUMMARY

In this chapter, we considered the problem of spectrum sharing in mutually interfering wireless systems and proposed a new algorithm for distributed power allocation based on a rate maximization approach with interference control. The proposed algorithm requires no central control or coordination and allows transmitters to gradually use more frequencies to allocate transmit power as long as the SIR in each frequency used is larger than one.

The proposed algorithm is illustrated with numerical results obtained from simulations, which compare the total link rate achieved when the proposed algorithm is applied for power allocation to that achieved when GADIA or water filling procedures are used. Results indicate that the proposed algorithm is a meaningful alternative to non-greedy power allocation based on the GADIA algorithm, as well as to greedy power allocation approaches based on water filling. The proposed algorithm leads to more efficient spectrum utilization with higher total link rates, in particular in a sparse environment, even when only a fraction of the mutually interfering wireless links apply it, while the remaining links use greedy water filling for power allocation.

CHAPTER 4

SECRET KEY GENERATION AND RECONCILIATION AT THE PHYSICAL LAYER

Wireless communication systems along with the services they provide have become an essential component of modern society. However, due to the shared nature of the transmission medium used – the radio frequency spectrum – wireless communications are inherently insecure and prone to eavesdropping. To protect against eavesdropping and to ensure confidentiality of transmitted data, many wireless systems employ encryption using secret keys available only to the transmitter and the corresponding legitimate receiver. However, guaranteeing agreement between the secret keys at transmitter and receiver poses a formidable challenge when the key must be exchanged over an insecure channel, and the agreement must be accomplished such that legitimate users can reveal the secret key while eavesdroppers are unable to do so. A common method of securely exchanging a secret key over an insecure channel is to employ public key cryptosystems, such as Rivest-Shamir-Adleman (RSA) [19, Ch. 14]. We note that, while public key cryptosystems are currently computationally secure, they are not unconditionally secure.

To avoid difficulties associated with secret key distribution and management, in recent years various physical layer approaches have been proposed for generating encryption keys using channel state information [20–22]. These approaches use the inherent randomness of wireless channels and take advantage of the reciprocity properties of the channel between a wireless transmitter and its corresponding legitimate receiver to establish secret keys which may not be recreated by eavesdroppers overhearing the information exchanged over an uncorrelated channel.

Physical layer generation of secret keys avoids the need for key distribution and exchange since the keys become known to the legitimate nodes, transmitter and receiver, during the generation process. Furthermore, with time-varying wireless channels, keys can be renewed

dynamically using new measurements of the channel state information. We note that for slowly varying channels, where the channel coherence time is large and the channel parameters change slowly in time, the rate of generating secret key elements becomes very small, and in such instances parasitic antenna arrays such as the RECAP [23] or ESPAR [24] arrays may be used to randomize the channel and decrease channel coherence time.

Secret key generation based on noisy channel measurements at transmitter and receiver is discussed in [25, 26], where the use of Slepian-Wolf coding [20, 27–30] with LDPC codes for key reconciliation is studied. We note that channel measurement based key generation approaches use knowledge of the statistical properties of the channel, which requires extensive time consuming measurements to estimate channel statistics. In this chapter, we present a practical method for secret key generation that has low complexity and is based on one-bit scalar quantization of the real and imaginary components of the complex channel gain between the transmitter and the legitimate receiver. The proposed method exploits the symmetry of the probability density function of the channel gain and requires no prior knowledge of the channel variance. Thus, no channel observation and variance estimation is needed, which speeds up the key generation. Furthermore, the method simplifies the LLR calculation used in the key generation for fast computation. Specifically, we propose a novel way of evaluating LLRs that is based on the difference between the channel estimates at the legitimate nodes, while still combining advantage distillation with information reconciliation and privacy amplification [25, 26] for key reconciliation using LDPC codes.

The chapter is organized as follows: in Section 4.1, we introduce the system model and formally state the problem studied in the chapter. In Section 4.2, we present the proposed channel quantization scheme and give the details of the LLR calculations. In Section 4.4, we present numerical results obtained from simulations and discuss the performance of the proposed method, comparing it with the that of the "censoring"-based scheme for key generation that is widely used in the literature [31, 32] as an alternative approach to reduce bit disagreement rate at the cost of key generation speed. We conclude the chapter with final remarks in Section 4.5.

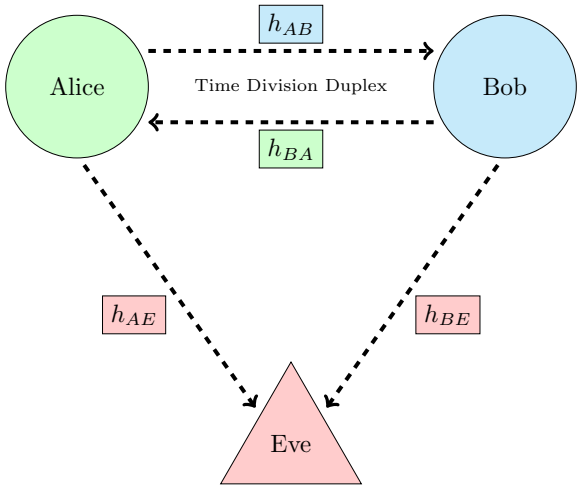


Figure 17. System model.

4.1 SYSTEM MODEL

We consider a system consisting of a transmitter, Alice, a legitimate receiver, Bob, and a passive eavesdropper, Eve, as shown in Fig. 17. Alice and Bob are trying to securely exchange information over a public wireless channel by using a secret key to encrypt their communication. In order to avoid exchanging information about the secret key, Alice and Bob will generate the key based on measurements of their wireless channels, which are assumed to be randomly changing over time with a known channel coherence time t_c. Alice and Bob use the channel in a time division duplex (TDD) mode to send pilot signals to each other over the same frequency repeatedly. We assume the channel does not change during one sequence of pilot transmissions by Alice and Bob, such that the channel estimation is done on the same channel instance. Consecutive channel measurements of a single node lead to uncorrelated samples as channel measurements have a time difference of t_c.

Upon transmission of the pilot signals by Alice and Bob, respectively, the corresponding channel estimates at time instant n for Alice and Bob are:

$$a[n] = h_{BA}[n] + w_A[n] \tag{7}$$

$$b[n] = h_{AB}[n] + w_B[n] \tag{8}$$

where $h_{AB}[n]$ and $h_{BA}[n]$ are zero mean circular complex Gaussian random variables, $w_A[n]$ and $w_B[n]$ denote the zero mean additive white Gaussian noise corrupting the channel measurements at Alice and Bob with variances σ_A^2 and σ_B^2, respectively. For simplicity, it is assumed that noise variances are equal, $\sigma_A^2 = \sigma_B^2 = \sigma_w^2$, and that due to TDD mode consecutive channels measurements done by both Alice and Bob in t_c period of time are identical, i.e., $h_{BA} = h_{AB}$.

We assume that Eve has infinite resources available and knows the pilot signals, so she can measure her corresponding channels to Alice and Bob h_{AE} and h_{BE}, respectively, using Alice and Bob's pilot transmissions. However, we assume that Eve is several wavelengths away from both Alice and Bob so that the channels h_{AE}, h_{BE}, and h_{BA} are all uncorrelated and Eve is not able to extract meaningful information related to Alice and Bob's measurements or to the generated secret key. Furthermore, Eve is assumed to be a passive eavesdropper, one who always listens but never transmits.

In this setup, we take advantage of the correlation between channel measurements at Alice and Bob and we employ Slepian-Wolf coding for reconciliation of the secret key bits generated by Alice and Bob [25]. This involves partial information exchange between Alice and Bob, which consists of parity bits (side information) generated at Alice by using LDPC codes. The side information is then encapsulated by a second LDPC code block for forward error correction and sent to Bob over a public channel as shown schematically in Fig. 18. Thus, our proposed approach for key generation involves two independent LDPC code blocks, one for generating the side information to employ Slepian-Wolf coding, and the other one for protecting the side information from errors during transmission over the public channel. We note that, even if Eve is able to intercept the side information transmitted over the public channel, she will not be able to reconstruct the secret key bits generated by both Alice and Bob since she will not have the additional information needed, which depends on the h_{BA} channel measurements.

4.2 KEY GENERATION BASED ON CHANNEL MEASUREMENTS

The secret key bits are generated at Alice and Bob simultaneously by exploiting the random characteristics of the wireless channel between them. Specifically, both Alice and

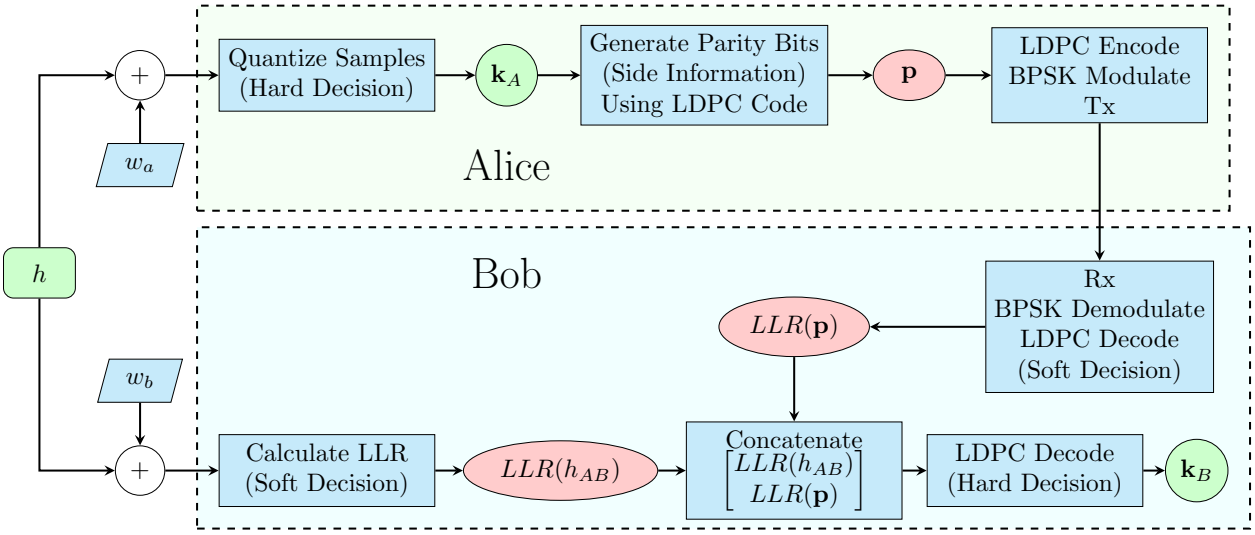


Figure 18. Proposed key generation mechanism.

Bob measure their corresponding (reciprocal) channels until the required number of samples for a secret key are obtained, and they generate the key based on the vector of sampled channel measurements. However, due to the independent noise corrupting Alice and Bob's channel measurements, bit disagreements between their generated keys might occur, and the probability of bit disagreement will be evaluated in Section 4.4 using Monte-Carlo simulations.

In the proposed key generation scheme, we assume that Alice is the leader node, which quantizes the channel measurement by hard decision and generates the secret key bits, while Bob is the follower, computing the key bits by using LLRs of his channel samples along with side information from Alice. Furthermore, Alice uses both the real and imaginary parts of the channel samples independently to generate independent key bits by 1-bit scalar quantization. Specifically, Alice quantizes the obtained samples with the following function to generate key bits:

$$k_A[n] = \begin{cases} 0, & e[n] > 0 \\ 1, & e[n] \leq 0. \end{cases} \tag{9}$$

where $e[n] \in \{\mathrm{Re}(a[n]), \mathrm{Im}(a[n])\}$. This is followed by generation of the parity vector $\mathbf{p}$ by

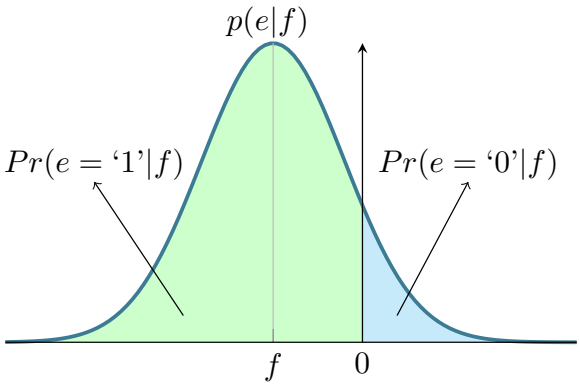


Figure 19. Illustrating calculation of the probabilities involved in the LLR calculation for the channel measurement at Bob. $Pr(\cdot)$ indicates probability and $p(\cdot)$ indicates the value of the probability density function. Note that f is assumed to be negative for this example but can take any real value.

Alice using the first LDPC encoder matrix $\mathbf{H}_p$ for Slepian-Wolf coding, which is encapsulated with the second LDPC encoder matrix $\mathbf{H}_s$ whose output vector $\mathbf{s}$ is transmitted to Bob using BPSK signaling.

At the other side, Bob measures the channel with Alice's pilot signals, but instead of using hard decoding as Alice does, Bob calculates the LLRs for Alice's measurements based on his own observations. In addition, Bob receives the side information $\mathbf{p}$ encapsulated in $\mathbf{s}$ from Alice via BPSK signaling and he demodulates the BPSK signal calculating LLRs, and extracting the parity vector $\mathbf{p}$ with soft decision. Note that the channel samples and received BPSK signals have different random properties; thus, they require different LLR calculations as will be described in detail. In the end, Bob concatenates both channel measurement LLRs and side information LLRs, and applies Slepian-Wolf decoding using the $\mathbf{H}_p$ matrix to determine the key $\mathbf{k}_B$, which is correlated with $\mathbf{k}_A$. We note that, ideally, $\mathbf{k}_A = \mathbf{k}_B$, although bit disagreements between k_A and k_B are possible as discussed in Section 4.4.

