KTH Electrical Engineering

Secrecy in Cognitive Radio Networks

FRÉDÉRIC GABRY

Doctoral Thesis in Telecommunications
Stockholm, Sweden 2014

TRITA-EE 2014:057
ISSN 1653-5146
ISBN 978-91-7595-332-8

KTH School of Electrical Engineering
SE-100 44 Stockholm
SWEDEN

Akademisk avhandling som med tillstånd av Kungliga Tekniska högskolan framlägges till offentlig granskning för avläggande av teknologie doktorsexamen i telekommunikation fredagen den 28 november 2014, kl. 14.00 i hörsal F3, Kungliga Tekniska Högskolan, Lindstedtsvägen 26, Stockholm.

Tryck: Universitetsservice US AB

Sammanfattning

Under de senaste årtiondena har användningen av trådlösa nätverk för digital kommunikation ökat avsevärt. Ett karaktärsdrag i trådlösa nätverk är att kommunikationen mellan två användare avläsas av en tredje (eller fler) användare. Detta leder till två koncept: samarbete och sekretess. En vänligt inställd tredje användare kan förbättra kommunikationen genom att samarbeta med de två första, medans en skadligt inställd tredje användare kan komma över potentiellt hemlig information. Hur samarbete kan modelleras mellan användarnoder har formaliserats i flera nätverksmodeller, till exempel i kognitiva radionät (CRN, för engelskans cognitive radio networks). I CRN har primära användare juridisk rätt till licensierat spektrum, men sekundära användare tillåts använda outnyttjat spektrum så länge de inte försämrar prestandan för de primära användarna. I den här avhandlingen studerar vi hur samarbete mellan användare (både primära och sekundära) i CRN kan förbättra säkerheten i nätverket. Vi riktar framförallt in oss på kognitiva nätverk där vi antar att det finns fientligt inställda sekundära avlyssnare (dvs passiva användare). För att lösa detta säkerhetsproblem, tillåter vi samarbete mellan primära och sekundära vänligt inställda sändare (dvs aktiva användare) eftersom detta kan förbättra säkerheten för det primära systemet, samtidigt som de sekundära sändarna gynnas genom att de får använda primära nätet för sin kommunikation. Baserat på den här nya kommunikatonsmodellen, studerar vi ett antal specialfall.

Först härleder vi uppnåeliga datatakter för ett antal system där det sekundära systemet antingen har, eller inte har, kunskap om meddelandet i det primära systemet. Vi tillhandahåller även insikter om effektallokering för dessa två fall. Vi formulerar och löser tre relevanta effektallokeringsproblem: maximering av datatakten hos primära och sekundära systemet samt minimering av sändareffekt av det sekundära systemet. Med Stackelbergs spelmodell analyserar vi en realistisk effektallokering som motsvarar en optimering av båda sändarnas resurser. Vi introducerar sedan ett multi-fas system som vi kallar clean relaying (CR) till CRN scenariot, och vi härleder uppnåeliga datatakter för detta system. En automatisk meddelande-lärning av den primära datan utförs hos de sekundära sändarna vid

design av systemet. Dessutom jämför vi CR med andra signalleringsstrategier, till exempel dirty paper coding och interference neutralization. Vi utökar sedan vår modell till fall där multipla sekundära sändar-/mottagarpar vill använda det primära spektrumet. För detta fall studerar vi flera typer av spelstrategier mellan primära och sekundära kommunikationspar, till exempel Stackelbergspel, effektkontrollspel och auktionsspel. För att återkoppla till ursprungsmodellen undersöker vi energieffektiviteten (EE) i nätverket och optimal effektallokering och effektmaximering för att maximera sekundära sändarnas energieffektivitet. Vi härleder ett viktigt EE Stackelberg-spel mellan två sändare, och inverkan av den spelteoretiska interaktionen analyseras. Vi motiverar och undersöker informationsteoretisk säkerhet med hjälp av tekniker för nyckel-överrenskommelse i trådlösa nätverk. Framförallt härleder vi uppnåeliga datatakter där hemliga nycklar kan genereras för två olika nyckelöverenskommelsestrategier i Gaussiska kanaler, där olika transmissionsstrategier används, till exempel effektkontroll och gemensam störning. Samspelet mellan sändande användare analyseras från ett spelteoretiskt perspektiv med hjälp av icke-kooperativ spelteori. För varje aspekt analyserad i avhandlingen illustrerar vi våra resultat genom numeriska exempel baserade på en geometrisk modell, där vi följande: inverkan av nodgeometrin för uppnåbara datatakter, optimala strategier, och inverkan av spelteoretisk interaktion mellan användare.

Abstract

With the considerable growth of wireless networks in recent years, the issue of network security has taken an important role in the design of communication devices and protocols. Indeed, due to the broadcast nature of these networks, communications can potentially be attacked by malicious parties, and therefore, the protection of transmitted data has become a main concern in today's communications. On the other hand the cooperation of nodes overhearing the transmission may potentially lead to a better performance. In this thesis we combine both fundamental concepts of cooperation and secrecy in wireless networks. In particular we investigate the cooperation between transmitters in a cognitive radio network where the secondary receiver is treated as a potential eavesdropper to the primary transmission. We study this novel model focusing on several fundamental aspects.

First we derive achievable rate regions for different transmission schemes, such as cooperative jamming and relaying, with and without primary message knowledge at the secondary transmitter. For these schemes, we formulate and solve three relevant power allocation problems: the maximization of the achievable primary and secondary rates, and the minimization of the secondary transmitting power. We model the interaction between the transmitting users as a Stackelberg game corresponding to a more realistic power allocation problem. We solve the game and illustrate its impact on the achievable rates.

Secondly we generalize our system model by introducing the multi-phase clean relaying (CR) scheme, which takes into account the message-learning constraint at the secondary transmitter, and we derive the achievable rate region for this scheme. We compare our CR scheme to other transmission strategies such as dirty paper coding, interference neutralization, and pure cooperative jamming.

Thirdly we extend our model to the generalized scenario where multiple secondary transmitter-receiver pairs wish to access the spectrum. For this scenario, we define and study several types of games between the primary network and the secondary pairs, such as Stackelberg games, power control games, and auction games. We derive the equilibrium of each game considered, which allows us to predict the

behavior of the users in the cognitive radio network with multiple secondary pairs.

Moreover we consider the important concept of energy efficiency (EE) for the performance of the cognitive radio network and we derive the power allocation and power splitting maximizing the secondary transmitter's energy efficiency. An important EE Stackelberg game between the two transmitters is formulated, and the impact of the game theoretic interaction is analyzed.

Finally we motivate and investigate information theoretic secrecy using key agreement techniques in wireless networks. In particular we derive achievable secret key rate regions for two different key agreement schemes in Gaussian channels using several transmission strategies such as power control and cooperative jamming. The interaction between transmitting users is analyzed from a game theoretic perspective using non-cooperative game theory.

For every fundamental perspective considered for the analysis of the model studied in the thesis, our results are illustrated through numerical examples based on a geometrical setup, highlighting the impact of the node geometry on the achievable rates, the optimal strategies, the games' equilibria and the impact of the game theoretic interaction between transmitters on the system performance.

Acknowledgments

The writing of this Ph.D. thesis, which started five years ago, has been a unique challenge, both exhausting and fulfilling. I would like to take this opportunity to thank the people who supported me during those years.

First and foremost, I would like to express my deepest gratitude to my research advisors Prof. Mikael Skoglund and Associate Prof. Ragnar Thobaben. I was *literally* on my way back to France when Mikael offered me to join the Communication Theory department as a Ph.D. student and I have never questioned my decision to come back since then. Mikael has always given me the guidance, the support and the freedom I needed to explore my own research interests. He was in many respects the best advisor I could have wished for. Whenever I needed help, Ragnar's door was open. His careful advice has always been invaluable, *e.g.*, to improve the quality of my writing, which was surely not the easiest of tasks. I now realize how much he has helped me become a better researcher.

I am very grateful to Dr. Somayeh Salimi for introducing me to several interesting research problems and for our enjoyable collaboration. I have learned a lot from her knowledge and experience and I would like to thank her for her useful comments and her valuable help during the writing of my Licentiate thesis and of our joint works.

I would like to thank Prof. Eduard Jorswieck for allowing me to visit his group at Technische Universität Dresden. I was especially looking forward to this opportunity for a cooperation with Eduard and his group and my expectations were exceeded. In particular I am very much indebted to Dr. Pin-Hsun Lin for broadening my knowledge so much since the start of our collaboration. I would like to express my sincere thanks to Pin-Hsun for sharing his knowledge with me and for all the help and careful comments. I would also like to thank Dr. Alessio Zappone for introducing me to an interesting area of research, and for our insightful discussions. I would like to thank the people at TU Dresden who made my stay enjoyable, in particular Sabrina Engelmann for her help.

I would like to express my thanks to Prof. Mérouane Debbah from Supelec for

acting as faculty opponent. I also want to thank the grading committee formed by Prof. Erik Ström from Chalmers University, Dr. Fredrik Rusek from Lund University and Associate Prof. Panos Papadimitratos from KTH. I would also like to acknowledge Associate Prof. Henrik Sandberg for the quality review of the thesis.

I am sincerely grateful to Dr. Mattias Andersson, Dr. Dennis Sundman, and Ragnar for proof reading parts of this thesis. I would also like to acknowledge the joint work with fellow colleagues Nan Li, Dr. Maksym Girnyk, and Dr. Nicolas Schrammar, which was a greatly enjoyable collaboration. I also want to thank Associate Prof. Tobias Oechtering for helping me develop teaching skills for the Signal Theory course, which led to a pleasant collaboration with two former Master students. I would like to thank Prof. Lars Kildehøj Rasmussen for many enjoyable research and non-research related discussions. Additionally I want to thank all my colleagues from the Communication Theory lab for providing a great working environment, which easily surpasses any expectations a Ph.D. student can have. In particular I am very grateful to Dennis Sundman for all the great discussions during *long* runs and for all the challenges we shared. I want to thank Mattias for our conversations and for our regular practice of game-theory applications. I also enjoyed great moments and humorous discussions with Dr. Ricardo Blasco Serrano and Nicolas. I would also like to mention Maksym, Nan, Zhao Wang, Farshad Naghibi, Dr. Saikat Chatterjee, Tai Do and Dr. Amirpasha Shirazinia for many discussions on various topics such as cinema, sports, politics, cooking, etc. (not respectively). It has also been a pleasure to share an office with fellow Ph.D. student Guang Yang during the last few months. Additionally I would like to thank Annika Augustsson, Irène Kindblom, Raine Tiivel and Dora Söderberg for taking care of the administrative issues.

I could always count on my friends' support wherever they were and I would like to thank my joyous group of friends: Antoine, Arnaud, Arthur, Axelle, Charles, Christophe, Joseph, Lucie, and Nicolas. In particular the presence of Antoine, Charles and Joseph in Stockholm during my first years as a Ph.D. student was really enjoyable, and we shared many great moments, including numerous unique discussions on game theory, life, and other topics.

I want to thank Merle for all her love, for all the great moments we shared over the last years, and for all her support and encouragement during the difficult times. Thank you for making me happy every day.

Finally, I would like to express my endless gratitude to my family. I would especially like to thank my mom, my dad, my sister Michèle, my brother Julian, and my grandfather, for their love and support. I have been away from home for more than ten years now, and they have always been there whenever I needed them. This thesis is dedicated to them.

Frédéric Gabry
Stockholm, November 2014

Contents

Chapter 1

Introduction

1.1 Background and Motivation

Wireless networks have developed considerably over the last few decades. As a consequence of the broadcast nature of these networks, transmissions can potentially be intercepted by malicious parties, and therefore, security plays a fundamental role in today's communications. Security issues in communication networks are usually addressed in layers above the physical layer (PHY), using cryptography methods [MvOV96]. However there are several shortcomings to relying exclusively on cryptography techniques for the security of wireless systems, such as the difficulty of key distribution in decentralized networks, the cost of key management in dynamic topologies, or the lack of security metrics to compare protocols. Other weaknesses are also inherent to the wireless nature of the transmission medium as keys or messages can be intercepted, potentially making cryptographic methods inadequate. In addition to the traditional cryptographic approaches, there exists a way to implement security protocols directly at the physical layer, possibly in conjunction with existing protocols at the above layers. This promising direction towards achieving secure communications is named information theoretic secrecy.

Information Theoretic Secrecy in Wireless Networks The information theoretic secrecy approach, initiated by Shannon [Sha49] and later developed by Wyner [Wyn75], exploits the randomness of the communication channels to ensure the secrecy of the transmitted messages. In [Wyn75], Wyner introduced the wiretap channel depicted in Figure 1.1, which is the simplest model to study secrecy in communications. In this figure, Alice aims at transmitting a message to Bob while keeping it secret from Eve. The information theoretic secrecy framework allows us to define formally security measures in this model and characterize the secrecy performance of the system in terms of secrecy capacity, representing the highest rates at which the message can be transmitted both reliably and securely, according to the defined secrecy measures [BB11]. Advanced channel coding techniques, e.g.,

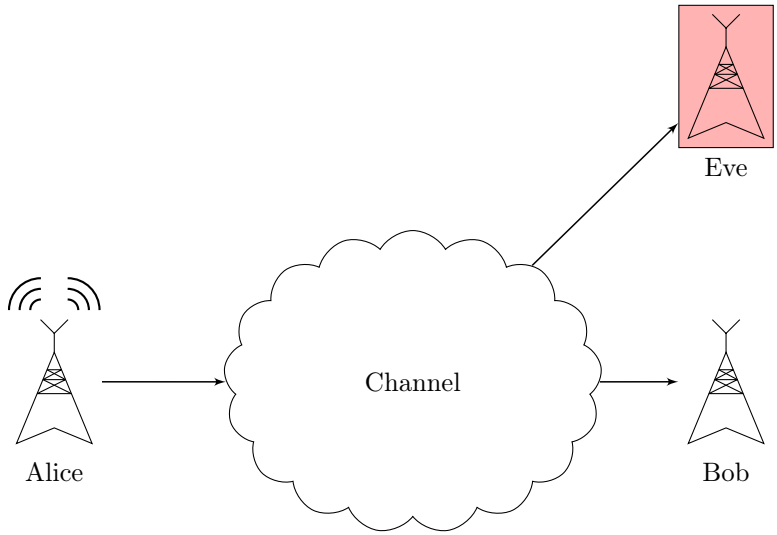


Figure 1.1: The wiretap channel.

in [And14], have recently been proposed to construct codes achieving secrecy capacity. However, similarly to communication networks without secrecy constraints, the overall performance is limited by the channels' conditions. In particular, to guarantee secure communications, Alice and Bob need to have some kind of advantage over Eve, e.g., a better channel quality or access to a feedback channel. Many techniques have been proposed to overcome this limitation, such as the use of multiple antenna systems, e.g., multiple-input multiple-output (MIMO) nodes in [OH08], [SLU09], [LS09]. Recently, there has been a substantial interest in the secrecy of multi-users systems [LPSS09], with a particular emphasis on a potential cooperation between users to enhance the secrecy of communications [EHT+13].

Cooperative Communications Improving the reliability of wireless communication systems can be achieved through cooperation, which involves multiple parties assisting each other in the transmission and decoding of messages. Indeed, albeit the broadcast nature of wireless communications leads to security issues, the cooperation of nodes overhearing the transmission may potentially lead to a better performance. Since the introduction of the relay channel in [vdM71], depicted in Figure 1.2, which is the simplest form of a cooperative communication network, cooperation in multi-node channel models and cooperative strategies have been deeply investigated in a tremendous number of works, e.g., in [LTW04], [KGG05]. Comprehensive reviews of the advances, ideas, and techniques related to the cooperative communications in wireless networks can be found in [EGK12], [KMY07].

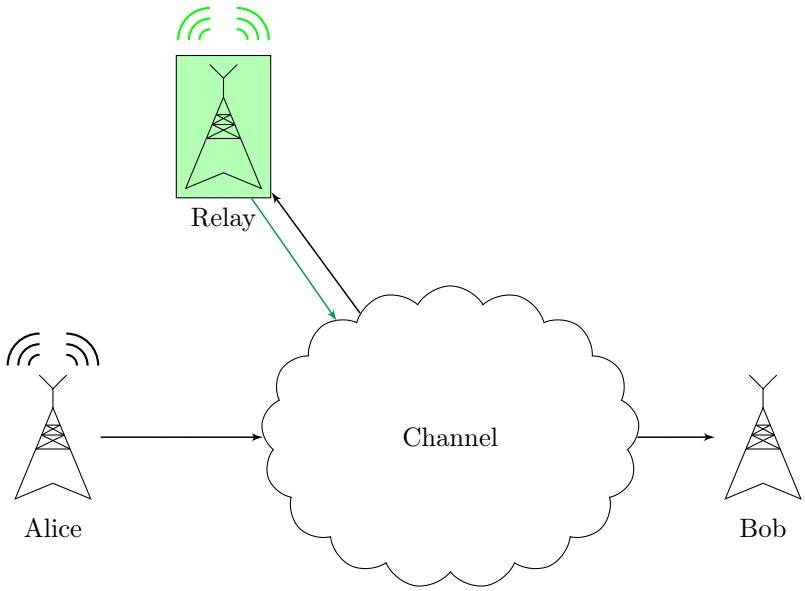


Figure 1.2: The relay channel.

Cooperation for Secrecy in Wireless Networks Combining the fundamental concepts of secrecy and cooperation in wireless networks leads to the new paradigm of cooperation for secrecy in wireless networks, described in its canonical form in Figure 1.3. There exist several cooperative strategies to improve the secrecy of legitimate transmissions in wireless networks. These strategies can be classified into two types. In the first type, cooperative parties improve the secrecy performance of the system by weakening the eavesdropping link. Hence, in contrast to wireless communications without secrecy where interference is considered as an undesired effect, interference can potentially be a beneficial phenomenon for secure communications. Many works have considered the impact of different variants of interference injection, under names such as noise-forwarding [LEG08], cooperative jamming [TY08b], [EHT$^+$13], or interference assisted secret communication [TLSP11]. The second type corresponds to the classical sense of cooperation, where the cooperating nodes strengthen the main transmission by using common relaying techniques such as decode-and-forward, amplify-and-forward [DHPP10], or compress-and-forward [KP11]. These techniques are applicable to more general multi-user cooperative networks with secrecy [LPSS09]. One should note however that although information theoretic secrecy for wireless networks has been studied extensively, there is a type of network for which the interest in the security at the physical layer has grown only recently: cognitive radio networks.

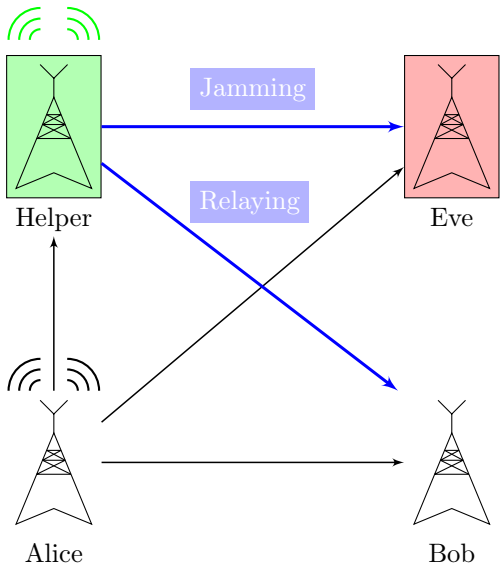


Figure 1.3: Cooperation for secrecy.

Cognitive Radio Networks Cognitive radio technology, introduced by Mitola in [Mit00], proposes an efficient way to sense the spectrum, decode information from detected signals, and use this knowledge to improve the overall performance of communication systems. In cognitive radio networks, secondary users are allowed to use the licensed spectrum as long as they do not degrade the data transmission of the primary users, which are the legacy owners of the spectrum. Therefore, the cognitive radio system is aware of its surroundings and dynamically adapts its transmission parameters, e.g., its frequency bands and coding schemes, to the changes of its environment. When both the primary and secondary networks consist of a single transmitter-receiver pair as depicted in Figure 1.4, the cognitive radio scenario can be investigated from an information theoretic perspective, as in [GJMS09], since it is captured by the interference channel model with some additional assumptions. In recent years, numerous cognitive radio techniques have been proposed for spectrum sharing, sensing, and management [ALVM06], which are based on the tools of multiple theoretical fields such as graph theory, linear programming, etc. [TZFS13]. One theoretical framework to analyze users' behavior in cognitive radio networks has received considerable attention in the last decades: game theory.

Game Theory in Communication Networks Game theory is a formal framework with a set of mathematical tools to study the complex interactions among interdependent rational players [HNS+12]. There has recently been a growing interest

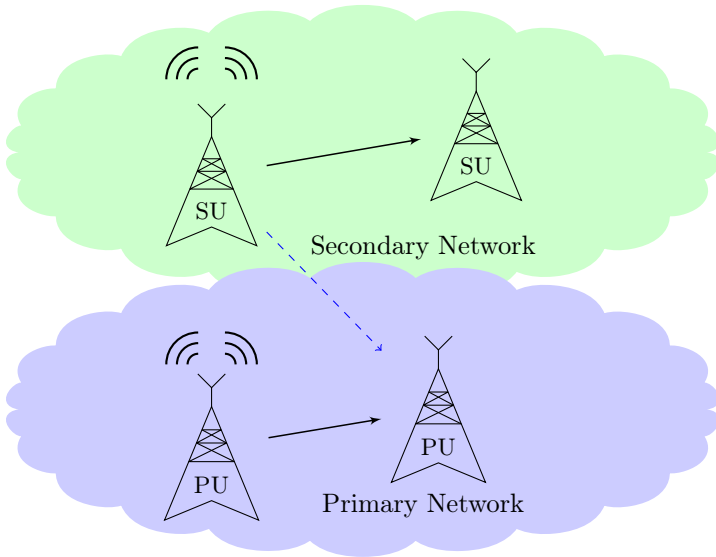


Figure 1.4: Cognitive radio networks.

in using game theoretical approaches to model and study communication systems as game theory provides indeed the mathematical tools to analyze the interactions between selfish users in networks. In particular, game theory has been applied to solve problems in many communication networks, as described in Figure 1.5, as well as several other fields such as political sciences or economics. In the figure, we highlight in blue the application areas that are related to those investigated in this thesis, e.g., cognitive radio as in [SHD+09], cooperative networks as in [HL08], and power control as in [HL05]. Many other applications of game theory in communication networks exist [HNS+12], since the new challenges emerging from the growth of decentralized wireless networks call for game theoretic solutions. Challenges for the design of the future generation of cognitive radio networks which can be analyzed through a game theoretic perspective include users' selfish behavior, energy efficiency, and the central topic of this thesis: secrecy.

Cooperation for Secrecy in Cognitive Radio Networks In recent years, due to the growth of cognitive radio networks (CRN), security issues have been the subject of increasing attention for these networks. While traditional security threats such as jamming and media access control layer (MAC-layer) attacks exist, CRN-specific threats such as exogenous attackers or selfish/intruding nodes exploiting the vulnerability of *ad hoc* cognitive networks must be considered. For eavesdropping attacks, the concept of information theoretic secrecy and the corresponding cooperative techniques for secrecy can naturally be applied to cognitive radio networks.

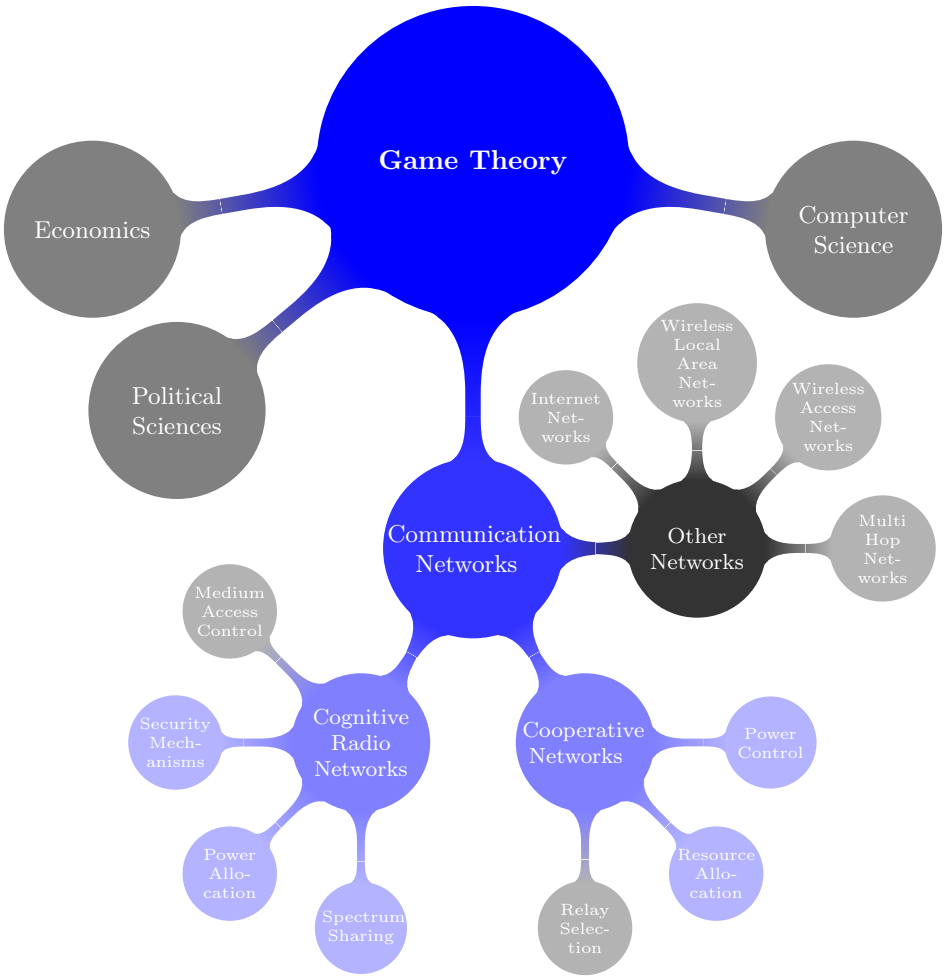


Figure 1.5: Game theory applications in communication networks.

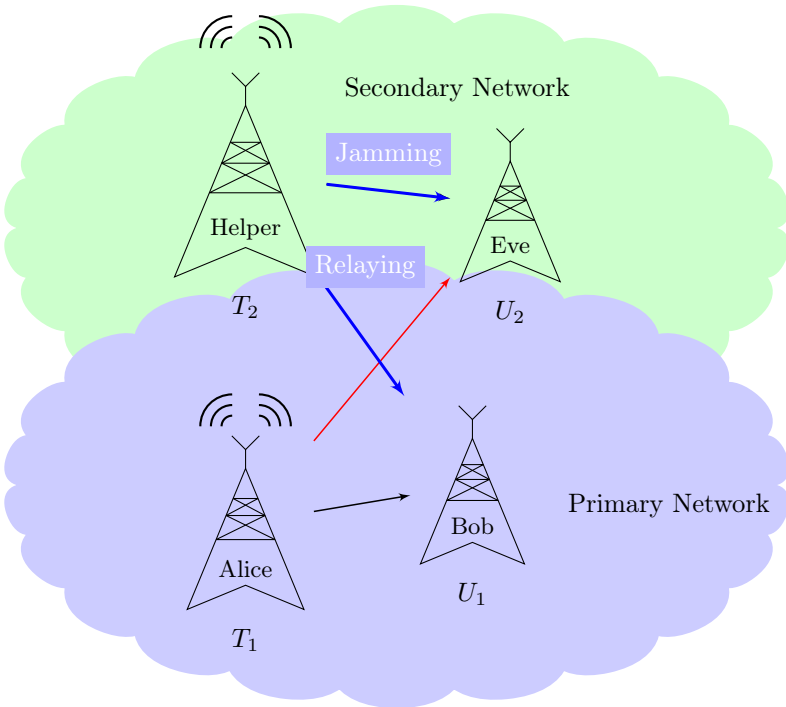


Figure 1.6: Cooperation for secrecy in cognitive radio networks.

As represented in Figure 1.6, which combines both models of Figure 1.3 and Figure 1.4, the traditional Alice-Bob-Eve channel with an external eavesdropper can be applied to cognitive radio channels where the secondary receiver is treated as a potential eavesdropper to the primary transmission. The primary transmitter is assisted in this model by the trustworthy secondary transmitter if the cooperation could improve the secrecy performance, while the secondary transmitter benefits by being awarded a share of the spectrum for its data transmission. Therefore secrecy concerns lay the foundation of mutual cooperation between primary and secondary transmitters. This novel and fundamental model is carefully studied throughout this thesis.

1.2 Outline and Contributions

This section outlines the thesis and summarizes the main contributions along with references to the corresponding publications. In this thesis we introduce the novel cognitive radio model with secrecy constraints depicted in Figure 1.6. This model allows us to utilize the advantages of cooperative techniques for secrecy in wireless

Figure 1.7: Mind map of concepts applied in this thesis.

networks, while alleviating some common weaknesses in the system assumptions for wiretap-based models, such as the knowledge of the external eavesdropper's channel state information (CSI), or the unconditional cooperation of a trustable helper. The aim of this thesis is to investigate this model thoroughly focusing on different fundamental aspects. In order to do so, several important concepts are put into practice in this thesis, as described in Figure 1.7, to analyze the key problems described in the following outline.

Chapter 2

In this chapter we give a review of the theoretical foundations of the work presented in this thesis. In particular we review fundamental notions of communication, information and game theory that will be put into practice later in the thesis. We introduce the concept of cooperation for secrecy in communication networks, which we investigate in particular through a case study in wireless networks. This study allows us to motivate the main model investigated in the thesis: the cognitive radio channel with secrecy constraints.

The material in this chapter is based on the following published papers and monographs:

- [Gab12] F. Gabry "**Cooperation for Secrecy in Wireless Networks**", Licentiate Thesis, KTH, September 2012.
- [GTS11c]: F. Gabry, R. Thobaben, and M. Skoglund, "**Outage Performance for Amplify-and-Forward, Decode-and-Forward and Cooperative Jamming Strategies for the Wiretap Channel**", in Proceedings of the IEEE Wireless Communications & Networking Conference (WCNC), Cancún, Mexico, March 2011.
- [GTS11b]: F. Gabry, R. Thobaben, and M. Skoglund, "**Outage Performance and Power Allocation for Decode-and-Forward Relaying and Cooperative Jamming for the Wiretap Channel**", in Proceedings of the IEEE Conference on Communications Workshops (ICC), Kyoto, Japan, June 2011.
- [GSTS13] F. Gabry, S. Salimi, R. Thobaben, and M. Skoglund, "**High SNR Performance of Amplify-and-Forward Relaying in Rayleigh Fading Wiretap Channels**", in Proc. 2013 Iran Workshop on Communication and Information Theory (IWCIT 2013), Tehran, Iran, May 2013.

Chapter 3

In this chapter we investigate the cognitive radio channel with secrecy constraints on the primary message. This chapter constitutes the reference model for the work in this thesis. We describe first how a cognitive transmitter can improve the secrecy of primary transmissions in cognitive radio networks. We then derive the

achievable rate regions with secrecy constraints for the additive white Gaussian noise (AWGN) cognitive radio channel model with and without primary message knowledge at the secondary transmitter and provide insights on the power allocation strategies for the two scenarios. We formulate and solve three relevant power allocation problems: the maximization of both rates and the minimization of the transmitting power. We analyze using Stackelberg game model a realistic power allocation problem corresponding to an optimization of both transmitters' utilities. Finally we illustrate our results through numerical examples based on a geometrical setup, highlighting the impact of the node geometry on the achievable rates and on the optimal strategy of the secondary transmitter, and compare those results to the game theoretic interaction.

The material in this chapter is based on the following published papers:

- [GSG+12] F. Gabry, N. Schrammar, M. Girnyk, N. Li, R. Thobaben, and L. K. Rasmussen, "**Cooperation for secure broadcasting in cognitive radio networks**", in Proc. of IEEE International Conference of Communications (ICC 2012), Ottawa, Canada, June 2012.

- [GLS+12] F. Gabry, N. Li, N. Schrammar, M. Girnyk, E. Karipidis, R. Thobaben, L. K. Rasmussen, and M. Skoglund, "**Secure Broadcasting in Cooperative Cognitive Radio Networks**", in Proc. of Future Networking and Mobile Summit (FNMS 2012), Berlin, Germany, July 2012.

- [GLG+14] F. Gabry, N. Li, N. Schrammar, M. Girnyk, L. K. Rasmussen and M. Skoglund, "**On the Optimization of the Secondary Transmitter's Strategy in Cognitive Radio Channels with Secrecy**", IEEE Journal on Selected Areas in Communications, (JSAC), Cognitive Radio Series Issue, March 2014.

Chapter 4

In this chapter we investigate clean relaying (CR) for secrecy in cognitive radio channels. The goal of this chapter is to generalize the results of Chapter 3 in three main directions: analyzing the impact of the learning phase at the secondary transmitter for the primary message, considering the cognitive scenario where the primary user does not have multi-user decoding capabilities, and using a stronger secrecy measure for the primary message. To that aim we introduce the CR scheme for our cognitive radio scenario with secrecy constraints. We derive the achievable rate region for the multi-phase scheme investigated in this chapter and compare the CR scheme to other signalling strategies: dirty paper coding (DPC), cooperative jamming (CJ), and interference neutralization (IN). Finally we use the geometrical model developed in previous chapters to numerically compare the secrecy performance of the schemes.

The material in this chapter is based on the following published or submitted papers:

- [LGT+14a] P.-H. Lin, F. Gabry, R. Thobaben, E. Jorswieck and M. Skoglund, "**Clean Relaying in Cognitive Radio Networks with Variational Distance Secrecy Constraint**", in Proc. IEEE Global Conference on Communications (GLOBECOM 2014), Austin, U.S.A, December 2014.

- [LGT+14b] P.-H. Lin, F. Gabry, R. Thobaben, E. Jorswieck and M. Skoglund, "**Clean Relaying in Cognitive Radio Networks with Variational Distance Secrecy Constraint**", Submitted to IEEE Transactions on Wireless Communications (TWC), November 2014.

Chapter 5

In this chapter we extend the cognitive channel model from previous chapters to larger cognitive radio networks with multiple secondary pairs. We investigate the spectrum sharing mechanisms using several game theoretic models, such as single-leader multiple-follower Stackelberg games, non-cooperative power control games and auction games. We illustrate through numerical simulations the equilibrium outcomes of the analyzed games and the impact of the competition between secondary transmitters on the secrecy performance of the primary transmission in the cognitive radio network.

The material in this chapter is based on the following submitted paper:

- [GTS14] F. Gabry, R. Thobaben and M. Skoglund, "**Secrecy Games in Cognitive Radio Networks with Multiple Secondary Users**", Submitted to IEEE Transactions on Communications, November 2014.

Chapter 6

In this chapter we investigate energy efficiency (EE) for cognitive radio channels with secrecy. After introducing the EE performance measure for cognitive radio networks with secrecy constraints. We investigate the optimal power allocation and power splitting at the secondary transmitter in terms of energy efficiency for our cognitive model under secrecy constraints for the primary message. We then formulate and analyze an important EE Stackelberg game between the two transmitters aiming at maximizing their utilities. Our analytical results are illustrated through our geometrical model highlighting the EE performance of the system as well as the role of the optimization parameters and the impact of the Stackelberg game on the overall performance and strategies.