4.3 LLR CALCULATIONS

The proposed system requires Bob to calculate LLRs for channel measurements through received pilot signals, and side information bits sent by Alice via BPSK transmission. The obtained LLRs are later used for key reconciliation with LDPC codes.

4.3.1 LLR CALCULATION FOR CHANNEL MEASUREMENTS

As mentioned earlier, Alice and Bob will obtain different values for the same channel sample due to the independent noise corrupting their measurements. By using Eqs. (7) and (8) in one dimension, we can define the noise variable based on the difference as follows.

$$e[n] - f[n] = w_e[n] - w_f[n] = w'[n], \tag{10}$$

where $f[n] \in \{\mathrm{Re}(b[n]), \mathrm{Im}(b[n])\}$, $w_e[n] \in \{\mathrm{Re}(w_a[n]), \mathrm{Im}(w_a[n])\}$, $w_f[n] \in \{\mathrm{Re}(w_b[n]), \mathrm{Im}(w_b[n])\}$ and $w'[n] \sim \mathcal{N}(0, \sigma_w^2)$. Therefore, the LLR for a given channel sample $h_{AB}[n]$ can be calculated as

$$\begin{aligned} LLR_{chan}[n] &= \ln \frac{\Pr(e[n] = \text{`0'}|f[n])}{\Pr(e[n] = \text{`1'}|f[n])} \\ &= \ln \frac{\Pr(e[n] > 0|f[n])}{\Pr(e[n] < 0|f[n])} \\ &= \ln \frac{\Pr(e[n] - f[n] > 0 - f[n])}{\Pr(e[n] - f[n] < 0 - f[n])} \\ &= \ln \frac{\Pr(e[n] - f[n] > -f[n])}{\Pr(e[n] - f[n] < -f[n])} \\ &= \ln \frac{\Pr(w'[n] > -f[n])}{\Pr(w'[n] < -f[n])}. \end{aligned} \tag{11}$$

Since we know $w'[n]$ is a Gaussian random variable with known parameters, the corresponding probabilities of e for known f are calculated as illustrated in Fig. 19 by integrating the probability density function (PDF) on both sides of the 0 quantization threshold separately to yield the LLR:

$$LLR_{chan}[n] = \ln \frac{\mathcal{Q}\left(\frac{-f[n]}{\sqrt{\sigma_w^2}}\right)}{1 - \mathcal{Q}\left(\frac{-f[n]}{\sqrt{\sigma_w^2}}\right)}. \tag{12}$$

We note that the LLR calculation in Eq. (12) uses the $\mathcal{Q}$-function [33], which requires numerical integration or a stored lookup table. For faster computation, one can compute

the LLRs as if the channel measurements are received BPSK signals from Alice and employ BPSK LLRs as a faster alternative. Note that this approximation is highly inaccurate at high signal-to-noise ratios (SNRs) and will lead to significant bit disagreements between $\mathbf{k}_A$ and $\mathbf{k}_B$ as will be discussed in Section 4.4.

4.3.2 LLR CALCULATION FOR RECEIVED PARITY VECTOR

For demodulation of the side information received from Alice, Bob uses a BPSK demodulator with soft decoding. The constellation points for the BPSK demodulator have coordinates $(\sqrt{E}, 0)$ and $(-\sqrt{E}, 0)$, and the LLRs are calculated as follows:

$$\begin{aligned} LLR_{side} &= \ln \frac{\Pr(e[n] = \text{`0'} | f[n])}{\Pr(e[n] = \text{`1'} | f[n])} \\ &= \ln \frac{p(f[n]|e[n] = \text{`0'}) \Pr(e[n] = \text{`0'}) / p(f[n])}{p(f[n]|e[n] = \text{`1'}) \Pr(e[n] = \text{`1'}) / p(f[n])} \\ &= \ln \frac{p(f[n]|e[n] = \text{`0'})}{p(f[n]|e[n] = \text{`1'})} \\ &= \ln \frac{\frac{1}{\sqrt{2\pi\sigma_w^2}} e^{\frac{-(f[n]-\sqrt{E})}{2\sigma_w^2}}}{\frac{1}{\sqrt{2\pi\sigma_w^2}} e^{\frac{-(f[n]+\sqrt{E})}{2\sigma_w^2}}} \\ &= \frac{(f[n]+\sqrt{E})^2 - (f[n]-\sqrt{E})^2}{2\sigma_w^2} = \frac{2f[n]\sqrt{E}}{\sigma_w^2}. \end{aligned} \tag{13}$$

4.4 NUMERICAL SIMULATIONS

In this section, we present numerical results obtained from simulations to evaluate the probability of bit disagreement between the two secret keys $\mathbf{k}_A$ and $\mathbf{k}_B$ generated by Alice and Bob, respectively, for the proposed key generation and reconciliation scheme for different SNR values and different LDPC code rates. We note that regular LDPC codes from the DVB-S.2 standard [34] have been used for generating the side information.

We also compare the proposed method with secret key generation based on a censoring approach [31, 32]. Specifically, in order to reduce the number of bit disagreements between

the generated keys, in [32] the channel measurement samples that fall in the region $[-\gamma, \gamma]$ at Alice's side are eliminated (censored) and they are not used for key generation, since bit disagreements between the generated keys are more likely to occur at those samples. The indices of the censored symbols are sent to Bob. The expected number of censored samples can be adjusted by changing the γ value. As γ increases, more samples are eliminated, leading to lower probability of bit disagreement between keys as well as slower key generation (in terms of bits generated per second). For a channel with short t_c coherence time, a fixed number of bits for a key can be generated quickly; therefore, censoring some of the channel measurements is a meaningful approach to decrease the probability of bit disagreements between keys. We note that the main disadvantage of the censoring scheme consists of the fact that Alice needs to transmit the indices of the samples that are used in the key generation to Bob since not all of the samples are used for key generation, and that even one bit error during this transmission can lead to different key lengths at Alice and Bob, failing to generate meaningful keys for them. To overcome this possibility in the simulations, we assume that the transmission of sample indices is done over an ideal, noiseless channel, with the censoring threshold set to $\gamma = \sigma^2_{h_{BA}}/10$. Thus, the simulation results corresponding to the censoring scheme serve only as a benchmark, since in practical scenarios it is difficult to ensure agreement between Alice and Bob on samples to discard in the key generation process.

For both the proposed method and the censoring scheme for secret key generation, we use an LDPC code block length of 64800, and for each SNR value the simulations are repeated for 1800 blocks, with exact and approximate LLR calculations for key reconciliation. For the approximate LLR calculation, the amplitude of the BPSK signal in Eq. (13) is set to $\sqrt{E} = 1$. The rate of the LDPC code for protecting side information from transmission errors from Alice to Bob is fixed at 1/2.

The simulation results, shown in Figs. 20 – 23, provide insight about the improvements in the probability of bit disagreement between keys implied by increasing SNR values, the effect of exact and approximate LLR calculations, and the effect of LDPC code rates.

For a given rate of the Slepian-Wolf LDPC code, we note that the probability of bit

disagreement between the keys generated by Alice and Bob using the proposed method decreases with increasing SNR, with a steep decrease to very low probability of bit disagreement after a given threshold. We also note that the SNR threshold for which the probability of bit disagreement becomes arbitrarily small increases with an increase in the rate of the Slepian-Wolf LDPC code rate, from about 3 dB for a code rate of 1/2 (Fig. 20), to 10 dB for a code rate of 3/4 (Fig. 21), 13 dB for a code rate of 4/5 (Fig. 22), and 21 dB for a code rate of 9/10 (Fig. 23).

This behavior was expected as a lower code rate implies that more side information is available for Bob to use to correct his key and match Alice's, reducing the probability of bit disagreement between Alice and Bob's secret keys to a value that is achievable with a lower SNR value. On the other hand, transmitting more side information from Alice to Bob means revealing more information to eavesdroppers such as Eve. As pointed out in [25], based on [35] and [36], in the final step after information reconciliation, termed privacy amplification, no more than twice the number of bits that were transmitted as side information to Bob must be discarded from the secret key using the process of a cryptographic hash function. This privacy amplification dictates that a Slepian-Wolf LDPC code rate greater than 2/3 must be used for generating side information if the final secret key is to be longer than 0 bits.

For a given rate of the Slepian-Wolf LDPC code we note that the difference between the probability of bit disagreement for keys generated using the exact versus approximate LLRs is of the order of a few dB at low SNRs, with significant degradation at high SNR values, above 15 dB. If the SNR exceeds 20 dB the probability of bit disagreement between the keys generated using the approximate LLRs flattens to 0.5, indicating that the keys generated at Alice and Bob are no longer correlated. Thus, for large SNR values, one should avoid using approximate LLRs in the key generation and reconciliation process, while for low SNRs, using the approximate LLRs provides a meaningful alternative.

We conclude by noting that the censoring scheme displays a similar behavior in terms of probability of bit disagreement for each value of the Slepian-Wolf LDPC code rate. The apparent advantage of the censoring scheme is due to the idealized information exchange between Alice and Bob assumed in the simulations, who agree on which channel measurements to discard over a noiseless channel, and comes at the expense of the generated key

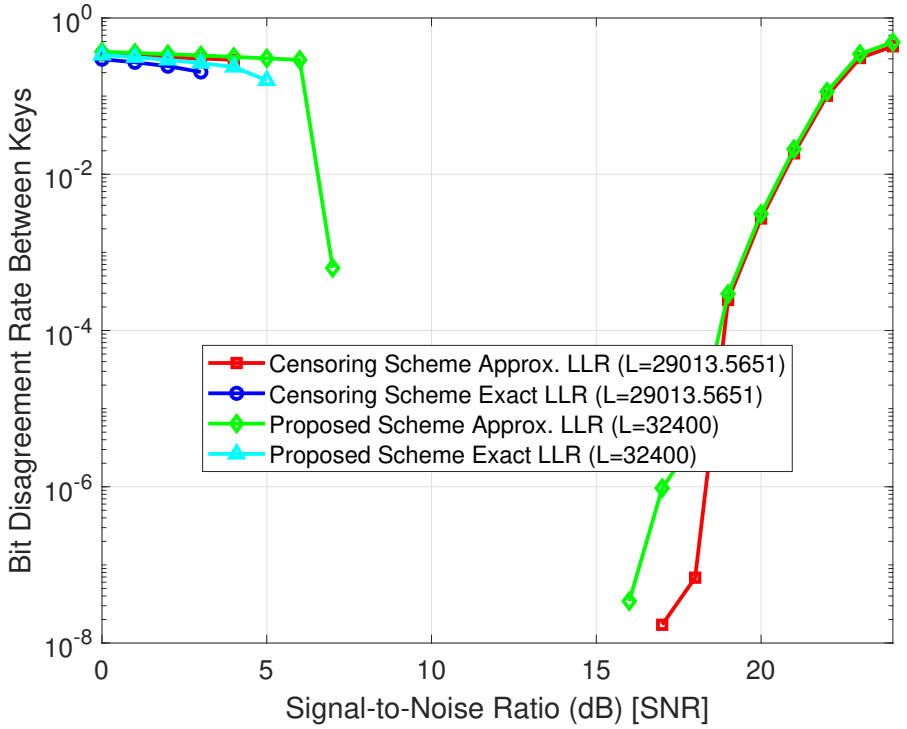


Figure 20. Simulation results for LDPC code rate 1/2. LDPC code block length is 32400, censoring scheme average key length is $L = 29013.5651$.

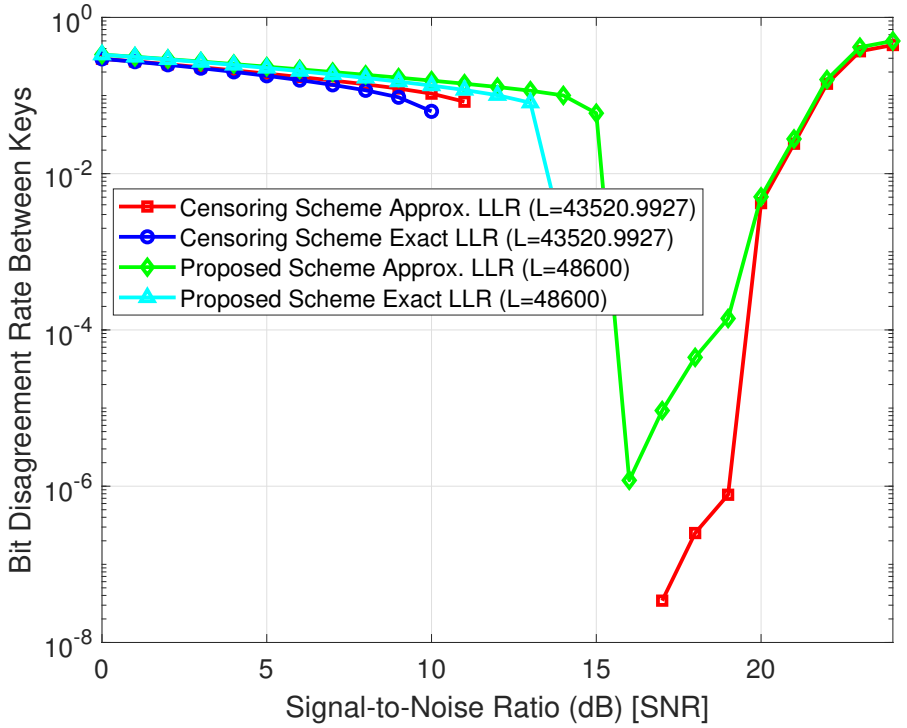


Figure 21. Simulation results for LDPC code rate 3/4. LDPC code block length is 48600, censoring scheme average key length is $L = 43520.9927$.

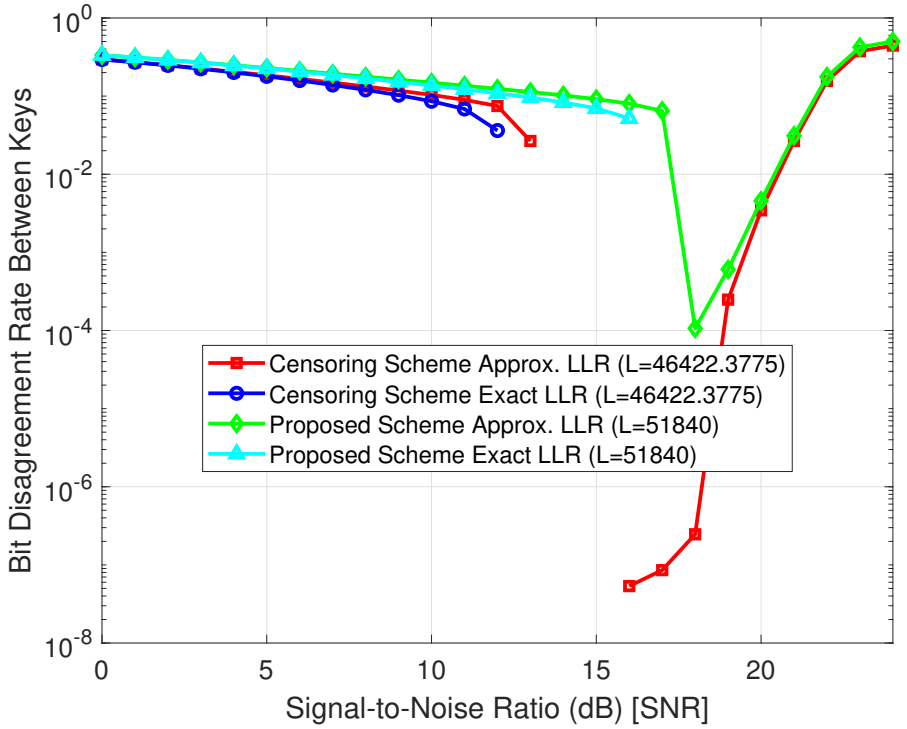


Figure 22. Simulation results for LDPC code rate 4/5. LDPC code block length is 51840, censoring scheme average key length is $L = 46422.3775$.

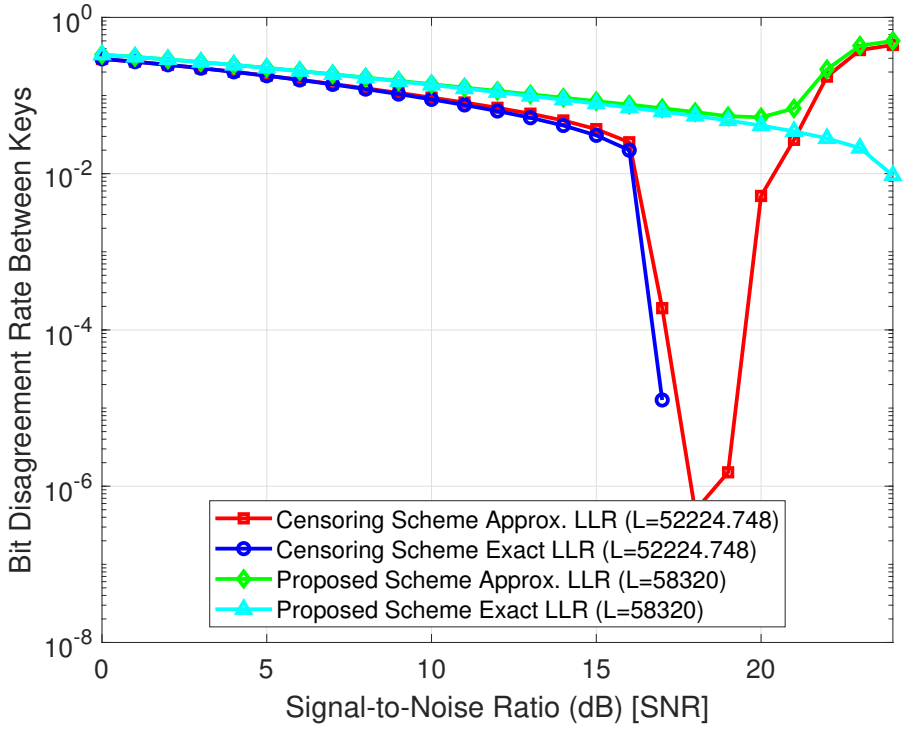


Figure 23. Simulation results for LDPC code rate 9/10. LDPC code block length is 58320, censoring scheme average key length is $L = 52224.748$.

length, which, for the same channel parameters, is shorter than the key length generated by our proposed approach as noted in Figs. 20 – 23. For the same value of the threshold used for discarding samples, the improvement in probability of bit disagreement depends on the Slepian-Wolf LDPC code rate: as Bob receives more side information, i.e., as the code rate decreases, more bit mismatches can be corrected, and there is less need for eliminating samples.

4.5 CHAPTER SUMMARY

In this chapter, we presented a new method for secret key generation that is based on one-bit quantization of channel measurements along with LLRs calculated using the difference between channel estimates at legitimate reciprocal nodes. The proposed approach eliminates the need for complex LLR calculations required by key generation based on vector quantization of channel measurements [25,26] while also implementing advantage distillation along with information reconciliation using Slepian-Wolf LDPC codes. Furthermore, no prior knowledge of the channel variance is required as the method takes advantage of the symmetry of the probability density function of the channel gains.

Numerical results were also presented in which the proposed scheme was compared to a censoring scheme for key generation that also uses channel state information, with exact and approximate calculations for LLRs. Both schemes were simulated for different SNR values and for different Slepian-Wolf LDPC code rates, and results confirmed that the probability of bit disagreement between the keys generated by Alice and Bob decreases with increasing SNR, reaching very low values after a given threshold that depends on the rate of the Slepian-Wolf LDPC code employed.

CHAPTER 5

MIMO EXTENSION FOR SECRET KEY GENERATION

In Chapter 4, secret key generation based on channel measurements and key reconciliation is introduced. One downside of this scheme is implied by the fact that, in the case of slowly varying channels where the channel coherence time is large and the channel parameters change slowly in time, the rate at which secret key bits are generated is low. In such instances, parasitic antenna arrays such as the RECAP [23] or ESPAR [24] arrays may be used to randomize the channel and decrease channel coherence time in order to increase the key generation rate at the expense of increasing the cost of the system through the use of specialized multiple antenna hardware. Furthermore, a common assumption made in the physical layer approaches for secret key generation is that the wireless channel over which a potential eavesdropper overhears a wireless transmission is uncorrelated with the wireless channel between the legitimate nodes. If this assumption is no longer satisfied, and the eavesdropper channel becomes correlated with the legitimate users' channel, then the eavesdropper may be able to extract enough information to generate the same secret key that the legitimate users do.

These motivate the work presented in this chapter, which proposes a new approach for physical layer key generation by which the legitimate transmitter and receiver nodes combine the one-bit quantization of channel measurements in [4] with MIMO precoding and role switching during the key generation process in order to prevent an eavesdropper whose channel is correlated to the legitimate channel to acquire information that can be used to generate the encryption key. In the proposed approach channel randomization is accomplished by using randomly generated MIMO precoder matrices rather than specialized antenna arrays, which ensures that the key generation rate does not depend on channel coherence time. Furthermore, the proposed reversal of roles of the legitimate transmitter and receiver during the key generation process further enhances the security of the wireless link by ensuring that potential eavesdroppers are unable to get the same amount of information as

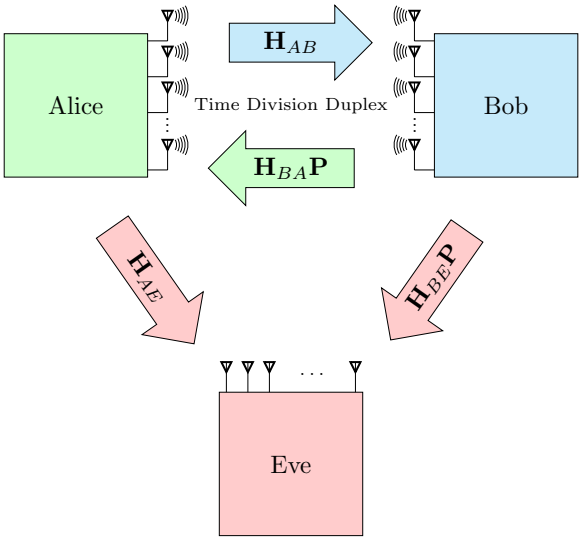


Figure 24. System model in MIMO scenario.

the legitimate users to generate secret key bits even when their channels are highly correlated with the legitimate channels.

The chapter is organized as follows: in Section 5.1, we introduce the system model and state the problem studied in the generalized MIMO case, followed by the description of the secret key generation mechanism by the legitimate users in Section 5.2. The eavesdropper perspective on secret key generation is discussed in Section 5.3, which discusses possible strategies that could be used by malicious users to also generate secret key bits. In Section 5.4, an information theoretic analysis of the key generation process is presented, and in Section 5.5 the proposed role reversal procedure is introduced, which strengthens the key generation process when the eavesdropper channel is correlated to the legitimate channel. Performance of the proposed secret key generation scheme is assessed using numerical results obtained from simulations in Section 5.6, and the chapter is concluded with final remarks in Section 5.7.

5.1 SYSTEM MODEL AND PROBLEM STATEMENT

We consider the system with three users shown in Fig. 24, where Alice and Bob are the legitimate users that are exchanging information over an open wireless channel, and Eve is a malicious user that is passively eavesdropping on the information exchange between

Alice and Bob. In order to secure their information exchange, Alice and Bob use a secret key to encrypt their communication. The key bits are generated using measurements of the MIMO wireless channels between Alice and Bob, which are acquired in a time division duplex (TDD) mode by repeatedly sending pilot signals to each other over the same frequency. It is assumed that the MIMO channels between Alice and Bob, $\mathbf{H}_{AB}$ and $\mathbf{H}_{BA}$ are reciprocal, that Eve knows all the parameters and techniques used for communication by Alice and Bob, and that all users have MIMO transceivers with M antennas such that all MIMO channel matrices have dimension $M \times M$. Furthermore, all wireless channels have coherence time t_c and are modeled as zero-mean circular complex Gaussian random processes with variance σ_h^2, and we assume that the wireless channel between Alice and Bob does not change during one sequence of pilot transmissions, such that channel estimation by Alice and Bob is done essentially on the same channel instance and consecutive channel measurements are done at time intervals of t_c to yield uncorrelated channel measurements.

In this setup, Alice and Bob establish the secret encryption key by precoding and quantizing the MIMO wireless channel measurements as outlined in Fig. 25 and discussed in detail in Section 5.2. The key generation mechanism starts with channel probing and precoding, and is followed by one-bit quantization of the MIMO channel measurements. To correct bit mismatches that may occur between the keys generated by Alice and Bob, Slepian-Wolf encoding using LDPC codes is employed, and, to prevent Eve from acquiring meaningful information about the secret key even when her channels are correlated with the legitimate channels, a role reversal procedure in the key generation process is proposed.

5.2 SECRET KEY GENERATION BY LEGITIMATE USERS

The mechanism employed by Alice and Bob to generate the bits of the secret key that is used to encode the information transmitted over the legitimate channel uses measurements of the wireless channel between Alice and Bob, and involves three distinct stages:

- **Channel probing and precoding**: Alice and Bob exchange pilot signals on the same frequency in TDD mode. The consecutive pilot signals are sent by Alice and Bob, respectively, within a length of time shorter than t_c, the channel coherence time, such that the corresponding channel measurements made by them are correlated, but not

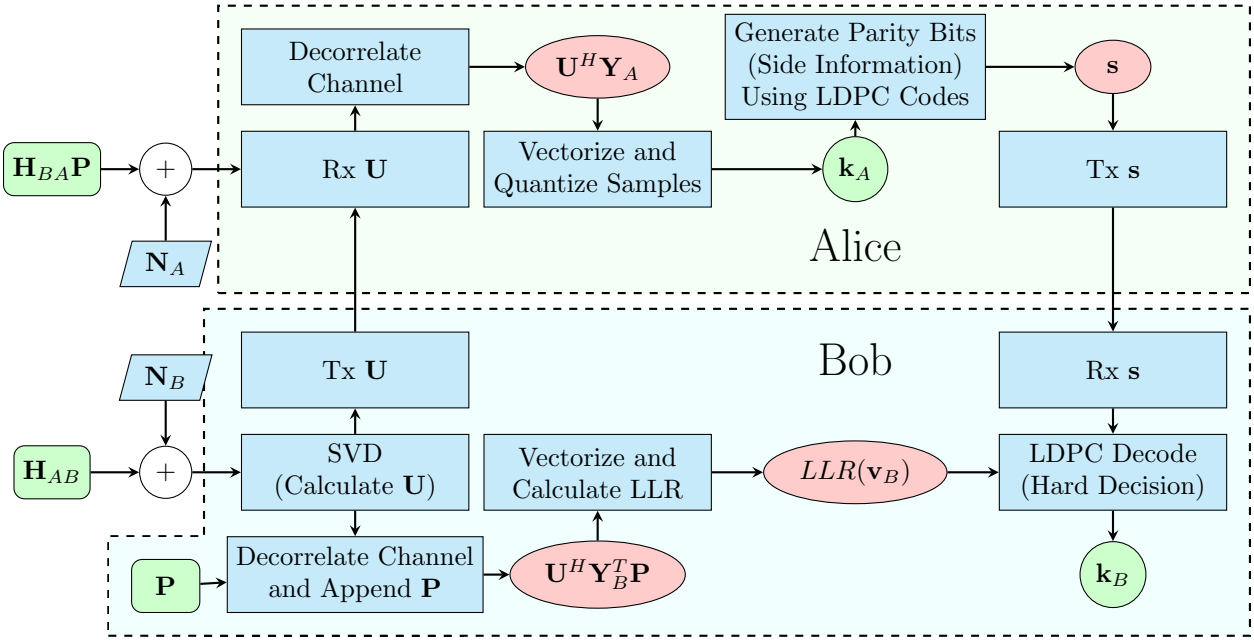


Figure 25. Key generation and reconciliation mechanism.

identical due to the independent noise at their corresponding receivers. It is assumed that receiver noise is also a zero-mean circular complex white Gaussian noise process with known variances σ_a^2 and σ_b^2 for Alice and Bob, respectively.