The material in this chapter is based on the following submitted paper:

- [GZJS14] F. Gabry, A. Zappone, E. Jorswieck and M. Skoglund "**Energy Efficiency Analysis of Cognitive Radio Networks with Secrecy Constraints**", Submitted to IEEE Communications Letters, November 2014.

Chapter 7

In this chapter we investigate information theoretic secrecy using key agreement techniques in wireless networks. We motivate this study by highlighting the importance of secret key agreement in the overall architecture of secure wireless systems and by establishing the connection to CRNs. We then derive achievable secret key rate regions for two different key agreement schemes in Gaussian channels using several transmission strategies such as power control and cooperative jamming. The complex interaction between both transmitting users is analyzed from a game theoretic perspective using non-cooperative games. We finally illustrate our results to characterize the performance of the key agreement schemes and to evaluate the impact of the game between both users.

The material in this chapter is based on the following published paper:

- [SGS13] S. Salimi, F. Gabry, and M. Skoglund "**Pairwise Key agreement over a Generalized Multiple Access Channel: Capacity Bounds and Game-Theoretic Analysis**", in Proceedings of the IEEE International Symposium on Wireless Communication Systems (ISWCS), Paris, France, August 2013.

In addition to this published contribution, two journal manuscripts are in preparation for a submission.

Chapter 8

In this chapter we conclude the thesis by summarizing the main contributions of our work and by suggesting future promising research directions.

Contributions not Included in This Thesis

The following publications are closely related to the study in this thesis, as they investigate information theoretic secrecy problems. However, the models in these works differ from this thesis for two fundamental assumptions made in this thesis, classified as follows.

Cooperation Against an Active Eavesdropper In this thesis we will assume that Eve is a *passive attacker*; i.e., Eve is restricted to passive eavesdropping strategies and does not attempt to temper with the communication channels. In the following publication, we studied a model where Eve also includes jamming as a strategy to decrease the secrecy performance of the legitimate parties, as depicted in Figure 1.8. We refer the interested reader to [Ama09] and [MS10] for details on active eavesdropping strategies in wireless channels.

- [GTS11a] F. Gabry, R. Thobaben, and M. Skoglund, "**Cooperation for Secrecy in Presence of an Active Eavesdropper: A Game-Theoretic**

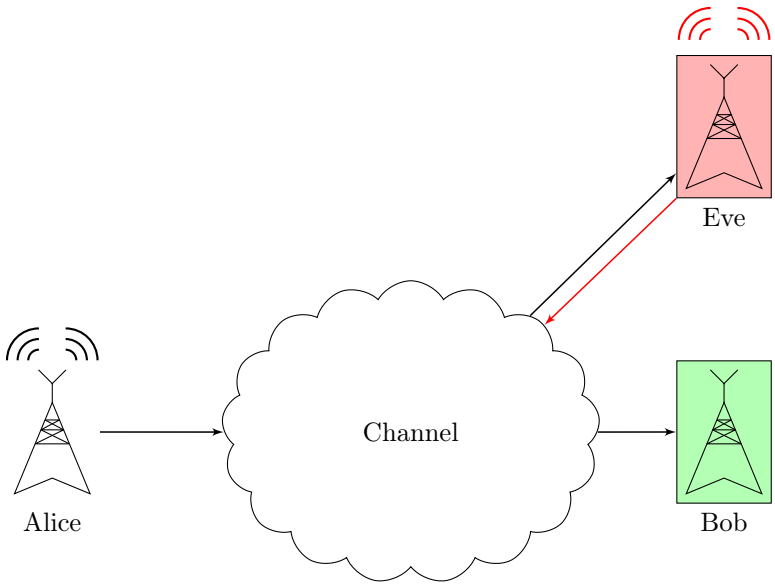


Figure 1.8: The wiretap channel with an active eavesdropper.

Perspective", in Proceedings of the IEEE International Symposium on Wireless Communication Systems (ISWCS), Aachen, Germany, November 2011.

Large System Analysis for MIMO Wiretap Channels In this thesis we will assume that the users in the networks are equipped with *single antenna nodes*, i.e., they cannot benefit from the advantages of multi-antenna transmission such as for MIMO channels. The wiretap channel and other multi-user wiretap scenarios have been generalized to their MIMO counterpart where all nodes are equipped with multiple antennas and extensively studied in the literature. In particular, the secrecy capacity of the MIMO wiretap channel has been characterized in [KW10], [LS09], [SLU09], and [OH08]. In [Gir14], powerful large-system analysis tools are applied to MIMO wiretap channels. However we will consider single antenna nodes in the remainder of this thesis, and therefore we must find a different manner to overcome the channels' limitations, e.g., by a cooperation between nodes for secrecy.

- [GGM+13a] M. Girnyk, F. Gabry, M. Vehkaperä, L. K. Rasmussen and M. Skoglund, "**On the Transmit Beamforming for MIMO Wiretap Channels: Large-System Analysis**", in Proc. International Conference on Information Theoretic Security (ICITS 2013), Singapore, November 2013.

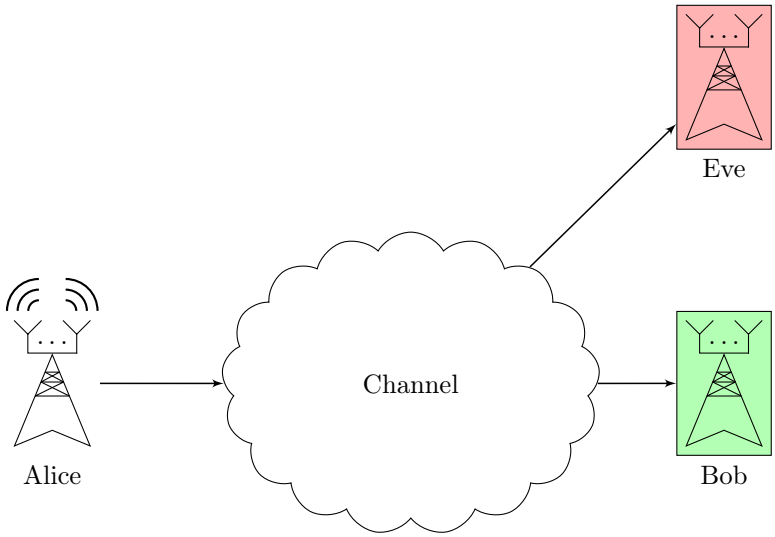


Figure 1.9: The MIMO wiretap channel.

- [GGM+13b] M. Girnyk, F. Gabry, M. Vehkaperä, L. K. Rasmussen and M. Skoglund, "**Large-system analysis of MIMO wire-tap channels with randomly located eavesdroppers**", in Proc. IEEE International Symposium on Wireless Communication Systems (ISWCS 2013), Illmenau, Germany, August 2013.
- [GGV+15] M. Girnyk, F. Gabry, M. Vehkaperä, L. K. Rasmussen and M. Skoglund, "**MIMO Wiretap Channels with Randomly Located Eavesdroppers: Large-System Analysis**", submitted to IEEE International Conference on Communications (ICC 2015), London, United Kingdom.

Contributions Outside the Scope of This Thesis In addition to the material covered in this thesis and the related papers not included in the thesis, a final contribution by the author is the following publication:

- [GBGO14] O. Goubet, G. Baudic, F. Gabry, and T.J. Oechtering, "**Low Complexity Scalable Iterative Algorithms for IEEE 802.11p Receivers**", accepted for publication in IEEE Transactions on Vehicular Technology, (TVT), October 2014.

This work is the result of a collaboration with two supervised Master thesis students on the topic of iterative algorithms for estimation and decoding at IEEE 802.11p receivers.

Copyright Notice

1.3 Notation and Acronyms

In this section we describe the notation, the nomenclature and the acronyms used in the thesis.

Notation

We will use the following notation throughout this thesis.

Information Measures

X	random variable
$\mathcal{X}$	alphabet or set
$\mathcal{X} \times \mathcal{Y}$	Cartesian product of sets $\mathcal{X}$ and $\mathcal{Y}$
$\lvert\mathcal{X}\rvert$	cardinality of a set $\mathcal{X}$
x	realization of X
P_X or $P_X(x)$ or $p(x)$	probability mass function (pmf) of X
$X \sim p(x)$	random variable X with pmf p
$P_{X,Y}$	joint probability mass function of X and Y
$X - Y - Z$	Markov Chain
$H(X)$	entropy of the discrete random variable X
$h(X)$	differential entropy of the continuous random variable X
$H(Y\lvert X)$	conditional entropy of Y given X
$\mathbb{E}_X$	expected value over random variable X
$I(X;Y)$	mutual information between X and Y
$I(X;Y\lvert Z)$	conditional mutual information between random variables X and Y conditioned on Z
X^n	vector of n random variables $X_1, \ldots, X_n$
x^n	vector of n realizations $x_1, \ldots, x_n$
W	message
$\hat{W}$	estimate of message W
$P\{X\}$	probability of event X

Functions and Operators

$\mathcal{N}(\mu, \sigma^2)$	normal distribution with mean μ and variance σ^2
$\mathcal{CN}(\mu, \sigma^2)$	complex normal distribution with mean μ and variance σ^2
$\lvert x \rvert$	absolute value of a complex number x
x^+	positive part of x, i.e., $x^+ = \max(x, 0)$
$\lceil x \rceil$	unique $n \in \mathbb{N}$ such that $x \leq n < x + 1$
$[x]_{x_{\min}}^{x_{\max}}$	$\min\{x_{\min}, \max\{x_{\max}, x\}\}$
log	logarithm to the base 2
$\mathcal{C}(\cdot)$	$\frac{1}{2}\log(1 + \cdot)$
$K_1(\cdot)$	first order modified Bessel function of the second kind
$E_1(\cdot)$	exponential integral, defined in Theorem 2.13

Game Theory Basics

$\mathcal{G}$	game
$\mathcal{S}_i$	set of strategies for player i
s_i	strategy of player i
s_{-i}	vector of strategies of all players except i
$\mathcal{U}_i$	utility of player i

Communication Channels

R_i	achievable rate for node i
P_i	transmission power at node i
x_i	transmitted signal from node i
y_i	received signal at node i
h_{ij}	channel coefficient between node i and node j
c_{ij}	$\lvert h_{ij} \rvert^2$
d_{ij}	Euclidian distance between node i and node j
α	path-loss exponent
γ_{ij}	instantaneous SNR between node i and node j
$\bar{\gamma}_{ij}$	average instantaneous SNR between node i and node j

Case Study in Section 2.6

$\mathcal{D}$	Destination
$\mathcal{E}$	Eavesdropper
$\mathcal{S}$	Source
$\mathcal{H}$	Helper
R	target secrecy rate
$R_s^{(i)}$	achievable secrecy rate with strategy i at the relay
$P_{out}^{(s_\mathcal{H})}(R)$	secrecy outage probability with strategy $s_\mathcal{H}$

	and secrecy rate R
$P_{out,c}^{(s_{\mathcal{H}})}(R)$	conditional secrecy outage probability with strategy $s_{\mathcal{H}}$ and secrecy rate R
T_s	secure throughput
$C_{\mathcal{H}_1}$, $C_{\mathcal{H}_2}$, and $C_{\mathcal{H}_3}$	Helper in $(0.1, 0.1)$, $(0.5, 0.1)$, and $(0.9, 0.1)$, respectively

Cognitive Radio Channel with Secrecy

T_1	primary transmitter
T_2	secondary transmitter
U_1	primary receiver
U_2	secondary receiver
w_1	primary secret message
w_2	secondary message
R_1^{WT}	wiretap rate without T_2
$\mathcal{S}_1$	scenario with message knowledge
$\mathcal{S}_2$	scenario without message knowledge
ρ	jamming parameter
β	common message parameter
γ	relaying parameter
$\mathcal{P}_{R_1}$	maximization of secondary rate
$\mathcal{P}_{R_2}$	maximization of primary rate
$\mathcal{P}_{P_2}$	minimization of secondary power
η_j	time splitting parameter for phase j for the CR scheme
$\mathbf{x}_i^{(j)}$	transmitted signal by T_i during phase j for the CR scheme
EE_2	secondary energy efficiency

CRNs with Multiple Secondary Networks

$T_{2,k}$	secondary transmitter k
$U_{2,k}$	secondary receiver k
$w_{2,k}$	message of $T_{2,k}$
(SF-SG)	single-follower Stackelberg game
(MF-SG)	multiple-follower Stackelberg game
(PC-G)	power control game
(VA)	Vickrey auction

Secret Key Agreement

K_{ij}	key to be shared between User i and User j
R_{ij}	secret key rate of K_{ij}
γ_i	power control parameter of User i
η_i	jamming parameter of User i

Nomenclature

In this thesis we use colored boxes for a better readability of the concepts and results. In particular we will use the following nomenclature: Proposition, Theorem, Lemma, Remark, Definition, Example.

List of Acronyms

AF	Amplify-and-forward relaying
AWGN	Additive white Gaussian noise
BC-CM	Broadcast channel with confidential messages
cdf	Cumulative distribution function
CF	Compress-and-forward relaying
CJ	Cooperative jamming
CR	Clean relaying
CRN	Cognitive Radio Network
CSI	Channel state information
CSOP	Conditional secrecy outage probability
DF	Decode-and-forward relaying
DMC	Discrete memoryless channel
DPC	Dirty paper coding
DT	Direct transmission
EE	Energy efficiency
IN	Interference neutralization
MAC-layer	Media access control layer
MAC	Multiple-access channel
MAC-WTC	Multiple-access wiretap channel
MF-SG	Multi-follower Stackelberg game
MIMO	Multiple-input and multiple-output
MRC	Maximum ratio combining
NE	Nash equilibrium
pdf	Probability density function
PHY	Physical layer
pmf	Probability mass function
RC	Relay channel
SE	Stackelberg equilibrium
SINR	Signal to interference plus noise ratio
SNR	Signal-to-noise ratio
SOP	Secrecy outage probability
WTC	Wiretap channel

Chapter 2

Review

In this chapter we give a review of the theoretical foundations of the work presented in the thesis. As for every chapter, we elaborate the list of the chapter's goals.

Objectives of the Chapter.

- Establish the notation and common expressions used throughout the thesis.
- Provide the necessary fundamentals in communication, information, and game theory for the understanding of the thesis.
- Introduce the notions of cooperation and secrecy in wireless networks, and connect both through the concept of cooperation *for* secrecy.
- Motivate the communication network model investigated throughout the thesis, i.e., the cognitive radio channel with secrecy constraints.

Organization of the Chapter This chapter consists of six sections. In Section 2.1 we review fundamental notions of communication and information theory and we introduce cooperative communication. Section 2.2 is devoted to an example of cooperative networks, namely cognitive radio networks. In Section 2.3 we introduce fundamental tools of game theory that will be put into practice later in the thesis. In Section 2.4 we introduce the concept and the motivation for information theoretic secrecy, and we give an overview of the main results for secrecy in wireless networks. In Section 2.5 we discuss the interactions between cooperation and secrecy in communication networks. In Section 2.6 we investigate a case study of cooperation for secrecy in wireless networks in order to introduce the model considered in this thesis.

2.1 Fundamentals of Communication Theory

In this section we summarize some of the most fundamental results in communication and information theory. In Section 2.1.1 we introduce the basic definitions of information theory used throughout this thesis. In Section 2.1.2 we investigate the point-to-point communication channel introduced by Shannon [Sha48]; in particular, we define the notion of channel capacity. Finally, in Section 2.1.3, we introduce the relay channel, which is the simplest model of a cooperative network.

2.1.1 Information Measures

In this section we introduce the most important definitions in the field of information theory required for the understanding of this thesis, namely the entropy and the mutual information. We refer the reader to [CT06] and [EGK12] for a more comprehensive introduction to the fundamental concepts of information theory.

Discrete Random Variables Let X be a discrete random variable with finite alphabet $\mathcal{X}$. We write its probability mass function (pmf) as $P_X(x)$ or more conveniently P_X or $p(x)$ which we denote as $X \sim p(x)$. If X and Y are two discrete random variables, we denote similarly their joint pmf $P_{X,Y}$, $P_{X,Y}(x,y)$ or $p(x,y)$. We define first some necessary concepts in probability theory, namely independence, the Markov chain, and the total variation distance.

Definition 2.1 (Independence)**.**

Let $(X,Y) \sim P_{X,Y}(x,y)$ with $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$. X and Y are called independent if

$$P_{X,Y}(x,y) = P_X(x)P_Y(y). \tag{2.1}$$

Definition 2.2 (Markov Chain)**.**

Let $(X,Y,Z) \sim P_{X,Y,Z}(x,y,z)$ with $X \in \mathcal{X}$, $Y \in \mathcal{Y}$ and $Z \in \mathcal{Z}$. X, Y and Z form a Markov chain, which we denote by $X - Y - Z$ if

$$P_{X,Y,Z}(x,y,z) = P_{X,Y}(x,y)P_{Z|Y}(z|y). \tag{2.2}$$

Definition 2.3 (Total Variation Distance)**.**

The total variation distance between the probability distributions P_X and $P_{X'}$ defined on the same alphabet $\mathcal{X}$ is

$$V(P_X, P_{X'}) \triangleq \frac{1}{2} \sum_{x \in \mathcal{X}} |P_X(x) - P_{X'}(x)|. \tag{2.3}$$

Entropy We define the entropy, which is a measure of the uncertainty of a random variable.

Definition 2.4 (Entropy)**.**

The entropy of the discrete random variable $X \sim P_X(x)$ is defined as

$$H(X) = -\sum_{x \in \mathcal{X}} P_X(x) \log P_X(x). \tag{2.4}$$

In the remainder of this thesis, the entropy is measured in bits, and we use the convention $0 \log 0 = 0$, where $\log(\cdot)$ is the binary logarithm.

Remark 2.1.

From (2.4), we observe that the entropy of X can be interpreted as the expected value of the random variable $-\log P_X(X)$, with $X \sim P_X(x)$. Therefore,

$$H(X) = -\mathbb{E}_X(\log P_X(x)).$$

Let X and Y be two discrete random variables with joint pmf $P_{X,Y}(x, y)$ and marginal pmf's $P_X(x)$ and $P_Y(y)$. We define the conditional entropy of Y given X as follows.

Definition 2.5 (Conditional Entropy)**.**

The conditional entropy $H(Y|X)$ for $(X, Y) \sim P_{X,Y}(x, y)$ is defined as

$$H(Y|X) = \sum_{x,y \in \mathcal{X} \times \mathcal{Y}} P_{X,Y}(x, y) \log P_{Y|X}(y|x). \tag{2.5}$$

Differential Entropy Similarly, we define the differential entropy for X a continuous random variable defined over $\mathcal{X}$ and with probability density function (pdf) $f(x)$ as follows.

Definition 2.6.

The differential entropy of the continuous random variable $X \sim f(x)$ is defined as

$$h(X) = -\int_{x\in\mathcal{X}} f(x)\log f(x) = -\mathbb{E}_X(\log f(x)). \tag{2.6}$$

Mutual Information We now introduce the mutual information, which is a measure of the amount of information that one random variable contains about another random variable.

Definition 2.7.

The mutual information $I(X;Y)$ between the random variables X and Y is defined as

$$I(X;Y) = \sum_{(x,y)\in\mathcal{X}\times\mathcal{Y}} P_{X,Y}(x,y)\log\frac{P_{X,Y}(x,y)}{P_X(x)P_Y(y)}. \tag{2.7}$$

Relation Between Entropy and Mutual Information From (2.4), (2.5) and (2.7), we deduce the following equality:

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X). \tag{2.8}$$

Therefore, the mutual information $I(X;Y)$ corresponds to the reduction in the uncertainty of X with the knowledge of Y, or equivalently, to the reduction in the uncertainty of Y with the knowledge of X. A similar interpretation of the relation between differential entropy and mutual information also holds for continuous random variables.

2.1.2 Point-to-Point Communication

In this section we consider the communication model depicted in Figure 2.1. This communication system model has been introduced by Claude E. Shannon in the paper [Sha48] which laid the foundations to the field of information theory. In this model, the transmitter wishes to send the message W to the receiver. This message

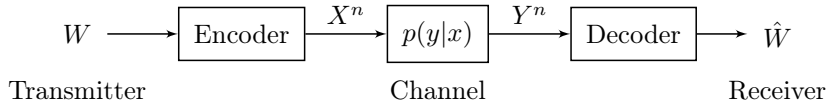


Figure 2.1: Communication model.

has to be sent through a communication channel, which is a representation of the physical medium shared by the transmitter and the receiver. Shannon introduced a probabilistic approach to model the communication channel which he represented as a discrete memoryless channel (DMC), defined by two finite sets $\mathcal{X}$ and $\mathcal{Y}$ and a collection of conditional pmf's $p(y|x)$. The collection of transition probabilities $p(y|x)$ describes the behavior of the channel, i.e., the response of the channel when it is fed by a given input. The memoryless property signifies that if X^n is transmitted over n channel uses, then the output Y_i at time $i \in \{1, \ldots, n\}$ is distributed according to $p(y_i|x^i, y^{i-1}) = p(y_i|x_i)$. In other words, the output of the channel at time i only depends of the input at the time i via the transition probability $p(y_i|x_i)$. The memoryless property implies that, if there is no feedback,

$$p(y^n|x^n) = \prod_{i=1}^{n} p(y_i|x_i). \tag{2.9}$$

Channel Capacity An essential parameter of the communication system is the communication rate, which roughly characterizes the proportion of information that the transmitter can convey through the channel to the receiver. Formally, we can define the communication rate as follows.

Definition 2.8 (Communication Rate)**.**

- The message W is chosen uniformly from a finite set $\mathcal{W}$ of size M.
- The encoder assigns a codeword $x^n(w) \in \mathcal{X}^n$ to each message $w \in \mathcal{W}$.
- The decoder assigns an estimate $\hat{W}$ or an error message to each received sequence $y^n \in \mathcal{Y}^n$.

Then the communication rate is given by

$$R = \frac{\log(M)}{n} \quad \text{bits per transmission,} \tag{2.10}$$

and we call the corresponding code a $(2^{nR}, n)$ code.

One crucial question arises: What is the maximum rate R at which we can reliably transmit W? In order to rigorously answer this question, we first need to define formally a measure of reliability and the concept of achievability.

Definition 2.9 (Reliability and Achievability)**.**

We define the average probability of error of a $(2^{nR}, n)$ code as

$$P_e^{(n)} = P\{\hat{W} \neq W\} = \frac{1}{|\mathcal{W}|} \sum_{w \in \mathcal{W}} P\{\hat{w} \neq w\}. \tag{2.11}$$

A rate R is then said to be achievable if there exists a sequence of $(2^{nR}, n)$ codes such that $P_e^{(n)} \to 0$ as $n \to \infty$.

Based on the two previous definitions, we introduce a fundamental quantity for the communication channel, the channel capacity, which represents a rigorous definition of the answer of our question.

Definition 2.10 (Capacity)**.**

The capacity C of the DMC is then defined as the supremum of all achievable rates. That is, for any rate $R < C$, the transmission of W with an arbitrarily low average probability of error is possible.

In his original work [Sha48], Shannon established the following fundamental theorem:

Theorem 2.1 (Channel Coding Theorem [Sha48])**.**

The capacity of the DMC $(\mathcal{X}, \mathcal{Y}, p(y|x))$ is given by

$$C = \max_{p(x)} I(X;Y). \tag{2.12}$$

The capacity of the DMC can consequently be derived by solving a maximization problem over all possible input distributions. This optimization can be arduous for certain channels, but one can alternatively look for lower and upper bounds on the capacity. If these bounds happen to coincide, then the capacity is found.

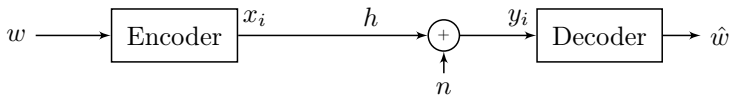


Figure 2.2: The AWGN channel.

Example 2.1 (The Gaussian Channel)**.**

We consider the real-valued additive white-noise Gaussian (AWGN) channel depicted in Figure 2.2 as follows:

$$y_i = hx_i + n, \quad \text{with} \quad n \sim \mathcal{N}(0, N), \tag{2.13}$$

where h represents the constant real-valued channel coefficient, and with the average power constraint

$$\frac{1}{n}\sum_i |x_i|^2 \leq P_s, \tag{2.14}$$

for every codeword $x^n = [x_1, \ldots, x_n]$. For this AWGN channel, the capacity is known and is given in the following theorem

Theorem 2.2 (AWGN Capacity [Sha48])**.**

The capacity of the AWGN channel with average power constraint P_s is given by

$$C = \frac{1}{2}\log\left(1 + \frac{h^2 P_s}{N}\right) \triangleq \mathcal{C}\left(\frac{h^2 P_s}{N}\right). \tag{2.15}$$

Fading Channels The model of Example 2.1 can be generalized to wireless channels. Wireless communication channels are usually modeled as fading channels, which implies that the channel coefficients are randomly distributed. We restrict ourselves in this thesis to the quasi-static fading model, i.e., the fading coefficients remain constant over the transmission of an entire codeword, and only change indepently from one codeword to another. One example of quasi-static fading channel is the Rayleigh fading channel. For quasi-static Rayleigh fading channels, we note h_{ij} the fading coefficient between node i and node j. From a codeword to another

the fading coefficients h_{ij} change randomly with some variance α_{ij} according to a complex Gaussian distribution, i.e., we have $h_{ij} \sim \mathcal{CN}(0, \alpha_{ij})$. A way to connect the behavior of the Rayleigh fading channel to the geometry of the communication system is by using a path-loss model.

Example 2.2 (Geometrical Model for Rayleigh Fading Channels)**.**

If we denote the Euclidian distance between node i and node j by d_{ij}, then we have

$$h_{ij} \sim \mathcal{CN}(0, 1/d_{ij}^{\alpha}), \tag{2.16}$$

where α represents the path-loss exponent. Furthermore, we define the instantaneous signal-to-noise ratio (SNR) as $\gamma_{ij} = \frac{P_i |h_{ij}|^2}{\sigma_i^2}$, where P_i is the transmission power of node i, and σ_i^2 represents the variance of the thermal noise. We assume in the remainder of the thesis the thermal noise to be the same for every node, i.e., $\sigma_i^2 = \sigma^2$, $\forall i$. The random variable γ_{ij} is exponentially distributed, with mean $\bar{\gamma}_{ij}$. That is, its probability density function is given by:

$$f_{\gamma}(x) = \begin{cases} \frac{1}{\bar{\gamma}_{ij}} \exp\left(-x/\bar{\gamma}_{ij}\right), & \text{if } x \geq 0 \\ 0, & \text{if } x < 0 \end{cases}$$

with

$$\bar{\gamma}_{ij} = \frac{P_i}{d_{ij}^{\alpha} \sigma^2}. \tag{2.17}$$

Outage Probability For fading channels, an outage event happens when the chosen communication rate R exceeds the capacity of the channel. If that event occurs, reliable communication is no longer possible according to the definition of the channel capacity. The outage probability is then naturally defined as the probability of such an event. For a fading channel between a source and a destination with instantaneous SNR γ_{sd} between the source and the destination, the outage probability is defined as [TV10]:

$$P_{out}(R) = P\left\{\log\left(1 + \gamma_{sd}\right) < R\right\}. \tag{2.18}$$

If the transmitter knows perfectly the channel coefficient, and thus γ_{sd}, it can accordingly design R such that an outage never occurs. However, if the channel realization is unknown, an outage occurs with a probability as in (2.18), which depends on the probability distribution of the channel coefficient.

While the capacity for the point-to-point communication model of Figure 2.1 has already been derived by Shannon in [Sha48], for many other communication

networks of interest, the problem stays open. In the following section we introduce cooperative communications and in particular the relay channel, a 3-node network whose capacity is still unknown, in spite of its apparent simplicity.

2.1.3 Cooperative Communications

Cooperation in communication networks is an emerging technique to improve the reliability of wireless communication systems, and it involves multiple parties assisting each other in the transmission and decoding of messages. Due to their broadcast nature, wireless communications from a source to destination can indeed potentially benefit from the cooperation of nodes that overhear the transmission. Since the introduction of the relay channel in [vdM71], which is the simplest form of cooperative communication network, fundamental multi-node channel models have been thoroughly investigated using results from network information theory. We refer the reader to [EGK12] for an overview of existing results for important multi-node networks and to [KMY07] for a comprehensive summary of cooperative communications. In order to illustrate cooperative transmission strategies in wireless networks, we introduce the simplest cooperative network: the relay channel.

Fundamental Example: The Relay Channel

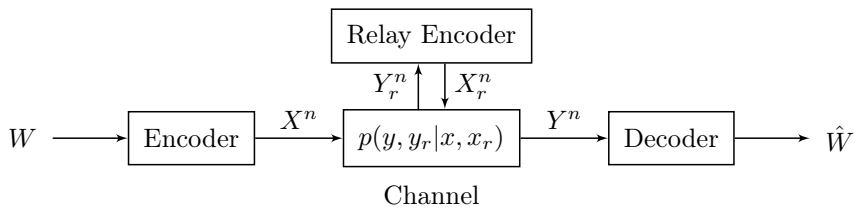


Figure 2.3: The relay channel.

The relay channel was introduced more than three decades ago in [vdM71]. This network, depicted in Figure 2.3, consists of three nodes: a transmitter, a relay, and a receiver. The sole purpose of the relay node is to help increase the rate of communication between the transmitter and the receiver.

Despite the simplicity of this model, the capacity of the general relay channel is still unknown. In their fundamental work [CEG79], Cover and El Gamal derived the cut-set upper-bound on the capacity. They also proposed achievable schemes, namely decode-and-forward (DF) relaying and compress-and-forward (CF) relaying, which result in lower bounds on the capacity of the general relay channel. Since then, the relay channel has been thoroughly investigated, and a comprehensive review of the advances, ideas, and techniques related to the relay channel can be found in [EGK12].

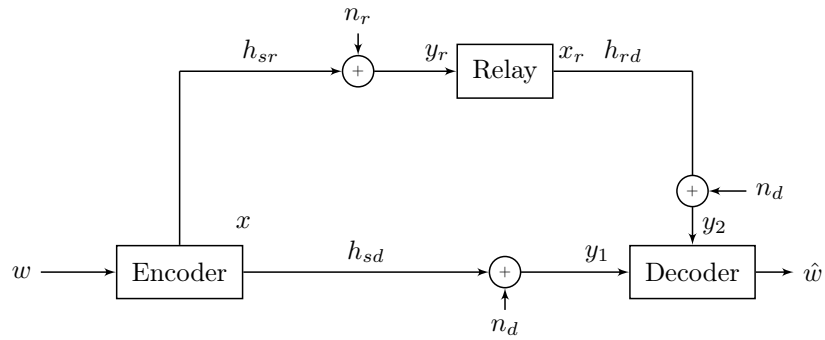


Figure 2.4: The orthogonal Gaussian relay channel.

The Orthogonal Gaussian Relay Channel We consider a special case of the relay channel, namely the Gaussian relay channel with orthogonal receivers, as shown in Figure 2.4. This model takes into account some practical constraints for wireless transceivers; specifically, the relay node cannot receive and transmit simultaneously on the same frequency channel. The relay is then said to operate in a half-duplex mode, in opposition to the full-duplex mode. Every relay node considered in this thesis is assumed to be half-duplex unless mentioned otherwise.

By definition, the relay channel is said to have orthogonal receivers if the destination receives $Y \equiv (Y_1, Y_2)$ with Y_1 and Y_2 respectively received from the source and the relay. The channel pmf simplifies as

$$p(y, y_r|x, x_r) = p(y_1, y_r|x)p(y_2|x_r) = p(y_1|x)(y_r|x)p(y_2|x_r), \tag{2.19}$$

where the second equality results from the independence of the channels in the scenario of Figure 2.4. The received signal at the relay y_r, and the received signals at the destination y_1 and y_2 are then given by:

$$\begin{aligned} y_r &= h_{sr}x + n_r, \\ y_1 &= h_{sd}x + n_d, \\ y_2 &= h_{sd}x_r + n_d. \end{aligned}$$

The thermal noises N_d at the destination and N_r at the relay are zero-mean AWGNs with unit variance, i.e., $N_d \sim \mathcal{N}(0,1)$ and $N_r \sim \mathcal{N}(0,1)$. Finally, we assume the following average power constraints on the transmitted signals:

$$\mathbb{E}[X^2] \leq P_s \quad \text{and} \quad \mathbb{E}[X_r^2] \leq P_r. \tag{2.20}$$

This model has been extensively investigated, e.g., in [EGMZ06], [HMZ05]. In particular, upper and lower bounds on the capacity of this channel have been found.

Furthermore, achievable rates have been derived for several relaying protocols, e.g., decode-and-forward and amplify-and-forward (AF). We describe these strategies briefly in the following, and we give their achievable rates for the orthogonal Gaussian relay channel.

Decode-and-Forward Relaying In the DF scheme, the relay decodes the transmission from the source and re-encodes the message before retransmitting it to the destination.
The rate achieved by DF is given by [EGMZ06]:

$$R^{(DF)} = \min\left\{\mathcal{C}(h_{sr}^2 P_r), \mathcal{C}(h_{sd}^2 P_s) + \mathcal{C}(h_{rd}^2 P_r)\right\}. \tag{2.21}$$

We observe that the rate achievable by the DF strategy is limited by the quality of the source-relay link.

Remark 2.2.

To achieve the rate of (2.21), the relay chooses codewords independent from the source codewords to transmit the information.
If the relay uses the same codewords as the source, i.e., repetition coding, $\mathcal{C}(h_{sd}^2 P_s)+\mathcal{C}(h_{rd}^2 P_r)$ in (2.21) becomes $\mathcal{C}(h_{sd}^2 P_s+h_{rd}^2 P_r)$. Indeed, this simple strategy for DF relaying is mathematically equivalent to a 1×2 single-input multiple-output system, with maximum ratio combining (MRC) being performed at the destination [EGK12]. This strategy is clearly suboptimal as $\mathcal{C}(h_{sd}^2 P_s + h_{rd}^2 P_r) < \mathcal{C}(h_{sd}^2 P_s) + \mathcal{C}(h_{rd}^2 P_r)$. However it has the advantage of simplicity regarding its implementation.

Amplify-and-Forward Relaying In the AF scheme, the relay simply forwards its received signal y_r after a power scaling such that the transmitted signal satisfies the relay power constraint P_r. Specifically, we have

$$x_r = \sqrt{\frac{P_r}{1 + h_{sr}^2 P_s}}\, y_r.$$

The rate achieved by AF is then given by [EGMZ06]:

$$R^{(AF)} = \mathcal{C}\left(h_{sd} P_s + \frac{h_{sr}^2 P_s h_{rd}^2 P_r}{1 + h_{sr}^2 P_s + h_{rd}^2 P_s}\right). \tag{2.22}$$

Remark 2.3.

Another representation of the half duplex constraint on the relay node is captured in the time-division relaying model, where the relay receives the source message during a fraction of the overall transmission window, and transmits the rest of the time. Achievable rates for the time-division relaying model are derived in [HMZ05] for different relaying strategies.