- **Quantization of channel measurements**: Alice and Bob establish the secret key bits for encrypting the information they exchange over the wireless link jointly, by precoding and quantizing the MIMO channel measurements acquired through probing.

- **Key reconciliation**: The key bits generated by Alice and Bob, which may be different due to the different noise that corrupts their channel measurements, are reconciled using Slepian-Wolf encoding and LDPC codes to correct bit mismatches.

The details of these three stages are outlined in Fig. 25 and described in more detail in the following sections.

5.2.1 CHANNEL PROBING AND PRECODING

Alice initializes the communication link by sending a plain pilot signal to Bob, which he uses to measure the channel. The corresponding channel measurement at Bob is:

$$\mathbf{Y}_B = \mathbf{H}_{AB} + \mathbf{N}_B, \tag{14}$$

where $\mathbf{H}_{AB}$ denotes Bob's $M \times M$ MIMO channel matrix. Upon receiving the pilot signal, Bob uses channel reciprocity to match Alice's channel by transposing the corresponding matrix, followed by decorrelation of the channel measurement matrix, which is needed to maximize the entropy of the secret key that will be generated using it. This is accomplished by using the singular value decomposition (SVD) on $\mathbf{Y}_B^T$, the noisy copy of $\mathbf{H}_{BA}$,

$$\mathbf{Y}_B^T = \mathbf{H}_{BA} + \mathbf{N}_B^T = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^H, \tag{15}$$

and using the left singular vector matrix $\mathbf{U}$ to obtain

$$\mathbf{U}^H\mathbf{Y}_B^T = \mathbf{U}^H(\mathbf{H}_{BA} + \mathbf{N}_B^T) = \mathbf{U}^H\mathbf{U}\mathbf{\Sigma}\mathbf{V}^H = \mathbf{\Sigma}\mathbf{V}^H. \tag{16}$$

Upon decorrelation of the channel measurements, Bob sends the matrix of left singular vectors $\mathbf{U}$ to Alice over a public, error-free channel. We note that $\mathbf{U}$ has no information related to the generated key; thus, its transmission does not disclose any information to Eve.

Following decorrelation, Bob generates a random unitary precoding matrix $\mathbf{P}$, which he uses to post-multiply his decorrelated matrix

$$\mathbf{U}^H\mathbf{Y}_B^T\mathbf{P} = \mathbf{\Sigma}\mathbf{V}^H\mathbf{P} \tag{17}$$

and to precode his pilot signal used by Alice to determine a precoded MIMO channel measurement matrix

$$\begin{aligned}\mathbf{Y}_A &= \mathbf{H}_{BA}\mathbf{P} + \mathbf{N}_A = (\mathbf{Y}_B^T - \mathbf{N}_B^T)\mathbf{P} + \mathbf{N}_A \\ &= \mathbf{U}\boldsymbol{\Sigma}\mathbf{V}^H\mathbf{P} - \mathbf{N}_B^T\mathbf{P} + \mathbf{N}_A. \end{aligned} \tag{18}$$

After this transmission, Alice gets the precoded channel measurement matrix instead of the actual one, and applies the $\mathbf{U}$ matrix received from Bob to decorrelate its channel measurement matrix:

$$\begin{aligned}\mathbf{U}^H\mathbf{Y}_A &= \mathbf{U}^H(\mathbf{U}\boldsymbol{\Sigma}\mathbf{V}^H\mathbf{P} - \mathbf{N}_B^T\mathbf{P} + \mathbf{N}_A) \\ &= \boldsymbol{\Sigma}\mathbf{V}^H\mathbf{P} - \mathbf{U}^H\mathbf{N}_B^T\mathbf{P} + \mathbf{U}^H\mathbf{N}_A. \end{aligned} \tag{19}$$

5.2.2 QUANTIZATION OF CHANNEL MEASUREMENTS

To obtain the individual bits of the secret key that will be used to encrypt the information transmitted over the legitimate wireless link, Alice and Bob apply one-bit scalar quantization [4] to the elements of the precoded MIMO channel measurement matrices in Eqs. (17) and (19), respectively, which are converted from $M \times M$ complex-valued matrices into real-valued vectors of size $2M^2 \times 1$ as follows:

$$\mathbf{v}_A = [vec\{\mathrm{Re}(\mathbf{U}^H\mathbf{Y}_A)\}^T \; vec\{\mathrm{Im}(\mathbf{U}^H\mathbf{Y}_A)\}^T]^T \tag{20}$$

$$\mathbf{v}_B = [vec\{\mathrm{Re}(\mathbf{U}^H\mathbf{Y}_B^T\mathbf{P})\}^T \; vec\{\mathrm{Im}(\mathbf{U}^H\mathbf{Y}_B^T\mathbf{P}\})^T]^T \tag{21}$$

where the $vec\{\cdot\}$ operation denotes the column stacking operation.

Alice quantizes the elements in $\mathbf{v}_A$ to generate the secret key bits in string $\mathbf{k}_A$ by making hard decisions using the following threshold rule:

$$k_A[n] = \begin{cases} 0, & v_A[n] > 0 \\ 1, & v_A[n] \leq 0. \end{cases} \tag{22}$$

Unlike Alice, Bob makes soft decisions in his scalar quantization process by calculating the log-likelihood ratio (LLR) of each element in $\mathbf{v}_B$ in order to increase his probability of matching Alice's generated key. As can be observed from Eqs. (17) and (19), despite channel reciprocity, Alice and Bob obtain different channel measurement values due to the independent noise corrupting their received signals. Upon decoupling of the real and imaginary parts in Eqs. (17) and (19) through the column stacking operation, the difference between $v_A[n]$ and $v_B[n]$ is determined by the receiver noise variable:

$$w'[n] = v_A[n] - v_B[n], \tag{23}$$

which is also Gaussian with zero mean and has variance equal to $(\sigma_A^2 + \sigma_B^2)/2$. Therefore, the LLR for a given sample $v_B[n]$ is calculated as:

$$\begin{aligned} LLR_B[n] &= \ln \frac{\Pr(v_A[n] = \text{`0'} | v_B[n])}{\Pr(v_A[n] = \text{`1'} | v_B[n])} \\ &= \ln \frac{\Pr(w'[n] > -v_B[n])}{\Pr(w'[n] < -v_B[n])}. \end{aligned} \tag{24}$$

Since $w'[n]$ is a Gaussian random variable with known parameters, we can use the $\mathcal{Q}$-function [33] to compute the LLR:

$$LLR_B[n] = \ln \frac{\mathcal{Q}\left(\frac{-v_B[n]}{\sqrt{\frac{\sigma_A^2+\sigma_B^2}{2}}}\right)}{1 - \mathcal{Q}\left(\frac{-v_B[n]}{\sqrt{\frac{\sigma_A^2+\sigma_B^2}{2}}}\right)}. \tag{25}$$

5.2.3 KEY RECONCILIATION

Because Alice initiates the transmission, Alice is considered to be the leader in the key generation process and the key bits generated by Alice will be treated as the "correct" encryption key bits. Bob follows Alice's lead and will attempt to match the key bits generated by Alice through the key reconciliation process. For this, Alice generates also the parity

vector $\mathbf{s}$ by using the LDPC encoder matrix $\mathbf{H}_s$ for Slepian-Wolf coding, which will be transmitted to Bob using a public, error-free channel.

Bob receives the side information $\mathbf{s}$ sent by Alice, and uses both the LLRs and the side information to apply Slepian-Wolf decoding with the $\mathbf{H}_s$ matrix to determine the key bits $\mathbf{k}_B$. We note that, ideally the keys generated at Alice and Bob coincide, i.e., $\mathbf{k}_A = \mathbf{k}_B$, although some bit mismatches between $\mathbf{k}_A$ and $\mathbf{k}_B$ may still occur, most likely caused by the bits that have an LLR value close to zero.

To further reduce the bit mismatch rate, Bob's samples that are close to the quantization threshold, i.e., the samples that have a high mismatch probability, can be removed from the key. In the literature, this process is referred to as censoring [31], and enables a trade-off between the key length and the bit mismatch rate.

A censoring scheme can be implemented with an arbitrary threshold value γ: the samples that fall in the interval $[-\gamma, \gamma]$ at Alice's side are eliminated (censored) and not included in generated key. Alice sends the indices of the censored symbols over the public channel to eliminate the same samples at Bob. Note that whether a sample is censored or not depends only on its distance from the quantization threshold and not on its sign, causing both binary values to have the same likelihood of being eliminated, i.e., the probability density of the generated key samples does not change. Thus, the entropy of the generated key remains the same, and the index information does not reveal any information about the sample to Eve. The expected number of censored samples can be adjusted by changing the threshold value γ. As the value of γ increases more samples will be eliminated and will not be used for generating key bits, leading to a lower probability of bit mismatch between keys at the cost of reducing the key generation rate.

5.3 EAVESDROPPER'S PERSPECTIVE

The security enabled by encryption keys generated based on channel measurements relies on the lack of correlation of the legitimate channel matrices $\mathbf{H}_{AB}$ and $\mathbf{H}_{BA}$, and the eavesdropping channel matrices between Alice and Eve $\mathbf{H}_{AE}$, and between Bob and Eve, $\mathbf{H}_{BE}$, respectively. However, if Eve is able to get physically closer to one of the legitimate nodes of the system, her channels will become correlated to the legitimate channels, and,

as a consequence, Eve may be able to extract information that will enable her to generate the secret key. Because of the precoding operation performed by Bob, which randomizes its channel, the pilot signals received by Alice and Bob will be different, and in order for Eve to generate encryption key bits she will have to use different strategies that depend on her proximity to Alice and Bob, the leader and follower nodes, respectively, in the legitimate key generation process. These strategies are outlined in the following subsections under worst case scenarios for secrecy, in order to evaluate how much key information Eve may be able to obtain in either scenario.

5.3.1 PROXIMITY TO THE LEADER NODE

In this case, Eve is located close to Alice, who is the leader node in the key generation process. Therefore, the channel over which Eve eavesdrops on Bob's transmission is correlated to the legitimate channel over which Bob transmits information to Alice, that is $\mathbf{H}_{BE} \approx \mathbf{H}_{BA}$, and Eve is able to receive the precoded pilot signal from Bob, who is the follower node in the key generation process:

$$\mathbf{Y}_{BE} = \mathbf{H}_{BE}\mathbf{P} + \mathbf{N}_{BE} = \mathbf{H}_{BA}\mathbf{P} + \mathbf{N}_{BE}. \tag{26}$$

Since transmission of the left singular matrix $\mathbf{U}$ occurs over a public channel, Eve will also receive it and may use it with her calculations. Noting that:

$$\begin{aligned} \mathbf{Y}_E &= \mathbf{U}^H(\mathbf{H}_{BA}\mathbf{P} + \mathbf{N}_{BE}) \\ &= \mathbf{\Sigma}\mathbf{V}^H\mathbf{P} - \mathbf{U}^H\mathbf{N}_B^T\mathbf{P} + \mathbf{U}^H\mathbf{N}_{BE} \end{aligned} \tag{27}$$

one can see that Eve may apply a column stacking operation similar to those applied by Alice and Bob in Eqs. (20) and (21), respectively, to obtain

$$\mathbf{v}_E = [vec\{\mathrm{Re}(\mathbf{Y}_E)\}^T \; vec\{\mathrm{Im}(\mathbf{Y}_E)\}^T]^T, \tag{28}$$

which can be quantized for soft-decision with the LLR calculated similar to Bob in Eq. (25):

$$LLR_E[n] = \ln \frac{\mathcal{Q}\left(\frac{-v_E[n]}{\sqrt{\frac{\sigma_A^2+\sigma_E^2}{2}}}\right)}{1-\mathcal{Q}\left(\frac{-v_E[n]}{\sqrt{\frac{\sigma_A^2+\sigma_E^2}{2}}}\right)}. \tag{29}$$

Using the same side information that Alice receives from Bob, Eve is now able to generate her own key bits, which will not be identical to those generated by Alice because their channels are not identical but rather only correlated, and the received signals at Alice and Bob are corrupted by distinct, independent noise variables. Thus, there will be bit mismatches between the keys generated by Alice and Eve, which Eve can potentially minimize based on the side information transmitted by Alice.