We refer the interested reader to [EGK12] where specific code constructions and transmission strategies for the different relaying protocols are detailed and alternative relaying strategies are also described.

2.2 Cognitive Radio Networks

In this section we discuss cognitive radio networks. In particular we introduce the promising approach of cognitive radio techniques in Section 2.2.1. In Section 2.2.2 we describe the conventional information theoretic models to analyze cognitive radio networks. Finally in Section 2.2.3 we briefly review existing approaches to analyze the behavior of cognitive radio networks.

2.2.1 Introduction to Cognitive Radio Networks

Fixed spectrum assignment policies of governmental agencies result in wasting spectrum resources which are valuable due to their scarcity. Cognitive radio technology, introduced by Mitola in [Mit00], proposes an efficient way to exploit the unused spectrum in an opportunistic manner. As tentatively defined by the Federal Communications Commission (FCC): "a cognitive radio is a radio that can change its transmitter parameters based on its interaction with the environment in which it operates. This interaction may involve active negotiation or communications with other spectrum users and/or passive sensing and decision making within the radio." CR devices have therefore the ability to interact with their environment and react to modifications, e.g., channel variations, by adapting their communication parameters such as coding schemes and frequency bands. In order to do so, CR devices use their fundamental functionality, namely spectrum sensing which allows them to monitor the spectrum bands, and consequently detect the available spectrum holes or the transmission of signals from other users. We refer the interested reader to [ALVM06] for a comprehensive survey on existing cognitive radio techniques for spectrum sharing, sensing, and management and a detailed description of the architecture of cognitive radio networks. Based on this detection, CR users decide whether to use the spectrum for their own transmission, according to several criteria depending on cognitive paradigms described in the following.

Cognitive radio networks are constituted of two types of networks, and thus two types of users: primary networks and secondary networks. Primary users are usually licensed users, i.e., the legacy owners of some spectrum bands, while secondary users do not have licensed access to the spectrum. Example of primary networks include existing wireless infrastructures, e.g., 3G networks or TV broadcast; see [TZFS13] for further existing examples of cognitive radio networks. Since secondary users are not licensed to access the spectrum bands, they use CR technology to detect transmission opportunities and temporarily access the spectrum in an opportunistic manner.

Cognitive radio systems are then usually classified into three main cognitive paradigms depending on the criterion used to allow secondary users to use the licensed spectrum:

Underlay Paradigm: The secondary transmitter knows the channels and can transmit simultaneously with the primary user as long as the interference caused is below a certain threshold. This corresponds, e.g., to secondary spectrum usage in licensed bands without cooperation.

Overlay Paradigm: The secondary transmitter knows the channels as well as the messages (and codebooks) of the primary user. It can transmit simultaneously with the primary user as long and the interference is mitigated by some cooperation, for instance via relaying. This corresponds, e.g., to secondary spectrum usage in licensed bands with cooperation.

Interweave Paradigm: The secondary transmitter uses the unused portions of spectrum, named sprectum holes or white spaces, e.g., TV white spaces, to transmit its messages.

2.2.2 Information Theoretic Models for Cognitive Radio

In the setting where both the primary and secondary networks consist of a single transmitter-receiver pair, the cognitive radio scenario is captured by the interference channel with some additional assumptions and constraints and hence it can be analyzed from an information theoretic perspective [GJMS09]. The Gaussian cognitive interference channel is depicted in Figure 2.5, both for the underlay and the overlay paradigm, depending on whether w_1 is available at the secondary cognitive transmitter.

Underlay Cognitive Radio The underlay cognitive radio network with two transmitters and two receivers is equivalent to the interference channel model, described in Figure 2.5 where w_1 is unknown at T_2. Despite being introduced decades ago, the capacity of the interference channel is still unknown. However in some interference regimes the capacity can be characterized [GJMS09]. The main encoding technique for the interference channel is rate-splitting, where the transmitters split

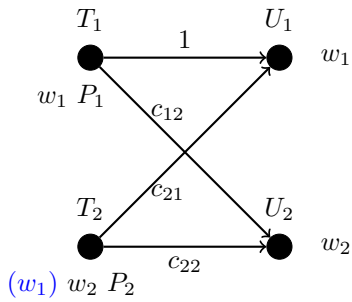


Figure 2.5: Cognitive interference channel.

their messages into two parts, one of which can be decoded by the receiver of the other user (e.g., U_1 decodes a part of w_2) and removed from the interference.

Overlay Cognitive Radio For the overlay cognitive radio network, the secondary transmitter may improve the primary transmission using different encoding techniques using its knowledge of w_1 in addition to rate-splitting. Such techniques include [GJMS09]:

- Superposition coding: The rates at which the information is encoded depends on the strength of the channels to the receivers. The messages destined to worse receivers are encoded at a lower rate, while the signals for better receivers (in terms of channel quality) are superimposed on the low rate messages. This ensures that better receivers can decode the low rate messages first, thus eliminating their interfering effect.
- Gelfand-Pinsker binning: Since the cognitive transmitter knows the interference caused by the primary transmission at the secondary receiver it can use binning against w_1 to improve its own rate. This technique is shown to be optimal in certain regimes for Gaussian channels, in which case the technique is labeled dirty paper coding (DPC), as introduced in [Cos83].
- Relaying: Since T_2 knows the primary message, it can cooperate by superimposing the primary user's message to its signal in order to increase the rate of w_1.

Recently, results on achievable rate regions and outer bounds for the Gaussian cognitive interference channel using these encoding techniques were derived in [RTD12].

Interweave Cognitive Radio The interweave paradigm can be described as the interference channel with time sharing where the time sharing factor is due to the

primary channel usage and the sensing/detection probability. In other terms, when the cognitive transmitter detects a transmission from the primary transmitter, it is not using the spectrum itself. When the spectrum is unused, the secondary transmitter is allowed to opportunistically transmit its message. Spectrum sensing must therefore be performed frequently, and the performance of interweave is limited by the probability of false alarms and missed detections of spectrum use.

2.2.3 Challenges for Cognitive Radio Networks

A recent exhaustive survey on spectrum assignment techniques can be found in [TZFS13] and the comprehensive list of references therein. Such techniques include game theory, graph theory, linear programming. The overall performance of CRNs can be evaluated through multiple criteria such as fairness, spectral efficiency, delay, throughput and connectivity. Challenges for the design of the next generation of cognitive radio networks are numerous. In particular they include users' selfish behavior [NH08], energy efficiency [sur14], and security concerns [ATV+12]. These three fundamental challenges will be addressed in this thesis.

2.3 Fundamentals of Game Theory

In this section we introduce game theory tools that will be applied in this thesis. Game theory can be defined as in [HNS+12] as: "a formal framework with a set of mathematical tools to study the complex interactions among interdependent rational players." In particular, we will use in this thesis two important branches of game theory, namely non-cooperative game theory and auction theory. Therefore, the aim of this section is to provide the fundamental concepts of non-cooperative game theory and auction theory used throughout this thesis. In Section 2.3.1 we introduce some fundamentals of non-cooperative game theory. Then, in Section 2.3.2 we provide the necessary background on auction theory. Finally in Section 2.3.3 we discuss game theory applications in communications networks, with an emphasis on cognitive radio networks applications.

2.3.1 Non-Cooperative Game Theory

In this section we introduce the basic concepts and terminology of non-cooperative game theory, which is one of the most important fields of game theory. Non-cooperative game theory provides a mathematical framework to analyze the decision-making processes of rational player with competitive interests, and has been used in numerous areas outside of communication networks, e.g., economics, political sciences or sociology.

Basics of Non-Cooperative Game Theory

As defined in [HNS+12], a non-cooperative game is a game describing a competitive situation where each player needs to take its decision independently of the other players, given the possible choices of the other players, and their effect on the player's objectives.

In order to describe a non-cooperative game, the concept of strategic form is the most common representation. A strategic game is composed of a set of players, their strategies, and their utilities, and is defined as follows:

Definition 2.11.

A non-cooperative game in strategic form is a triplet $\mathcal{G} = (\mathcal{N}, (\mathcal{S}_i)_{i\in\mathcal{N}}, (\mathcal{U}_i)_{i\in\mathcal{N}})$ where:

- $\mathcal{N}$ is a finite set of players, i.e., $\mathcal{N} = \{1, \ldots, N\}$,
- $\mathcal{S}_i$ is the set of available strategies for player i,
- $\mathcal{U}_i : \mathcal{S} \to \mathbb{R}$ is the utility function (also called payoff) of player i, with $\mathcal{S} \triangleq \mathcal{S}_1 \times \ldots \times \mathcal{S}_N$.

Given this definition of a strategic game, we denote by s_{-i} the vector of strategies of all players except player i, and $s = (s_i, s_{-i}) \in \mathcal{S}$ is then called a strategy profile. For a game in strategic form, each player selects a strategy to optimize its utility function, and when each player i chooses a strategy s_i with probability 1, this strategy is said to be a pure strategy.

In wireless networks, a common way to model security games involving an attacker and a defender is a zero-sum game, where the attacker's gains correspond to the defender's losses [AB11]. However, many problems can also be modeled as non-zero sum games, in which all players can be viewed as maximizers or minimizers without any constraint on the total sum of utilities. As an example of non-zero sum game in wireless networks, we can consider the power-control non-cooperative game, where the players are the users, their strategies are the chosen transmit powers, and their utilities are the communication rates.

Static Non-Cooperative Games

In this section we consider static non-cooperative games in their strategic form. In particular, we use two classic examples of non-cooperative games to illustrate some fundamental concepts such as the Nash equilibrium (NE). A two-player static non-cooperative game in strategic form is commonly represented in a matrix format, where the rows and columns represent the strategies of the players and the entries of the matrix give the utilities for the two players. The rows represent the strategies

Table 2.1: Prisoner's Dilemma.

	Prisoner 2	
Prisoner 1	Confess	Not confess
Confess	$(-8, -8)$	$(0, -10)$
Not confess	$(-10, 0)$	$(-4, -4)$

Table 2.2: Matching Pennies.

	Player 2	
Player 1	Heads	Tails
Heads	$(-1, 1)$	$(1, -1)$
Tails	$(1, -1)$	$(-1, 1)$

of Player 1 while the columns represent the strategies of Player 2 such that the entry (x, y) in row i and column j show the utility x of Player 1 and the utility y of Player 2 for the strategy profile $(s_1, s_2) = (i, j)$.

Example 2.3 (Prisoner's Dilemma)**.**

The classic prisoner's dilemma is represented in matrix form in Table 2.1. The players in the prisoner's dilemma game are both suspects of a crime. Each of the suspects can either confess and implicate the other, or not confess. If both confess, they both go to jail for 8 years, while if they both deny, they both go to jail for 4 years. If only one confesses while the other denies, the one that did not confess will go 10 years in jail while the other will be set free. This game is clearly a non-zero sum game.

Example 2.4 (Matching Pennies)**.**

In the game of matching pennies, represented in Table 2.2, both players secretly choose to turn a penny to heads or tails. The outcome of the game is the following: if both pennies match, Player 2 wins a Swedish krona (SEK) from Player 1, while if the pennies show different sides, Player 1 wins a SEK from Player 2. This game is a two-player zero-sum game.

For Examples 2.3 and 2.4, we have expressed the game in its matrix form. The next step of the analysis is to solve the game, i.e., to predict the strategies that the players will adopt, and hence to determine the corresponding outcome. In the

following we discuss a fundamental solution concept for non-cooperative games: the Nash equilibrium.

Nash Equilibrium The Nash equilibrium, introduced by Nash in [Nas50], is the most accepted solution concept for non-cooperative games. Formally, it is defined as follows:

Definition 2.12 (Nash Equilibrium)**.**

A pure-strategy Nash equilibrium of a non cooperative game $\mathcal{G} = (\mathcal{N}, (\mathcal{S}_i)_{i\in\mathcal{N}}, (u_i)_{i\in\mathcal{N}})$ is a strategy profile $s^* \in \mathcal{S}$, such that $\forall i \in \mathcal{N}$, we have:

$$\mathcal{U}_i(s_i^*, s_{-i}^*) \geq \mathcal{U}_i(s_i, s_{-i}^*) \qquad \forall s_i \in \mathcal{S}_i. \tag{2.23}$$

Therefore, a strategy profile is a pure-strategy NE if no player can improve its utility by unilaterally deviating to another strategy, given the other players' fixed strategies. To illustrate the NE concept, we use the two previous examples.

For Example 2.3, we find by inspection of Table 2.1 that {Confess,Confess} is the unique NE of the game. Indeed, no player has an incentive to deviate from the strategy "Confess" to the strategy "Not Confess", when the other player does not change its strategy, as the player deviating would in this case go to jail 10 years instead of 8. Similarly, we can inspect Table 2.2 to conclude that there exists no pure-strategy NE for Example 2.4, since we notice that for any entry in the matrix, one of the players can increase its utility by changing its strategy.

Based on the two examples, we can make the following important remark:

Remark 2.4.

The NE does not necessarily lead to the best outcome in terms of payoffs, as we can deduce from Example 2.3. If both players choose "Not Confess", their utilities are larger than in the unique NE of the game. However the strategy profile {Not Confess, Not Confess} is not a NE. In this thesis we will not discuss the issue of the efficiency of the equilibrium. A discussion on equilibrium selection based on efficiency criteria, such as the Pareto optimality, can be found in [HNS+12].

Dynamic Non-Cooperative Games

In this section we investigate dynamic non-cooperative games. In contrast to the static games previously considered, in dynamic games players have some information about the actions chosen by the others. In particular, we study in this section

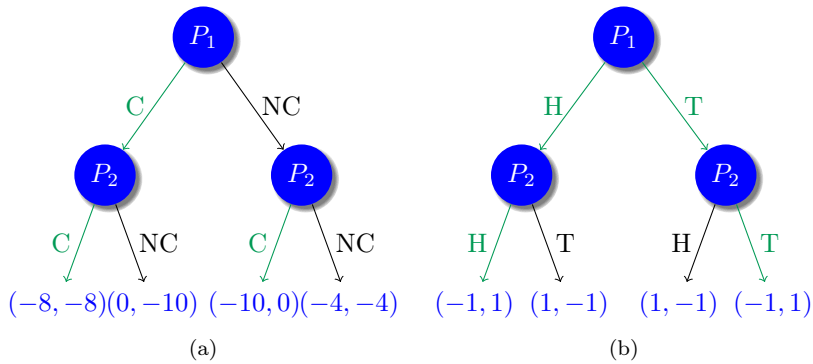


Figure 2.6: Extensive form representation for (a) the prisoner's dilemma game in Example 2.3 and (b) the matching pennies game in Example 2.4.

sequential games, in which the players take their actions (i.e., select their strategies) in a definite order. Therefore, some players observe the actions of the players who acted before them, and they can choose their strategy accordingly. For simplicity, we will restrict the analysis of sequential games to sequential games with perfect information, where each player knows perfectly the actions of the players moving before itself.

Extensive Form Representation Dynamic sequential games are usually represented in their extensive form as a game tree, which depicts the order of the moves of the players. The root node represents the initial decision to be made by one of the players, and the edges show the moves made by a player at a certain node.

We represent the two examples of the previous section, the prisoner's dilemma and the matching pennies, in respectively Figure 2.6a and Figure 2.6b. For both games, we assume that Player 1 acts first, and that Player 2 observes Player 1's move and accordingly chooses its best response.

The method to find equilibria in a dynamic game in extensive form with perfect information is backward induction. The first step is to determine the optimal choice of the last player acting for every possible previous move of the first player. Then, the optimal action of the first player is determined, given the possible best responses of the second player. For example, in Figure 2.6a, if the first player confesses ("C"), then the second player will choose C, while if the first player does not confess ("NC"), then the second player will choose C, each time to maximize its utility. Finally, given those best responses of Player 2, Player 1 will choose C to maximize its utility, and the equilibrium is given by (C,C).

For the zero-sum game of the matching pennies, depicted in Figure 2.6b, we observe that by choosing heads (H) when Player 1 chose H, and tails (T) when Player

1 chose T, Player 2 maximizes its utility. This leads to two equilibria (H,H) and (T,T). Thus, in a two player zero-sum game, acting last is an important advantage, since maximizing its own payoff corresponds to minimizing the other's utility.

Stackelberg Games The Stackelberg game is a game model where there exists a hierarchy among the competing players. For instance, in economics, a Stackelberg competition models the game between the leader firm which moves first and the follower firms, which move after the leader [SC73]. The leader holds the best position as it can impose its own strategy upon the followers.

We consider for the following definitions a two-player non-cooperative game between a leader (Player 1) and a follower (Player 2), with respective strategy sets $\mathcal{S}_1$ and $\mathcal{S}_2$. The optimal response set $\mathcal{R}_2(s_1)$ of Player 2 to the strategy $s_1 \in \mathcal{S}_1$ of Player 1 is defined as:

$$\mathcal{R}_2(s_1) \triangleq \{s_2 \in \mathcal{S}_2 : \mathcal{U}_2(s_1, s_2) \geq \mathcal{U}_2(s_1, s), \forall s \in \mathcal{S}_2\}. \tag{2.24}$$

We are now able to define the Stackelberg equilibrium (SE) strategy as follows:

Definition 2.13 (Stackelberg Equilibrium)**.**

A strategy $s_1^* \in \mathcal{S}_1$ is called a Stackelberg equilibrium strategy for the leader, if

$$\min_{s_2 \in \mathcal{R}_2(s_1^*)} \mathcal{U}_1(s_1^*, s_2) = \max_{s_1 \in \mathcal{S}_1} \min_{s_2 \in \mathcal{R}_2(s_1)} \mathcal{U}_1(s_1, s_2) \triangleq \mathcal{U}_1^*. \tag{2.25}$$

Furthermore, if $s_1^* \in \mathcal{S}_1$ is a Stackelberg strategy for the leader, then any strategy $s_2^* \in \mathcal{R}_2(s_1^*)$ that is in equilibrium with s_1^* is an optimal strategy for the follower. The pair (s_1^*, s_2^*) is then called a Stackelberg solution for the game, and the corresponding Stackelberg equilibrium outcome is given by $(\mathcal{U}_1(s_1^*, s_2^*), \mathcal{U}_2(s_1^*, s_2^*))$.

Given those definitions, we have the following important result [BO99]:

Theorem 2.3 ([BO99])**.**

Every two-person finite game admits a Stackelberg strategy for the leader. Moreover, let $\mathcal{U}_1^*$ and $\mathcal{U}_1^{\text{NE}}$ be, respectively, the Stackelberg utility and the Nash equilibrium utility for Player 1. If $\mathcal{R}_2(s_1)$ is a singleton set $\forall s_1 \in \mathcal{S}_1$, then

$$\mathcal{U}_1^* \geq \mathcal{U}_1^{\text{NE}}. \tag{2.26}$$

Theorem 2.3 shows that the leader in the Stackelberg solution performs at least as well as at the Nash equilibrium, if the follower has a single optimal response for every strategy of the leader.

Finally, if we assume that the two-person Stackelberg game is also a zero-sum game, we can make the following observation.

Remark 2.5.

The Stackelberg solution of the game is the same as the solution of the dynamic game where the follower acts first and the leader acts second after observing the follower's move.

Remark 2.5 follows from the definition of a zero-sum game and Definition 2.13. Therefore, in that case, we can visualize the advantage of being the leader in the Stackelberg game, as it corresponds to acting last in the zero-sum dynamic sequential game.

2.3.2 Auction Theory

Auction theory is a branch of game theory which analyzes the behavior of players in auction markets. There exist several types of auctions and manners to design auctions, i.e., to fix the set of rules which define the outcome of a given auction. In this section we define the basics of auction theory and we give some examples of auction types.

Basics of Auction Theory We define here formally the term "auction" [HNS+12].

Definition 2.14.

An auction is a market mechanism conducted by an auctioneer in which an object or set of objects is exchanged on the basis of bids from potential buyers, also called bidders. An auction provides a specific set of rules that will determine the outcome of the auction, i.e., how the objects are allocated and their corresponding prices.

There are several ways to classify auctions, and we give in the following example the 4 main types of auctions.

Example 2.5.

The 4 traditional types of auctions can be defined as follows:

First-Price Auction: Simultaneous (sealed-bid) auction in which the bidder who submits the highest bid is awarded the object for a price equal to the value of its bid.

Second-Price Auction: Simultaneous (sealed-bid) auction in which the bidder who submits the highest bid is awarded the object for a price equal to the value of the second highest bid.

English Auction: Sequential auction for which the auctioneer asks bidders to increase the current bid, by a predefined increment, at every round starting from a low price. The auction ends when only one bidder is left, who wins the object and pays its bid.

Dutch Auction: Sequential auction in which the price for the object is higher than what any bidder is prepared to pay. The prize decreases until a bidder accepts the price, and wins the object for its price of acceptance.

We can notice some similarities between first-price and Dutch auctions, as well as between second-price and English auctions. In fact these auctions are actually equivalent under certain conditions stated by the *revenue equivalence theorem*. We refer the interested reader to [HNS+12] for details on the equivalencies between auction types.

Vickrey Auctions A Vickrey auction [Kri10] is a sealed-bid auction in which bidders submit bids without knowing the bids of other players. The highest bidder wins the auction and pays the second highest bid. This type of auction gives bidders an incentive to bid their true value, since bidding the maximum amount they would be willing to pay is optimal [Kri10]. Due to this truthful-bidding property, Vickrey auctions have been widely used in wireless communication problems, e.g., in [HHCP08]. In the following section we will give further examples of applications of auction theory in communication networks.

2.3.3 Game Theory Applications in Communication Networks

There has recently been a growing interest in using game theoretical approaches to model and study communication systems. This surge of interest is due to game theory being a particularly suitable framework to tackle fundamental problems in communication networks. Game theory provides indeed the mathematical tools to

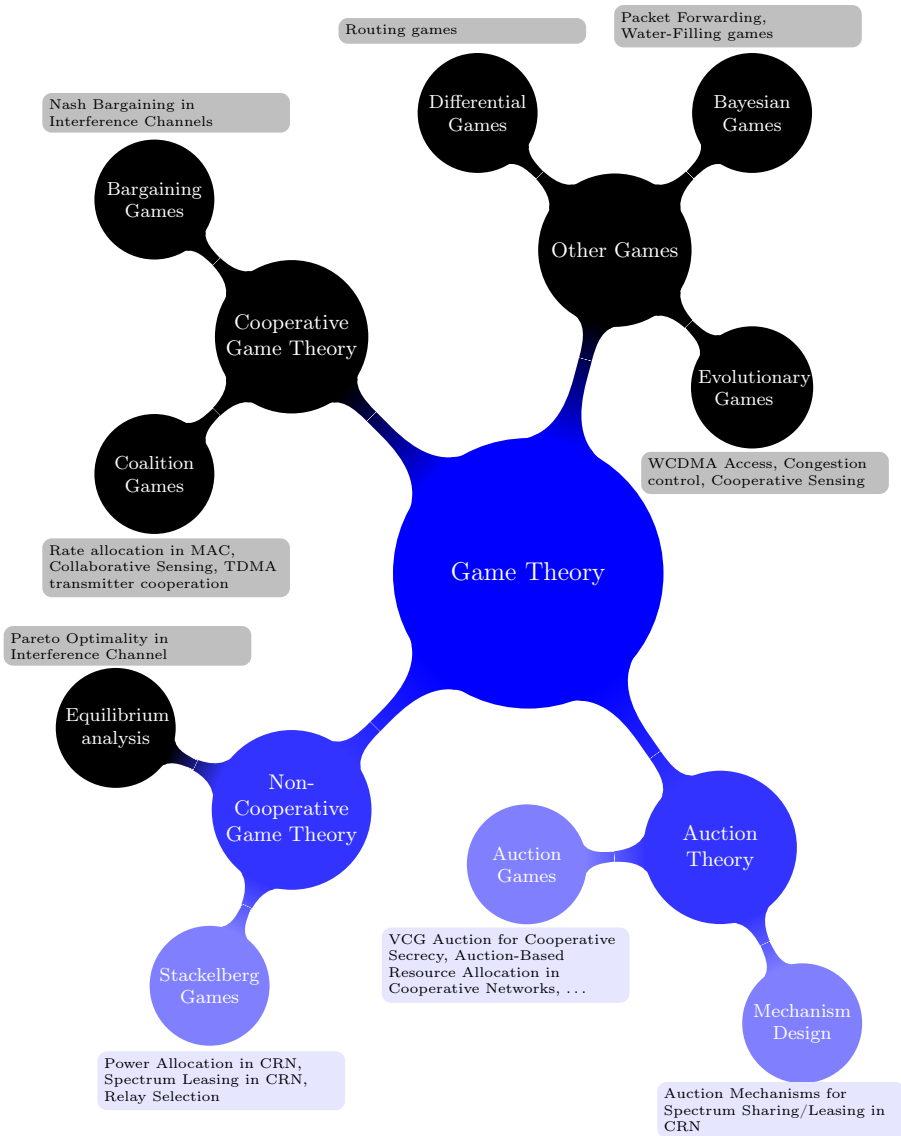


Figure 2.7: Game theory concepts applied to communication networks.

analyze the interactions between rational players, which can naturally be applied to selfish users in networks. In Figure 2.7 we describe the use of game theoretic tools in communication networks as we show the different branches of game theory, and the corresponding game theory concepts applied to wireless networks problems. We highlight the areas investigated throughout this thesis. We also refer to [HNS+12] and references therein for the description of the game theory concepts applied to the communication networks problems.

Game Theory Applications in CRNs In recent years game theory has been applied to fundamental cognitive radio networks' problems. Game theory solution concepts allow for efficient distributed approaches for dynamic problems, e.g., spectrum sharing, and are therefore highly suitable to the analysis of CRNs. We refer the interested reader to [WWL10] where the authors provide an overview of the game theory tools already applied to CRNs and the corresponding references. A chapter in [HNS+12] is devoted to applications of game theory for CRNs, e.g., cooperative spectrum sensing, power control, medium access control, spectrum access, sharing and leasing. These problems are studied through various perspectives, such as non-cooperative game theory, as in [NH08] and [SSS+08] and auction games for spectrum allocation, as in [WLX+10]. Other methods not considered in this thesis include repeated games, cooperative game theory and mechanism designs for auction-based spectrum allocation.

2.4 Information Theoretic Secrecy

In this section we introduce the notion of information theoretic secrecy. Compared to conventional cryptographic techniques, information theoretic secrecy aims to secure communication networks without using an encryption key. In Section 2.4.1 we discuss the motivation for an information theoretic approach on security problems in communication networks. In Section 2.4.2 we introduce the fundamental simplest model of secrecy network, namely the wiretap channel. In Section 2.4.3 we extend the wiretap channel discussion to the practical case of wireless channels.

2.4.1 Motivation for Information Theoretic Secrecy

With the considerable growth of wireless networks in recent years, the issue of network security has taken an important role in the design of communication devices and protocols. Indeed, due to the broadcast nature of these networks, communications can potentially be attacked by malicious parties, and therefore, the protection of transmitted data has become a main concern in today's communications. These attacks are usually addressed in layers above the physical layer, using techniques based on cryptography [MvOV96] for authentication and encryption. However, until recently, not much attention was given to the possibility of implement security protocols at the physical layer, possibly in conjunction with existing protocols at the

Table 2.3: Comparison of information theoretic secrecy and traditional cryptography.

Information Theoretic Secrecy	**Cryptography**
• Technology not available • No assumptions on the eavesdropper's capabilities but passive eavesdropper assumed • Security metrics but based on average measures • No key management needed: lower complexity • Assumptions on channels, such as CSI or channel advantage over Eve • Adapted to the broadcast nature of wireless networks, e.g., man in the middle attack	• Technology already available • Unproven complexity assumptions, protocols might not be secure as technologies evolve • No security metrics to compare security protocols • Difficult key distribution in decentralized networks, key management expensive in dynamic topologies • No assumptions on channels, • Keys can be intercepted, e.g., for public-key algorithms

above layers. This promising direction towards achieving secure communications is labeled information theoretic secrecy. In Table 2.3, we highlight the advantages as well as the shortcomings of the information theoretic approach to security compared to traditional cryptographic schemes.

The information theoretic secrecy approach was initiated by Shannon [Sha49] using a model where a transmitter attempts to conceal its message from a passive eavesdropper. The idea of Shannon consisted of using a secret key in order to generate sufficient randomness to confuse the eavesdropper such that no secret information could be obtained from its observations. The idea to exploit the randomness of the communication channels to ensure the secrecy of the transmitted messages was later developed by Wyner in his fundamental work [Wyn75]. We will devote this section to describing Wyner's wiretap channel model and the existing information theoretic secrecy results, as well as their implication for the secrecy of wireless networks.

2.4.2 The Wiretap Channel

The information theoretic secrecy approach was introduced by Wyner in his fundamental work [Wyn75], in which he introduced the wiretap channel, which is the simplest model to study secrecy in communications.

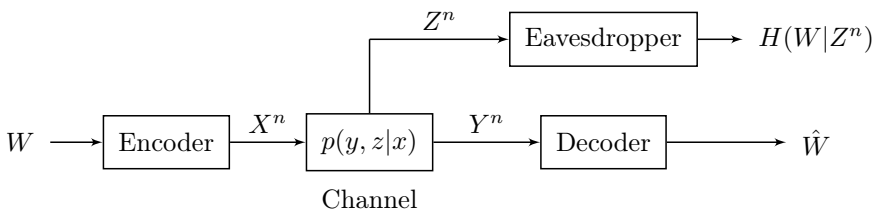


Figure 2.8: The wiretap channel.

The wiretap channel (WTC) is a 3-node network depicted in Figure 2.8. As for the point-to-point channel, the source message W is chosen uniformly from a message set $\mathcal{W}$. The encoder then assigns (stochastically) a codeword $x^n(w) \in \mathcal{X}^n$ to each message $w \in \mathcal{W}$. x^n is transmitted over the DMC channel with transition probability $p_{YZ|X}(\cdot\,|\,\cdot)$ and there are two output sequences y^n and z^n received at the legitimate receiver and the eavesdropper, respectively. The decoder assigns an estimate $\hat{w} \in \mathcal{W}$ of the message to each received sequence $y^n \in \mathcal{Y}^n$.

This wiretap channel model generalizes the model introduced by Wyner in [Wyn75], where it was assumed that the broadcast channel to the receiver and the eavesdropper was physically degraded; i.e., the eavesdropper received a noisy version of the channel output at the legitimate receiver. This more general model was investigated by Csiszár and Körner in [CK78], in a work that establishes the main results on the general WTC.

Secrecy Measures For the wiretap channel, we are interested in two performance measures: reliability and secrecy, which we define as follows.

Definition 2.15.

For information theoretically secure communications, we use the following two measures.

Reliability: The reliability is measured, as in Section 2.1.2, by the average probability of error defined as

$$P_e^{(n)} = P\{\hat{W} \neq W\} = \frac{1}{|\mathcal{W}|} \sum_{w \in \mathcal{W}} P\{\hat{w} \neq w\}. \tag{2.27}$$

Secrecy: Secrecy is measured by the equivocation rate $R_e^{(n)}$ defined as

$$R_e^{(n)} = \frac{1}{n} H(W|Z^n). \tag{2.28}$$

The equivocation rate describes the level of confusion of the eavesdropper about the message W, given its observations Z^n. Therefore, the level of secrecy increases when the equivocation rate increases. We then define an achievable rate-equivocation pair (R, R_e) as follows:

Definition 2.16.

A rate-equivocation pair (R, R_e) is achievable if there exists a sequence of message sets $\mathcal{W}_n$ with $|\mathcal{W}| = \lceil 2^{nR} \rceil$, and a sequence of encoder-decoder pairs, such that

$$P_e^{(n)} \xrightarrow[n\to\infty]{} 0 \qquad \text{(Reliability)} \tag{2.29}$$

$$R_e \leq \lim_{n\to\infty} \inf R_e^{(n)}. \qquad \text{(Secrecy)} \tag{2.30}$$

The capacity-equivocation region $\mathscr{C}$ is then defined as the closure of all achievable rate-equivocation pairs (R, R_e).

The rate-equivocation pair (R, R_e) shows the confidential rate R achieved under a secrecy level R_e. Whenever $R_e < R$, information is leaking to the eavesdropper. When $R = R_e$, we have perfect secrecy and R is called a perfect secrecy rate, or more usually a secrecy rate. The notion of perfect secrecy is particularly important in this thesis, as we will look for achievable perfect secrecy rates for different cooperative network models.

We note that a stronger notion of secrecy has also been considered, see e.g., [LPSS09], in which the condition (2.30) is replaced by:

$$nR_e \leq \lim_{n\to\infty} \inf H(W|Z^n). \tag{2.31}$$

This notion is called strong secrecy, in contrast with the weak secrecy constraint in (2.30), which is the notion considered in this thesis, unless mentioned otherwise, as e.g., in Chapter 4. Other secrecy measures exist, and we refer the reader to [BL13] for a detailed characterization of the different security measures and their interdependence.

As for the point-to-point channel without eavesdropper, the highest achievable secrecy rate is a fundamental measure: this is the secrecy capacity.

Definition 2.17.

The secrecy capacity C_s is the largest rate achievable with perfect secrecy, i.e.,

$$C_s = \max_{(R,R)\in\mathscr{C}} R. \tag{2.32}$$

For the wiretap channel described in Figure 2.8, the secrecy capacity is given by the following theorem [CK78]:

Theorem 2.4 (Secrecy Capacity of the Wiretap Channel [CK78])**.**

The secrecy capacity of the wiretap channel is given by

$$C_s = \max_{p_{UX}p_{YZ|X}} [I(U;Y) - I(U;Z)]^+, \tag{2.33}$$

where the auxiliary random variable U satisfies the Markov chain $U - X - (Y, Z)$ and U is bounded in cardinality by $|\mathcal{U}| \leq |\mathcal{X}| + 1$.

Theorem 2.4 implies that for every rate $R < C_s$, the message W can be reliably transmitted while being kept perfectly secret from the eavesdropper.

We should note that the expression of Theorem 2.4 for the secrecy capacity can be simplified for several classes of wiretap channels [LPSS09]. The secrecy capacity of the WTC was first derived in [CK78], by generalizing the WTC to a broadcast channel with confidential messages. A rigorously detailed proof of the theorem can be found in [BB11].

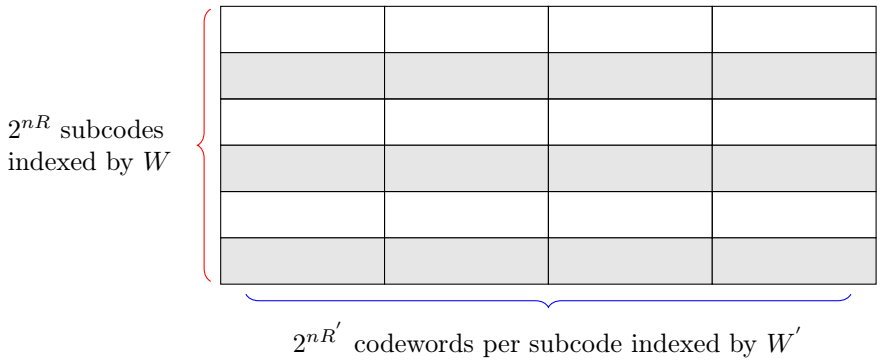


Figure 2.9: Wiretap coding with nested codes.

Coding for the Wiretap Channel In his original work [Wyn75], Wyner describes the basic strategy for designing practical codes to achieve secrecy for wiretap channels. This strategy can be interpreted with the notion of nested codes, which we summarize here. In Figure 2.9 we depict the nested structure of wiretap codes. A wiretap code consists of all codewords contained in the table and it has to be decodable by Bob. The wiretap code is split into subcodes and every message is mapped to one subcode. For encoding, one codeword from the chosen subcode is picked uniformly at random and transmitted. In other terms, for each secret message $W \in \{1, 2^{nR}\}$, there are $2^{nR'}$ codewords $X(W, W')$ chosen at random (stochastic encoder) as $W' \in \{1, 2^{nR'}\}$. Each set of codewords forms a bin, which is a subcode of the wiretap code. It is shown that if each subcode is capacity-achieving for Eve's channel, i.e., R' is chosen as the capacity of Eve's channel, then Eve is unable to decode any information, and in particular, the index of the subcode that contains the information about the source message. Hence, since we must choose $R + R'$ below the capacity of Bob's channel from the channel coding Theorem 2.1, we obtain the code design parameters R and R' by $R + R' < C_b$ and $R' < C_e$ where C_b and C_e denote the capacity of the main and the eavesdropper's channel respectively. We refer the reader to [BB11] for a more detailed description of coding mechanisms for the wiretap channel. For examples of existing channel codes achieving secrecy over certain classes of wiretap channels, we refer the interested reader to [And14].

2.4.3 Secrecy in Wireless Networks

In this section we extend the secrecy capacity results of Section 2.4.2 to the case of Gaussian and wireless channels. Gaussian channels are particularly important since they represent a reasonable approximation of the effects on the channels at the physical layer. Moreover, the analysis of Gaussian channels is fundamental for

the study of more general wireless channels.

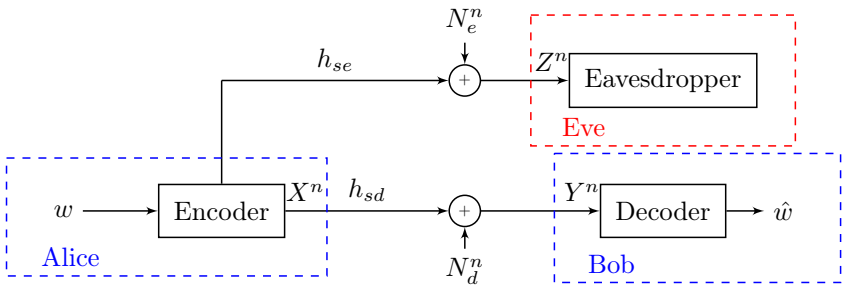


Figure 2.10: The complex Gaussian wiretap channel.

The Gaussian Wiretap Channel The complex Gaussian WTC is depicted in Figure 2.10. The source, commonly named Alice in the literature, transmits X^n over the channel. The received signals at the destination (Bob) and the eavesdropper (Eve) are Y^n and Z^n, respectively. For $i \in \{1, \ldots, n\}$, we have:

$$y_i = h_{sd} x_i + n_{d,i} \tag{2.34}$$

$$z_i = h_{se} x_i + n_{e,i}, \tag{2.35}$$

where the noise sources are complex and circularly symmetric, i.e., $n_{d,i} \sim \mathcal{CN}(0, \sigma_d^2)$ and $n_{e,i} \sim \mathcal{CN}(0, \sigma_d^2)$, $h_{sd} \in \mathbb{C}$ and $h_{se} \in \mathbb{C}$ are constant coefficients. Finally, we assume the following average power constraint on the transmitted signal:

$$\frac{1}{n} \sum_i |x_i|^2 \leq P_s. \tag{2.36}$$

For this complex Gaussian WTC, the secrecy capacity is known and given in the following theorem [BB11]:

Theorem 2.5 (Secrecy Capacity of the Complex Gaussian WTC [BB11])**.**

The secrecy capacity of the complex Gaussian WTC is

$$C_s = \left(\log\left(1 + \frac{|h_{sd}|^2 P_s}{\sigma_d^2}\right) - \log\left(1 + \frac{|h_{se}|^2 P_s}{\sigma_e^2}\right) \right)^+ = (C_d - C_e)^+, \tag{2.37}$$

where $C_d \triangleq 2\mathcal{C}(\frac{|h_{sd}|^2 P_s}{\sigma_d^2})$ is the capacity of the legitimate channel and $C_e \triangleq 2\mathcal{C}(\frac{|h_{se}|^2 P_s}{\sigma_e^2})$ is the capacity of the eavesdropper's channel.

We make several important observations here:

- Theorem 2.5 is a consequence of Theorem 2.4. In particular the achievability follows from Theorem 2.4 with the choice of the auxiliary random variable $U \sim \mathcal{CN}(0, P_s)$, and $X \triangleq U$. A rigorous proof can be found in [BB11].

- Theorem 2.5 can be viewed as an extension of the secrecy capacity of the real Gaussian WTC, found by Leung-Yan-Chong and Hellman in [LYCH78], by:

$$C_s = \left(\frac{1}{2}\log\left(1+\frac{P_s}{\sigma_d^2}\right) - \frac{1}{2}\log\left(1+\frac{P_s}{\sigma_e^2}\right)\right)^+ = (C_d - C_e)^+. \tag{2.38}$$

  The factor 2 results from the complex Gaussian WTC being equivalent to two parallel real Gaussian WTCs.

- From (2.37), we deduce that secure communication is possible if and only if the legitimate receiver has a better SNR than the eavesdropper. In practice, this can be interpreted as the eavesdropper being further away from the legitimate transmission.

The Quasi-Static Fading Wiretap Channel We generalize here the model of Figure 2.10 to wireless channels. In particular, the communication channels are now modeled as fading channels; i.e., h_{sd} and h_{se} are randomly distributed. We restrict ourselves to the quasi-static fading model defined in Section 2.1.2. This model differs from the ergodic-fading model and the block-fading model, which have also been considered in the literature, e.g., in [BB11]. The model reduces to a complex Gaussian WTC defined by (2.34) and (2.35) for each coherence interval. Secure communication over quasi-static channels is therefore determined by the instantaneous fading realization. Alice, Bob, and Eve are assumed to have perfect knowledge of the instantaneous realizations of the fading coefficients (h_{sd}, h_{se}), such that the wiretap code is chosen opportunistically for each realization of the fading. The secure communications rate over a long period of time, i.e., the average secrecy capacity, is then given in the following theorem [BBRM08]:

Theorem 2.6 ([BBRM08]).

With full channel state information, the average secrecy capacity of a quasi-static fading wiretap channel is

$$C_s^{avg} = \mathbb{E}_{H_{sd},H_{se}}[C_s(H_{sd}, H_{se})], \tag{2.39}$$

where $C_s(h_{sd}, h_{se})$ is the instantaneous secrecy capacity, defined as

$$C_s(h_{sd}, h_{se}) = \left(\log\left(1 + \frac{|h_{sd}|^2 P_s}{\sigma_d^2}\right) - \log\left(1 + \frac{|h_{se}|^2 P_s}{\sigma_e^2}\right)\right)^+. \tag{2.40}$$

The assumption of full channel state information in Theorem 2.6 is essential. As a matter of fact, when the transmitter does not know the fading coefficient h_{se}, the average secrecy capacity for the quasi-static fading channel is 0 [BB11].

However, within each coherence interval, the transmitter can guarantee reliability by adapting the rate of the code, but perfect secrecy cannot be assured, as the realization h_{se} is unknown. Consequently, one needs to adopt a probabilistic view of security. In particular, the probability that information is leaked to the eavesdropper for a chosen transmission rate should be considered. This leads to the fundamental notion of secrecy outage probability.

Secrecy Outage Probability For wireless networks with secrecy constraints, the assumption of perfect channel knowledge from the source to the eavesdropper is commonly used for the computation of the secrecy capacity or achievable secrecy rates. This limiting assumption can be justified in certain types of networks where the eavesdropper is also part of the system; e.g., it can be a legitimate receiver for the messages of certain users and simultaneously be viewed as an eavesdropper for the messages of other users as in [LSBP$^+$09], [WL11]. However, in the case of a passive external eavesdropper, this assumption is far too optimistic and we must assume that the transmitter has only limited channel state information on the eavesdropper's channel. A common assumption for this scenario is that only the channel statistics, i.e., the average SNR, of the eavesdropper's channel are known, but not the instantaneous realizations of the channel. This corresponds to the path-loss model for quasi-static Rayleigh fading channels scenario where only the location of Eve is known. For that model, the secrecy outage probability (SOP) is a suitable measure of the system performance. The notion of secrecy outage probability was first introduced in [BBRM08], in the case of the quasi-static Rayleigh fading wiretap channel. Similar to the outage probability without secrecy constraint, it was defined as the probability that the instantaneous secrecy capacity is less than a target secrecy rate. The meaning of the secrecy outage probability can be explained as follows.

Without the channel state information (CSI) on Eve's channel, but with the knowledge of the instantaneous capacity C_d of the main channel, Alice is forced to choose a secrecy rate R. In some sense, Alice is assuming that the capacity of the eavesdropper's channel is $C_e = C_d - R$. As long as $R \leq C_s$, i.e., the chosen rate is below the instantaneous secrecy capacity, the assumption is optimistic as Eve's channel is worse than the source's estimate and the wiretap codes ensure perfect secrecy. However, if $R > C_s$, secrecy is compromised. We can also interpret the secrecy outage in terms of wiretap code design. Optimally, the nested secure code consists of the linear code pair $(\mathcal{C}_0, \mathcal{C}_s)$ where $\mathcal{C}_0$ is a linear code with rate C_d, and $\mathcal{C}_s$ is a linear code with rate $C_s = C_d - C_e$. However, without CSI on Eve's channels, the source is forced to choose $R \triangleq \hat{R}_s = C_d - \hat{C}_e$ for the rate of the fine code, and the secrecy constraint is violated when $\hat{R}_s > C_s$.

This analysis shows that the secrecy outage probability is a secrecy measure particularly adapted to the situation where the legitimate nodes have limited CSI about the eavesdropper's channels, as the transmitter must choose the secrecy rate R without the exact information on the eavesdropper's channels. Formally, we can then define the secrecy outage probability as follows:

Definition 2.18.

The secrecy outage probability is defined as the probability that the chosen transmission rate R exceeds the achievable instantaneous secrecy rate C_s:

$$P_{out}(R) = P\{C_s < R\}. \tag{2.41}$$

Alternative definitions of the secrecy outage probability exist, e.g., in [GSJ12].

2.5 Cooperation for Secrecy

In this section we investigate the interaction between cooperation, introduced in its simplest form with the relay channel in Section 2.1.3, and secrecy in communication networks. There has been a substantial interest in the secrecy of multi-user systems [LPSS09], with a particular emphasis on potential cooperation between users to enhance the secrecy of communications. We should note that, in this section, we assume that the cooperative node(s) can be trusted and aim at increasing the secrecy of the transmission in the presence of an external eavesdropper. A more complex kind of interaction between cooperation and secrecy has been the subject of several recent works, e.g., in [HY10] and [YLE11], in which the cooperative nodes are also treated as potential eavesdroppers. In this model, it is not clear whether cooperation can, in fact, improve secrecy, or whether there is a trade-off between cooperation and secrecy. For instance, if the untrusted cooperative

node performs a decode-and-forward strategy to convey the information to the destination, cooperation and secrecy appear to be conflicting goals.

However, we focus here on achieving secrecy with a trusted cooperative node. This scenario was first captured in [LEG08], by the relay-eavesdropper channel model. We first introduce this model in Section 2.5.1. Several cooperative strategies aiming at increasing the secrecy of the transmission in the presence of a possible external eavesdropper have been proposed and they can be classified into two types. For the strategies of the first type, the cooperating parties improve the secrecy performance of the system by weakening the eavesdropping link. Hence, in contrast to wireless communications without secrecy, where interference is considered as an undesired effect, interference can potentially be a beneficial phenomenon for secure communications. The second type corresponds to the classical sense of cooperation, where the cooperating nodes strengthen the main transmission by using common relaying techniques such as decode-and-forward or amplify-and-forward. We characterize these two different types of cooperation, namely oblivious cooperation in Section 2.5.2 and active cooperation in Section 2.5.3.

2.5.1 The Relay-Eavesdropper Channel

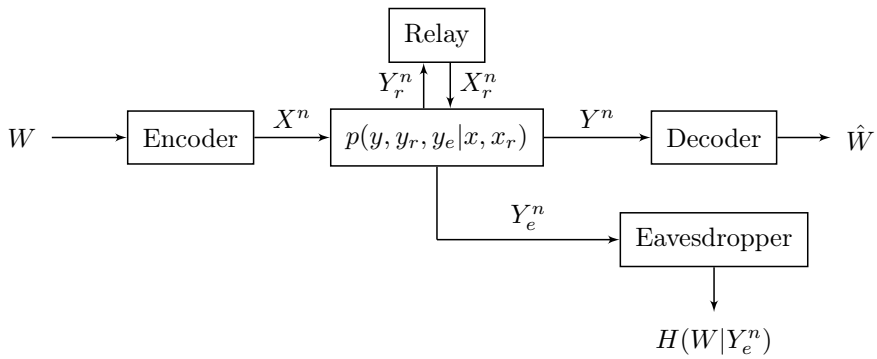


Figure 2.11: The relay-eavesdropper channel.

We introduce first the relay-eavesdropper channel as the canonical example of cooperation for secrecy. The relay-eavesdropper channel model is represented in Figure 2.11. It was introduced and deeply investigated in [LEG08]. This 4-node network is composed of a source, a relay, a destination and an eavesdropper. This model combines to some extent the simplest cooperative network, namely the relay channel, and the simplest network with secrecy constraints, namely the wiretap channel.

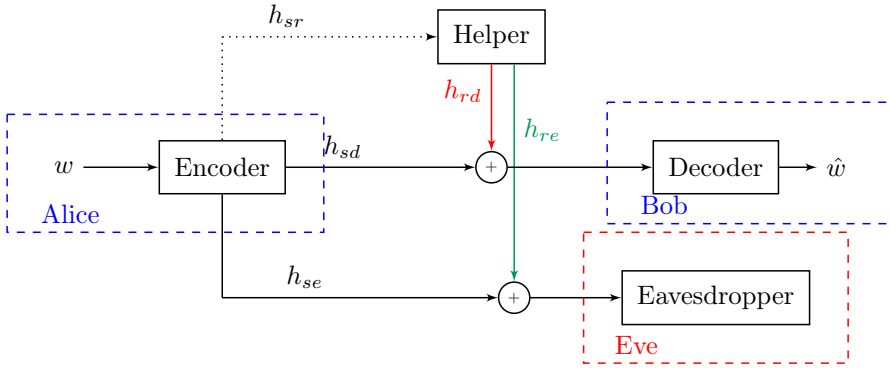


Figure 2.12: Cooperative jamming for the Gaussian relay-eavesdropper channel.

In [LEG08], achievable secrecy rates are derived for different strategies for the relay. These strategies fall into two categories, as later characterized in [LT09, Chapter 7]. In the first category, the relay attempts to confuse the eavesdropper by sending codewords independent of the source's message, this strategy is labeled noise-forwarding (NF) in [LEG08]. In the other category, the relay implements a classical relaying scheme; e.g., DF and CF are proposed in [LEG08]. In the following, we describe the two types of cooperation in the case of Gaussian channels.

2.5.2 Oblivious Cooperation: Cooperative Jamming

In this section we discuss a cooperative strategy where the helper does not need to have any information regarding the transmitted message, namely cooperative jamming (CJ). This model is represented in Figure 2.12. We notice that this relay-eavesdropper channel with a relay ignoring the transmitter's message is equivalent to a multiple-access wiretap channel (MAC-WTC), as in [TY08a].

Before describing the cooperative jamming strategy used throughout this thesis, we should note that several implementations of cooperative jamming exist in the literature. For instance, the noise forwarding scheme introduced in [LEG08] can be interpreted as a form of a cooperative scheme although a fundamental different exists. For NF, the helper sends dummy codewords from a codebook to confuse the eavesdropper and increase the achievable secrecy rate. In particular, if the helper-receiver link is stronger than the helper-eavesdropper link, the receiver is able to decode the dummy codewords sent by the helper, while the eavesdropper is not able to decode them. A similar scheme is coined interference assisted secret communication in [TLSP11], where both NF and CJ are investigated.

Instead of the noise-forwarding strategy, the helper might instead explicitly attack the eavesdropper. This is the main idea of cooperative jamming, introduced in [TY08b] for the MAC-WTC, and later used for different channel models, e.g., the

interference channel with secrecy constraints [TLSP11]. In Gaussian channels, this attack is implemented by injecting additional Gaussian noise to the channel. Due to the broadcast nature of the channels, this noise also hurts the legitimate receiver; however, if the helper-eavesdropper link is stronger than the helper-receiver link, the eavesdropper is more affected by the jamming.

To illustrate this mechanism, we consider Figure 2.12. If the helper is not present, the following secrecy rate is achievable (this is the Gaussian WTC secrecy capacity):

$$\left(\log\left(1+\gamma_{sd}\right)-\log\left(1+\gamma_{se}\right)\right)^{+}. \tag{2.42}$$

Now, if the helper transmits Gaussian noise with power P_r, the following secrecy rate is achievable

$$\left(\log\left(1+\frac{\gamma_{sd}}{1+\gamma_{rd}}\right)-\log\left(1+\frac{\gamma_{se}}{1+\gamma_{re}}\right)\right)^{+}. \tag{2.43}$$

From the expression of (2.43), we observe that CJ is making both channels noisier than they actually are, resulting in a lower signal-to-interference ratio (SINR). This strategy can thus be thought of as sending dummy codewords whose rate is above the decoding capability of both the eavesdropper and the receiver. The achievable secrecy rate of (2.43) might improve the secrecy capacity of the Gaussian WTC in (2.42), if the helper-eavesdropper channel is strong enough, i.e., if jamming hurts the eavesdropper more than the legitimate receiver.

While cooperative jamming with Gaussian noise has the advantage of simplicity, the non-decodability of the noisy signals are always hurting the legitimate receiver. Consequently, more elaborate cooperative jamming strategies have been recently proposed in the literature to mitigate this negative effect, e.g., in [BU13] such as cooperative jamming with structured codes, or cooperative jamming via alignment. We refer the interested reader to [EHT+13] for a survey of existing jamming techniques for secrecy.

2.5.3 Active Cooperation: Relaying Schemes

In the previous section, the helper helped the main receiver by weakening the eavesdropping link without using any knowledge of the message being transmitted. In this section we review cooperative schemes where the helper helps the main receiver by strengthening the main link, i.e., by acting as a relay.

Active cooperation was first considered for the relay-eavesdropper channel in [LEG08]. We show the model for Gaussian channels in Figure 2.13. In [LEG08], inner bounds on the secrecy capacity, i.e., achievable secrecy rates, are given for different relaying strategies for the general discrete memoryless relay-eavesdropper channel of Figure 2.11. In particular, DF and CF strategies in the presence of an eavesdropper are investigated. In [DHPP10], DF and AF are compared to CJ for Gaussian channels, and achievable secrecy rates are derived. In [Yuk08], achievable

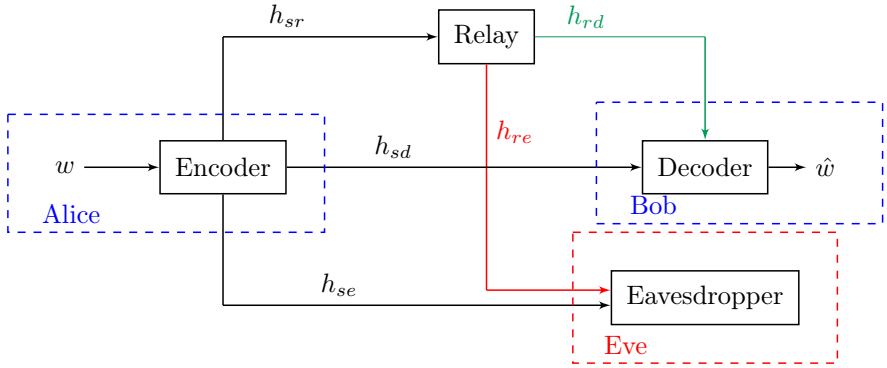


Figure 2.13: Active cooperation for the Gaussian relay-eavesdropper channel.

secrecy rates are also given for CF in the case of Gaussian channels and time-division relaying. More recently, DF strategies in multiple relay networks with secrecy constraints were investigated in [BU12]. As for the relay channel without an eavesdropper, the performance of DF depends on the quality of the transmitter-relay link as the overall rate is limited by the rate of this link. Moreover, in the relay-eavesdropper channel, the relative strengths of the relay-receiver and the relay-eavesdropper links become critical. For example, if the relay-eavesdropper link is stronger than the relay-receiver link, then all of the information sent by the relay will be decodable by the eavesdropper. In this case, the relay may not improve the secrecy of the transmitter. A similar analysis based on the relative strength of the links can be performed for AF and CF, as e.g., in [ZYC+09].

Finally, we should note that other cooperative networks with secrecy have been deeply investigated in recent works, such as the relay-broadcast channel with secrecy constraints in [EU11], or the cognitive interference channel with secrecy constraints in [LSBP+09]. A comprehensive review of the main results for multi-user networks with secrecy can be found in [LPSS09]. For a recent summary of advances in the field of cooperation for secrecy, we refer the reader to the survey [EHT+13].

2.6 Cooperative Secrecy in Wireless Networks: A Case Study

In this section we investigate cooperation for secrecy for wireless channels through a case study. The aim of this section is highlight several difficulties in the secrecy analysis of the relay-eavesdropper channel inherent to some crucial assumptions from Wyner's wiretap channel model. Consequently, we will introduce in the next chapter the system model investigated throughout this thesis that allows us to eliminate the shortcomings highlighted in this case study.

We consider in particular quasi-static Rayleigh fading channels. In such an environment, the common assumption of perfect knowledge of Eve's channels is not satisfying, and the performance of the schemes must be analyzed from an outage perspective [BB11, Chapter 5]. As explained in the previous section, cooperation can improve secrecy in two ways: either by improving the quality of the legitimate transmission or by decreasing the amount of information obtained by the eavesdropper. For the former way, we consider decode-and-forward and amplify-and-forward as possible strategies for the helping node, while for the latter, we consider cooperative jamming with noise. We introduce important secrecy measures for the cooperative schemes, namely the secrecy outage probability, the conditional secrecy outage probability and the secure throughput. These measures take into account the fading model as well as the limited CSI about Eve's channels. We derive closed-form expressions for these measures. Moreover, we illustrate the performance of the schemes for different scenarios to characterize the effect of the nodes' geometry.

This study is divided into three sections. In the first Section 2.6.1 we describe the model and the cooperative strategies investigated throughout this chapter. In the second Section 2.6.2 we analyze and compare the secrecy outage probability and the conditional secrecy outage probability performance of the cooperative schemes. Finally in the last Section 2.6.3 we elaborate a global system optimization regarding strategy selection, node positioning, power allocation, and rate design.

2.6.1 System Description

In this section we first describe the system model investigated throughout this study. Secondly, we give achievable secrecy rates for the considered cooperative schemes in this model. Finally we define our performance measures, namely the secrecy outage probability and the conditional secrecy outage probability.

System Model We will consider the four-node network illustrated in Figure 2.14. The source ($\mathcal{S}$) wishes to communicate a message to the destination ($\mathcal{D}$) in the presence of the helping node ($\mathcal{H}$) and the eavesdropper ($\mathcal{E}$).

Network Model We make the following assumptions regarding the considered network:

- The source transmits with a fixed power $P_s = P_{\max}$ and the relay transmits with a power $P_r \in [0, P_{\max}]$.
- The additive noise n for all nodes is zero-mean white complex Gaussian with variance σ^2. For simplicity, we will assume that $\sigma^2 = 1$ and that $\mathrm{SNR}_{\max} \triangleq \frac{P_{\max}}{\sigma^2} = 10$ dB.
- All channels are Rayleigh quasi-static fading channels. From a codeword to another, the fading coefficients h_{ij} change randomly according to a complex

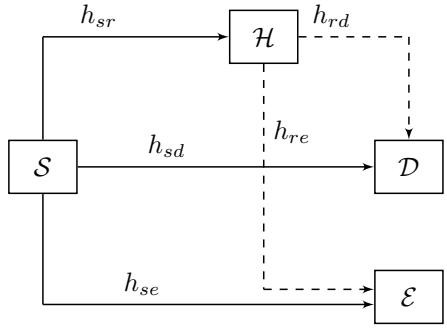


Figure 2.14: Relay-eavesdropper channel model.

Gaussian distribution:

$$h_{ij} \sim \mathcal{CN}\left(0, 1/d_{ij}^{\alpha}\right), \tag{2.44}$$

where α represents the path-loss exponent, and d_{ij} is the Euclidian distance between node i and node j.

- We note $\gamma_{ij} = P_i \left|h_{ij}\right|^2$ the instantaneous SNR between node i and node j, where P_i is the transmission power of node i. The random variable γ_{ij} is exponentially distributed, with mean $\bar{\gamma}_{ij} = \frac{P_i}{d_{ij}^{\alpha}}$.

Transmission Model For the relaying schemes, we assume that a time division is imposed by the network such that the source transmits in the first time slot and the relay transmits in the second time slot. The source remains silent during the second time slot. Both time slots have the same length. In the first time slot, we have

$$\begin{aligned} y_r &= h_{sr} x_s + n_r^{(1)}, \\ y_d^{(1)} &= h_{sd} x_s + n_d^{(1)}, \\ y_e^{(1)} &= h_{se} x_s + n_e^{(1)}, \end{aligned}$$

while in the second time slot, we have

$$\begin{aligned} y_d^{(2)} &= h_{rd} x_r + n_d^{(2)}, \\ y_e^{(2)} &= h_{re} x_r + n_e^{(2)}. \end{aligned}$$

We also consider the cooperative jamming scheme described in the previous section where the helper transmits the Gaussian noise x_j with power P_r while the source transmits in the first time slot. In the first time slot, we have

$$y_d^{(1)} = h_{sd} x_s + h_{rd} x_j + n_d^{(1)},$$

$$y_e^{(1)} = h_{se}x_s + h_{re}x_j + n_e^{(1)},$$

while we assume that both source and helper remain silent in the second time slot such that the comparison between the relaying schemes and cooperative jamming is fair in terms of average power consumption.

Transmission Schemes In this section we describe the cooperative transmission schemes, namely direct transmission (DT), decode-and-forward relaying, amplify-and-forward relaying, and cooperative jamming. We assume that full channel state information on all channels is available at the legitimate nodes. This particular assumption will then be discussed in the next section. We relegate the achievable instantaneous secrecy rates expressions to Appendix 2.A for a better readability of the study.

Direct Transmission For DT, the relay is turned off and the source simply transmits the message to the destination during the first time slot. We are therefore treating DT as a special case of the considered relaying schemes.

Decode-and-Forward Relaying In the first time-slot, the source broadcasts the message x_s. Then in the second stage, the relay decodes the information transmitted by the source and re-encodes it using the same codebook (repetition coding) as the source to transmit the information to the destination. The receiver uses maximum ratio combining (MRC) to optimally combine both observations. Furthermore, we assume that DF is implemented only if $\gamma_{sd} < \gamma_{sr}$. This particular DF scheme is considered in [DHPP10]. Other strategies can be implemented by the relay which lead to different achievable secrecy rates (e.g., in [Yuk08], an independent codebook is used at the relay).

Amplify-and-Forward Relaying In the AF scheme, the relay scales the signal received after the first time slot, and then it simply forwards it such that

$$x_r = \sqrt{P_r}y_r \quad \text{with } P_r \in \left[0, \frac{P_{\max}}{1+\gamma_{sr}}\right],$$

i.e., $\exists \beta \in \left[0, \frac{1}{1+\gamma_{sr}}\right]$ with $P_r = \beta P_{\max}$.
Again, the receiver combines the observations optimally by using MRC.

Cooperative Jamming In the CJ scheme, the helper interferes via transmitting Gaussian noise as described in Section 2.5 while the source is transmitting its message, in order to confuse the eavesdropper.

The aim of this section is to consider cooperative schemes which are simple to implement and easily adaptable. Hence we choose the DF and AF strategies previously described. Furthermore, more elaborated relaying schemes often require

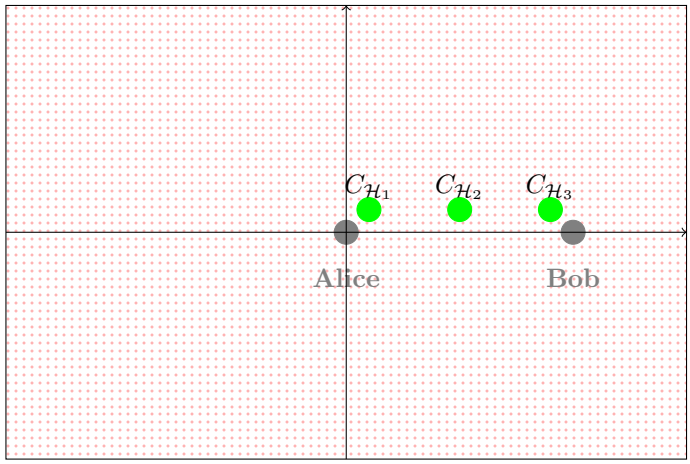


Figure 2.15: Geometrical model.

perfect CSI on all channels and they also are sensible to modifications of the channels' coefficients, and thus, they are less suitable for the scenario studied in this study.

Geometrical Model We consider throughout this section the geometrical model where the source and the destination are located at the respective fixed positions $(0,0)$ and $(0,1)$, which means that the distances between different nodes in this model are normalized w.r.t. the source-destination distance. The geometrical model is depicted in Figure 2.15. $\mathcal{E}$ can be located at any position $(x_e, y_e) \in \mathcal{P}$, with $\mathcal{P} \triangleq x_e \in [-1.5, 1.5] \cap y_e \in [-1, 1.5]$ while we will consider in this chapter three possibilities for the positioning of the helping node:

Case $C_{\mathcal{H}_1}$: The helping node is located in $(0.1, 0.1)$ i.e., close to the source. In other terms, $\bar{\gamma}_{sr} \gg \bar{\gamma}_{sd} \approx \bar{\gamma}_{rd}$.

Case $C_{\mathcal{H}_2}$: The helping node is located in $(0.5, 0.1)$ i.e., in the middle of the transmission. In other terms, $\bar{\gamma}_{sr} \approx \bar{\gamma}_{rd}$.

Case $C_{\mathcal{H}_3}$: The helping node is located in $(0.9, 0.1)$ i.e., close to the destination. In other terms, $\bar{\gamma}_{rd} \gg \bar{\gamma}_{sd} \approx \bar{\gamma}_{sr}$.

Secrecy Outage In our case study, we assume that the legitimate nodes have full CSI on the legitimate channels (i.e., the channels between $\mathcal{S}$, $\mathcal{D}$ and $\mathcal{H}$). We will also assume that only the channel statistics, i.e., the average SNRs, of the eavesdropper's channels are known but not the instantaneous realizations of these

channels. This corresponds to the path-loss model for quasi-static Rayleigh fading channels scenario where only the location of Eve is known. For that model, we will naturally use the secrecy outage probability as a measure of the system performance. For the relay-eavesdropper channel considered in this case study, the instantaneous secrecy capacity is unknown. However, according to the instantaneous achievable secrecy rates for different strategies defined in the previous section, we can then define the secrecy outage probability as follows:

Definition 2.19.

The secrecy outage probability for the strategy $s_{\mathcal{H}}$ of the helper is defined as the probability that the chosen transmission rate R exceeds the achievable instantaneous secrecy rate R_s, i.e.,

$$P_{out}^{(s_{\mathcal{H}})}(R) = P\{R_s < R\}. \tag{2.45}$$

Remark 2.6.

For DT and CJ, the achievable instantaneous secrecy rates given in Section 2.6.1 coincide with the instantaneous secrecy capacity, that is $R_s^{(DT)} = C_s^{(DT)}$ and $R_s^{(CJ)} = C_s^{(CJ)}$ [VBBM11]. In this case, if $R_s < R$, then a secrecy outage occurs certainly since the secrecy capacity is the supremum of all achievable secrecy rates. However, we notice that our performance measure is somewhat pessimistic for the relaying schemes, since the $R_s^{(DF)}$ and $R_s^{(AF)}$ obtained in Section 2.6.1 are only achievable secrecy rates for the proposed strategies; i.e., there could be higher achievable rates within the secrecy capacity region of these strategies.

We also define an alternative measure of secrecy, based on our CSI assumptions. With the assumption of full CSI on the legitimate channels, a secrecy outage probability conditioned on the known fading coefficients becomes meaningful. Since the channel coefficients are known during the transmission of the whole codeword under the quasi-staticity assumption, the distribution of the fading coefficients will not influence the outage events during this transmission. Therefore, γ_{sr}, γ_{rd} and γ_{sd} are not considered as random variables, but as given realizations of the channels. This leads to the notion of conditional secrecy outage probability (CSOP), which we define as follows:

Definition 2.20.

The conditional secrecy outage probability for the strategy $s_{\mathcal{H}}$ of the helper is defined as the probability that the chosen transmission rate R exceeds the achievable instantaneous secrecy rate R_s, given γ_{sr}, γ_{rd} and γ_{sd}, i.e.,

$$P_{out,c}^{(s_{\mathcal{H}})}(R) = P\left\{R_s < R | \gamma_{sr}, \gamma_{rd}, \gamma_{sd}\right\}. \tag{2.46}$$

We should note that there exists a mathematical relation between the SOP and the CSOP of the scheme $s_{\mathcal{H}}$:

$$P_{out}^{(s_{\mathcal{H}})}(R) = \mathbb{E}_{\gamma_{sr},\gamma_{rd},\gamma_{sd}} P_{out,c}^{(s_{\mathcal{H}})}(R). \tag{2.47}$$

2.6.2 Secrecy Outage Performance of Cooperation

In this section we consider the cooperative schemes described previously. We investigate the performance of the different schemes in terms of our two performance measures: the secrecy outage probability and the conditional secrecy outage probability. We provide closed-form expressions for the SOP and the CSOP of the different schemes. For each cooperative strategy we give first closed-form expressions for the SOP. Then, we analyze the conditional secrecy outage probability. This measure of performance is particularly relevant since it takes into account the CSI knowledge of the legitimate nodes about their channel realizations. In some sense, the CSOP takes into account that only the uncertainty about Eve's channels remains. Finally, we give numerical examples based on our geometrical model previously introduced. We will use the Case $C_{\mathcal{H}_2}$ since this particular positioning of the helper appeared to be advantageous in the light of the results in [Gab12].

Direct Transmission Performance

We consider first the wiretap channel without any cooperation of the helper. We can view it as the reference model to which we will compare the performance of the proper cooperative schemes.

Secrecy Outage Probability In the following theorem, previously shown in [BBRM08], we give the secrecy outage probability for the direct transmission strategy.