5.3.2 PROXIMITY TO FOLLOWER NODE

In this case, Eve is located close to Bob, who is the follower node in the key generation process. This implies that the channel over which Eve eavesdrops on Alice's transmission is correlated to the legitimate channel over which Alice transmits information to Bob, that is $\mathbf{H}_{AE} \approx \mathbf{H}_{AB}$, while the channel over which Eve overhears Bob's transmission to Alice is almost ideal, that is $\mathbf{H}_{BE}$ is close to the identity matrix $\mathbf{I}_M$. In this scenario, Eve will get the precoding matrix from Bob's pilot signal (since Bob is responsible for generating the precoding matrix), along with the channel measurements from Alice. Therefore, Eve will have the following information available:

$$\mathbf{Y}_{AE} = \mathbf{H}_{AE} + \mathbf{N}_{AE} = \mathbf{H}_{AB} + \mathbf{N}_{AE} = \mathbf{H}_{BA} + \mathbf{N}_{AE}^T \tag{30}$$

and since $\mathbf{H}_{BE} \approx \mathbf{I}_M$,

$$\mathbf{Y}_{BE} = \mathbf{H}_{BE}\mathbf{P} + \mathbf{N}_{BE} = \mathbf{P} + \mathbf{N}_{BE}. \tag{31}$$

With the transmission of the left singular matrix $\mathbf{U}$ occurring over a public channel, Eve

will also receive it and will again be able to generate her own vector $\mathbf{v}_E$. Noting that:

$$\begin{aligned}\mathbf{Y}_E &= \mathbf{U}^H(\mathbf{H}_{BA} + \mathbf{N}_{AE}^T)(\mathbf{P} + \mathbf{N}_{BE}) \\ &= \mathbf{\Sigma}\mathbf{V}^H\mathbf{P} + \mathbf{\Sigma}\mathbf{V}^H\mathbf{N}_{BE} + (-\mathbf{U}^H\mathbf{N}_B^T + \mathbf{U}^H\mathbf{N}_{AE}^T)(\mathbf{P} + \mathbf{N}_{BE}),\end{aligned} \tag{32}$$

it can be seen that, again, Eve may apply column stacking operation described in Eq. (28) to obtain $\mathbf{v}_E$ from $\mathbf{Y}_E$. Then, she can proceed by soft-decision quantization with LLR calculation given in Eq. (29), and using also the side information received from Alice, Eve can generate her own key bits. However, in addition to having only correlated channel information that depends on her distances to Alice and Bob, in this scenario Eve has to contend also with additional noise terms in the expression of $\mathbf{Y}_E$ compared to the previous case as demonstrated by Eqs. (27) and (32), which will result in additional bit mismatches between the keys generated by Alice and Eve more than the previous scenario. Thus, the key generated by the legitimate users in this scenario can be considered more secure, which is confirmed by the information theoretic analysis presented in the following section.

5.4 INFORMATION THEORETIC ANALYSIS

Let I_K be the maximum number of key bits that can be extracted by Alice and Bob for each channel use. This can be calculated as [37, 38]

$$I_K = \log_2 \frac{|\mathbf{R}_A||\mathbf{R}_B|}{|\mathbf{R}_{AB}|}, \tag{33}$$

where

$$\mathbf{R}_A = \mathrm{E}\left[\mathbf{v}_A\mathbf{v}_A^H\right], \quad \mathbf{R}_B = \mathrm{E}\left[\mathbf{v}_B\mathbf{v}_B^H\right], \quad \text{and} \quad \mathbf{R}_{AB} = \begin{bmatrix} \mathrm{E}\left[\mathbf{v}_A\mathbf{v}_A^H\right] & \mathrm{E}\left[\mathbf{v}_A\mathbf{v}_B^H\right] \\ \mathrm{E}\left[\mathbf{v}_B\mathbf{v}_A^H\right] & \mathrm{E}\left[\mathbf{v}_B\mathbf{v}_B^H\right] \end{bmatrix}, \tag{34}$$

for vectors $\mathbf{v}_A$ and $\mathbf{v}_B$ defined in Eqs. (20) and (21), respectively. The value of I_K depends essentially on the mutual information between channel measurements of Alice and Bob and is affected by the variance σ_h^2 of their MIMO wireless channel, as well as by the noise variances σ_a^2 and σ_b^2 at Alice and Bob, respectively. We note that, due to the precoding with random

unitary matrix $\mathbf{P}$, it is possible to generate different key bits repeatedly from the same channel measurement by generating new $\mathbf{P}$ for each use. Note that the keys generated by the same channel measurement will have the same I_K value regardless of the random $\mathbf{P}$ matrices used as I_K value only depend on the channel variance σ_h^2. We also note that, while I_K is a measure of how many key bits can be extracted by Alice and Bob based on their respective channel measurements, it does not give any indication about how much of the generated bit information can also be extracted by Eve.

As Eve's physical location gets closer to the location of either one of the legitimate users, the MIMO channel matrices $\mathbf{H}_{AE}$ and $\mathbf{H}_{BE}$ over which Eve eavesdrops on the transmissions from Alice and Bob, respectively, may become correlated to the legitimate channel matrices $\mathbf{H}_{AB}$ and $\mathbf{H}_{BA}$, respectively. In this case, Eve will get channel measurements that are correlated to those of Alice or Bob, which could potentially contain information that can reveal bits of the secret key established by the legitimate users. The number of key bits that remain secret I_{SK} can be calculated as [37, 38]

$$I_{SK} = \log_2 \frac{|\mathbf{R}_{AE}||\mathbf{R}_{BE}|}{|\mathbf{R}_E||\mathbf{R}_{ABE}|}, \tag{35}$$

where

$$\begin{aligned}
\mathbf{R}_E =& \mathrm{E}\left[\mathbf{v}_E\mathbf{v}_E^H\right] \\
\mathbf{R}_{AE} =& \begin{bmatrix} \mathrm{E}\left[\mathbf{v}_A\mathbf{v}_A^H\right] & \mathrm{E}\left[\mathbf{v}_A\mathbf{v}_E^H\right] \\ \mathrm{E}\left[\mathbf{v}_E\mathbf{v}_A^H\right] & \mathrm{E}\left[\mathbf{v}_E\mathbf{v}_E^H\right] \end{bmatrix}, \quad \mathbf{R}_{BE} = \begin{bmatrix} \mathrm{E}\left[\mathbf{v}_B\mathbf{v}_B^H\right] & \mathrm{E}\left[\mathbf{v}_B\mathbf{v}_E^H\right] \\ \mathrm{E}\left[\mathbf{v}_E\mathbf{v}_B^H\right] & \mathrm{E}\left[\mathbf{v}_E\mathbf{v}_E^H\right] \end{bmatrix}, \text{and} \\
\mathbf{R}_{ABE} =& \begin{bmatrix} \mathrm{E}\left[\mathbf{v}_A\mathbf{v}_A^H\right] & \mathrm{E}\left[\mathbf{v}_A\mathbf{v}_B^H\right] & \mathrm{E}\left[\mathbf{v}_A\mathbf{v}_E^H\right] \\ \mathrm{E}\left[\mathbf{v}_B\mathbf{v}_A^H\right] & \mathrm{E}\left[\mathbf{v}_B\mathbf{v}_B^H\right] & \mathrm{E}\left[\mathbf{v}_B\mathbf{v}_E^H\right] \\ \mathrm{E}\left[\mathbf{v}_E\mathbf{v}_A^H\right] & \mathrm{E}\left[\mathbf{v}_E\mathbf{v}_B^H\right] & \mathrm{E}\left[\mathbf{v}_E\mathbf{v}_E^H\right] \end{bmatrix}
\end{aligned} \tag{36}$$

are covariance matrices defined for vectors $\mathbf{v}_A$, $\mathbf{v}_B$, and $\mathbf{v}_E$. From Eq. (35), it can be observed that as correlations between Eve's generated vector and Alice or Bob's vectors converge to zero, the matrices $\mathbf{R}_{AE}$ and $\mathbf{R}_{BE}$ become diagonal matrices and their determinants can be reformulated as $|\mathbf{R}_{AE}| = \left|\mathrm{E}\left[\mathbf{v}_A\mathbf{v}_A^H\right]\right| \left|\mathrm{E}\left[\mathbf{v}_E\mathbf{v}_E^H\right]\right| = |\mathbf{R}_A|\,|\mathbf{R}_E|$ and

$|\mathbf{R}_{BE}| = \left|\mathrm{E}\left[\mathbf{v}_B\mathbf{v}_B^H\right]\right| \left|\mathrm{E}\left[\mathbf{v}_E\mathbf{v}_E^H\right]\right| = |\mathbf{R}_B|\,|\mathbf{R}_E|$, respectively. Moreover, $|\mathbf{R}_{ABE}|$ converges to $|\mathbf{R}_{ABE}| = |\mathbf{R}_{AB}|\,|\mathbf{R}_E|$. As a result, $|\mathbf{R}_E|$ terms in the numerator and denominator cancel out each other, and resulting I_{SK} becomes equal to I_K. Therefore, all the information that can be extracted by Alice and Bob can be considered safe. By contrast, as the correlation of Eve's channels to legitimate channels increase, I_{SK} converges to zero, meaning all information can be acquired by Eve and there is no secrecy. As a result, in practical applications, I_{SK} is always between zero and I_K.

5.5 ROLE REVERSAL FOR ENHANCED SECURITY

As discussed in Section 5.3, the process by which Eve obtains the elements of vector $\mathbf{v}_E$ that are needed to generate the secret key bits depends on whether Eve is physically located closer to Alice or Bob. In Figs. 26 and 27, simulation results showing I_K and I_{SK} are presented for the case when Eve is located closer to Alice and Bob, respectively. From these figures it can be seen that, for the same channel correlation coefficients the I_{SK} values are closer to I_K when Eve is closer to Bob, which indicates that the system is more secure in this case.

Since Alice and Bob are unable to determine the location of a passive eavesdropper, they may protect against eavesdropping and improving the worst case scenario by changing their roles during the key generation process. Specifically, after the bits for the first half of the secret key are generated, Bob will become the leader node in the key generation process and establishes the secret key bits by hard decisions following the threshold rule Eq. (22), and Alice node becomes the follower node that uses soft decisions with LLR calculations in Eq. (25). From their new roles they continue generating the second half of the key, and when all the key bits are generated, the two halves are concatenated by the legitimate users to obtain the secret key that will secure the legitimate link. Thus, even when Eve is very close to one of the legitimate users and may be able to obtain half of the key bits with high accuracy, the other half of her key bits will have more mismatches from the key generated by the legitimate users. The effect of the role reversal procedure is presented in Fig. 28, which shows the results when the key is generated in two parts: Alice is the leader node in the first half and Bob is the follower node. In the second half, the roles are reversed and Bob

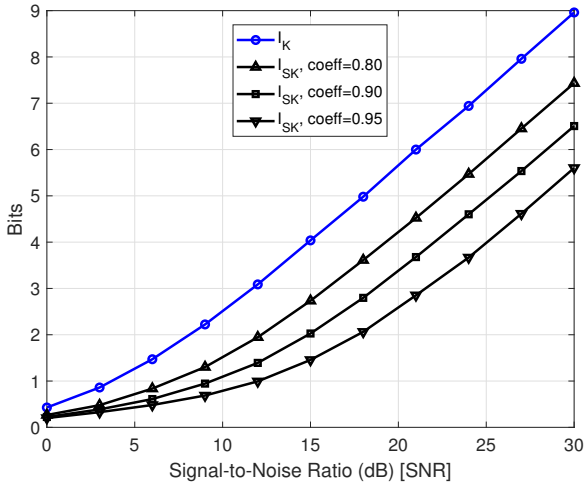


Figure 26. I_K and I_{SK}, when Eve is located closer to Alice.

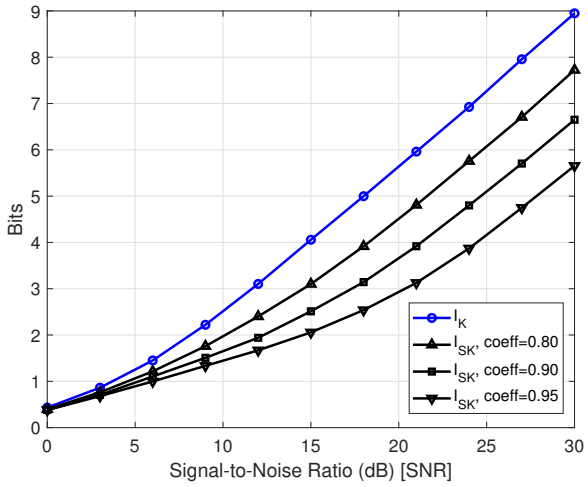


Figure 27. I_K and I_{SK}, when Eve is located closer to Bob.

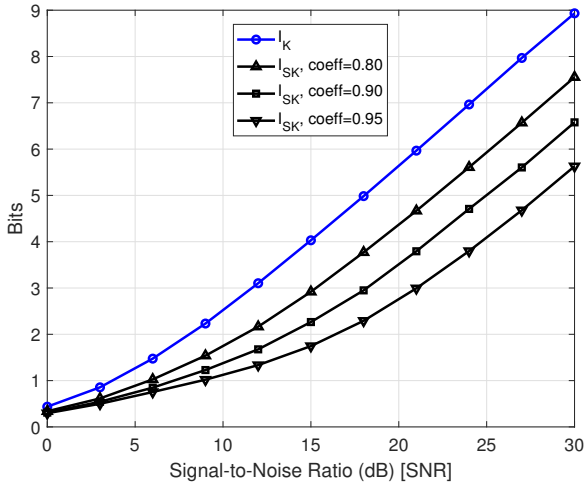


Figure 28. I_K and I_{SK}, when Eve is located closer to one of the nodes with role reversal.

becomes leader node and Alice is follower. As a result, Eve is closer to the leader node half the time and closer to the follower node in the other half, which leads to an improved worst case scenario for I_{SK}.