Theorem 2.7 (SOP for Direct Transmission [BBRM08])**.**

The secrecy outage probability for DT is given by

$$P_{out}^{(DT)}(R) = 1 - \frac{\bar{\gamma}_{sd}}{\bar{\gamma}_{sd} + 2^{2R}\bar{\gamma}_{se}} e^{-\frac{2^{2R}-1}{\bar{\gamma}_{sd}}}. \tag{2.48}$$

We can analyze the secrecy outage expression for several extreme cases:

$\bar{\gamma}_{sd} \to \infty$**:** When the average SNR of the main channel is arbitrarily large then from (2.48) it follows that

$$P_{out}^{(DT)}(R) \to 0.$$

$\bar{\gamma}_{se} \to \infty$**:** When the average SNR of the eavesdropper's channel is arbitrarily large then from (2.48) it follows that

$$P_{out}^{(DT)}(R) \to 1.$$

$R \to 0$**:** In this case, we have:

$$P_{out}^{(DT)}(R) \to \frac{\bar{\gamma}_{se}}{\bar{\gamma}_{se} + \bar{\gamma}_{sd}},$$

which means that even for an arbitrarily small target secrecy rate, there will always be a strictly positive probability that the transmission is not secure, due to the fading nature of the channels.

Conditional Secrecy Outage Probability We now consider the CSOP for the direct transmission scheme. We first need to define the following auxiliary function $Q_{a,b}(R)$, which will be useful in this section:

$$Q_{a,b}(R) \triangleq \frac{2^{-2R}(1+a) - 1}{b}. \tag{2.49}$$

where $R \in [0, 1/2 \log(1+a)]$, $a > 0$, and $b > 0$.

In the following theorem, we give the conditional secrecy outage probability given γ_{sd} for the direct transmission strategy.

Theorem 2.8.

The conditional secrecy outage probability for DT is given by

$$P_{out,c}^{(DT)}(R) = e^{-\frac{2^{-2R}(1+\gamma_{sd})-1}{\bar{\gamma}_{se}}} = e^{-Q_{\gamma_{sd},\bar{\gamma}_{se}}(R)}, \tag{2.50}$$

with $R \in [0, \mathcal{C}(\gamma_{sd})]$ to ensure the reliability of the DT scheme.

Proof. We refer to [Gab12] for the proof of the theorem. ■

We can analyze the conditional secrecy outage expression for several extreme cases:

$\bar{\gamma}_{sd} \to \infty$**:** When the average SNR of the main channel is arbitrarily large, then from (2.48) we have

$$P_{out,c}^{(DT)}(R) \to 0.$$

$\bar{\gamma}_{se} \to \infty$**:** When the average SNR of the eavesdropper's channel is arbitrarily large, then from (2.48) we deduce that

$$P_{out,c}^{(DT)}(R) \to 1.$$

$R \to 0$**:** In this case, we have:

$$P_{out,c}^{(DT)}(R) \to e^{-\frac{\gamma_{sd}}{\gamma_{se}}},$$

which means that even for an arbitrarily small target secrecy rate, there will always be a strictly positive probability that the transmission is not secure, due to the fading nature of the channels.

$R \to \frac{1}{2}\log(1+\gamma_{sd})$**:** In this case, we have:

$$P_{out,c}^{(DT)}(R) \to 1.$$

Decode-and-Forward Relaying Performance

In this section we analyze the SOP and the CSOP performance of the DF scheme. As for DT, we first investigate the SOP, and then, we consider the CSOP.

Secrecy Outage Probability In the following theorem, we give a closed-form expression for the secrecy outage probability for the considered DF scheme.

Theorem 2.9 (DF Secrecy Outage Probability)**.**

The secrecy outage probability for the DF strategy is given by

$$\begin{aligned} P_{out}^{(DF)}(R) &= \frac{a_{\bar{\gamma}_{sr}}(\bar{\gamma}_{re}) - a(_{\bar{\gamma}_{sr}}\bar{\gamma}_{se})}{(\bar{\gamma}_{re} - \bar{\gamma}_{se})} \\ &+ \bar{\gamma}_{sr}\frac{a_{\bar{\gamma}_{sr}}(\bar{\gamma}_{se})\left(h(\bar{\gamma}_{se}, \bar{\gamma}_{sd}) - h(\bar{\gamma}_{se}, \bar{\gamma}_{rd})\right)}{2^{2R}(\bar{\gamma}_{re} - \bar{\gamma}_{se})(\bar{\gamma}_{rd} - \bar{\gamma}_{sd})} \\ &- \bar{\gamma}_{sr}\frac{a_{\bar{\gamma}_{sr}}(\bar{\gamma}_{re})\left(h(\bar{\gamma}_{re}, \bar{\gamma}_{sd}) - h(\bar{\gamma}_{re}, \bar{\gamma}_{rd})\right)}{2^{2R}(\bar{\gamma}_{re} - \bar{\gamma}_{se})(\bar{\gamma}_{rd} - \bar{\gamma}_{sd})}, \end{aligned} \tag{2.51}$$

where we define the following auxiliary functions

$$\begin{cases} h(x,y) = \dfrac{y\bar{\gamma}_{sr}}{x(y + \bar{\gamma}_{sr}) + \bar{\gamma}_{sr}2^{-2R}y}, \\ a_y(x) = \dfrac{x^2}{y2^{-2R} + x}e^{-\frac{\left(2^{-2R}-1\right)}{x}}. \end{cases} \tag{2.52}$$

Proof. Theorem 2.9 is proven in Appendix 2.B. ■

Conditional Secrecy Outage Probability In the following theorem, we give the conditional secrecy outage probability given $(\gamma_{sd}, \gamma_{sr}, \gamma_{rd})$ for the DF strategy.

Theorem 2.10.

The conditional secrecy outage probability for the DF scheme is given by:

$$P_{out,c}^{(DF)}(R) = \frac{\bar{\gamma}_{re}e^{-Q_{\min(\gamma_{sr},\gamma_d),\bar{\gamma}_{re}}(R)} - \bar{\gamma}_{se}e^{-Q_{\min(\gamma_{sr},\gamma_d),\bar{\gamma}_{se}}(R)}}{\bar{\gamma}_{re} - \bar{\gamma}_{se}}, \tag{2.53}$$

with $R \in [0, \mathcal{C}(\min(\gamma_{sr}, \gamma_d))]$ to ensure the reliability of the DF scheme.

Proof.

$$\begin{aligned} P_{out,c}^{(DF)}(R) &= P\{\min(\log(1+\gamma_{sr}), \log(1+\gamma_d)) < \log(1+\gamma_e) + 2R\} \\ &= P\left\{2^{-2R}(1 + \min(\gamma_{sr}, \gamma_d)) - 1 < \gamma_e\right\} \\ &= \int_{(1+\min(\gamma_{sr},\gamma_d))2^{-2R}-1}^{\infty} g_{\gamma_e}(\gamma_e)\, d\gamma_e, \end{aligned}$$

and the result of Theorem 2.10 follows from standard integration. ■

Remark 2.7.

We notice that when $P_r \to 0$, $P_{out,c}^{(DF)}(R) \to P_{out,c}^{(DT)}(R)$.

In the following proposition we give a condition for DF to improve the CSOP performance in comparison to DT.

Proposition 2.1.

If we have

$$|h_{rd}|^2 > 2^{2R}\mathbb{E}[|h_{re}|^2], \tag{2.54}$$

and if we assume that $\min(\gamma_{sr}, \gamma_d) = \gamma_d$, i.e., the source-relay link is strong, then there exists a power $P_r > 0$ used by the helper such that DF improves the CSOP performance.

Proof. We note $P_r = \beta P_{\max}$. From (2.53) we derive

$$\frac{\partial P_{out,c}^{(DF)}(R)}{\partial \beta}_{\beta \to 0} = \left(\frac{\mathbb{E}[|h_{re}|^2] - 2^{-2R}|h_{rd}|^2}{\bar{\gamma}_{se}} \right) e^{-\frac{2^{-2R}(1+\gamma_{sd})-1}{\bar{\gamma}_{se}}} \tag{2.55}$$

The relay is used if $P_{out,c}^{(DF)}(R)$ is a decreasing function of the power when evaluated in 0, i.e.,

$$\frac{\partial P_{out,c}^{(DF)}(R)}{\partial \beta}_{\beta \to 0} < 0 \tag{2.56}$$

Proposition 2.1 follows from (2.55) and (2.56). ■

Proposition 2.1 shows that we can opportunistically activate the relay to improve the CSOP performance with DF relaying when the strength of the relay-destination link is above a threshold depending on the strength of the relay-eavesdropper link.

Amplify-and-Forward Relaying Performance

In this section we analyze the SOP and the CSOP performance of the AF scheme. As for the previous schemes, we first investigate the SOP, and then, we consider the CSOP.

Secrecy Outage Probability The secrecy outage probability for the AF scheme is defined as

$$\begin{aligned}
P_{out}^{(AF)}(R) &= P\left\{R_d^{(AF)} - R_e^{(AF)} \leq 2R\right\} \\
&= P\left\{\mathcal{C}\left(\gamma_{sd} + \frac{\gamma_{sr}\gamma_{rd}}{1+\gamma_{sr}+\gamma_{rd}}\right) - \mathcal{C}\left(\gamma_{se} + \frac{\gamma_{sr}\gamma_{re}}{1+\gamma_{sr}+\gamma_{re}}\right) \leq R\right\} \\
&= P\left\{\left(\gamma_{sd} \leq \left(2^{2R}\left(1+\gamma_{se}+\frac{\gamma_{sr}\gamma_{re}}{1+\gamma_{sr}+\gamma_{re}}\right) - \left(1+\frac{\gamma_{sr}\gamma_{rd}}{1+\gamma_{sr}+\gamma_{rd}}\right)\right)\right)\right\} \\
&= \int\limits_{(\mathbb{R}^+)^4} \int\limits_{0}^{m} f_\gamma(\gamma_{se}) f_\gamma(\gamma_{rd}) f_\gamma(\gamma_{re}) f_\gamma(\gamma_{sr}) d\gamma_{sd} d\gamma_{se} d\gamma_{rd} d\gamma_{re} d\gamma_{sr}, \qquad (2.57)
\end{aligned}$$

with

$$m \triangleq \left(2^{2R}\left(1+\gamma_{se}+\frac{\gamma_{sr}\gamma_{re}}{1+\gamma_{sr}+\gamma_{re}}\right) - \left(1+\frac{\gamma_{sr}\gamma_{rd}}{1+\gamma_{sr}+\gamma_{rd}}\right)\right).$$

The integral expression (2.57) cannot be simplified. However, under a *high SNR* assumption, we can simplify the secrecy outage probability to obtain a closed-form expression. This expression is given in the following theorem.

Theorem 2.11 (AF Secrecy Outage Probability for high SNR)**.**

The secrecy outage probability for the AF strategy and for high SNR is given by

$$P_{out}^{(AF)}(R) = \frac{\bar{\gamma}_{d'}\left(a_{\bar{\gamma}_{d'}}(\bar{\gamma}_{e'}) - a_{\bar{\gamma}_{d'}}(\bar{\gamma}_{se})\right) - \bar{\gamma}_{sd}\left(a_{\bar{\gamma}_{sd}}(\bar{\gamma}_{e'}) - a_{\bar{\gamma}_{sd}}(\bar{\gamma}_{se})\right)}{(\bar{\gamma}_{e'} - \bar{\gamma}_{se})(\bar{\gamma}_{d'} - \bar{\gamma}_{sd})} \qquad (2.58)$$

with $a_y(x)$ is defined as in (2.52), and where $\bar{\gamma}_{d'}$ and $\bar{\gamma}_{e'}$ are defined as follows

$$\frac{1}{\bar{\gamma}_{d'}} \triangleq \frac{1}{\bar{\gamma}_{sr}} + \frac{1}{\bar{\gamma}_{rd}}, \qquad (2.59)$$

$$\frac{1}{\bar{\gamma}_{e'}} \triangleq \frac{1}{\bar{\gamma}_{sr}} + \frac{1}{\bar{\gamma}_{re}}. \qquad (2.60)$$

Proof. We give the proof of Theorem 2.11 in Appendix 2.C. ■

Conditional Secrecy Outage Probability We now consider the CSOP of AF relaying. In the following theorem, we derive the conditional secrecy outage probability given $(\gamma_{sd}, \gamma_{sr}, \gamma_{rd})$ under a *high SNR* assumption for the AF strategy.

Theorem 2.12.

The CSOP for the AF strategy and for high SNR is given by:

$$P_{out,c}^{(AF)}(R) = \frac{e^{-\frac{c_{AF}+\gamma_{sr}}{\bar{\gamma}_{se}}}\left(\bar{\gamma}_{se}e^{\frac{\gamma_{sr}}{\bar{\gamma}_{se}}} + \gamma_{sr}e^{\frac{1}{\bar{\gamma}_{re}}}E_1\left(1/\bar{\gamma}_{re} - \gamma_{sr}/\bar{\gamma}_{se}\right)\right)}{\bar{\gamma}_{se}}, \quad (2.61)$$

where $E_1(x) \triangleq \int_x^\infty \frac{e^{-t}}{t}dt$, $c_{AF} \triangleq 2^{-2R+R_d^{(AF)}} - 1$ with $R_d^{(AF)}$ defined in (2.80a), and $R \in \left[0, R_d^{(AF)}\right]$ to ensure the reliability of the AF scheme.

Proof. We give the proof of Theorem 2.12 in Appendix 2.D. ■

Cooperative Jamming Performance

In this section we analyze the SOP and the CSOP performance of the CJ scheme.

Secrecy Outage Probability First, we investigate the SOP performance of CJ. In the following theorem, we give the SOP for the CJ scheme.

Theorem 2.13 (CJ Secrecy Outage Probability [BBVM10])**.**

The secrecy outage probability for the CJ strategy is given by

$$\begin{aligned} P_{out}^{(CJ)}(R) =& 1 + \frac{e^{-c_{\mathrm{CJ}}}}{\bar{\gamma}_{re}\bar{\gamma}_{rd}l}\left(\frac{1}{g} - \frac{1}{hlg^2}\right)F(g+gh) \\ &+ \frac{e^{-c_{\mathrm{CJ}}}}{\bar{\gamma}_{re}\bar{\gamma}_{rd}l}\left(\left(\frac{1}{hlg^2} + \frac{1}{hg}\right)F\left(\frac{1+h}{h\bar{\gamma}_{re}}\right) - \frac{\bar{\gamma}_{re}}{g}\right), \end{aligned} \quad (2.62)$$

where

$$c_{\mathrm{CJ}} \triangleq \frac{2^{2R}-1}{\bar{\gamma}_{sd}},\ g \triangleq \frac{1+\bar{\gamma}_{rd}c}{\bar{\gamma}_{rd}}, h \triangleq \frac{\bar{\gamma}_{sd}}{\bar{\gamma}_{se}(1+\bar{\gamma}_{sd}c)},$$
$$E_1(x) = \int_x^\infty \frac{e^{-t}}{t}dt,\ l \triangleq 1 - \frac{1}{\bar{\gamma}_{re}gh},\ F(x) = e^x E_1(x).$$

Proof. The proof of Theorem 2.13 is given in [BBVM10] and [Gab12]. ■

Conditional Secrecy Outage Probability We now consider the CSOP. In the following theorem, we derive the conditional secrecy outage probability given $(\gamma_{sd}, \gamma_{sr}, \gamma_{rd})$ for the CJ strategy.

Theorem 2.14.

The conditional secrecy outage probability for the CJ scheme is given by:

$$P_{out,c}^{(CJ)}(R) = \frac{e^{-Q_{\frac{\gamma_{sd}}{1+\gamma_{rd}},\bar{\gamma}_{se}}(R)}}{1+\bar{\gamma}_{re}Q_{\frac{\gamma_{sd}}{1+\gamma_{rd}},\bar{\gamma}_{se}}(R)}, \tag{2.63}$$

where $R \in \left[0, \mathcal{C}\left(\frac{\gamma_{sd}}{1+\gamma_{rd}}\right)\right]$ to ensure the reliability of the CJ scheme.

Proof. The proof follows is similar to the proof of Theorems 2.8 and 2.10, and it is therefore omitted here. ■

Remark 2.8.

As for DF, when $P_r \to 0$, $P_{out,c}^{(CJ)}(R) \to P_{out,c}(R)^{(DT)}$.

Similar to Proposition 2.1, we derive in the following proposition a criterion for CJ to improve the CSOP performance in comparison to DT.

Proposition 2.2.

If we have

$$|h_{rd}|^2 < 2^{2R}\mathbb{E}[|h_{re}|^2]\left(\frac{2^{-2R}(1+\gamma_{sd})-1}{\gamma_{sd}}\right), \tag{2.64}$$

then there exists a power $P_r > 0$ used by the helper such that CJ improves the CSOP performance.

Proof. We note $P_r = \beta P_{\max}$. From (2.63) we have

$$\frac{\partial P_{out,c}^{(CJ)}(R)}{\partial \beta} \underset{\beta\to 0}{=} \left(\frac{2^{-2R}(\mathbb{E}[|h_{re}|^2](2^{2R}-1-\gamma_{sd})+\gamma_{sd}|h_{rd}|^2)}{\bar{\gamma}_{se}}\right) e^{-\frac{2^{-2R}(1+\gamma_{sd})-1}{\bar{\gamma}_{se}}} \tag{2.65}$$

The helper is used if $P_{out,c}^{(CJ)}(R)$ is a decreasing function of the power when evaluated in 0, i.e.,

$$\frac{\partial P_{out,c}^{(CJ)}(R)}{\partial \beta}_{\beta \to 0} < 0 \tag{2.66}$$

Proposition 2.2 follows from (2.65) and (2.66). ■

Numerical Examples

We will now consider the CSOP of the cooperative schemes, and we choose $\gamma_{sd} = \bar{\gamma}_{sd}$, $\gamma_{sr} = \bar{\gamma}_{sr}$, and $\gamma_{rd} = \bar{\gamma}_{rd}$ in our numerical examples.

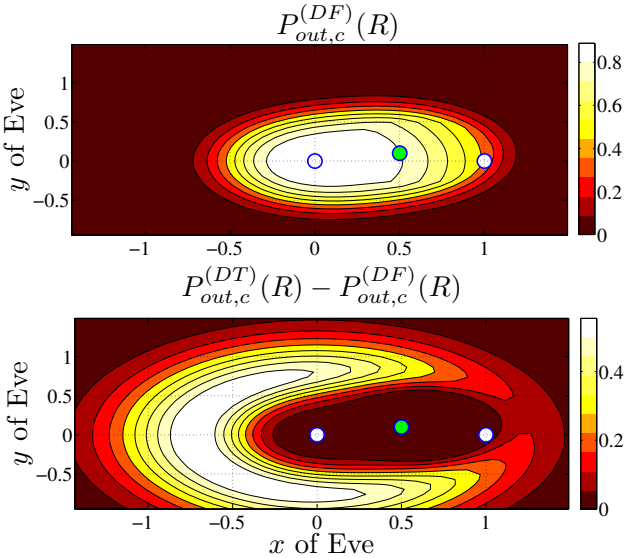


Figure 2.16: Conditional secrecy outage probability for DF for Case $C_{\mathcal{H}_2}$.

Numerical Example for Decode-and-Forward In Figure 2.16 we illustrate the conditional secrecy outage probability for DF in the Case $C_{\mathcal{H}_2}$ and we also show how DF performs in comparison with DT.

The upper plot in Figure 2.16 depicts the CSOP for the DF scheme. The darker a point in the plot is, the lower the CSOP for an eavesdropper located at this point is. We observe that the CSOP is particularly high when Eve is located in the middle of the transmission. When the eavesdropper gets further away, the CSOP decreases. Thus, the CSOP has a similar behavior as for the wiretap channel without relay, i.e., for the DT strategy.

In order to quantify the benefit provided by the DF scheme compared to DT, we now analyze the lower plot in Figure 2.16, where the difference $P_{out,c}^{(DT)}(R) -$

Case	$\max_{\mathcal{E}\in\mathcal{P}} D_\varepsilon$	$E_{\mathcal{E}\in\mathcal{P}}[D_\varepsilon]$
$C_{\mathcal{H}_1}$	14.9%	5.2%
$C_{\mathcal{H}_2}$	15.8%	5.2%

Table 2.4: Validity of the high SNR approximation with $\mathcal{E} \in \mathcal{P}$.

$P_{out,c}^{(DF)}(R)$ is represented. A large difference is equivalent to a large decrease of the CSOP using the DF scheme, which corresponds to the desired effect of the scheme.

We can distinguish 3 main areas for the location of the eavesdropper:

- When the eavesdropper is in the middle of the transmission, secrecy is highly compromised, and increasing the reliability via DF relaying is useless.
- When the eavesdropper is far away, the CSOP was already close to 0 without the relay, and the CSOP can thus not be further decreased.
- There is a half circular area around the source for Eve's location, for which the helper can securely relay the source message. This leads to a decrease of the CSOP, up to a difference $P_{out,c}^{(DT)}(R) - P_{out,c}^{(DF)}(R) \approx 0.4$.

Numerical Example for Amplify-and-Forward First we measure the accuracy of the high SNR approximation in Table 2.4. We define the relative error as $D_\varepsilon \triangleq \frac{\left|P_{out}^{(AF)}(R) - P_{out,s}^{(AF)}(R)\right|}{P_{out,s}^{(AF)}(R)}$, where $P_{out,s}^{(AF)}(R)$ is numerically evaluated using Monte-Carlo simulations with 50000 iterations. The average relative error of the approximation in our case of study is around 0.05 with a maximum relative error of 0.158 in Case $C_{\mathcal{H}_2}$, thus the high SNR approximation is satisfying. In Figure 2.17 we compare the secrecy outage probability of AF and DT depending on the location of the eavesdropper. $\mathcal{S}$ and $\mathcal{D}$ are represented with the white circles and $\mathcal{H}$ with the green circle. For each location of $\mathcal{E}$, we compare the SOP of DT and AF. We observe that in both cases there exists an area for which AF strictly improves the SOP in comparison to DT. When $\mathcal{E}$ is in the middle of the transmission, the SOP does not decrease since secure transmission is not possible. When $\mathcal{E}$ is far away, AF cannot improve the SOP performance since the SOP is already close to zero. We should note that the comparison between both schemes is fair since the average power constraint is equivalent for both schemes. An opportunistic use of a relaying node depending on the location of $\mathcal{E}$ could thus decrease the SOP. Moreover if several helping nodes are potentially available, this performance could be further increased by relay selection.

Numerical Example for Cooperative Jamming In Figure 2.18 we illustrate the CSOP performance for the CJ scheme in the Case $C_{\mathcal{H}_2}$. The first observation is that CJ performs differently than the relaying schemes depending on Eve's location.

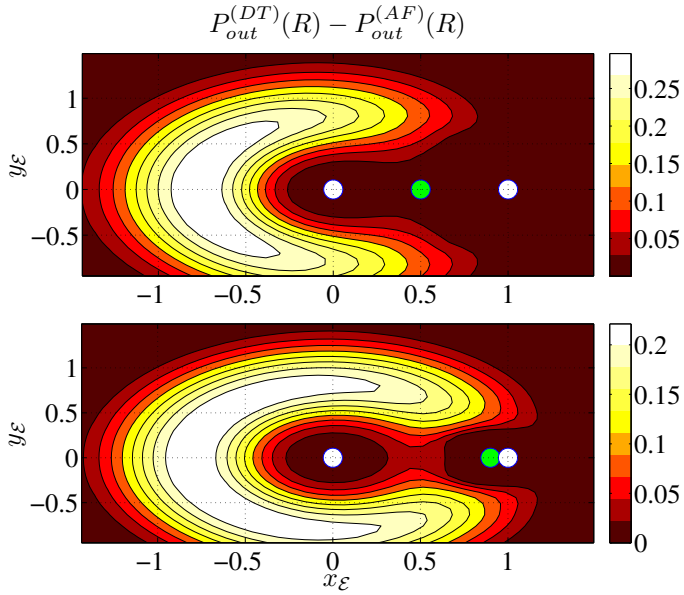


Figure 2.17: SOP increase for AF for Cases $C_{\mathcal{H}_2}$ and $C_{\mathcal{H}_3}$. The upper plot depicts the Case $C_{\mathcal{H}_2}$ while the lower plot shows the Case $C_{\mathcal{H}_3}$.

In particular, when the eavesdropper is close to the helper, the performance is significantly improved due to the efficiency of jamming Eve. When the eavesdropper is further away, no jamming power is used by the helper, and the scheme reduces to DT as shown in the lower plot in Figure 2.18. The difference of CSOP over DT is $P_{out,c}^{(DT)}(R) - P_{out,c}^{(CJ)}(R) \approx 0.7$, which is a more substantial improvement of performance than the relaying schemes.

Secrecy Outage Decrease In Figure 2.19 we illustrate the difference in terms of CSOP for the optimal strategy $\tilde{s}_{\mathcal{H}}$ in comparison to DT in the Case $C_{\mathcal{H}_2}$. We make the following observations:

- Using the helper in the Case $C_{\mathcal{H}_2}$ leads to an improvement in terms of CSOP up to around 0.7 when the eavesdropper is located close to the helper using CJ.
- When DF relaying is chosen, the decrease of CSOP is less compared to CJ, however there is still a benefit in terms of CSOP performance.
- The gain is extremely low when the eavesdropper is located far away from the transmission. The explanation is two-fold. First the conditional secrecy outage probability for DT in this case is already low, and it can therefore be

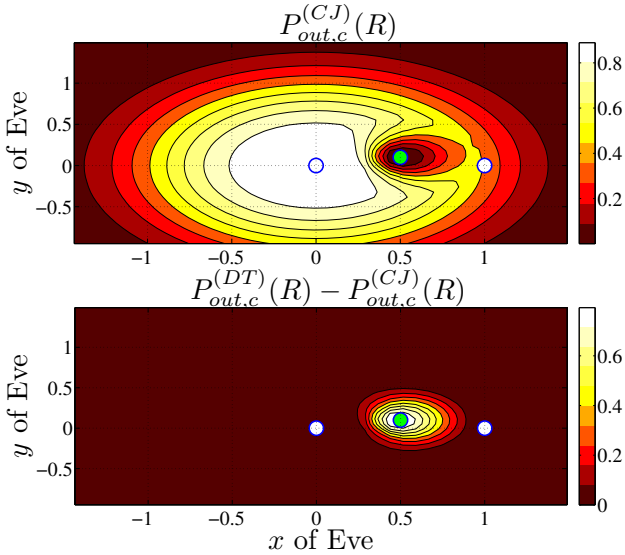


Figure 2.18: Conditional secrecy outage probability for CJ for $C_{\mathcal{H}_2}$.

hardly improved. Furthermore, CJ is not efficient for these locations of the eavesdropper, and the helper is thus bounded to increase the reliability of the transmission.

Conclusions We can draw some general conclusions from our observations concerning the secrecy outage performance of the different schemes. First the presence of a helper allows higher secrecy rates, and it also leads to lower secrecy outage probabilities. When the eavesdropper is close to the helper, CJ decreases the probability of a secrecy outage by significantly reducing the amount of information obtained by the eavesdropper. When the eavesdropper is further away from the helper, the relaying schemes improve the reliability of the main transmission, and therefore they lower the probability of a secrecy outage by increasing the achievable secrecy rates.

2.6.3 System Optimization

In this section we investigate the global optimization of the system. We first introduce a new performance measure, namely the secure throughput. Then, we describe how the legitimate nodes would proceed to optimize the system performance in terms of CSOP and secure throughput.

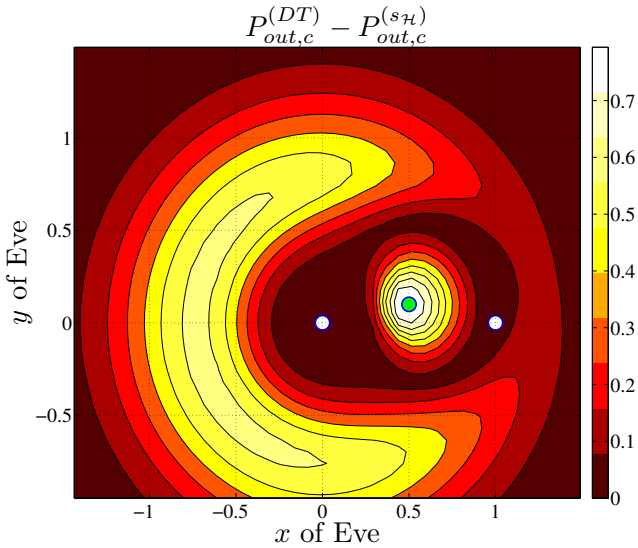


Figure 2.19: Conditional secrecy outage probability decrease for the optimal strategy for $C_{\mathcal{H}_2}$.

Secure Throughput

We recapitulate our assumptions:

1. $(\gamma_{sd}, \gamma_{sr}, \gamma_{rd})$ are known to the legitimate nodes.
2. The helper can choose between the cooperative strategies and three possible locations given by the Cases $C_{\mathcal{H}_1}$, $C_{\mathcal{H}_2}$ and $C_{\mathcal{H}_3}$.
3. The performance measure is given by the conditional secrecy outage probability, which depends on the eavesdropper location, the fixed secrecy rate R and the power allocation at the helper characterized by β defined as follows:

$$P_r = \beta P_{\max}. \tag{2.67}$$

First, we have the following lemma:

Lemma 2.1.

For any strategy $s_\mathcal{H} \in \{\text{DT,DF,AF,CJ}\}$ chosen by the helper, $P_{out,c}^{(s_\mathcal{H})}(R)$ is an increasing function in R.

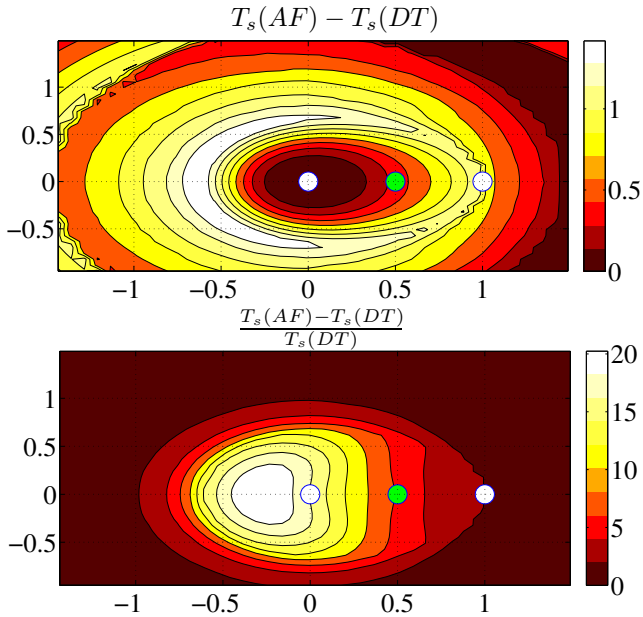


Figure 2.20: Secure throughput increase and relative increase for Case $C_{\mathcal{H}_2}$ for AF.

The consequence of Lemma 2.1 is that the optimal rate to optimize the system performance in terms of CSOP is $R = 0$, which is clearly not a satisfactory result. Therefore, we introduce the following performance measure, which evaluates the performance in terms of throughput.

Definition 2.21.

We define the secure throughput of the strategy $s_{\mathcal{H}}$ given $(\gamma_{sd}, \gamma_{sr}, \gamma_{rd})$ for a secrecy rate R by

$$T_s \triangleq R\left(1 - P_{out,c}^{(s_{\mathcal{H}})}(R)\right). \tag{2.68}$$

The secure throughput characterizes the rate of information transferred to the destination without secrecy outage.

Secure Throughput Performance In Figure 2.20 we illustrate the secure throughput measure by comparing the secure throughput of AF and DT depending on the location of the eavesdropper. The upper plot depicts the difference $T_s(AF) - T_s(DT)$ in the Case $C_{\mathcal{H}_1}$ while the lower plot represents the relative difference $\frac{T_s(AF)-T_s(DT)}{T_s(DT)}$. We observe that using AF relaying leads to an increase up to 1.5

bits per channel use. This corresponds to a relative increase factor of 20 for the optimal locations of $\mathcal{E}$.

Optimization

Using Definition 2.21, we are now able to develop the optimization steps in this section. We describe how the legitimate nodes proceed to optimize the system performance in terms of CSOP and secure throughput. We assume that the helper is at a fixed location. Three parameters can be optimized by the legitimate nodes: the target secrecy rate R, the helper's strategy $s_{\mathcal{H}}$ and the power allocation β. We give in the following proposition the successive steps to optimize the system performance, in terms of conditional secrecy outage probability and secure throughput.

Proposition 2.3.

The optimal $\left(\tilde{R}, \tilde{s}_{\mathcal{H}}, \tilde{\beta}_{s_{\mathcal{H}}}\right)$, where R is the secrecy rate, $s_{\mathcal{H}}$ is the strategy of the helper, and β represents the power allocation, are the solution of:

$$\tilde{\beta}_{s_{\mathcal{H}}}(R) = \arg\min_{\beta_{s_{\mathcal{H}}}} P_{out,c}^{(s_{\mathcal{H}})}\left(R, \beta_{s_{\mathcal{H}}}\right) \tag{2.69}$$

$$\tilde{s}_{\mathcal{H}}(R) = \arg\min_{s_{\mathcal{H}}} P_{out,c}^{(s_{\mathcal{H}})}\left(R, \tilde{\beta}_{s_{\mathcal{H}}}\right) \tag{2.70}$$

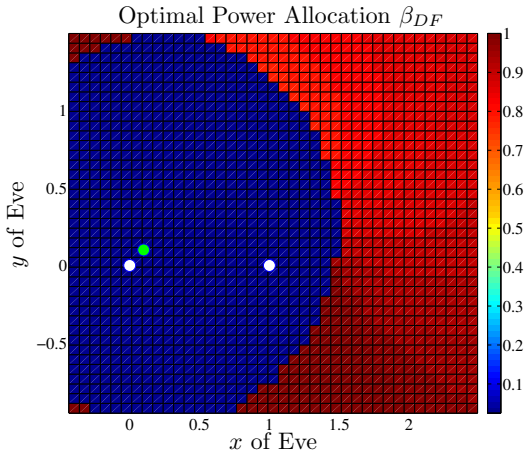
$$\tilde{R} = \arg\max_{R} T_s = \arg\max_{R} R\left(1 - P_{out,c}^{(\tilde{s}_{\mathcal{H}})}\left(R, \tilde{\beta}_{\tilde{s}_{\mathcal{H}}}\right)\right). \tag{2.71}$$

Therefore, the optimization must follow the successive steps:

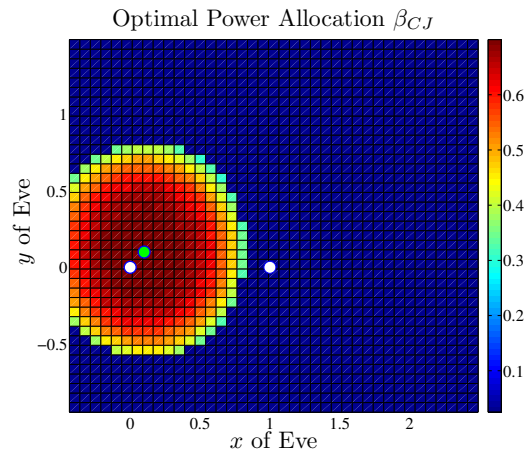
1. For every strategy $s_{\mathcal{H}}$ of the helper, choose the power allocation $\tilde{\beta}_{s_{\mathcal{H}}}$ that minimizes the conditional secrecy outage probability for a given secrecy rate R.
2. Once the power allocations are optimized, choose the strategy $\tilde{s}_{\mathcal{H}}$ that minimizes the conditional secrecy outage probability for a given secrecy rate R.
3. Finally, choose the secrecy rate maximizing the secure throughput.