5.6 BIT MISMATCH PERFORMANCE

In this section, we present numerical results obtained from Monte-Carlo simulations of the proposed key generation and reconciliation scheme with role reversal to observe the probability of bit mismatch between the secret keys generated by Alice and the secret keys generated by Bob and Eve, for different SNR values, different LDPC code rates and different correlation values between the legitimate channel and the eavesdropper channel.

We consider the scenario where Eve is located close to Bob and their channels are highly correlated. We note that the scenario where Eve is close to Alice is similar due to the role reversal approach in key generation, which ensures that Eve will be close to either the leader or the follower node for only half of the key generation process. Thus, Eve's proximity to either Alice or Bob will not affect her key bit mismatch rate.

Regular LDPC codes from the DVB-S.2 standard [34] with a block size of 64,800 bits have been used for generating side information, and the censoring threshold is set to $\gamma = \sigma_a^2/2$. Noise variances for all nodes are assumed to be equal, i.e., $\sigma_a^2 = \sigma_b^2 = \sigma_e^2$. For each SNR value, the simulations are repeated for 4,096 blocks.

In the first simulation experiment we studied the bit mismatch rate for Bob and Eve for LDPC code rate equal to 1/2 and channel correlation coefficients equal to 0.8, 0.9, and 0.95. Results from this experiment are shown in Fig. 29, from which we note that, despite the high correlation between the legitimate and the eavesdropper channels, the bit mismatch rate at Eve will be larger at Eve than at Bob, and it will not improve with increasing SNR. This behavior is due to the fact that, as the SNR increases, Eve's confidence in her own channel measurements increases and the LLRs for channel measurements at Eve increase in magnitude, which in turn reduces the effect of Alice's side information on the final key generated by Eve. Since Alice's and Eve's channel measurements are different, Eve's LDPC result gets closer to Eve's own measurements, but it does not help with getting closer to Alice's key. As the correlation coefficient between Alice's and Eve's channel with

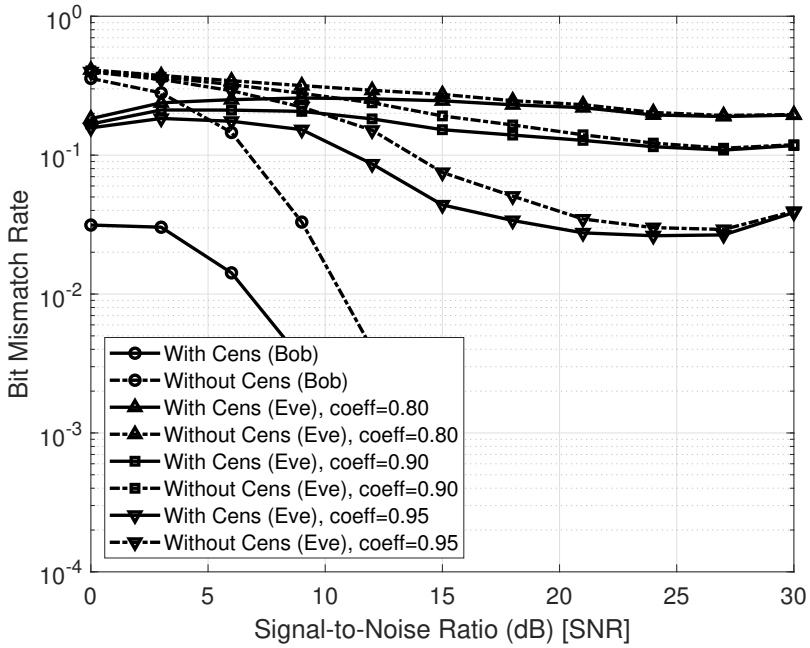


Figure 29. Bit mismatch rates at Bob and Eve for LDPC code rate 1/2 and different channel correlation coefficients.

Bob increases, the bit mismatch rate for Eve improves, while still being significantly larger than Bob's bit mismatch rate.

In the second simulation experiment we studied the bit mismatch rate for Bob and Eve for a channel correlation coefficient equal to 0.9 and LDPC code rates equal to 1/2, 3/4, and 4/5. Results from this experiment are shown in Fig. 30, from which we note that Eve's bit mismatch rate increases with the increase in the LDPC code rate. We note that, for visual simplicity we have only shown Bob's key mismatch rate for LDPC code rate 4/5 in Fig. 30, which corresponds to the least amount of side information revealed to Bob, leading to highest mismatch rate among the considered LDPC code rates. For this value of the LDPC code rate, Bob's highest bit mismatch rate is significantly lower than Eve's bit mismatch rate for the same SNR value. This result is due to the fact that, as the LDPC code rate increases, the parity vector $\mathbf{s}$ sent by Alice to Bob over public channel reveals less information about the actual key bits, so Eve has limited information for her key reconciliation. Thus, because of privacy amplification [25, 35, 36] this difference of mismatches can result in completely different generated keys due to the nature of hash functions.

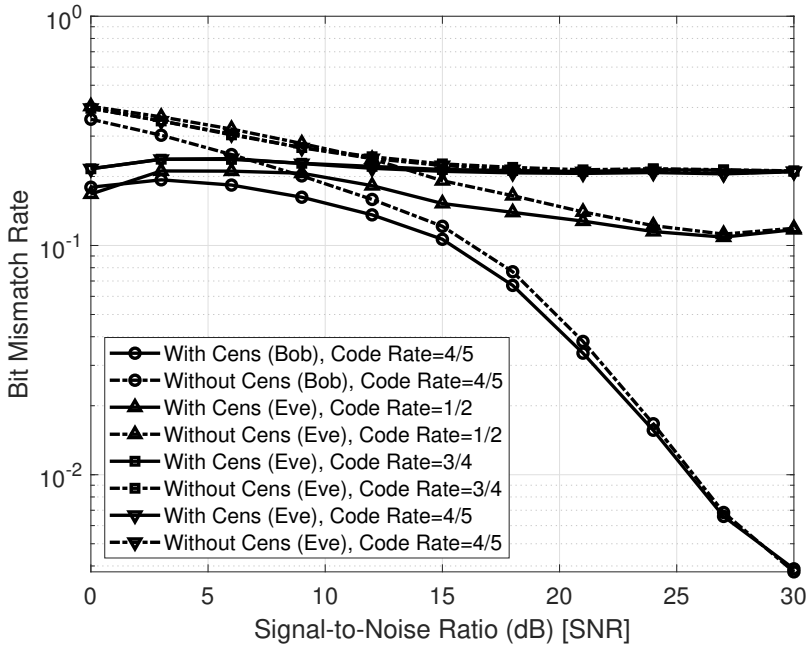


Figure 30. Bit mismatch rates at Bob and Eve for channel correlation coefficient of 0.9 and different LDPC code rates.

Simulation results shown in Figs. 29 and 30 illustrate also the improvement in bit mismatch rate that is obtained when censoring is employed. Specifically, we can see that the bit mismatch rate decreases as the samples in the censoring region $[-\gamma, \gamma]$ are eliminated and not considered for key generation. Thus, censoring can be used as an optional step to further reduce the bit mismatch rate in the system. We note that transmitting the indices of the censored samples increases the information transmitted over the public channel, but it does not reveal any meaningful information about the secret key generated by legitimate users and therefore, the eavesdropper cannot use this information to make an educated guess about the secret key. We also note that the side effect of censoring is a reduction in the average key length due to the removal of channel measurement samples.

5.7 CHAPTER SUMMARY

In this chapter we studied secret key generation in wireless systems based on channel state information and proposed a new approach that prevents an eavesdropper from obtaining information about the key even when its channel is highly correlated with the legitimate users' channel. The proposed approach uses a randomly generated precoding matrix to generate multiple key bits from the same set of MIMO channel measurements, which makes the key generation process independent of the channel coherence time. Furthermore, the quantization process used to obtain the key bits does not rely on knowledge of the statistical properties of the channel and eliminates the need for estimating the channel statistics, and the role reversal of legitimate users halfway through the key generation process ensures that an eavesdropper cannot acquire meaningful information to generate the key even if its channel is correlated to the legitimate channel.

Numerical simulation results corroborate our analysis and show that the legitimate users can achieve significantly lower bit mismatch rates than the eavesdropper, even when the eavesdropper is close to one of them and has highly correlated channel measurements with them.

CHAPTER 6

CONCLUSIONS AND FUTURE WORK

In this chapter, a brief summary of the contributions of the dissertation is presented and future research directions and ideas are discussed.

6.1 CONCLUSIONS

Wireless communication is at the center of our lives, with constantly increasing importance. Both our personal and business lives depend on it to the point that we cannot simply think about spending a day without it. This dependence on wireless connectivity creates an ever-increasing need for more connectivity and transmission speed. However, the fundamental resource wireless systems depend on, radio frequency spectrum, is limited and usable frequencies are already assigned to current systems that are in use. As a result, for years, the only way to use new technologies was to deprecate old systems and reassign the usable frequency bands to newer technologies wherever possible. However, with the introduction of cognitive radio, efficiently sharing the spectrum became an important topic.

In this dissertation, we contributed to efficient sharing of the spectrum where all users have the same access rights to the spectrum and there is no enforcement mechanism to regulate the use of the frequency, as it occurs in cognitive radio or ISM bands. It is shown that, the well-known waterfilling algorithm maximizes a users transmission rate based on interference plus noise measurement, yet creates interference to other users in the system, reducing the system throughput. Moreover, this causes other users to update their power control calculations, which in turn creates a need for other users update their power control calculations due to newly introduced interference. This individual transmission rate maximization attempt with its resulting cycle of updating is harmful to the system throughput supported by the literature. We proposed a novel self-enforcing power control mechanism that respects other users in the system and tries to use the available spectrum with other users' needs in mind. Furthermore, no information exchange by users is needed to employ the

algorithm; therefore, it can be employed independently of other users' power allocation. It is also shown that the proposed system is robust to the presence of selfish users. In both dense and sparse environments, the system with users who employ proposed algorithm reaches to higher throughput than a system where users selfishly employ waterfilling algorithm.

Fundamentally, wireless communication systems depend on radio signals propagation in order to send information from transmitter to receiver. At the core, propagating radio waves loaded with information can be received by both intended and unintended receivers. To ensure the information transmitted is private between a legitimate transmitter and receiver pair, traditionally an encryption system is used before RF transmission phase. This encryption ensures that an eavesdropper who can receive the signals cannot get meaningful information. Although the encryption systems in use for decades work, they come with their own problems: key generation and distribution in symmetric key cryptography or encryption and decryption complexity on top of requirement of trusted third party public key distributors. Recent advancements in this field created a new joint secret key generation and distribution mechanism that exploits randomness of the wireless channels. In this dissertation, we defined the problem statement and explained the mechanism for the new system. We proposed a simple, quick to establish and practical system to generate and distribute secret keys followed by key reconciliation with LDPC codes to ensure low bit mismatch rates. We extended our work to MIMO cases and with a novel role reversal mechanism to further increase secrecy of our system for the worst case scenario, i.e. a passive eavesdropper listening to the communication while being physically close to one of the nodes. With information theory calculations, it is shown that the proposed system creates secret communication between legitimate nodes.

6.2 FUTURE WORK

Throughout the research in this dissertation, several potential future research areas have been identified. These areas have the potential to improve the results presented in this dissertation, or change the direction of the research altogether.

The spectrum sharing system considered in this dissertation assumes constant transmission of all users at all times. However, in practice, it is common for communication systems

to transmit signals in bursts with maximum transmission power and stop transmission until the next burst is transmitted. This temporal noncontinuous transmission can be potentially exploited to more efficiently share the spectrum in both frequency domain and time domain. The addition of time domain into the system model can lead to better system throughput and should be considered as a future work.

Another area that can be studied further is identified in the key reconciliation mechanism with LDPC codes. LDPC codes are traditionally designed for error detection and correction on communication channels. In general, parity bits are created prior to transmission and then the block is sent to the receiver. In the key reconciliation steps we discussed in Chapters 4 and 5, the key is generated at both legitimate nodes at the same time with approximately equal LLRs. Unlike traditional communication systems where LLRs of the information bits at the receiver cannot be known by the transmitter, in key reconciliation, both nodes have this information prior to the generation and transmission of parity bits. Therefore, it might be possible to create the optimal generator matrix for the LDPC code that will be used for key reconciliation based on the known LLRs so that error correction success can be maximized. In such a case, the generator matrix itself can be sent to the follower node over a public channel as it will not reveal any information to the eavesdropper about the key itself.

APPENDIX A

WATERFILLING ALGORITHM

The waterfilling algorithm maximizes channel capacity of a user in a wireless communication system by optimally allocating power over multiple parallel Gaussian channels. The algorithm finds the optimal signal plus noise level for transmission power to maximize capacity. If the wireless environment has interference, calculation can be done for signal plus noise plus interference level with the assumption that interference can be treated as a Gaussian random process.

The appendix is presented as follows. In Section A.1, capacity is defined for Gaussian channels. In Section A.2, optimal power allocation for transmission rate maximization problem is solved, and as a result the waterfilling algorithm is formally defined.

A.1 GAUSSIAN CHANNEL CAPACITY

Gaussian channel is the basis of modern communication theory introduced by Shannon [39]. Gaussian channel is a time-discrete, continuous alphabet channel with independent identically distributed (i.i.d.) additive white noise at output.

$$Y_i = X_i + Z_i \quad \text{where} \quad Z \sim \mathcal{N}(0, N). \tag{37}$$

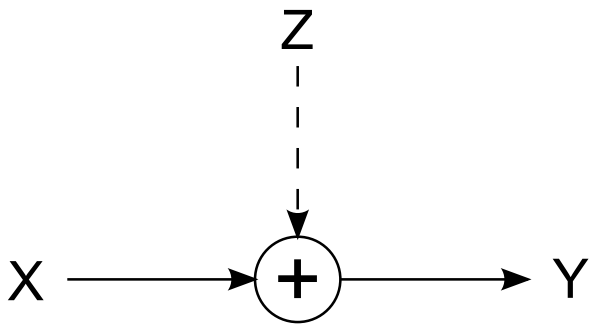


Figure 31. Gaussian channel model

where X_i and Y_i are the input and output signals respectively and Z_i is the additive noise. The limit on mutual information between input and output is the information capacity of the Gaussian channel. The information capacity for a Gaussian channel with power constraint is defined as [40]

$$C \triangleq \max_{E[X^2] \leq \bar{P}} I(X;Y) \tag{38}$$

where $\bar{P}$ is the power constraint and and $E[X^2]$ is the expectation of the power of input signal X. We can calculate the information capacity by expanding mutual information between X and Y,

$$\begin{aligned} I(X;Y) &= h(Y) - h(Y|X) && (39)\\ &= h(Y) - h(X+Z|X) \\ &= h(Y) - h(Z|X) \\ &= h(Y) - h(Z) && (40) \end{aligned}$$

since Z is independent of X. Since $h(Z) = \frac{1}{2}\log 2\pi eN$ is known, we can calculate

$$E[Y^2] = E[(X+Z)^2] = E[X^2] + 2E[X]E[Z] + E[Z^2] = P + N. \tag{41}$$

By using this equality in Eq. (40), we get

$$\begin{aligned} I(X;Y) &= h(Y) - h(Z) \\ &\leq \frac{1}{2}\log\Big(2\pi e(P+N)\Big) - \frac{1}{2}\log(2\pi eN) \\ &= \frac{1}{2}\log\Big(1 + \frac{P}{N}\Big) && (42) \end{aligned}$$

Therefore, the capacity is found as

$$C \triangleq \max_{E[X^2] \leq P} I(X;Y) = \frac{1}{2}\log\Big(1 + \frac{P}{N}\Big) \tag{43}$$

since the maximum is achieved when $X \sim \mathcal{N}(0, P)$.

A.2 OPTIMAL POWER CONTROL ON PARALLEL GAUSSIAN CHANNELS WITH WATERFILLING

In wireless communication systems, some techniques divide the communication channel into subchannels and a transmitter is assigned to multiple subchannels for communication. Thus, the transmitter needs to distribute powers according to a common power constraint. This approach is extremely important against nonwhite Gaussian noise since all subchannel components will represent different frequencies and be affected by noises at different levels. The capacity of the system can be found by optimal distribution of power to subchannels. The system can be represented as,

$$Y_j = X_j + Z_j, \quad j = 1, 2, \ldots, k, \tag{44}$$

where Z_j is i.i.d. white Gaussian noise with distribution $Z_j \sim \mathcal{N}(0, N_j)$ for channel j. The capacity of the system can be represented as,

$$C = \max_{\sum_1^k E[X_i^2] \le \bar{P}} I(X_1, X_2, \ldots, X_k; Y_1, Y_2, \ldots, Y_k). \tag{45}$$

Similar to the capacity derivation of Gaussian channel in Eqs. (39)–(40), capacity of parallel Gaussian channels can be derived as,

$$\begin{aligned}
&I(X_1,X_2,\ldots,X_k;Y_1,Y_2,\ldots,Y_k) \\
&\quad = h(Y_1,Y_2,\ldots,Y_k) - h(Y_1,Y_2,\ldots,Y_k|X_1,X_2,\ldots,X_k) \\
&\quad = h(Y_1,Y_2,\ldots,Y_k) - h(Z_1,Z_2,\ldots,Z_k|X_1,X_2,\ldots,X_k) \\
&\quad = h(Y_1,Y_2,\ldots,Y_k) - h(Z_1,Z_2,\ldots,Z_k) \\
&\quad = \sum_i h(Y_i) - \sum_i h(Z_i) \\
&\quad \le \sum_i h(Y_i) - h(Z_i) \\
&\quad \le \sum_i \frac{1}{2}\log\left(1 + \frac{P_i}{N_i}\right)
\end{aligned} \tag{46}$$

and the maximum is achieved when X is i.i.d and $X_i \sim \mathcal{N}(0, P_i)$.

The optimal power allocation scheme that maximizes capacity subject to common power constraint in parallel Gaussian channels can be found by using Lagrange multipliers. Lagrangian can be expressed as

$$\mathcal{L}(P_1, \ldots, P_k) = \sum_i \frac{1}{2} \log\Big(1 + \frac{P_i}{N_i}\Big) + \lambda\Big(\sum_i P_i\Big), \tag{47}$$

and differentiating with respect to P_i, we get

$$\frac{1}{2}\frac{1}{P_i + N_i} + \lambda = 0 \tag{48}$$

which can be turned into

$$P_i = (v - N_i) \tag{49}$$

where, $v = -\frac{1}{2\lambda}$. Since P_i cannot be negative, the equation becomes

$$P_i = (v - N_i)^+. \tag{50}$$

Therefore we can choose v such that

$$\sum_i (v - N_i)^+ = \bar{P}. \tag{51}$$

The result of this derivation can be interpreted as, if there are multiple channels with different noise levels, the available power must be distributed such that, sum of noise and transmission powers in channels must be equal to each other, just like filling a pool with water. Therefore, this solution is referred to *waterfilling* in the literature.

A.3 EXTENSION TO MULTIPLE ACCESS CHANNELS

The waterfilling algorithm maximizes a single user's transmission rate by allocation power over available frequency bands based on the observed noise. In multiple access channels,

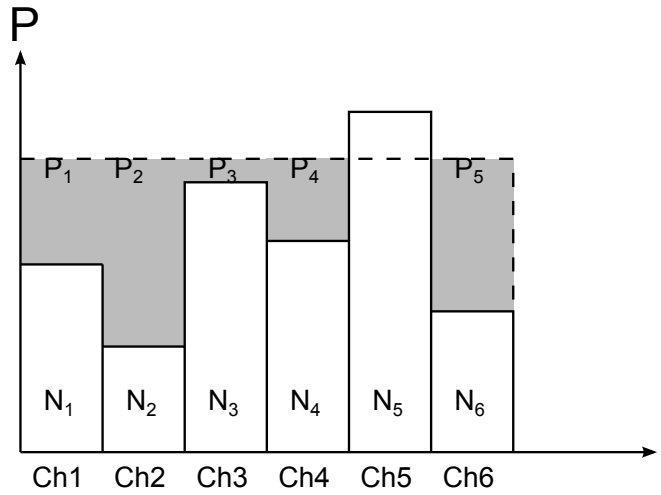


Figure 32. Waterfilling in parallel Gaussian channels. The dashed line represents the optimum power level and gray area under it is the powers used for each channel.

interference in addition to the noise becomes the limiting factor of capacity. A user still can apply waterfilling to maximize its transmission rate. However, as one users updates their power allocation, the interference that is observed by other users in the system will change. In addition, unlike noise, interference changes over time and cannot be assumed static over long time periods.

In [8], it is proved that for a multiple access channel, all users can apply waterfilling simultaneously to maximize their own transmission rates. With every iteration, the system converges to a point on the edge of capacity region. This result shows that the iterative waterfilling algorithm can be used to find a stable point for user power allocations in multiple access channels without a central organization mechanism. Note that the equilibrium point may not be the sum rate maximization point [9, 10].

APPENDIX B

LOW-DENSITY PARITY-CHECK CODES

Low-density parity-check (LDPC) codes are a class of linear block error correcting codes. LDPC codes have near-capacity performance on large transmissions (large block sizes) over communication channels, and an iterative decoding process with low error floor.

LDPC codes were first proposed by Gallager in his doctoral dissertation [41] in 1960, Tanner generalized LDPC codes in 1981 [42] and introduced graphical representation, Tanner graphs. Despite the advantages of LDPC codes in terms of high performance, they were not used due to high required computational power until the mid 1990's when MacKay, Luby and others [43, 44] rediscovered LDPC codes independent of Gallager's work.

The appendix is presented as follows. Fundamentals and two equivalent representations of LDPC codes are introduced in Section B.1, code construction methods are discussed in Section B.2 and finally decoding implementations are briefly discussed in Section B.3.

B.1 FUNDAMENTALS AND REPRESENTATION

Low-density parity-check codes can be represented in two forms: matrix and graph representations. We will first discuss fundamentals of LDPC codes in matrix form in the following subsection, then we will continue the section with graph representation. We will give a sample LDPC code in both matrix and graph form for clarity.

B.1.1 MATRIX REPRESENTATION

A low-density parity-check code is a linear block code with a sparse parity-check matrix, i.e., parity-check matrix has low density of 1's as elements. Each LDPC block has two main type of nodes; the original information to be transmitted, variable nodes (v-nodes) and the redundant information that is designed to ensure correct transmission of original information, check nodes (c-nodes). Any (n,k) LDPC code block consists of n number of nodes: k v-nodes and $n-k$ c-nodes. For k v-nodes, c-nodes are calculated by using a $k \times n$ *generator matrix*

$\mathbf{G}$, such that $\mathbf{xG}^T = 0$ where $\mathbf{x}$ denotes the original information, i.e. v-nodes in vector form. To check the integrity of the transmitted signals, the $(n-k) \times n$ *parity-check matrix* $\mathbf{H}$ is used to satisfy $\mathbf{cH}^T = 0$, where $\mathbf{c}$ denotes c-nodes in vector form. Since c-nodes are functions of v-nodes, they can be written as binary addition of related v-nodes; therefore, in the literature, sometimes they are called function nodes.

There are two types of LDPC codes, regular and irregular codes. Regular codes have parity-check matrix $\mathbf{H}$ with exactly the same amount of 1s in each row, i.e, v-node degree. Irregular codes on the other hand can have varying amount of 1's in each row of parity-check matrix, i.e., c-node degree. This property is easier to see in graphical representation of LDPC codes. Regular or irregular, LDPC codes have a fundamental property called code rate which is defined as the ratio of the number of new information bits to block length, and calculated as k/n.

B.1.2 GRAPH REPRESENTATION

Tanner realized a different representation of LDPC codes are possible and considered LDPC codes as bipartite graphs [42]. A bipartite graph is a type of graph that has two distinct group of nodes and each type of node can only be connected to the other type of nodes. Therefore, v-nodes and c-nodes can be considered as two types of nodes on a graph where each v-node is only connected to c-nodes and each c-node is only connected to v-nodes. This type of visualization makes LDPC codes easier to study.

Graph representation of LDPC codes helps in understanding the performance of a particular block based on the smallest *loop* (or *cycle*) that is present in the graph. A loop of length l on a graph is defined as a closed path that has l number of edges. By definition, the shortest loop length an LDPC code block can have is 4; however, cleverly designed LDPC codes can have minimum-length loops longer than 4. The length of the shortest loop in the LDPC block affects the performance of the LDPC code and should be a design consideration.

For further clarity, a sample parity-check matrix for an (10,5) LDPC code of block length 15 with code rate 1/2 is provided below. The parity-check matrix of the LDPC code considered is given below and a block of LDPC code is visualized in Fig. 33.

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \tag{52}$$

Note that each row vector of **H** represents c-node connections and each column vector represents v-node connections. As a result, we can write c-node calculation steps as individual binary additions as follows.

$$c_0 = x_0 \oplus x_1 \oplus x_2 \oplus x_3, \tag{53}$$

$$c_0 = x_0 \oplus x_4 \oplus x_5 \oplus x_6, \tag{54}$$

$$c_0 = x_1 \oplus x_4 \oplus x_7 \oplus x_8, \tag{55}$$

$$c_0 = x_2 \oplus x_5 \oplus x_7 \oplus x_9, \tag{56}$$

$$c_0 = x_3 \oplus x_6 \oplus x_8 \oplus x_9, \tag{57}$$

where $\oplus$ denotes binary addition operation. In Fig. 33, the same block is presented in bipartite graph form. The connections between v-nodes and c-nodes can be clearly seen visually as edges on the graph. The thick edges represent the shortest length loop, which is length 6-cycle in this particular sample.

B.2 LDPC CODE CONSTRUCTION CONSIDERATIONS

There are multiple important considerations for LDPC code construction. A good LDPC code should be generated by following an algorithm to remove randomness, have low v-node and c-node degrees for lower calculation steps for encoding and decoding and most importantly should have a long minimum-length loop to keep the error-floor low. In the literature, many LDPC code construction methods are proposed, [41, 43, 44] for various applications. In this section, we only define main considerations for LDPC construction

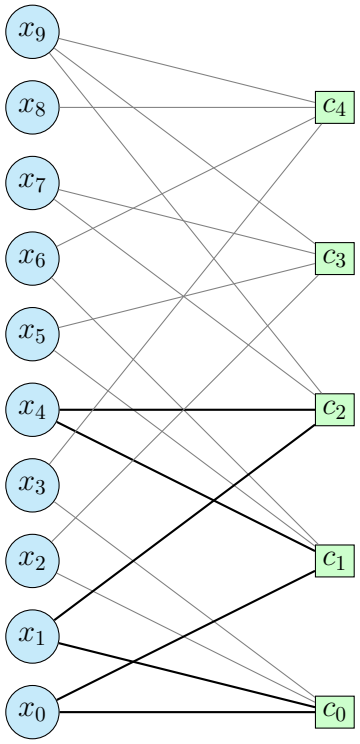


Figure 33. The bipartite graph representation of the sample LDPC code with parith-check matrix **H**. Blue and green nodes represent the v-nodes and c-nodes respectively.

methods rather than the construction algorithms.