Proof. We refer to [Gab12] for the proof. ■

The positioning and the strategy of the helper have been discussed in previous sections. In the following, we will focus on the parameters β and R.



(a) Decode-and-forward.



(b) Cooperative jamming.

Figure 2.21: Optimal power allocation β at the helper, in the Case $C_{\mathcal{H}_1}$, for (a) Decode-and-forward and (b) Cooperative jamming.

Discussion on the Optimization of the Power Allocation β

In this section we illustrate the first step of the optimization 2.3, namely the power allocation β for the helping node. Finding a closed-form solution for

$$\tilde{\beta}_{s_{\mathcal{H}}} = \arg\min_{\beta_{s_{\mathcal{H}}}} P_{out,c}^{(s_{\mathcal{H}})}\left(R, \beta_{s_{\mathcal{H}}}\right),$$

using (2.53) and (2.63) is not possible due to the complexity of the expressions.

However, we obtain the following condition for the optimal β_{CJ}:

Proposition 2.4.

If $\beta_{CJ} \in [0,1]$ is an optimal power allocation for the CJ scheme then β_{CJ} is a solution of the polynomial equation

$$a_3 X^3 + a_2 X^2 + a_1 X + a_0 = 0, \tag{2.72}$$

where

$$\begin{aligned}
a_0 &= 2^{2R}\bar{\gamma}_{se}(\mathbb{E}[|h_{re}|^2](2^{2R} - 1 - \gamma_{sd}) + \gamma_{sd}\,|h_{rd}|^2),\\
a_1 &= |h_{rd}|^2 \left(\bar{\gamma}_{se}\gamma_{sd}(\mathbb{E}[|h_{re}|^2](-2^{2R} + 1 + \gamma_{sd}))\right)\\
&\quad + |h_{rd}|^2 \left(2^{2R}\bar{\gamma}_{se}(\mathbb{E}[|h_{re}|^2](-3 + 3 \times 2^{2R} - \gamma_{sd}) + \gamma_{sd}\,|h_{rd}|^2)\right),\\
a_2 &= (-1 + 2^{2R})\mathbb{E}[|h_{re}|^2](3 \times 2^{2R}\bar{\gamma}_{se} - \gamma_{sd})\,|h_{rd}|^4, \text{ and}\\
a_3 &= 2^{2R}(-1 + 2^{2R})\bar{\gamma}_{se}\mathbb{E}[|h_{re}|^2]\,|h_{rd}|^6.
\end{aligned}$$

Proof. We refer to [Gab12] for the proof. ■

We use our numerical example to illustrate the optimal power allocation. In Figure 2.21a and 2.21b we illustrate the behavior of β_{DF} and β_{CJ}, respectively, depending on the eavesdropper's location for $C_{\mathcal{H}_1}$. For DF, we can observe that in the regions where DF performs well (see, e.g., Figure 2.16), the power used by the relay is a high fraction of the maximal available power, close to $\beta_{DF} = 0.8$.

In comparison to DF, CJ needs less power ($\beta_{DF} \approx 0.6$) where it outperforms the other schemes, i.e., Eve being close to the helper. This observation could be justified by the fact that there is no need to use a large amount of power to confuse the eavesdropper when it is located close to the helper, as using additional power might only disrupts the main transmission.

With the aim of verifying this justification, we represent in Figure 2.22 the optimal power allocation β_{CJ} for the Case $C_{\mathcal{H}_2}$. We observe that for the optimal regions, a small fraction of the available power is used $\beta_{CJ} \approx 0.1$. This means that CJ performs well, and that, moreover, it does not require a high power consumption.

Discussion on the Optimization of the Secrecy Rate R Finally we discuss the optimization of the last parameter: the target secrecy rate R. The objective is to design R such that $R = \tilde{R}$ according to

$$\tilde{R} = \arg\max_R T_s = \arg\max_R R\left(1 - P_{out,c}^{(\tilde{s}_{\mathcal{H}})}\left(R, \tilde{\beta}_{\tilde{s}_{\mathcal{H}}}\right)\right). \tag{2.73}$$

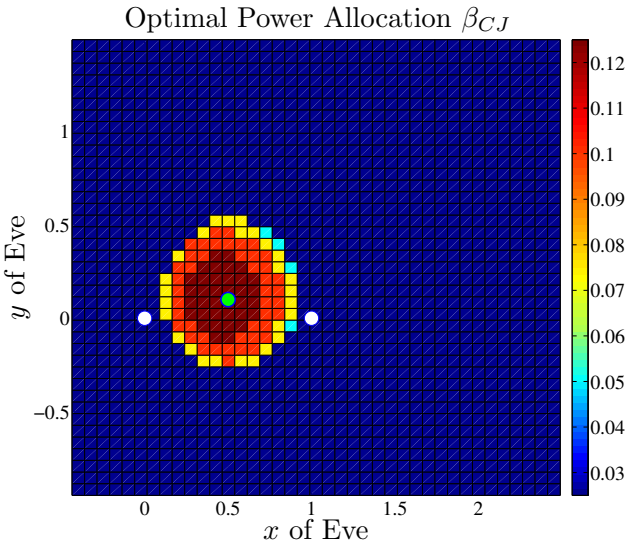


Figure 2.22: Optimal power allocation β at the helper, in the Case $C_{\mathcal{H}_2}$ and for cooperative jamming.

In the following proposition, we argue that there exists at least one optimal value of R which maximizes the secure throughput T_s.

Proposition 2.5.

There exists (at least) one optimal target secrecy rate $\tilde{R}$ for every strategy $s_{\mathcal{H}} \in \{DT, DF, AF, CJ\}$, such that

$$\tilde{R} = \arg\max_{R} T_s. \tag{2.74}$$

Proof. We refer to [Gab12] for the proof. ■

In Figure 2.23 we show how cooperation increases the secure throughput by computing the difference between the secure throughput T_s obtained with the optimization protocol and the secure throughput with direct transmission. Figure 2.23 shows that, in general, higher secure throughput is achieved with cooperation. Moreover, it seems that the secure throughput increase is higher in the regions where DF is optimal compared to CJ. We distinguish in particular the optimal CJ area located around the helper, and the optimal DF region when Eve is further away. However, we observe that there is an area surrounding the source and the

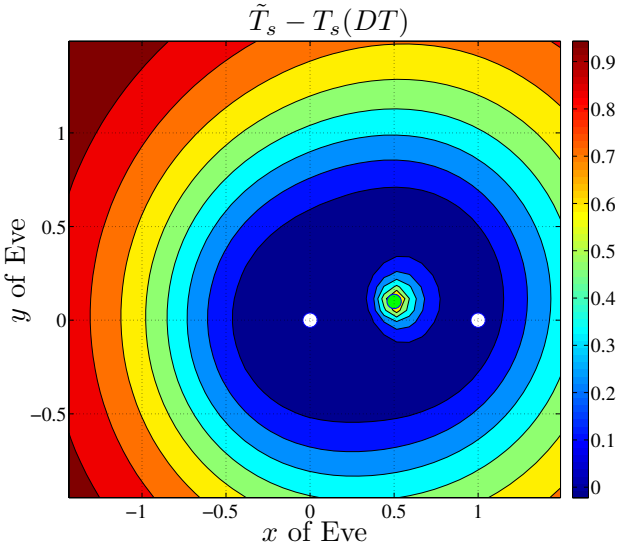


Figure 2.23: Secure throughput increase with cooperation and optimal design parameters.

destination for which the secure throughput is not increased by cooperation, since $\tilde{T}_s - T_s(DT) = 0$.

Conclusions

In Section 2.6 we investigated the cooperative schemes introduced in Section 2.5 for wireless channels. Our model takes into consideration the fading nature of the channels, and the limited CSI on the eavesdropper's channels, which are both reasonable and practical assumptions. Based on our study, we are able to highlight several fundamental weaknesses of the considered model.

1. **External Eavesdropper Assumption**: This assumption is hardly combinable with the perfect CSI assumption on Eve's channels, even though this is a common assumption in the existing literature.

2. **CSI Knowledge**: Full CSI knowledge on Eve's channels is not easily justifiable if Eve is not a legitimate user in the system. With limited CSI assumptions, the analysis of the cooperative schemes is difficult as shown in our case study.

3. **Trustable Helper**: The assumption of the existence of a cooperative node whose sole aim is to help the secrecy of the legitimate transmission is somewhat optimistic as today's communications networks are constituted of selfish nodes. Moreover, we assumed in our study that this helper would be unconditionally cooperative and trustable. If the cooperative node cannot be trusted, it is unclear where cooperation for secrecy is possible, see e.g., [HY10], [YLE11].

4. **Secrecy Measures**: While we were able to investigate the secrecy performance of cooperation through new secrecy measures, namely the CSOP and the secure throughput, these measures are not fully satisfying to design the transmission system, e.g., the secure channel codes.

To remedy these weaknesses, we investigate in this thesis a novel scenario: the cognitive radio channel with secrecy constraints, where the helper and the eavesdropper are legitimate secondary nodes in the system. This model allows us to alleviate the shortcomings of the relay-eavesdropper channel model as it will be described in the following chapters.

2.A Achievable Secrecy Rates for DT, DF, AF and CJ.

In this appendix, we give achievable secrecy rates of the cooperative transmission schemes, namely direct transmission, decode-and-forward relaying, amplify-and-forward relaying, and cooperative jamming.

Direct Transmission

Theorem 2.15 (Instantaneous Secrecy Rate for DT [BB11])**.**

For quasi-static Rayleigh fading channels with instantaneous SNRs γ_{sd} and γ_{se} on the links from $\mathcal{S}$ to $\mathcal{D}$ and from $\mathcal{S}$ to $\mathcal{E}$, respectively, an instantaneous achievable secrecy rate is given by

$$R_s^{(DT)} = \frac{1}{2}\left(R_d^{(DT)} - R_e^{(DT)}\right)^+, \tag{2.75}$$

where

$$R_d^{(DT)} = \log\left(1+\gamma_{sd}\right), \tag{2.76a}$$
$$R_e^{(DT)} = \log\left(1+\gamma_{se}\right). \tag{2.76b}$$

Remark 2.9.

We can make the following two remarks regarding the achievable instantaneous secrecy rate for DT:

1. The factor 1/2 comes from the fact that the source only transmits during the first time slot.
2. The achievable secrecy rate in (2.75) is the instantaneous secrecy capacity in this case.

Decode-and-Forward The instantaneous achievable secrecy rate is given in the following theorem.

Theorem 2.16 (Instantaneous Secrecy Rate for DF [DHPP10])**.**

For quasi-static Rayleigh fading channels with instantaneous SNRs γ_{sd}, γ_{rd}, γ_{sr}, γ_{se} and γ_{re}, an achievable instantaneous secrecy rate for the described decode-and-forward scheme with repetition coding is given by

$$R_s^{(DF)} = \frac{1}{2}\left(R_d^{(DF)} - R_e^{(DF)}\right)^+, \tag{2.77}$$

where

$$R_d^{(DF)} = \min\left(\log\left(1+\gamma_{sr}\right), \log\left(1+\gamma_{sd}+\gamma_{rd}\right)\right), \tag{2.78a}$$

$$R_e^{(DF)} = \log\left(1+\gamma_{se}+\gamma_{re}\right). \tag{2.78b}$$

As noted in [DHPP10], this particular DF scheme is mathematically equivalent to a 1×2 single-input multiple-output wiretap channel, for which the secrecy capacity (and thus achievable secrecy rates) is known (e.g., [OH08], [SLU09]). (2.78a) represents simply the achievable rate for DF without eavesdropper, while (2.78b) characterizes the amount of information leaked to the eavesdropper during the transmission.

Amplify-and-Forward

Theorem 2.17 (Instantaneous Secrecy Rate for AF [DHPP10])**.**

For quasi-static Rayleigh fading channels with instantaneous SNRs γ_{sd}, γ_{rd}, γ_{sr}, γ_{se} and γ_{re}, an achievable secrecy rate for the described amplify-and-forward scheme is given by

$$R_s^{(AF)} = \frac{1}{2}\left(R_d^{(AF)} - R_e^{(AF)}\right)^+, \tag{2.79}$$

where

$$R_d^{(AF)} = \log\left(1+\gamma_{sd}+\frac{\gamma_{sr}\gamma_{rd}}{1+\gamma_{sr}+\gamma_{rd}}\right), \tag{2.80a}$$

$$R_e^{(AF)} = \log\left(1+\gamma_{se}+\frac{\gamma_{sr}\gamma_{re}}{1+\gamma_{sr}+\gamma_{re}}\right). \tag{2.80b}$$

Cooperative Jamming The achievable instantaneous secrecy rate for CJ is given in the following theorem.

Theorem 2.18 (Instantaneous Secrecy Rate for CJ [VBBM11])**.**

For quasi-static Rayleigh fading channels with instantaneous SNRs γ_{sd}, γ_{rd}, γ_{se} and γ_{re}, an achievable secrecy rate for the described cooperative jamming scheme is given by

$$R_s^{(CJ)} = \frac{1}{2}\left(R_d^{(CJ)} - R_e^{(CJ)}\right)^+, \tag{2.81}$$

where

$$R_d^{(CJ)} = \log\left(1 + \frac{\gamma_{sd}}{1+\gamma_{rd}}\right) \tag{2.82a}$$

$$R_e^{(CJ)} = \log\left(1 + \frac{\gamma_{se}}{1+\gamma_{re}}\right). \tag{2.82b}$$

2.B Proof of Theorem 2.9

Proof. In order to prove Theorem 2.9, we need to define the following random variables:

$$\gamma_d \triangleq \gamma_{sd} + \gamma_{rd} \tag{2.83}$$

$$\gamma_e \triangleq \gamma_{se} + \gamma_{re} \tag{2.84}$$

We give in the following the probability density functions of the two newly defined random variables.

Lemma 2.2.

The probability density function of γ_d (resp. γ_e) is given by

$$g_{\gamma_d}(\gamma) = g_{\gamma_{sd}+\gamma_{rd}}(\gamma) = \frac{1}{\bar{\gamma}_{rd} - \bar{\gamma}_{sd}}\left(e^{-\frac{\gamma}{\bar{\gamma}_{rd}}} - e^{-\frac{\gamma}{\bar{\gamma}_{sd}}}\right), \tag{2.85}$$

$$g_{\gamma_e}(\gamma) = g_{\gamma_{se}+\gamma_{re}}(\gamma) = \frac{1}{\bar{\gamma}_{re} - \bar{\gamma}_{se}}\left(e^{-\frac{\gamma}{\bar{\gamma}_{re}}} - e^{-\frac{\gamma}{\bar{\gamma}_{se}}}\right). \tag{2.86}$$

Lemma 2.2 results from the probability density function of the sum of two independent random variables being the convolution of their separate density functions.

According to (2.45), the secrecy outage probability can be formulated as:

$$P_{out}^{(DF)}(R) = P\left\{\left(\mathcal{C}\left(\min\left(\gamma_{sr}, \gamma_{sd}+\gamma_{rd}\right)\right)\right) < \mathcal{C}\left(\gamma_{se}+\gamma_{re}\right) + 2R\right\}. \tag{2.87}$$

We can notice that this formulation takes into account the possibility of a secrecy outage occurring during the first time slot. Indeed, we are in secrecy outage after the first phase if:

$$R_d^{(DF)} - \log\left(1+\gamma_{se}\right) < 2R. \tag{2.88}$$

Similarly, we are in secrecy outage after the second phase if:

$$R_d^{(DF)} - \log\left(1+\gamma_{se}+\gamma_{re}\right) < 2R. \tag{2.89}$$

Since (2.88) implies (2.89), we can deduce that we are in secrecy outage if and only if (2.89) holds. The outage probability for the DF scheme can therefore be written as:

$$\begin{aligned} P_{out}^{(DF)}(R) &= P\left\{\min\left(\log\left(1+\gamma_{sr}\right),\log\left(1+\gamma_d\right)\right) < \log\left(1+\gamma_e\right)+2R\right\} \\ &= P\left\{2^{-2R}\left(1+\gamma_d\right)-1 < \gamma_e \cap \gamma_{sr} > \gamma_d\right\} \\ &+ P\left\{2^{-2R}\left(1+\gamma_{sr}\right)-1 < \gamma_e \cap \gamma_{sr} < \gamma_d\right\}, \end{aligned}$$

which gives

$$\begin{aligned} P_{out}^{(DF)}(R) = &\int_{(\mathbb{R}^+)} \int_{\gamma_d}^{\infty} \int_{(1+\gamma_d)2^{-2R}-1}^{\infty} g_{\gamma_d}(\gamma_d)\, g_{\gamma_e}(\gamma_e)\, f_{\gamma_{sr}}(\gamma_{sr})\, d\gamma_e d\gamma_{sr} d\gamma_d \\ &+ \int_{(\mathbb{R}^+)} \int_{0}^{\gamma_d} \int_{(1+\gamma_{sr})2^{-2R}-1}^{\infty} g_{\gamma_d}(\gamma_d)\, g_{\gamma_e}(\gamma_e)\, f_{\gamma_{sr}}(\gamma_{sr})\, d\gamma_e d\gamma_{sr} d\gamma_d. \end{aligned}$$

Theorem 2.9 follows from standard integration calculus. ■

2.C Proof of Theorem 2.11

Proof. The secrecy outage probability for the AF scheme is defined as:

$$\begin{aligned} &P_{out}^{(AF)}(R) = P\left\{\left(R_d^{(AF)} - R_e^{(AF)} \le 2R\right)\right\} \\ &= P\left\{\left(\mathcal{C}\left(\gamma_{sd}+\frac{\gamma_{sr}\gamma_{rd}}{1+\gamma_{sr}+\gamma_{rd}}\right) - \mathcal{C}\left(\gamma_{se}+\frac{\gamma_{sr}\gamma_{re}}{1+\gamma_{sr}+\gamma_{re}}\right) \le R\right)\right\} \\ &\approx P\left\{\left(\log\left(1+\gamma_{sd}+\frac{\gamma_{sr}\gamma_{rd}}{\gamma_{sr}+\gamma_{rd}}\right) - \log\left(1+\gamma_{se}+\frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}}\right) \le 2R\right)\right\}. \end{aligned}$$

where the last inequality is a consequence of the high SNR assumption.

We will use the following lemma [HA03]:

Lemma 2.3.

If X_1 and X_2 are two independent exponential random variables with parameters γ_1 and γ_2, respectively, (i.e., with respective means $1/\gamma_1$ and $1/\gamma_2$), then the harmonic mean X of X_1 and X_2 given by $X = \frac{X_1 X_2}{X_1+X_2}$ has for cumulative distribution function (cdf) $F_X(x)$:

$$F_X(x) = 1 - 2x\sqrt{(\gamma_1\gamma_2)}e^{-x/(\gamma_1+\gamma_2)}K_1\left(2x\sqrt{(\gamma_1\gamma_2)}\right)$$

where $K_1(.)$ is the first order modified Bessel function of the second kind.

Applying the lemma for $X = \frac{\gamma_{sr}\gamma_{rd}}{\gamma_{sr}+\gamma_{rd}}$, we obtain

$$\begin{aligned} F_X(x) &= 1 - 2x\sqrt{(1/\gamma_{sr}\gamma_{rd})}e^{-x/\left(\frac{1}{\gamma_{sr}+\gamma_{rd}}\right)}K_1\left(2x\sqrt{(1/\gamma_{sr}\gamma_{rd})}\right) \\ &\approx 1 - e^{-x/\left(\frac{1}{\gamma_{sr}+\gamma_{rd}}\right)}, \end{aligned}$$

since $K(x) \approx 1/x$ for small x (high SNR assumption).

This cdf corresponds to the CDF of an exponential random variable $\gamma_{d'}$ with parameter $\frac{1}{\bar{\gamma}_{d'}} = \frac{1}{\bar{\gamma}_{sr}} + \frac{1}{\bar{\gamma}_{rd}}$.

Similarly, we define $\gamma_{e'}$ with parameter $\frac{1}{\bar{\gamma}_{e'}} = \frac{1}{\bar{\gamma}_{sr}} + \frac{1}{\bar{\gamma}_{re}}$.

The secrecy outage probability becomes:

$$\begin{aligned} P_{out}^{(AF)}(R) &\approx P\left\{\log(1+\gamma_{sd}+\gamma_{d'}) - \log(1+\gamma_{se}+\gamma_{e'}) \le 2R\right\} \\ &= P\left\{\log(1+\gamma_{d''}) - \log(1++\gamma_{e''}) \le 2R\right\} \\ &= P\left\{2^{-2R}(1+\gamma_{d''}) - 1 < \gamma_{e''}\right\} \\ &= \int_0^{\infty} \int_{(1+\gamma_{d''})2^{-2R}-1}^{\infty} g_{\gamma_{d''}}(\gamma_{d''})\, g_{\gamma_e}(\gamma_{e''})\, d\gamma_{e''} d\gamma_{d''} \end{aligned}$$

since $\gamma_{d''} \triangleq \gamma_{sd} + \gamma_{d'}$ and $\gamma_{e''} \triangleq \gamma_{se} + \gamma_{e'}$ have for PDF

$$g_{\gamma_{i''}}(\gamma) = g_{\gamma_{si}+\gamma_{i'}}(\gamma) = \frac{1}{\bar{\gamma}_{i'} - \bar{\gamma}_{si}}\left(e^{-\frac{\gamma}{\bar{\gamma}_{i'}}} - e^{-\frac{\gamma}{\bar{\gamma}_{si}}}\right), \tag{2.90}$$

where $i \in \{e, d\}$. (2.90) results from the pdf of the sum of two independent random variables being the convolution of their separate density functions. The result of Theorem 2.11 follows from standard integral calculations. ■

2.D Proof of Theorem 2.12

Proof. The conditional outage probability for the AF scheme is defined as:

$$P_{out,c}^{(AF)}(R) = P\left\{\left(R_d^{(AF)} - R_e^{(AF)} \leq 2R|\gamma_{sd},\gamma_{sr},\gamma_{rd}\right)\right\}$$
$$= P\left\{\left(\gamma_{se} + \frac{\gamma_{sr}\gamma_{re}}{1+\gamma_{sr}+\gamma_{re}}\right) \geq c_{AF}\right\},$$

with c_{AF} defined in Theorem 2.12.

First we have

$$\frac{\gamma_{sr}\gamma_{re}}{1+\gamma_{sr}+\gamma_{re}} \approx \frac{\gamma_{re}}{1+\frac{\gamma_{re}}{\gamma_{sr}}}, \tag{2.91}$$

as a consequence of the high SNR assumption.
Since $\frac{\gamma_{re}}{\gamma_{sr}} \sim \exp(\bar{\gamma}_{re}\gamma_{sr})$, it follows that the random variable $U \triangleq 1 + \frac{\gamma_{re}}{\gamma_{sr}}$ is Benktander -Weibull distributed with pdf given by

$$f_U(x) = \frac{1}{\bar{\gamma}_{re}\gamma_{sr}} e^{(\frac{1-x}{\bar{\gamma}_{re}\gamma_{sr}})} \text{ for } x > 1.$$

The pdf $g_Y(y)$ of the random variable $Y \triangleq \frac{\gamma_{re}}{U}$ is then obtained according to the ratio distribution formula as

$$g_Y(y) = \int_{-\infty}^{\infty} f_{\gamma_{re}}(yz) f_U(z) |z| \, dz$$
$$= e^{-(\frac{y}{\bar{\gamma}_{re}\gamma_{sr}})} \frac{(\gamma_{sr} + \bar{\gamma}_{re}\gamma_{sr} + y)}{\bar{\gamma}_{re}(\gamma_{sr}+y)^2}.$$

Finally the pdf $h_T(t)$ of the random variable $T \triangleq Y + \gamma_{se}$ is given by

$$h_T(t) = \int_0^{\infty} g_Y(y) f_{\gamma_{se}}(t-y) dy. \tag{2.92}$$

The conditional outage probability for the AF scheme is then written as

$$P_{out,c}^{(AF)}(R) = \int_{c_{AF}}^{\infty} h_T(t) dt, \tag{2.93}$$

and the result of Theorem 2.12 follows from combining (2.92) and (2.93). ■

Chapter 3

Transmission Strategies for Cognitive Radio Channels with Secrecy

In this chapter we investigate the cognitive radio channel with secrecy constraints on the primary message. First we present the list of the chapter's goals.

Objectives of the Chapter.

- Describe how a cognitive transmitter can improve the secrecy of primary transmissions in cognitive radio networks.
- Derive the achievable rate regions with secrecy constraints for the AWGN cognitive radio channel model with and without primary message knowledge at the secondary transmitter and provide insights on the power allocation strategies for the two scenarios.
- Formulate and solve three relevant power allocation problems, namely the maximization of the primary rate and of the secondary rate, and the minimization of the transmitting power.
- Analyze using a Stackelberg game model a realistic power allocation problem corresponding to an optimization of both transmitters' utilities.
- Illustrate our results through numerical examples based on a geometrical setup, highlighting the impact of the node geometry on the achievable rates and on the optimal strategy of the secondary transmitter and compare those results to the game theoretic interaction.

Organization of the Chapter This chapter consists of eight sections. In Section 3.1 we introduce cognitive radio networks with security concerns. In Section 3.2 we define our system model, the notation, and the two different cognitive scenarios. In Section 3.3 we derive the achievable rate regions for the given setup under the AWGN channel model. In Section 3.4 we investigate three important optimization problems for the cognitive radio channel with secrecy. In Section 3.5 we analyze the interaction between both transmitters from a game theoretic perspective. In Section 3.6 we extend our results to the practical case of multiple secondary receivers. In Section 3.7 we illustrate our results through numerical simulations taking into account the geometry of the nodes. In Section 3.8 we close the chapter with concluding remarks.

3.1 Introduction to Cognitive Radio Networks with Secrecy Constraints

In this section we introduce the necessary background and references on security challenges in cognitive radio networks (CRN).

Security Issues in Cognitive Radio Networks In recent years, security issues in cognitive radio networks have been the subject of increasing interest. Indeed, with the growth of these networks, security challenges have become a critical issue for cognitive radio technologies. While traditional security threats such as jamming, eavesdropping and MAC-layer attacks exist, one must also consider CRN-specific threats such as exogenous attackers or selfish/intruding nodes exploiting the vulnerability of *ad hoc* cognitive networks. We refer the reader to [ATV+12] and references therein for a comprehensive survey of security challenges in CRN and potential solutions to those challenges. Other attacks specific to the infrastructure of CRNs include spectrum sensing data falsification, or primary user emulation (PUE) attacks [SQC13]. In [WLZZ13], a PHY-layer framework to defend against security threats in CRN is developed. While investigating solutions to PHY-layer attacks such as PUE or reporting false sensing data as in [WLZZ13] is outside the scope of this thesis, we know from Chapter 2 the suitable framework to study eavesdropping in CRN: information theoretic secrecy.

Information Theoretic Secrecy for CRN Although security problems for classic wireless networks have been studied for many years, the interest in the security at the physical layer of cognitive radio networks has grown, albeit considerably, only recently. The concept of information theoretic secrecy, and the corresponding cooperative techniques for secrecy can naturally be applied to cognitive radio networks. In [WL11], a scenario where an external eavesdropper attempts to decode the primary user's message is considered. In exchange of cooperation from the secondary user to improve its own secrecy rate, the primary user allows the secondary user a share of the spectrum. In [SY11] and [LCK13], a cognitive scenario

with an external eavesdropper is investigated under a spectrum leasing perspective. While the authors of [LCK13] consider the case where the transmitters are equipped with multiple antennas and the secondary transmitter knows the primary message, the work in [SY11] investigates cooperative jamming for secrecy for single-antenna nodes. Secure multiple-input single-output cognitive radio channels are studied in [PLZ+10] in the presence of an external eavesdropper. A different setup is investigated in [LSBP+09]: the secondary user wants to keep its message confidential to the primary network; i.e., the primary receiver is viewed as an eavesdropper from the secondary network perspective. In [BSSA10], the case where both receivers are eavesdroppers to the other user's message is investigated, and inner and outer bounds on the capacity-equivocation region are derived.

Our Contribution In this chapter we explore the novel case where the secondary receiver is treated as a potential eavesdropper with respect to the primary transmission. Since the primary users are the legacy owners of the spectrum, the confidentiality of the primary message should be considered. In this context, the primary transmitter may be assisted by the trustworthy secondary transmitter if the cooperation could improve the secrecy performance, while the secondary transmitter benefits as it is awarded a share of the spectrum for its data transmission. This model is particularly relevant since it describes, for example, a scenario where the primary user subscribes for a premium content while the secondary user only subscribes for free content. Both transmitters belong to the same entity, thus the cognitive transmitter can help the primary transmission, but it should ensure that no premium content is leaked to the secondary user. Furthermore, this model has the advantage of providing a justification for the common assumption of the knowledge of the eavesdropper's channels, since the eavesdropper is actually a legitimate user in the network. We consider the two types of cooperation for secrecy techniques described in Chapter 2 for the cognitive transmitter: oblivious cooperation by cooperative jamming and cooperation with knowledge of primary transmitter's message by relaying. In the first case, the secondary transmitter is unaware of the primary transmitter's message and acts as a deaf helper to enhance the secrecy of the primary transmission, whereas in the second case, relaying of the primary message is also within its capabilities.

3.2 System Model

We begin our study by first introducing our system model. In particular we describe our network model in Section 3.2.1, our channel model and the notation of the chapter in Section 3.2.2, and the information theoretic secrecy constraints specific to this chapter in Section 3.2.3.

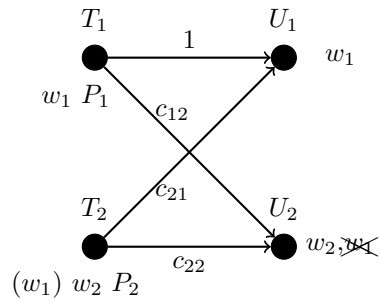


Figure 3.1: Cognitive channel with secrecy constraints.

3.2.1 Network Model and Cognitive Scenarios

In this chapter we investigate the cognitive radio network described in Figure 3.1. The cognitive radio network consists of the following single antenna nodes: a primary transmitter T_1, a cognitive secondary transmitter T_2, a primary receiver U_1 and a secondary receiver U_2. T_1 wishes to transmit the secret message w_1, which is intended to U_1, and which should be kept secret from U_2, whereas T_2 wants to transmit the message w_2 (without secrecy constraints) to the secondary receiver U_2. In this setup, we consider two different cooperative scenarios. In the first scenario $\mathcal{S}_1$, T_2 has no knowledge of the secret message w_1. In the second scenario $\mathcal{S}_2$, T_2 knows the secret message w_1 perfectly.

3.2.2 Channel Model and Notation

We consider the following AWGN channel model

$$\mathbf{y}_1 = \mathbf{x}_1 + \sqrt{c_{21}}\mathbf{x}_2 + n_1, \tag{3.1a}$$

$$\mathbf{y}_2 = \sqrt{c_{12}}\mathbf{x}_1 + \sqrt{c_{22}}\mathbf{x}_2 + n_2, \tag{3.1b}$$

where the noises n_1, n_2 are real-valued Gaussian distributed with unit variance, i.e., $n_1, n_2 \sim \mathcal{N}(0,1)$. All channel coefficients are assumed to remain constant during the transmission of a codeword. Moreover, we consider the path-loss channel model so that $c_{i,j} = d_{i,j}^{-\alpha}$, where $d_{i,j}$ is the distance between transmitter i and receiver j and α is the path-loss exponent.

The transmitters use the channel by encoding their messages into codewords of length n. T_1 encodes message w_1 into the codeword $\mathbf{x}_1 = (x_{1,1}, \ldots, x_{1,n})$. T_2 assigns a codeword $\mathbf{x}_2 = (x_{2,1}, \ldots, x_{2,n})$ to the message w_2 or, possibly, to the set of messages (w_1, w_2) in the scenarios $\mathcal{S}_1$ and $\mathcal{S}_2$, respectively. The codewords have to satisfy average power constraints P_1 and P_2 respectively, i.e.,

$$\frac{1}{n}\sum_{k=1}^{n} |x_{i,k}|^2 \leq P_i \quad \text{for} \quad i \in \{1,2\}. \tag{3.2}$$

The receivers decode their receptions $\mathbf{y}_1$ and $\mathbf{y}_2$ into message estimates $\hat{w}_1$ and $\hat{w}_2$, respectively.

3.2.3 Information Theoretic Secrecy

A rate pair (R_1, R_2) for the messages w_1 and w_2 is said to be achievable, if the average error probabilities $P_{e,1} \triangleq P\{\hat{w}_1 \neq w_1\}$ and $P_{e,2} \triangleq P\{\hat{w}_2 \neq w_2\}$ can be made arbitrarily small, while the message w_1 stays secure from the secondary receiver. In other terms, for any $\varepsilon > 0$ and a sufficiently large n, the following conditions hold:

$$\max\{P_{e,1}, P_{e,2}\} \leq \varepsilon \quad \text{(Reliability)} \tag{3.3a}$$

$$I(w_1; \mathbf{y}_2) \leq n\varepsilon \quad \text{(Secrecy)}. \tag{3.3b}$$

When T_2 does not transmit, the maximum achievable rate R_1^{WT} such that both the reliability and secrecy conditions are fulfilled is known as the secrecy capacity of the wiretap channel [Wyn75] and is given by:

$$R_1^{\mathrm{WT}} = \left(\mathcal{C}(P_1) - \mathcal{C}(c_{12}P_1)\right)^+. \tag{3.4}$$

We observe that the secrecy capacity is only positive if the primary link has better quality than the link between T_1 and U_2. Therefore, secrecy concerns lay the foundation of mutual cooperation between primary and secondary transmitters since cooperation from T_2 could allow strictly positive secrecy rates, while allowing the secondary network to transmit its own message.

3.3 Achievable Rate Regions

In this section we derive the achievable rate regions for the cognitive interference channel with secrecy constraint on the primary message. In Section 3.3.1 we consider the scenario $\mathcal{S}_1$, while in Section 3.3.2, the scenario $\mathcal{S}_2$ is investigated.

3.3.1 Cooperation without Message Knowledge at Secondary Transmitter

We first consider the cognitive scenario $\mathcal{S}_1$, i.e., the second transmitter does not know the secret message w_1. This scenario was previously considered in [TKEG10]. Here, we present the achievable rate region obtained in that work and describe the corresponding achievable scheme.

Encoding Scheme The secondary transmitter T_2 transmits $\mathbf{x}_2(q) = V_{2c}(q) + V_{2s}(q) + V_{2j}(q)$, with $V_{2c}(q) \sim \mathcal{N}(0, P_{2c}(q))$, $V_{2s}(q) \sim \mathcal{N}(0, P_{2s}(q))$, $V_{2j}(q) \sim \mathcal{N}(0, P_{2j}(q))$, and q is the time-sharing parameter. Note that in the following, we restrict ourselves to a deterministic time-sharing variable. In other words, T_2 splits its available power P_2 into three parts: $P_{2\mathrm{s}}$ for its own message w_2, $P_{2\mathrm{c}}$ for the

common message which should be decoded by both receivers and $P_{2\mathrm{j}}$ for a jamming signal, such that $P_2 = P_{2\mathrm{s}} + P_{2\mathrm{c}} + P_{2\mathrm{j}}$ and $R_2 = R_{2\mathrm{s}} + R_{2\mathrm{c}}$. The corresponding achievable rate region is given in the following theorem [TKEG10].

Theorem 3.1.

The achievable rate pair (R_1, R_2) is given by the following region $\mathcal{R}_1$:

$$R_1 < \left(\mathcal{C}\left(\frac{P_1}{1 + c_{21}P_{2\mathrm{s}} + c_{21}P_{2\mathrm{j}}}\right) - \mathcal{C}\left(\frac{c_{12}P_1}{1 + c_{22}P_{2\mathrm{j}}}\right)\right)^+ \tag{3.5a}$$

$$R_{2\mathrm{c}} < \mathcal{C}\left(\frac{c_{21}P_{2\mathrm{c}}}{1 + c_{21}P_{2\mathrm{s}} + c_{21}P_{2\mathrm{j}}}\right) \tag{3.5b}$$

$$R_1 + R_{2\mathrm{c}} < \left(\mathcal{C}\left(\frac{P_1 + c_{21}P_{2\mathrm{c}}}{1 + c_{21}P_{2\mathrm{s}} + c_{21}P_{2\mathrm{j}}}\right) - \mathcal{C}\left(\frac{c_{12}P_1}{1 + c_{22}P_{2\mathrm{j}}}\right)\right)^+ \tag{3.5c}$$

$$R_{2\mathrm{s}} < \mathcal{C}\left(\frac{c_{22}P_{2\mathrm{s}}}{1 + c_{12}P_1 + c_{22}P_{2\mathrm{j}}}\right) \tag{3.5d}$$

$$R_{2\mathrm{c}} + R_{2\mathrm{s}} < \mathcal{C}\left(\frac{c_{22}P_{2\mathrm{c}} + c_{22}P_{2\mathrm{s}}}{1 + c_{12}P_1 + c_{22}P_{2\mathrm{j}}}\right) \tag{3.5e}$$

for every possible power splitting $P_2 = P_{2\mathrm{s}} + P_{2\mathrm{c}} + P_{2\mathrm{j}}$, and with $R_2 = R_{2\mathrm{c}} + R_{2\mathrm{s}}$.

Proof. This theorem and its proof appear in [TKEG10]. However, we give another proof in Appendix 3.A for the rate region $\mathcal{R}_1$, as the extension to multiple secondary users in Section 3.6 follows from this alternative proof. ■

The achievable rate region can be interpreted as follows. First, T_2 uses the rate splitting technique introduced by Han and Kobayashi in [HK81]. Rate splitting allows a significant rate improvement in the "strong interference" regime. Furthermore, T_2 uses a power $P_{2\mathrm{j}}$ for a Gaussian jamming signal. We notice that, while this jamming signal can only decrease the secondary rate R_2 since it is not decodable by U_2, it can possibly increase the achievable rate of the primary user since the interference injection increases the confusion of U_2 about the primary message w_1. This effect is reflected by the influence of $P_{2\mathrm{j}}$ in Equation (3.5a). The positive term in (3.5a) can be interpreted as the achievable primary rate without secrecy constraints while the negative term represents the amount of rate T_1 has to sacrifice to guarantee a secure transmission.

Remark 3.1.

In order to represent the rate region efficiently, we also reformulate $\mathcal{R}_1$ using the Fourier-Motzkin elimination [EGK12]:

$$
\begin{aligned}
R_1 &< \left(\mathcal{C}\left(\frac{P_1}{1+c_{21}P_{2\mathrm{s}}+c_{21}P_{2\mathrm{j}}}\right)-\mathcal{C}\left(\frac{c_{12}P_1}{1+c_{22}P_{2\mathrm{j}}}\right)\right)^+,\\
R_2 &< \min\left(\mathcal{C}\left(\frac{c_{22}P_{2\mathrm{c}}+c_{22}P_{2\mathrm{s}}}{1+c_{12}P_1+c_{22}P_{2\mathrm{j}}}\right),\right.\\
&\left.\mathcal{C}\left(\frac{c_{21}P_{2\mathrm{c}}}{1+c_{21}P_{2\mathrm{s}}+c_{21}P_{2\mathrm{j}}}\right)+\mathcal{C}\left(\frac{c_{22}P_{2\mathrm{s}}}{1+c_{12}P_1+c_{22}P_{2\mathrm{j}}}\right)\right),\\
R_1+R_2 &< \left(\mathcal{C}\left(\frac{P_1+c_{21}P_{2\mathrm{c}}}{1+c_{21}P_{2\mathrm{s}}+c_{21}P_{2\mathrm{j}}}\right)-\mathcal{C}\left(\frac{c_{12}P_1}{1+c_{22}P_{2\mathrm{j}}}\right)\right)^+\\
&+\mathcal{C}\left(\frac{c_{22}P_{2\mathrm{s}}}{1+c_{12}P_1+c_{22}P_{2\mathrm{j}}}\right). \qquad (3.6)
\end{aligned}
$$

3.3.2 Cooperation with Message Knowledge at Secondary Transmitter

In this section we assume that the secondary transmitter T_2 knows the primary message w_1 perfectly. The assumption is justified whenever primary and secondary transmitter are connected by a link with sufficiently high secrecy capacity. Such a connection can for instance be realized by a wired link, which has a capacity of at least R_1. This assumption will be further investigated in Chapter 4. As in the previous scenario, T_1 encodes into the codeword $\mathbf{x}_1$, independently of the encoding at T_2. Now with the knowledge of w_1, T_2 is able to encode (w_1, w_2) into $\mathbf{x}_2$ based on four strategies as follows:

1. **Transmission of a common message:** As in $\mathcal{S}_1$, the common message, encoded by $V_{2\mathrm{c}}$ binned against $\mathbf{x}_1$ has to be decoded by both users U_1 and U_2.

2. **Transmission of the secondary message:** As in $\mathcal{S}_1$, w_2 encoded into $V_{2\mathrm{s}}$ to be decoded by the secondary user U_2 only.

3. **Jamming:** $\mathcal{S}_1$, the jamming signal is encoded into J_2 to confuse the eavesdropping secondary user U_2.

4. **Relaying (or broadcasting) of the primary message:** w_1 is encoded into V_{1p}, binned against $V_{2\mathrm{s}}$ conditioned on $V_{2\mathrm{c}}, \mathbf{x}_1$ to be decoded only by the primary user U_1.

Therefore, this encoding scheme results in T_2 splitting its transmission power into $P_2 = P_{2\mathrm{s}} + P_{2\mathrm{c}} + P_{2\mathrm{j}} + P_{2p}$, where the new term P_{2p} is the power allocated to V_{1p} encoding the primary message.

Theorem 3.2.

The achievable rate pair (R_1, R_2), with $R_2 = R_{2\mathrm{c}} + R_{2\mathrm{s}}$ is given by the following region $\mathcal{R}_2$:

$$R_1 < \left(\mathcal{C}\left(\frac{P_1 + c_{21}P_{2p}}{1 + c_{21}P_{2\mathrm{s}} + c_{21}P_{2\mathrm{j}}}\right) - \mathcal{C}\left(\frac{c_{12}P_1 + c_{22}P_{2p}}{1 + c_{22}P_{2\mathrm{j}}}\right)\right)^+ \tag{3.7a}$$

$$R_1 + R_{2\mathrm{c}} < \mathcal{C}\left(\frac{P_1 + c_{21}P_{2\mathrm{c}} + c_{21}P_{2p}}{1 + c_{21}P_{2\mathrm{s}} + c_{21}P_{2\mathrm{j}}}\right) \tag{3.7b}$$

$$R_{2\mathrm{s}} < \mathcal{C}\left(\frac{c_{22}P_{2\mathrm{s}}}{1 + c_{12}P_1 + c_{22}P_{2\mathrm{j}} + c_{22}P_{2p}}\right) \tag{3.7c}$$

$$R_{2\mathrm{c}} + R_{2\mathrm{s}} < \mathcal{C}\left(\frac{c_{22}P_{2\mathrm{c}} + c_{22}P_{2\mathrm{s}}}{1 + c_{12}P_1 + c_{22}P_{2\mathrm{j}} + c_{22}P_{2p}}\right), \tag{3.7d}$$

for every possible power splitting $P_2 = P_{2\mathrm{s}} + P_{2\mathrm{c}} + P_{2\mathrm{j}} + P_{2p}$.

Proof. The proof is similar to the proof of Theorem 3.1 in Appendix 3.A and is therefore omitted here. This scenario is a special case of the setup investigated in [BSSA10] where the secrecy of w_2 with respect to U_1 is also required. In that setup, an achievable rate-equivocation region for the general case of a discrete memoryless interference channel is derived. Our scenario reduces to a subset of equations in this region, since we have no constraints on the secrecy of the secondary message. Furthermore, we consider here the more general scheme from [RTD12] where the secondary user can also relay the primary message instead of the scheme employed for obtaining equations (6)-(9) in Theorem 1 in [BSSA10]. Finally, we specialize the result in [BSSA10] to Gaussian channels, by defining the auxiliary random variables and joint distributions. The region $\mathcal{R}_2$ follows from choosing the joint distributions as in [TKEG10], except for $\mathbf{x}_2$ as we allocate the power P_{2p} for broadcasting the message w_1 at T_2, i.e., $\mathbf{x}_2 = V_{2\mathrm{c}} + V_{2\mathrm{s}} + J_2 + V_{1p}$, with $V_{1p} \sim \mathcal{N}(0, P_{2p})$ (our V_{1p} corresponds to U_{2pb} in [RTD12]). ■

This choice of the auxiliary variables leading to $\mathcal{R}_2$ is not optimal; however, it leads to a more tractable rate region for the optimization analysis in the following sections.

Remark 3.2.

We can also reformulate the region $\mathcal{R}_2$ by using Fourier-Motzkin elimination:

$$\begin{aligned} R_1 &< \left(\mathcal{C}\left(\frac{P_1 + c_{21}P_{2p}}{1 + c_{21}P_{2\mathrm{s}} + c_{21}P_{2\mathrm{j}}} \right) - \mathcal{C}\left(\frac{c_{12}P_1 + c_{22}P_{2p}}{1 + c_{22}P_{2\mathrm{j}}} \right) \right)^+ \\ R_2 &< \mathcal{C}\left(\frac{c_{22}P_{2\mathrm{c}} + c_{22}P_{2\mathrm{s}}}{1 + c_{12}P_1 + c_{22}P_{2\mathrm{j}} + c_{22}P_{2p}} \right) \\ R_1 + R_2 &< \mathcal{C}\left(\frac{P_1 + c_{21}P_{2\mathrm{c}} + c_{21}P_{2p}}{1 + c_{21}P_{2\mathrm{s}} + c_{21}P_{2\mathrm{j}}} \right) \\ &\quad + \mathcal{C}\left(\frac{c_{22}P_{2\mathrm{s}}}{1 + c_{12}P_1 + c_{22}P_{2\mathrm{j}} + c_{22}P_{2p}} \right) \end{aligned} \tag{3.8}$$

Finally, for convenience in the remainder of this chapter, we will parameterize the power fractions devoted to jamming, common message, relaying and own message as

$$P_{2j} = \rho P_2, \tag{3.9}$$
$$P_{2c} = \beta(1-\rho)P_2, \tag{3.10}$$
$$P_{2p} = \gamma(1-\beta)(1-\rho)P_2, \tag{3.11}$$
$$P_{2s} = (1-\gamma)(1-\beta)(1-\rho)P_2, \tag{3.12}$$

respectively. The parameter $\rho \in [0,1]$ denotes the fraction of the total power P_2 used for jamming. The remaining power $(1-\rho)P_2$ is divided by the parameter $\beta \in [0,1]$, where the fraction $\beta(1-\rho)P_2$ is used for the strategy of transmitting a common message. Finally, the parameter $\gamma \in [0,1]$ divides the remaining power $(1-\beta)(1-\rho)P_2$ into power fractions for relaying the primary message w_1 and transmitting the secondary message w_2.

3.4 System Optimization

In this section we derive closed-form solutions for a set of interesting optimization problems. Firstly, we define two new rate regions for the important case $P_{2\mathrm{c}} = 0$, where T_2 is unable to use a common message. Note that the common message has to be decoded by the primary receiver along with the primary message w_1. Instead, the receiver might use the legacy codebook to decode w_1 and treat the remaining signal components as noise. In this situation, T_2 has to refrain from using a common message. The cognitive scenario where U_1 does not have multi-user decoding capabilities is further investigated in Chapter 4. The motivation for studying this case is that the legacy system might not provide the necessary

decoding capability to decode both the primary and the common message. This is a reasonable assumption if the secondary system is supposed to cooperate with a primary system, which is not designed for this kind of cooperation. Therefore we define the following rate regions:

Definition 3.1.

For the scenario $\mathcal{S}_1$ without common message, our rate region, denoted as $\mathcal{S}_{1,\mathrm{SD}}$, simplifies to:

$$R_1 < \left(\mathcal{C}\left(\frac{P_1}{1+c_{21}P_2}\right) - \mathcal{C}\left(\frac{c_{12}P_1}{1+c_{22}\rho P_2}\right)\right)^+, \tag{3.13a}$$

$$R_2 < \mathcal{C}\left(\frac{c_{22}(1-\rho)P_2}{1+c_{12}P_1+c_{22}P_2\rho}\right). \tag{3.13b}$$

Definition 3.2.

For the scenario $\mathcal{S}_2$ without common message, we consider the rate region $\mathcal{S}_{2,\mathrm{SD}}$:

$$R_1 < \left(\mathcal{C}\left(\frac{P_1+c_{21}(1-\rho)\gamma P_2}{1+c_{21}(1-\gamma+\gamma\rho)P_2}\right) - \mathcal{C}\left(\frac{c_{12}P_1+c_{22}(1-\rho)\gamma P_2}{1+c_{22}\rho P_2}\right)\right)^+, \tag{3.14}$$

$$R_2 < \mathcal{C}\left(\frac{c_{22}(1-\rho)(1-\gamma)P_2}{1+c_{12}P_1+c_{22}P_2(\rho+\gamma-\rho\gamma)}\right). \tag{3.15}$$

Note that the rate region $\mathcal{S}_{2,\mathrm{SD}}$ reduces to the region $\mathcal{S}_{1,\mathrm{SD}}$ with $\rho = 0$. Hence, studying the region $\mathcal{S}_{2,\mathrm{SD}}$ covers both cases of cooperation with and without message knowledge.

In this section we consider optimization under the assumption of full cooperation between primary and secondary systems. The two transmitters jointly find the optimal operation strategy for the given constraints. This is in contrast to a game theoretic approach which we consider in the subsequent section 3.5. We consider three important optimization scenarios for the strategy of the secondary transmitter. On the one hand, T_2 could either aim at maximizing its own achievable rate, under the constraint that the resulting rate achievable by the primary network is not lower than the wiretap rate $R_1 \geq R_1^{\mathrm{WT}}$ achievable without cooperation (problem $\mathcal{P}_{R_2}$). The motivation is that R_1^{WT} is the achievable rate if the secondary transmitter is not present, and the secondary user acts as an eavesdropper. On the other hand, the goal of T_2 could also be to minimize its transmit power, under

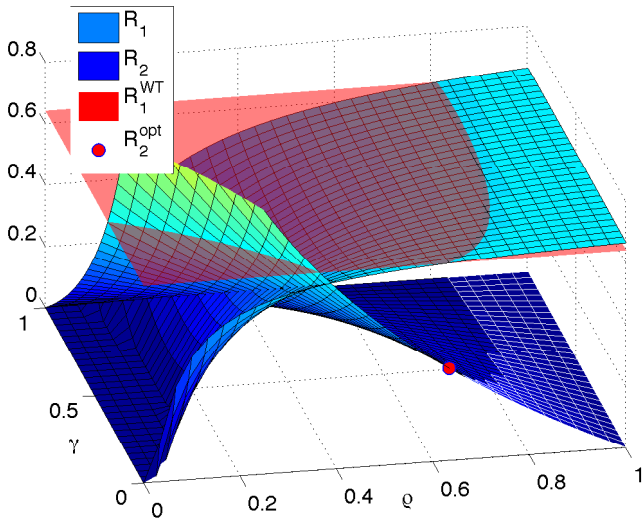


Figure 3.2: Maximization problem $\mathcal{P}_{R_2}(\bar{\beta})$.

the constraints that the rates of both users are above a certain threshold (problem $\mathcal{P}_{P_2}$). At last, T_2 aims at maximizing the primary rate R_1 subject to the constraint $R_2 \geq R_2^{\text{thr}}$ (problem $\mathcal{P}_{R_1}$).

3.4.1 Maximization of Secondary Rate $\mathcal{P}_{R_2}$

We first investigate the optimization problem $\mathcal{P}_{R_2}$. In particular we consider the optimization $\mathcal{P}_{R_2}(\bar{\beta})$ (no common message) defined as follows.

Definition 3.3 ($\mathcal{P}_{R_2}(\bar{\beta})$)**.**

The optimization $\mathcal{P}_{R_2}(\bar{\beta})$ is defined as

$$\max_{\gamma,\rho,P_2} \; R_2 \tag{3.16a}$$

$$\text{s.t. } R_1 \geq R_1^{\text{WT}} \quad \text{and} \quad P_2 \leq P_2^{\text{thr}}. \tag{3.16b}$$

Further, we define $\mathcal{P}_{R_2}(\bar{\beta}, \bar{\gamma})$ as

$$\max_{\gamma=0,\rho,P_2} \; R_2 \tag{3.17}$$

$$\text{s.t. } R_1 \geq R_1^{\text{WT}} \quad \text{and} \quad P_2 \leq P_2^{\text{thr}}. \tag{3.18}$$

The first constraint means that the secondary system must not degrade the performance of the primary system, whereas the second constraint reflects a limited transmit power of the secondary transmitter. The maximization $\mathcal{P}_{R_2}(\bar{\beta})$ is depicted in Figure 3.2 for $c_{22} = 8$, $c_{12} = 0.354$, $c_{21} = 0.716$ and $P_1 = 10$.[1] The figure shows the rates R_1 and R_2 as functions of ρ and γ. The surface that attains its maximum at $\rho = 1$ corresponds to R_1; the other surface with maximum at $\rho = \gamma = 0$ corresponds to R_2. The constraint R_1^{WT} is depicted by the red plane. The feasible set of parameters ρ and γ corresponds to the region where R_1 is above that plane. This region is projected down on R_2 and marked by white grid lines. Within this region we find the point that maximizes R_2, depicted by the red dot labeled R_2^{opt}.

Closed-form Expression for $\mathcal{P}_{R_2}(\bar{\beta}, \bar{\gamma})$ Since problem $\mathcal{P}_{R_2}(\bar{\beta})$ is non-convex, to simplify the analysis, we consider the special case of $\mathcal{P}_{R_2}(\bar{\beta}, \bar{\gamma})$, i.e., $\gamma = 0$, where T_2 does not relay the primary message. By the equality of the rate regions $\mathcal{S}_{1,\mathrm{SD}}$ and $\mathcal{S}_{2,\mathrm{SD}}$ for $\beta = 0$, this is also the case where T_2 does not possess the primary message, i.e., the deaf helper case. The general case for arbitrary γ will be considered in Section 3.7. We obtain the following result:

Proposition 3.1.

There exists at most a unique closed-form solution $(\rho^\star, P_2^\star)$ to the optimization problem $\mathcal{P}_{R_2}(\bar{\beta}, \bar{\gamma})$.

Proof. Proposition 3.1 is proven in Appendix 3.B and closed-form expressions for $(\rho^\star, P_2^\star)$ are given in the steps of the proof. ■

We also illustrate in Figure 3.3 R_1 and R_2 as functions of ρ and β for the optimization:

$$\max \; R_2 \;\; \text{s.t. } R_1 \geq R_1^{\mathrm{WT}}, \tag{3.19}$$

for scenario $\mathcal{S}_1$. We see that there is a trade-off between R_1 and R_2 in both parameters. This is reasonable because R_1 increases with ρ (jamming) and decreases with β while R_2 has the opposite behavior. The feasible set of parameters ρ and β is the region where R_1 is above that plane and the constraint of (3.19) is represented by the cyan plane. Within this region we find the maximum $R_2^\star$, which is marked by a red dot.

The simulation results of Figure 3.13 in Section 3.7 further reflect our solution, especially in the column for $\mathcal{P}_{R_2}(\bar{\beta})$, the secrecy constraint results in an unfeasible area in which the secondary transmitter can not improve the performance.

[1] These values correspond to the basic scenario considered in Section 3.7.

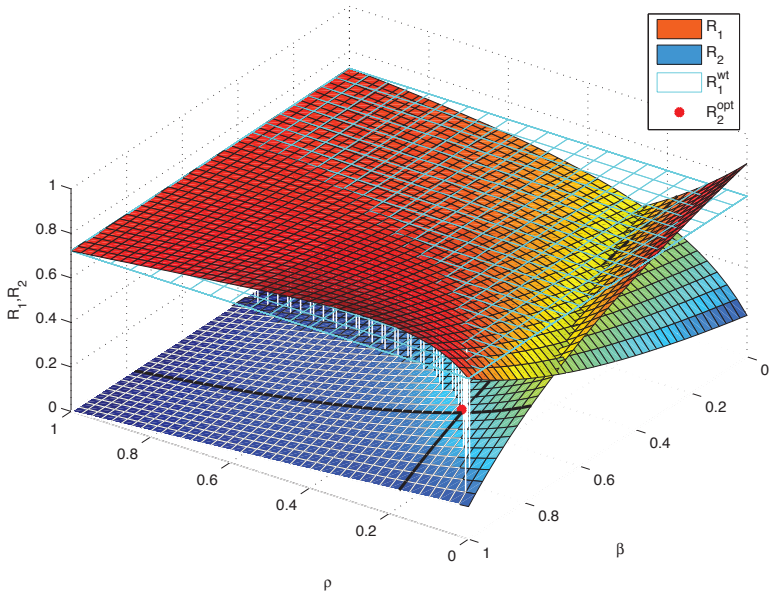


Figure 3.3: Achievable rate region (R_1, R_2) as functions of β and ρ for $\mathcal{S}_1$.

3.4.2 Minimization of Secondary Transmission Power $\mathcal{P}_{P_2}$

Similarly, we consider the minimization of secondary transmit power without common message $\mathcal{P}_{P_2}(\bar{\beta})$ defined as follows.

Definition 3.4 ($\mathcal{P}_{P_2}(\bar{\beta})$)**.**

We define $\mathcal{P}_{P_2}(\bar{\beta})$ defined as

$$\min_{\rho,\gamma} \; P_2 \tag{3.20a}$$

$$\text{s.t. } R_1 \geq R_1^{\mathrm{WT}} \tag{3.20b}$$

$$R_2 \geq R_2^{\mathrm{thr}}. \tag{3.20c}$$

Similarly to $\mathcal{P}_{R_2}$, we define the sub-problems $\mathcal{P}_{P_2}(\bar{\beta}, \bar{\gamma})$ and $\mathcal{P}_{P_2}(\bar{\beta}, \bar{\rho})$ as $\mathcal{P}_{P_2}(\bar{\beta}, \gamma = 0)$ and $\mathcal{P}_{P_2}(\bar{\beta}, \rho = 0)$ respectively.

The primary rate R_1 is constrained by the wiretap rate R_1^{WT}, and the secondary rate R_2 should at least meet the required threshold R_2^{thr}.

The motivation for this optimization is energy consumption control, which can be applied to green communications. Green communications technologies provide solutions to contribute to the reduction of carbon footprint, an objective that is

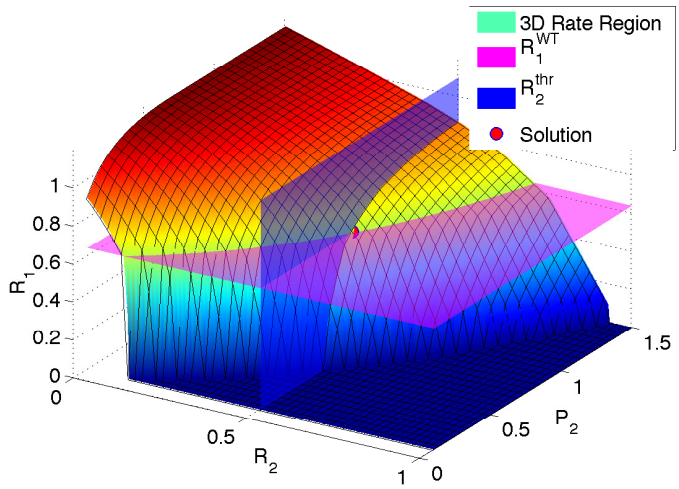


Figure 3.4: Minimization problem $\mathcal{P}_{P_2}(\bar{\beta})$.

realized by increasing the energy efficiency of communications networks in a wireless environment. For cognitive radio networks, the cognitive properties can further help make the communication more efficient and flexible [GA11]. Efficiency for cognitive radio networks with secrecy constraints will be considered further in Chapter 6.

The minimization $\mathcal{P}_{P_2}(\bar{\beta})$ of P_2 is depicted in Figure 3.4. The figure shows the rate region (R_1, R_2) for different values of P_2. Furthermore, the constraints R_1^{WT} and R_2^{thr} are depicted as pink and blue planes, respectively. The rate region must contain at least one point that fulfill both constraints in order for the corresponding value of P_2 to be feasible. The point that minimizes P_2 is depicted as a red dot.

Considering the problems $\mathcal{P}_{P_2}(\bar{\beta}, \bar{\gamma})$ and $\mathcal{P}_{P_2}(\bar{\beta}, \bar{\rho})$, we are able to obtain the following result.

Proposition 3.2.

There exists at most a unique closed-form solution $(\rho^\star, P_2^\star)$, respectively $(\gamma^\star, P_2^\star)$ to the problem $\mathcal{P}_{P_2}(\bar{\beta}, \bar{\gamma})$, respectively $\mathcal{P}_{P_2}(\bar{\beta}, \bar{\rho})$.

Proof. Proposition 3.2 is proven in Appendix 3.C where the corresponding optimal parameters are derived in closed-form. ■

A visualization of our solution is given in Figure 3.15. Consider the first column, which depicts the scenario without common message ($\beta = 0$). Clearly there are two dominating strategies: If the secondary transmitter T_2 is located close to the

primary receiver, it mainly relays the primary message. The strategy we analyzed above is used when T_2 is close to the secondary receiver. It is a combination of jamming and transmitting the secondary message w_2.

3.4.3 Maximization of Primary Rate $\mathcal{P}_{R_1}$

In the last part we discuss the maximization problem of primary rate $\mathcal{P}_{R_1}$. In this problem, we focus on protecting the priority of the primary system.

Definition 3.5 ($\mathcal{P}_{R_1}(\bar{\beta})$)**.**

We define the maximization problem $\mathcal{P}_{R_1}(\bar{\beta})$ as

$$\max_{\rho,\gamma,P_2} \; R_1 \tag{3.21a}$$

$$\text{s.t. } R_2 \geq R_2^{\text{thr}} \tag{3.21b}$$

$$P_2 \leq P_2^{\text{thr}}. \tag{3.21c}$$

Further we define $\mathcal{P}_{R_1}(\bar{\beta}, \bar{\gamma})$ as $\mathcal{P}_{R_1}(\bar{\beta}, \gamma = 0)$.

The constraints imply that by using a limited transmit power, T_2 needs to support as much the primary rate gain as possible while maintaining a certain transmission rate on its own.

Closed-form Expression for $\mathcal{P}_{R_1}(\bar{\beta}, \bar{\gamma})$ As for the previous two optimization problems, we obtain the following result:

Proposition 3.3.

There exists at most a unique closed-form solution $(\rho^\star, P_2^\star)$, to the problem $\mathcal{P}_{R_1}(\bar{\beta}, \bar{\gamma})$.

Proof. Proposition 3.3 is proven in Appendix 3.D where the corresponding optimal parameters are derived in closed-form. ■

Consider Figure 3.14 for a visualization of the solution. Similar as for the previous optimization $\mathcal{P}_{P_2}(\bar{\beta}, \bar{\gamma})$, the optimization $\mathcal{P}_{R_1}(\bar{\beta}, \bar{\gamma})$ yields a solution when the secondary transmitter T_2 is close to the secondary receiver. Interestingly, it is not required to utilize all available secondary power P_2 to maximize R_1. The reason is that R_1 could only be maximized by increasing the jamming. This, however, demands for a higher power P_{2s} for transmitting the secondary message w_2 to meet

the requirement on R_2. Both jamming and transmitting w_2 cause interference to the primary receiver. The interference is too high to justify the jamming.

3.5 Optimization with Game Theoretic Cooperation

In this section we analyze the cooperation between primary and secondary transmitters through a game theoretic framework. Since T_1 and T_2 have their own interests and thus do not cooperate unconditionally, non-cooperative game theory is a natural approach to model their interaction in cognitive radio networks with secrecy constraints as e.g., in [TKEG10] and [WL11]. A Stackelberg game between T_1 and T_2 as introduced in Chapter 2 is a common model for the cognitive scenario. In this perspective, we consider T_1 as the game leader selling some fraction of its spectrum to T_2 and, subsequently, T_2 as the follower being awarded a share of the spectrum for its cooperation, similarly to [SSS+08] (CRN without secrecy constraints) and to [SY11] (with secrecy). In the proposed Stackelberg game, it is assumed that the primary transmitter operates at a fixed power P_1 and the secondary transmitter is allowed to use some power to transmit its own data. At the same time, the latter user has to help the primary system to reduce the possible leakage to the secondary receiver by employing some Gaussian jamming (or relaying of the primary message, if applicable).

The next step of the analysis is to solve the game, i.e., to predict the strategies that the rational players would adopt, and hence, to determine the corresponding outcome. For the Stackelberg game model, the outcome of this competitive and decentralized behavior can be described by the solution concept called the Stackelberg equilibrium (SE). In this section we define the Stackelberg equilibrium of the power-control game between T_1 and T_2 and we derive it in a closed-form expression for some important cases.

Oblivious Cooperation

If the primary message is not available at the secondary receiver, the corresponding rate region reduces to the one formed by (3.13a) and (3.13b). Throughout the two following subsections we consider a case where $P_{2c} = 0$, and hence no common message is available.

Definition of the Game T_2 can be modeled as a buyer of the resource from the primary system which wants to maximize its achievable rate minus the cost of the power. The utility function of T_2 is then defined as

$$\mathcal{U}_2(\rho, P_2) = R_2 - \theta P_2, \tag{3.22}$$

where θ represents the price per unit power for the secondary transmitter. T_2 intends to maximize its utility, i.e., to solve the following maximization problem:

$$\max_{P_2} \mathcal{U}_2(\rho, P_2). \tag{3.23}$$

T_1 can be seen as a seller aiming to earn a payment from T_2 for the power used. We define its utility function as

$$\mathcal{U}_1(\rho, P_2) = R_1 + \theta P_2, \tag{3.24}$$

Similarly, T_1 wants to maximize its utility; i.e.,:

$$\max_{\rho} \mathcal{U}_1(\rho, P_2). \tag{3.25}$$

The SE of the game is then given by [SC73]

$$P_2^*(\rho) = \arg\max_{P_2} \mathcal{U}_2(\rho, P_2), \tag{3.26a}$$

$$\rho^* = \arg\max_{\rho} \mathcal{U}_1(\rho, P_2^*). \tag{3.26b}$$

The corresponding equilibrium utilities are $(\mathcal{U}_1(\rho^*, P_2^*(\rho^*)), \mathcal{U}_2(\rho^*, P_2^*(\rho^*)))$.

The Stackelberg interaction can be explained as follows. T_1, as a leader, sets some value to the parameter ρ, which T_2, as a follower, takes into account. The secondary transmitter then optimizes P_2 to maximize its own utility $\mathcal{U}_2(\rho, P_2)$. One can show that the second derivative of $\mathcal{U}_2(\rho, P_2)$ is given by

$$\begin{aligned}&\frac{\partial^2}{\partial P_2^2}\mathcal{U}_2(\rho, P_2) = \\ &-(1-\rho)\frac{c_{22}^2(c_{12}P_1+1)(\rho+(1+\rho)c_{12}P_1+2\rho c_{22}P_2+1)}{2\ln 2(c_{12}P_1+c_{22}P_2+1)^2(c_{12}P_1+\rho c_{22}P_2+1)^2}.\end{aligned} \tag{3.27}$$

Since $\rho \in [0,1]$, function $\mathcal{U}_2(\rho, P_2)$ is concave in P_2 and therefore, the optimal power as a function of the jamming power fraction is found by setting the derivative $\frac{\partial}{\partial P_2}\mathcal{U}_2(\rho, P_2)$ to zero. The optimal power allocation is then given by

$$P_2^*(\rho) = \left[\frac{\sqrt{(1-\rho)c\left[(1-\rho)bc+2\rho a\right]}}{\rho a\sqrt{b}} - \frac{(1+\rho)c}{\rho a}\right]_0^{P_2^{\max}}, \tag{3.28}$$

where $a \triangleq 2c_{22}$, $b \triangleq 2\ln 2\theta$, $c \triangleq 1 + c_{12}P_1$ and $[a]_{a_{\min}}^{a_{\max}} \triangleq \min\{a_{\min}, \max\{a_{\max}, a\}\}$.

Further, T_1 can compute the optimal jamming fraction ρ^* maximizing its own utility function $\mathcal{U}_1(\rho, P_2^*)$:

$$\rho^* = \arg\max_{0\le\rho\le 1} \mathcal{U}_1(P_2^*(\rho), \rho). \tag{3.29}$$

The optimal jamming fraction ρ^* is then plugged into (3.28) to obtain the optimal power level of the secondary transmitter $P_2^*(\rho^*)$. Thus, a pair $(P_2^*(\rho^*), \rho^*)$ determines the Stackelberg equilibrium for the game, i.e., the optimal power allocation for the secondary user.

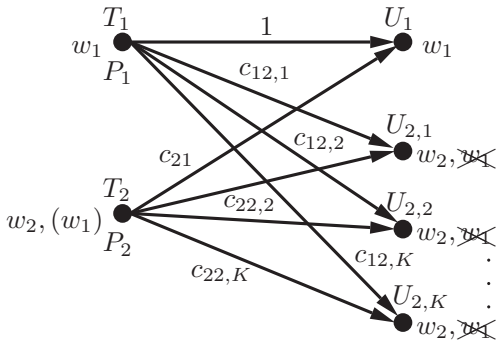


Figure 3.5: Cognitive radio channel with secrecy constraints and multiple secondary receivers.