Gallager proposed an algorithm to generate regular LDPC codes in his dissertation [41]. His approach was to generate submatrices that follows a special form and combine them to construct the parity-check matrix **H**. The encoder has low complexity and by creating the submatrices cleverly, his design could avoid length-4 cycles. The performance of the designed LDPC code was moderate. These type of codes were studied for code-division multiple-access communication channels [45].

MacKay designed algorithms to construct LDPC codes semi-randomly, and these codes can be found on his personal website [46]. MacKay's procedure includes randomly generating columns of **H** while ensuring any pair of columns will have no greater than one overlap of 1's. This procedure was repeated until full-rank invertible **H** was found. The encoder for this procedure was high complexity and the generated matrix was generally not sparse. The technique was further improved with revisions to the steps.

Luby *et al.* [47] and Richardson *et al.* [48, 49] proposed procedures to construct irregular

LDPC codes. The main contribution of their algorithms were changing the degrees of both v-nodes and c-nodes depending on the channel properties instead of finding a fixed solution that fits all and optimizing the degrees in an additional step called density evolution. These codes achieve high performance very close to the channel capacity for long block lengths, yet their performance drops quickly as the block size decreases.

In this section, we only covered the basics of the code construction considerations and named a few methods. LDPC encoder design is still a very active area of research that is constantly evolving.

B.3 DECODING

Decoding LDPC codes is a complex task and only the main idea will be discussed in this section for simplicity.

As LDPC code block has v-nodes as the new information and c-nodes for parity check, it is easy to generate c-nodes based on received v-nodes and compare the received c-nodes with the result. Any mismatch will mean there was an error during transmission. However, this is a very simple approach that uses only binary symbols and cannot be used for error correction. A more advanced aproach would be using log-likelihood ratios of individual bits after transmission and generate c-nodes with this information. The closer the LLR to the received c-node, one can be more confident in the received bit.

Gallager designed a decoding algorithm that is near optimal that uses LLR of the received bits to further improve the confidence on the bits received [41]. In his approach, each of the c-nodes provide *a posteriori* probability for v-nodes based on the check node calculations. The LLR value of a v-node can be a starting point, and with the LLR of the connected c-nodes, confidence on the v-node can be increased. After v-node's confidence increases, the same technique is applied to c-nodes. With each iteration of the algorithm, the LLR calculations of the nodes start to converge to a point where quantization should provide the correct binary value that was transmitted. This iterative decoding process is has various names in the literature such as belief propagation algorithm, sum-product algorithm or message passing algorithm.

The iterative process for decoding has various benefits if used cleverly. First of all, as the

number of iterations increase, the accuracy of the decoded bits increase and bit error rate decreases. The main two limitations on the number of iterations can be used for decoding are computation time and length of shortest loop in the LDPC code block. Former is the main limitation for real-time systems. For a real-time system the decision has to be made within a fixed time period; therefore, based on the computational power, only a certain number of iterations can be made before the time limit is reached. For non-real-time applications, the latter becomes the main limitation. An LDPC code with shortest-length loop of length l, can have only $l/2$ iterations before the decoding algorithm loops back on itself, creating a feedback loop that does not improve confidence in the received bits. This limitation creates a lower limit for bit error rate called *error floor* and limits the performance of the LDPC code.

BIBLIOGRAPHY

[1] S. Baksi and D. C. Popescu, "Distributed Power Allocation For Rate maximization in Cognitivew Radio Networks with Horizontal Spectrum Sharing," in *Proceedings 2015 IEEE Wireless Communications and Networking Conference – WCNC*, New Orleans, LA, March 2015, pp. 950–954.

[2] S. Baksi and D. C. Popescu, "Horizontal Spectrum Sharing and Coexistence Scenarios for Mutually Interfering Systems," in *Proceedings* 3^{rd} *IEEE International Black Sea Conference on Communications and Networking – BlackSeaCom 2015*, Constanta, Romania, May 2015, pp. 34–37.

[3] S. Baksi and D. C. Popescu, "Distributed power allocation for spectrum sharing in mutually interfering wireless systems," *Physical Communication*, vol. 22, pp. 42 – 48, March 2017.

[4] S. Baksi, J. Snoap, and D. C. Popescu, "Secret key generation using one-bit quantized channel state information," in *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, March 2017, pp. 1–6.

[5] S. Baksi and D. C. Popescu, "Secret key generation in mimo wireless systems using precoded channel measurements," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Oct 2017, pp. 1–5.

[6] S. Baksi and D. C. Popescu, "Submitted to secret key generation with precoding and role reversal in mimo wireless systems," *Trans. on Wireless Communications, IEEE*, July 2018.

[7] A. B. Carleial, "Interference Channels," *IEEE Transactions on Information Theory*, vol. 24, no. 1, pp. 60–70, January 1978.

[8] W. Yu, W. Rhee, S. Boyd, and J. M. Cioffi, "Iterative Water-Filling for Gaussian Vector Multiple-Access Channels," *IEEE Transactions on Information Theory*, vol. 50, no. 1, pp. 145–152, January 2004.

[9] O. Popescu, D. C. Popescu, and C. Rose, "Simultaneous Water Filling in Mutually Interfering Systems," *IEEE Transactions on Wireless Communications*, vol. 6, no. 3, pp. 1102–1113, March 2007.

[10] O. Popescu, C. Rose, and D. C. Popescu, "Signal space partitioning versus simultaneous water filling for mutually interfering systems," in *IEEE Global Telecommunications Conference, 2004. GLOBECOM '04.*, vol. 5, Nov 2004, pp. 3128–3132 Vol.5.

[11] R. Etkin, A. Parekh, and D. Tse, "Spectrum Sharing for Unlicensed Bands," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 3, pp. 517–528, April 2007.

[12] C. A. Gizelis and D. D. Vergados, "A survey of pricing schemes in wireless networks," *Communications Surveys Tutorials, IEEE*, vol. 13, no. 1, pp. 126–145, First 2011.

[13] C. Saraydar, N. B. Mandayam, and D. Goodman, "Efficient power control via pricing in wireless data networks," *IEEE Transactions on Communications*, vol. 50, no. 2, pp. 291–303, Feb 2002.

[14] G. Ginis and J. M. Cioffi, "Vectored Transmission for Digital Subscriber Line Systems," *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 5, pp. 1085–1104, June 2002.

[15] W. Yu, G. Ginis, and J. M. Cioffi, "Distributed Multiuser Power Control for Digital Subscriber Lines," *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 5, pp. 1105–1115, June 2002.

[16] R. Menon, A. B. MacKenzie, R. M. Buehrer, and J. Reed, "Interference avoidance in networks with distributed receivers," *IEEE Transactions on Communications*, vol. 57, no. 10, pp. 3078–3091, October 2009.

[17] R. Menon, A. B. Mackenzie, J. Hicks, R. M. Buehrer, and J. H. Reed, "A game-theoretic framework for interference avoidance," *IEEE Transactions on Communications*, vol. 57, no. 4, pp. 1087–1098, April 2009.

[18] B. Babadi and V. Tarokh, "GADIA: A Greedy Asynchronous Distributed Interference Avoidance Algorithm," *IEEE Transactions on Information Theory*, vol. 56, no. 12, pp. 6228–6252, December 2010.

[19] B. Sklar, *Digital Communications: Fundamentals and Applications*, 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 2001.

[20] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, June 2010.

[21] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," in *2007 IEEE International Conference on Ultra-Wideband*, Sept 2007, pp. 270–275.

[22] L. Lai, Y. Liang, H. V. Poor, and W. Du, "Key Generation from Wireless Channels," in *Physical Layer Security in Wireless Communications*, X. Zhou, L. Song, and Y. Zhang, Eds. Boca Raton, FL: CRC Press, 2013, pp. 47–92.

[23] R. Mehmood and J. W. Wallace, "MIMO Capacity Enhancement Using Parasitic Reconfigurable Aperture Antennas (RECAPs)," *IEEE Transactions on Antennas and Propagation*, vol. 60, no. 2, pp. 665–673, February 2012.

[24] J. Cheng, M. Hashiguchi, K. Iigusa, and T. Ohira, "Electronically Steerable Parasitic Array Radiator Antenna for Omni- and Sector Pattern Forming Applications to Wireless Ad Hoc Networks," *IEE Proceedings on Microwaves, Antennas, and Propagation*, vol. 150, no. 4, pp. 203–208, August 2003.

[25] J. Etesami and W. Henkel, "LDPC Code Construction for Wireless Physical-Layer Key Reconciliation," in *Proceedings First IEEE International Conference on Communications in China – ICCC*, Beijing, China, August 2012, pp. 208–213.

[26] O. Graur, N. Islam, A. Filip, and W. Henkel, "Quantization Aspects in LDPC Key Reconciliation for Physical Layer Security," in *Proceedings of 10th IEEE International ITG Conference on Systems, Communications and Coding – SCC 2015*, Hamburg, Germany, February 2015.

[27] X. Sun, X. Wu, C. Zhao, M. Jiang, and W. Xu, "Slepian-Wolf Coding for Reconciliation of Physical Layer Secret Keys," in *Proceedings 2010 IEEE Wireless Communications and Networking Conference – WCNC*, Sydney, Australia, April 2010.

[28] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly gaussian random variables," in *2006 IEEE International Symposium on Information Theory*, July 2006, pp. 2593–2597.

[29] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[30] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1484–1497, Oct 2012.

[31] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless Secret Key Generation Exploiting Reactance-Domain Scalar Response of Multipath Fading Channels," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, November 2005.

[32] M. A. Tope and J. C. McEachen, "Unconditionally Secure Communications Over Fading Channels," in *Proceedings 2001 IEEE Military Communications Conference – MILCOM*, vol. 1, McLean, VA, October 2001, pp. 54–58.

[33] R. D. Yates and D. J. Goodman, *Probability and Stochastic Processes. A Friendly Introduction for Electrical and Computer Engineers*, 1st ed. New York, NY: John Wiley and Sons, 1999.

[34] European Telecommunications Standards Institute, "ETSI Standard EN 302 307 V1.1.1: Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications (DVB-S2)," March 2005.

[35] C. Cachin and U. Maurer, "Linking Information Reconciliation and Privacy Amplification," *Journal of Cryptology*, vol. 10, no. 2, pp. 97–110, 1997.

[36] C. Cachin, "Entropy Measures and Unconditional Security in Cryptography," Ph.D. dissertation, Swiss Federal Institute of Technology, Zurich, Switzerland, 1997.

[37] J. Wallace, "Secure physical layer key generation schemes: Performance and information theoretic limits," in *2009 IEEE International Conference on Communications*, June 2009, pp. 1–5.

[38] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal mimo wireless channels: Measurement and analysis," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 381–392, Sept 2010.

[39] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, July 1948. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/j.1538-7305.1948.tb01338.x

[40] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York, NY, USA: Wiley-Interscience, 1991.

[41] R. G. Gallager, "Low-density parity-check codes," Ph.D. dissertation, Massachusetts Institute of Technology, 1960.

[42] R. Tanner, "A recursive approach to low complexity codes," *IEEE Transactions on Information Theory*, vol. 27, no. 5, pp. 533–547, September 1981.

[43] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 399–431, March 1999.

[44] N. Alon and M. Luby, "A linear time erasure-resilient code with nearly optimal recovery," *IEEE Transactions on Information Theory*, vol. 42, no. 6, pp. 1732–1736, Nov 1996.

[45] V. Sorokine, F. R. Kschischang, and S. Pasupathy, "Gallager codes for cdma applications: generalizations, constructions and performance," in *1998 Information Theory Workshop (Cat. No.98EX131)*, June 1998, pp. 8–9.

[46] D. J. C. Mackay, "Gallager code resources," date accessed (2018-09-25). [Online]. Available: http://www.inference.org.uk/mackay/

[47] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, "Improved low-density parity-check codes using irregular graphs," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 585–598, Feb 2001.

[48] T. J. Richardson and R. L. Urbanke, "Efficient encoding of low-density parity-check codes," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 638–656, Feb 2001.

[49] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 619–637, Feb 2001.

VITA

Saygın Bakşi
Department of Electrical & Computer Engineering
Old Dominion University
Norfolk, VA 23529

Education

- Ph.D. Electrical and Computer Engineering, December 2018, Old Dominion University
- M.Sc. Electronics Engineering, June 2013, Işık University
- B.Sc. Electronics Engineering, January 2010, Işık University

Select Publications

- S. Bakşi, D.C. Popescu, "Secret Key Generation with Precoding and Role Reversal in MIMO Wireless Systems", *Submitted to IEEE Transactions on Wireless Communications*, July 2018.
- S. Bakşi, D.C. Popescu, "Distributed Power Allocation for Spectrum Sharing in Mutually Interfering Wireless Systems", *Physical Communication*, vol. 22, pp. 42–48, 2017.
- S. Bakşi, D.C. Popescu, "Secret Key Generation in MIMO Wireless Systems Using Precoded Channel Measurements",*IEEE PIMRC 2017*, Montreal, Canada, Oct. 2017.
- S. Bakşi, J. Snoap, D.C. Popescu, "Secret Key Generation Using One-Bit Quantized Channel State Information", *IEEE Wireless Communications and Networking Conference (WCNC)*, San Francisco, CA, March 2017.
- S. Bakşi, D.C. Popescu, "Horizontal Spectrum Sharing and Coexistence Scenarios for Mutually Interfering Wireless Systems", *IEEE BlackSeaCom 2015*, Constanta, Romania, May 2015.
- S. Bakşi, D.C. Popescu, "Distributed Power Allocation for Rate Maximization in Cognitive Radio Networks with Horizontal Spectrum Sharing", *IEEE Wireless Communications and Networking Conference*, New Orleans, LA, April 2015.

Typeset using LaTeX.