Cooperation with Primary Message Knowledge at the Secondary Transmitter

Defining the utility functions in the same way, we let the primary transmitter set parameters ρ and γ. For ease of exposition, we define two following quantities. Let $\lambda \triangleq \rho + (1-\rho)\gamma$ be the fraction of the power the secondary transmitter devotes to helping the primary system (viz., it includes both jamming and relaying) and let $\mu \triangleq \frac{\rho}{\lambda}$ be the fraction of this power devoted only to jamming.

The procedure of the Stackelberg game is similar to the previous case. The secondary transmitter, as a follower, takes λ into account, and computes its power $P_2^*(\lambda)$ according to precisely the same solution as given in (3.28). Meanwhile, the primary transmitter can compute the optimal pair (λ^*, μ^*) maximizing its own utility function (3.24):

$$(\lambda^*, \mu^*) = \underset{\substack{0\leq\lambda\leq 1\\ 0\leq\mu\leq 1}}{\arg\max}\, \mathcal{U}_1(P_2^*(\lambda), \lambda, \mu). \tag{3.30}$$

Finally, knowing the optimal λ^* and μ^*, the secondary transmitter can compute its final power allocation $P_2^*(\lambda^*, \mu^*)$.

3.6 Extension to Multiple Secondary Receivers

In this section we extend our cognitive radio scenario to a network consisting of a primary transmitter T_1, a cognitive secondary transmitter T_2, a primary receiver U_1 and K secondary receivers $U_{2,k}$ with $k \in \{1, 2, \ldots, K\}$. T_1 intends to transmit the secret message w_1, which is intended to U_1, and which should not be decoded by the secondary receivers. T_2 transmits the message w_2 (without secrecy constraints) to the secondary receivers. Similarly to the previous sections, we investigate two different cooperative scenarios and their respective extensions to K secondary receivers, as represented in Figure 3.5. In the first scenario, T_2 has no knowledge of

the secret message w_1, it will therefore cooperate in the sense of a "deaf helper". In the second scenario, T_2 has knowledge of the secret message w_1.

Model Modifications

The primary and secondary receivers now receive:

$$\mathbf{y}_1 = \mathbf{x}_1 + \sqrt{c_{21}}\mathbf{x}_2 + n_1, \tag{3.31}$$

$$\mathbf{y}_{2,i} = \sqrt{c_{12,i}}\mathbf{x}_1 + \sqrt{c_{22,i}}\mathbf{x}_2 + n_{2,i}. \tag{3.32}$$

Information Theoretic Secrecy We are interested in the achievable rate pair (R_1, R_2) of messages w_1 and w_2, such that average error probabilities (noted $P_{e,1}$ and $P_{e,2}$) for both messages can be made arbitrarily small, while the message w_1 stays perfectly secure from the secondary receivers. In other terms, for any $\varepsilon > 0$ and a sufficiently large n:

$$\max\{P_{e,1}, P_{e,2}\} \leq \varepsilon \tag{3.33}$$

$$I(w_1; Y_{2,i}) \leq n\varepsilon \; \forall i \in \{1, 2, .., K\}. \tag{3.34}$$

Finally, without the cognitive transmitter T_2, the achievable secrecy rate is well-known as the channel reduces to the wiretap channel [Wyn75]:

$$R_{1,K}^{\mathrm{WT}} = \frac{1}{2}\left(\log(1 + P_1) - \max_i \log(1 + c_{12,i}P_1)\right)^+. \tag{3.35}$$

3.6.1 Cooperation without Message Knowledge at Secondary Transmitter

In this scenario, T_2 does not know the message w_1. T_2 splits its available power P_2 into three parts: $P_{2\mathrm{s}}$ for its own message w_2, $P_{2\mathrm{c}}$ for the common message and $P_{2\mathrm{j}}$ for a Gaussian jamming signal, such that $P_2 = P_{2\mathrm{s}} + P_{2\mathrm{c}} + P_{2\mathrm{j}}$. According to this power allocation, we have $R_2 = R_{2\mathrm{s}} + R_{2\mathrm{c}}$. According to this strategy, we give in the following theorem an achievable rate region for the case of multiple secondary receivers. We assume that the secondary message should be sent to a subset $\mathcal{S} \subseteq \{1, \ldots, K\}$ of secondary receivers.

Theorem 3.3.

The achievable rate pair (R_1, R_2), with $R_2 = R_{2\mathrm{c}} + R_{2\mathrm{s}}$ is given by the following region $\mathcal{R}_{1,m}$:

$$R_1 < \frac{1}{2}\left(\log\left(1+\frac{P_1}{1+c_{21}P_{2\mathrm{s}}+c_{21}P_{2\mathrm{j}}}\right) - \max_{k\in\{1,\ldots,K\}}\log\left(1+\frac{c_{12,k}P_1}{1+c_{22,k}P_{2\mathrm{j}}}\right)\right) \tag{3.36}$$

$$R_{2\mathrm{c}} < \frac{1}{2}\log\left(1+\frac{c_{21}P_{2\mathrm{c}}}{1+c_{21}P_{2\mathrm{s}}+c_{21}P_{2\mathrm{j}}}\right) \tag{3.37}$$

$$R_1 + R_{2\mathrm{c}} < \frac{1}{2}\left(\log\left(1+\frac{P_1+c_{21}P_{2\mathrm{c}}}{1+c_{21}P_{2\mathrm{s}}+c_{21}P_{2\mathrm{j}}}\right) - \max_{k\in\{1,\ldots,K\}}\log\left(1+\frac{c_{12,k}P_1}{1+c_{22,k}P_{2\mathrm{j}}}\right)\right) \tag{3.38}$$

$$R_{2\mathrm{s}} < \frac{1}{2}\min_{k\in\mathcal{S}}\log\left(1+\frac{c_{22,k}P_{2\mathrm{s}}}{1+c_{12,k}P_1+c_{22,k}P_{2\mathrm{j}}}\right) \tag{3.39}$$

$$R_{2\mathrm{c}} + R_{2\mathrm{s}} < \frac{1}{2}\min_{k\in\mathcal{S}}\log\left(1+\frac{c_{22,k}P_{2\mathrm{c}}+c_{22,k}P_{2\mathrm{s}}}{1+c_{12,k}P_1+c_{22,k}P_{2\mathrm{j}}}\right) \tag{3.40}$$

for every power splitting $P_2 = P_{2\mathrm{s}} + P_{2\mathrm{c}} + P_{2\mathrm{j}}$.

Proof. With multiple secondary receivers, $\mathcal{R}_{1,\mathrm{MAC}}$ stays unchanged. However the pair $(R_{2\mathrm{s}}, R_{2\mathrm{c}})$ should now belong to the separate decoding region of every secondary receiver, i.e., $(R_{2\mathrm{s}}, R_{2\mathrm{c}}) \in \cup_i \mathcal{R}_{2,i,\mathrm{SD}}$. This justifies the minimum terms in (3.39) and (3.40). Furthermore, by choosing $R_{1,e} = \max_{k\in\{1,\ldots,K\}}\log\left(1+\frac{c_{12,k}P_1}{1+c_{22,k}P_{2\mathrm{j}}}\right)$, we notice that $\forall R_2$, $R_{1,e} \notin \mathcal{R}_{i,e,\mathrm{MAC}} \cap \mathcal{R}_{i,e,\mathrm{SD}}$. We then obtain the achievable region $\mathcal{R}_{1,m}$ as in the single secondary receiver case. The two special cases defined above can as well be investigated for the multi-receiver case. ■

3.6.2 Cooperation with Message Knowledge at Secondary Transmitter

In this section we now assume that the secondary transmitter T_2 knows the primary message w_1 perfectly. We derive the achievable rate region in the case of multiple secondary receivers.

Theorem 3.4.

The achievable rate pair (R_1, R_2), with $R_2 = R_{2c} + R_{2s}$ is given by the following region $\mathcal{R}_2$:

$$R_1 < \frac{1}{2}\left(\log\left(1+\frac{P_1+c_{21}P_{2,1}}{1+c_{21}P_{2s}+c_{21}P_{2j}}\right) - \max_{k\in\{1,\dots,K\}}\log\left(1+\frac{c_{12,k}P_1+c_{22,k}P_{2,1}}{1+c_{22,k}P_{2j}}\right)\right) \tag{3.41}$$

$$R_1 + R_{2c} < \frac{1}{2}\log\left(1+\frac{P_1+c_{21}P_{2c}+c_{21}P_{2,1}}{1+c_{21}P_{2s}+c_{21}P_{2j}}\right) \tag{3.42}$$

$$R_{2s} < \frac{1}{2}\min_{k\in\mathcal{S}}\log\left(1+\frac{c_{22,k}P_{2s}}{1+c_{12,k}P_1+c_{22,k}P_{2j}+c_{22,k}P_{2,1}}\right) \tag{3.43}$$

$$R_2 < \frac{1}{2}\min_{k\in\mathcal{S}}\log\left(1+\frac{c_{22,k}P_{2c}+c_{22,k}P_{2s}}{1+c_{12,k}P_1+c_{22,k}P_{2j}+c_{22,k}P_{2,1}}\right), \tag{3.44}$$

for every power splitting $P_2 = P_{2s} + P_{2c} + P_{2j} + P_{2,1}$.

Proof. The proof is similar to the previous ones and it is therefore omitted here. ■

3.7 Numerical Results

In this section we present the results of numerical simulations and some related discussion. We divide the numerical results in two sections as follows. In Section 3.7.1 we aim at investigating the influence of the distances and the power splitting on the achievable rate regions. In Section 3.7.2 we elaborate on a more sophisticated geometrical framework to study the three optimization problems in terms of optimal rates, transmit power and strategies as well the impact of the Stackelberg game on those aforementioned variables.

3.7.1 Varying Setup

Our main objectives in this section are understanding the influence of the power splitting on the achievable rate pairs, comparing the rate regions with and without knowing the message w_1 at the secondary transmitter, and analyzing how the channel gains of the cognitive radio channel influence the rate regions. To achieve this goal, we consider a base setup where the distances between nodes are $d_{11} = d_{22} = 1$ and $d_{12} = d_{21} = 1.56$. The normalized transmit power at both transmitters is $P_1 = P_2 = 6$, the path-loss exponent is $\alpha = 3$.

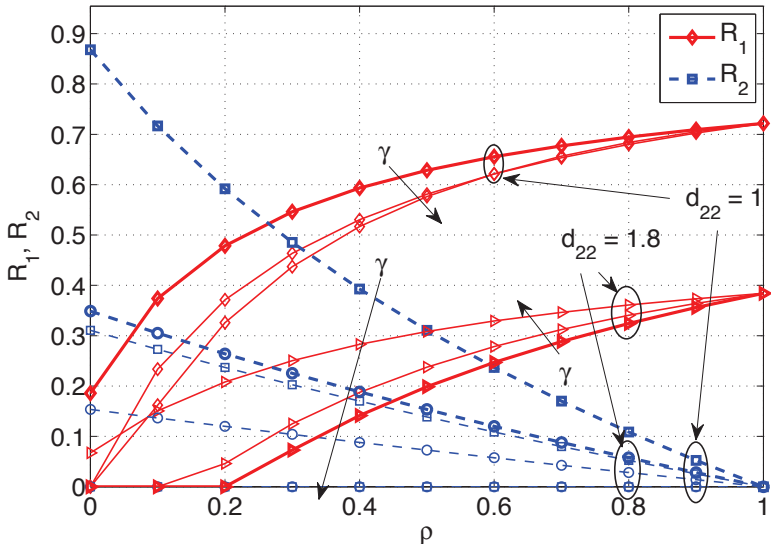


Figure 3.6: Achievable rates as functions of splitting variables ρ and γ for $\mathcal{S}_{2,\mathrm{SD}}$.

Rates as Functions of Power Splitting

In Figure 3.6, we observe the behavior of R_1 and R_2 for scenario $\mathcal{S}_{2,\mathrm{SD}}$. For our base case, $d_{22} = 1$, we see that increasing γ, i.e., the fraction of power used for transmitting w_1, decreases both rates. The decrease in R_1 comes from the fact that, in this case, U_2 is closer to T_2 than U_1, thus transmitting w_1 causes more leakage than gain in rate. R_2 also decreases since by increasing γ, we decrease the fraction of power available for transmitting w_2. When $d_{22} = 1.8$, i.e., U_2 is now further away from T_2, transmitting w_1 at U_2 is now beneficial, which explains the increase R_1 when γ increases.

Rate Regions as Functions of Distances

By taking the convex hull over all variations of the parameters ρ, β, and γ we obtain the achievable rate region. Figures 3.7, 3.8, 3.9 and 3.10 show those rate regions with (dashed) and without (solid) knowledge of w_1 at the secondary transmitter. The corresponding wiretap rate R_1^{WT} is depicted by the dash-dotted line. In each of the first three figures we change one of the three variable distances.

Decreasing d_{22} in Figure 3.7 increases R_1 and R_2 due to improved jamming and transmission of w_2, respectively. This also increases the optimum R_2^{opt} which is found at the intersection of the dash-dotted line and hull of the respective rate region. The benefit of knowing w_1 on R_2^{opt} is large.

The cross-distance d_{21} does not change the rate regions significantly in Figure 3.8. For the case without w_1 (solid), R_2^{opt} increases with decreasing d_{21} due to improved use of the common message. With w_1, however, the effect is reversed.

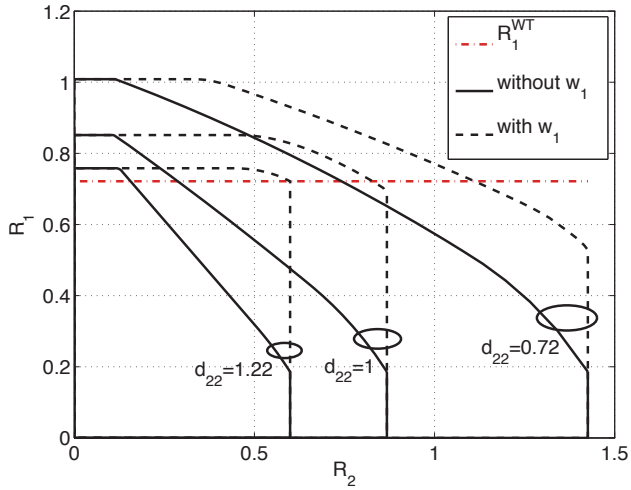


Figure 3.7: Rate regions with and without knowledge of w_1 for varying distance d_{22}.

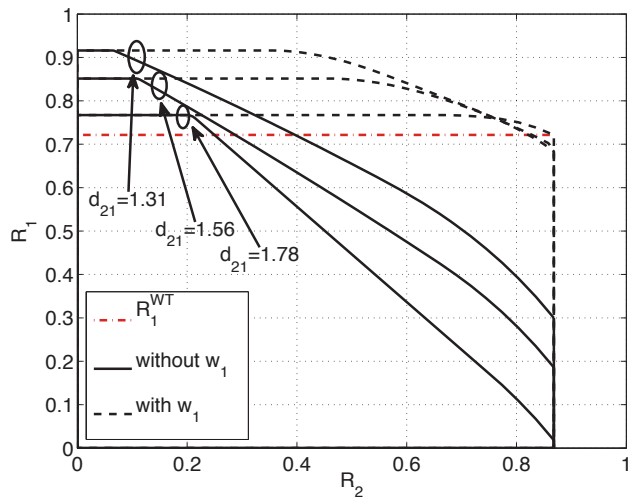


Figure 3.8: Rate regions with and without knowledge of w_1 for varying distance d_{21}.

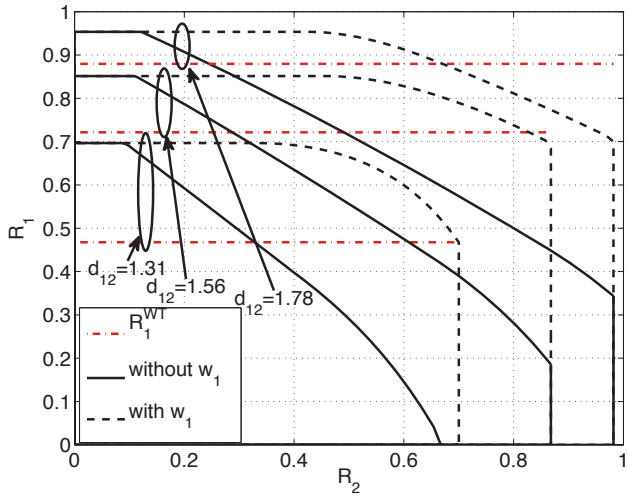


Figure 3.9: Rate regions with and without knowledge of w_1 for varying distance d_{12}.

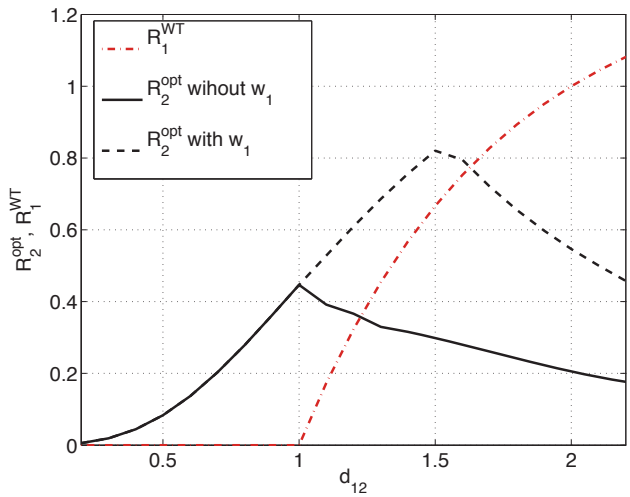


Figure 3.10: Optimal secondary rate with and without knowledge of w_1 for varying distance d_{12}.

This is because R_2^{opt} is achieved close to the maximum R_2. At this point T_2 transmits almost exclusively its own message. Hence, decreasing d_{21} increases the interference at U_1.

Increasing the second cross-distance d_{12} in Figure 3.9 increases R_1 and R_2 due to less leakage and less interference, respectively. Since the wiretap rate R_1^{WT} depends on d_{12}, we see an interesting effect on R_2^{opt}, which we investigate further in Figure 3.10. Without knowing w_1, the optimum R_2^{opt} increases as long as $R_1^{\text{WT}} = 0$.

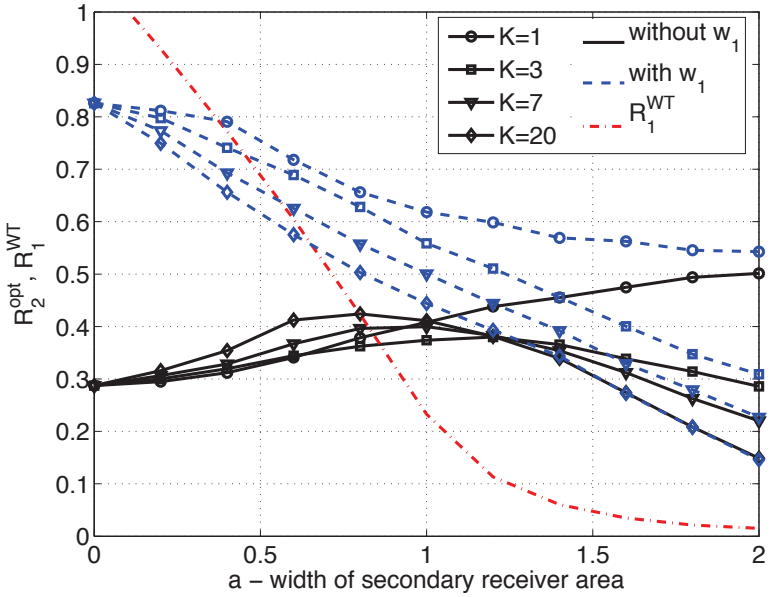


Figure 3.11: Optimal R_2 for multiple secondary receivers.

Due to the steep increase of R_1^{WT}, R_2^{opt} decreases subsequently. However, with knowledge of w_1 we can increase R_2^{opt} further, reaching more than two times the value of R_2^{opt} without knowledge of w_1. For d_{12} above a threshold of about 1.5, R_2^{opt} decreases for both cases, because leakage becomes negligible and R_1^{WT} approaches the point-to-point capacity of the link d_{11}. Overall, we conclude that knowing w_1 enlarges the rate regions significantly. The important figure of merit, R_2^{opt}, increases by more than 100% in some cases.

Multi-User Scenario

Finally, we consider the scenario with multiple secondary receivers. The K receivers are randomly located in a square of length a centered at the position of the secondary receiver in our base case. The locations are uniformly and independently distributed. Figure 3.11 shows how the optimum R_2^{opt} depends on K and a for the cases without (solid) and with (dashed) knowing w_1. The gain of knowing the message w_1 depends highly on the square size a. This is because if the square is large, a secondary receiver may appear close to the primary transmitter. In this case all power P_2 has to be used to jam that user; hence, there is no gain from knowing w_1. The probability of having such a critical receiver increases with K. Therefore this effect is more visible for high K.

To explain why R_2^{opt} obtains a maximum for high K without knowing w_1, we plot the wiretap rate $R_{1,K}^{\mathrm{WT}}$ for $K = 20$. It is steeply decreasing with a for $a < 1$. In this range the secondary transmitter can improve the system's performance and,

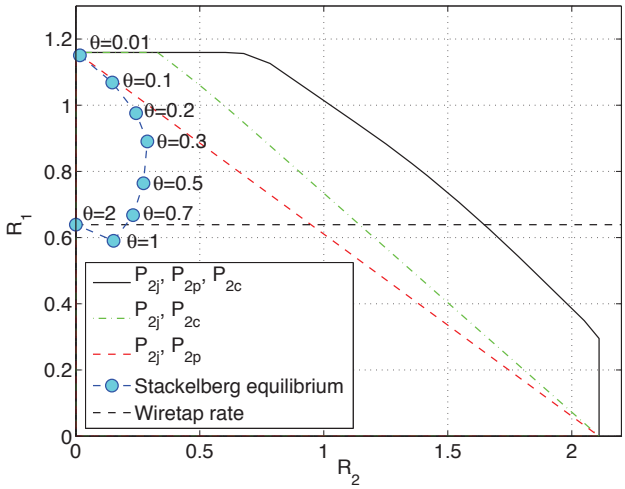


Figure 3.12: Rate regions for T_2 at $(0.5, 0)$.

hence, R_2^{opt}. However, when $R_{1,K}^{\text{WT}}$ flattens out, there is little room for improvement. T_2 has to sacrifice most of its power for jamming, which diminishes R_2.

3.7.2 Fixed Wiretap Channel Setup

In this section we develop a study framework by fixing the location of the primary transmitter and receiver at the coordinates $(0, 1)$ and $(1, 1)$, respectively. The secondary receiver is fixed at $(1, 0)$. We assume a path-loss model with path-loss exponent $\alpha = 3$, i.e., $c_{ij} = d_{ij}^{-3}$. The power constraints at both transmitters are $P_1^{\max} = P_2^{\max} = 10$. Each set of parameters (ρ, β, γ) yields a pentagon-shaped rate region. We vary the parameters over a sufficiently fine grid and take the convex hull over all corresponding rate regions.

We start by plotting the rate regions for a particular topology of interest revealing the importance of the different strategies of the secondary system, such as jamming, relaying and using a common message. We then reconsider the three optimization problems from the previous section – maximization of R_2 ($\mathcal{P}_{R_2}$), maximization of R_1 ($\mathcal{P}_{R_1}$), and minimization of P_2 ($\mathcal{P}_{P_2}$) – as well as the Stackelberg game. We study the secondary rate attained, as well as the consumed secondary power. In particular, we are interested in how the system behaves for different locations of the secondary transmitter.

3.7.3 Performance Optimization

In Figure 3.12 we plot the rate regions for T_2 being at the position $(0.5, 0)$. The black solid line corresponds to the region $\mathcal{S}_1$, where T_2 knows the primary message and can use all strategies: jamming, relaying and common message transmission.

The green dash-dotted line depicts the rate region $\mathcal{S}_2$ achievable by the oblivious helper that does not possess the primary message, $\gamma = 0$. If the primary receiver cannot decode a common message, $\beta = 0$, the regions $\mathcal{S}_{1,\mathrm{SD}}$ and $\mathcal{S}_{2,\mathrm{SD}}$ coincide. They are depicted by the dashed red line. In other words, knowing the primary message is not beneficial, if no common message can be sent. This is because T_2 is too far away from R_1 for relaying to be beneficial.

Furthermore, Figure 3.12 shows the optimal solution obtained by solving (3.50) and the SE points obtained by solving (3.29) for different cost values θ (blue dots). Note that for the case where power is cheap, i.e., θ is small, the rate of the secondary user R_2 tends to zero. This is due to the fact that even though the allowed power level P_2 for the secondary user is large, a larger fraction of jamming ρ is demanded by the primary user for the possibility to operate. Therefore, the secondary user becomes just a generous jammer that helps the primary system to reduce the leakage through link c_{12}. On the other hand, for large values of cost θ, the secondary user's utility $\mathcal{U}_2$ is dominated by the second term, i.e., $-\theta P_2$. Hence, utility maximization at the first step of the Stackelberg procedure reduces to minimization of the secondary power P_2. This yields $P_2 \to 0$ and the setup reduces to the wiretap channel. That is why the achievable rate R_1 for the primary user reduces to the wiretap rate R_1^{WT} for high costs θ. Thus, there exists an optimal value of the cost maximizing the secondary rate.

3.7.4 Performance Comparison

In this section we compare the results obtained from numerical solution of the optimization problems investigated in Section 3.4, i.e., problems $\mathcal{P}_{R_2}$, $\mathcal{P}_{R_1}$ and $\mathcal{P}_{P_2}$ (and their respective special cases), together with the Stackelberg equilibrium rate and power outcomes. We fix the positions of the primary terminals and the secondary receiver at the previous locations and vary the position of the secondary transmitter within a rectangle $\mathcal{R}$, with $\mathcal{R} \triangleq \{x_{T_2} \in [-1, 2] \cap y_{T_2} \in [-1, 2]\}$.

We furthermore illustrate the impact of this game on the achievable rates and on the transmission strategies of T_2, which we compare to the optimal rates, transmit power, and the strategies obtained from $\mathcal{P}_{R_2}$, $\mathcal{P}_{R_1}$ and $\mathcal{P}_{P_2}$.

Secondary Rate Maximization and Stackelberg Equilibrium

Figure 3.13 compares the achievable transmission rates R_2 of the secondary system, tolerable powers and necessary power splitting for different positions of the secondary transmitter. Each subfigure depicts the same spatial region, where the positions of the primary transmitter-user pair as well as the secondary user are marked by white circles. The colors show how the secondary rate and the different power fractions change as the secondary transmitter changes its position.

Figure 3.13 is constituted of three columns. The first column depicts the equilibrium outcomes of the Stackelberg game between T_1 and T_2, where the cost is set to $\theta = 0.1$. The second column represents the maximization $\mathcal{P}_{R_2}(\bar{\beta})$ of R_2 subject to

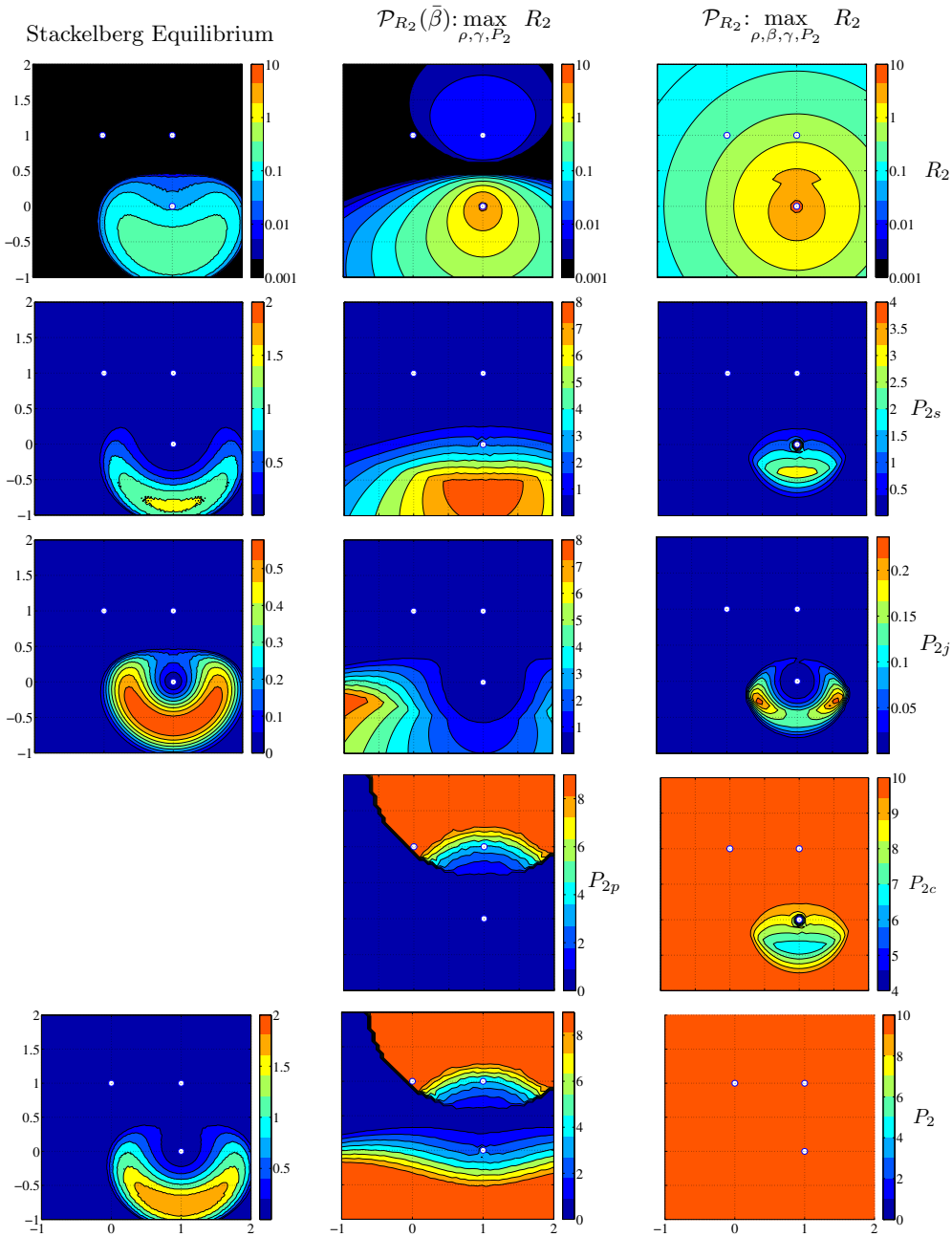


Figure 3.13: Operating secondary rates and powers depending on the position of T_2 for $\mathcal{P}_{R_2}$ and the Stackelberg game.

$R_1 \geq R_1^{\mathrm{WT}}$ with $\beta = 0$. The third column corresponds to the general optimization problem $\mathcal{P}_{R_2}$. The first row of subplots depicts the achievable secondary rate R_2 in logarithmic scale. The remaining rows show the power fractions $P_{2\mathrm{s}}$, $P_{2\mathrm{j}}$, $P_{2\mathrm{p}}$ for $\mathcal{P}_{R_2}(\bar{\beta})$ and $P_{2\mathrm{c}}$ for $\mathcal{P}_{R_2}$, while the last row shows the total required power P_2. In the fourth row for $\mathcal{P}_{R_2}$, $P_{2\mathrm{p}}$ is not presented since it is observed that the relaying power is always zero, i.e., T_2 prefers using common message to relaying for $\mathcal{P}_{R_2}$.

First, we compare the achievable R_2 for the three optimization problems in the first row. As expected, we observe that the Stackelberg equilibrium leads to lower rates, since T_2 maximizes its utility after T_1's maximization. Moreover, there is a cost for the power used in the Stackelberg model, whereas power conservation is not crucial in the other rate maximization problems. Higher rates are achieved for $\mathcal{P}_{R_2}$ than for $\mathcal{P}_{R_2}(\bar{\beta})$ since more strategies are available at T_2.

We also note that for the maximization of R_2, the peak of the achievable rate is located exactly at the position of the secondary receiver U_2, which reflects the fact that for the path-loss channel model the closer the communicating terminals, the higher the transmission rate. Interestingly, in contrast to this result, for the Stackelberg equilibrium solution, the optimal location of the secondary transmitter that maximizes the utility $\mathcal{U}_2$ is shifted further away from the primary system. To conclude the analysis of the game theoretic solution, we note the low power consumption of T_2 in the SE (around 20% of the allowed transmission power) which justifies the lower R_2. The Stackelberg strategy represents balancing between own message power $P_{2\mathrm{s}}$, necessary to achieve a strictly positive utility, and jamming power $P_{2\mathrm{j}}$ needed in order not to deteriorate the primary transmission in terms of secrecy.

We now compare the second and third columns of Figure 3.13, corresponding to $\mathcal{P}_{R_2}(\bar{\beta})$ and $\mathcal{P}_{R_2}$, respectively. First, we notice that for $\mathcal{P}_{R_2}$, all the available power is utilized for all locations of T_2, while this is not the case for $\mathcal{P}_{R_2}(\bar{\beta})$. This is due to the fact that when there is no common message, a power threshold exists above which T_2 cannot transmit without breaching the constraint $R_1 \geq R_1^{\mathrm{WT}}$, by either creating additional interference at the primary user from $P_{2\mathrm{s}}$ or $P_{2\mathrm{j}}$ or by leaking information to the secondary user from $P_{2\mathrm{p}}$.

Comparing the figures in the first row, we notice that the achievable secondary rates R_2 are significantly higher for $\mathcal{P}_{R_2}$. Furthermore, for some topologies the problem $\mathcal{P}_{R_2}(\bar{\beta})$ does not yield a positive secondary rate R_2, which means that the secondary system cannot operate. This is the case in the black regions. Thus, there exists a considerable performance improvement between the cases with and without common message. Opportunity to transmit a message that can be decoded by both users is game changing. It should be noted, though, that this demands advanced decoding capabilities, which might not be provided by the primary system.

Finally, we discuss the power allocations for $\mathcal{P}_{R2}(\bar{\beta})$ and $\mathcal{P}_{R2}$. For $\mathcal{P}_{R2}$, most of the power is allocated to the common message as expected, while the power allocated for jamming and own message is concentrated in the locations close to U_2. For $\mathcal{P}_{R2}(\bar{\beta})$, we observe that the power allocations depending on (x_{T_2}, y_{T_2}) conforms to the intuition: a high proportion (up to 90%) of the power is used for

relaying when T_2 is located close to U_1. Moreover, $P_{2\mathrm{s}}$ is higher when T_2 is close to U_2 and on the opposite side from U_1, so that interference is low at U_1. Meanwhile, jamming is used in high proportions for locations of T_2 where it cannot hurt the primary transmission.

We conclude that the secondary system benefits strongly if U_1 can decode a common message. Transmitting a common message is the predominant strategy. If no common message can be used ($\beta = 0$), the system has to rely on relaying and jamming. This reduces the secondary rate or even prohibits the operation of the secondary system. The Stackelberg game results in much less total power consumption P_2 at the cost of reduced secondary rate. Note that this trade-off can be changed to some extent by adjusting the cost ϑ.

Primary Rate Maximization

Figure 3.14 illustrates problem $\mathcal{P}_{R_1}$, namely the maximization of the primary rate R_1, and the corresponding secondary transmit power allocation. The threshold on the secondary rate R_2^{thr} is set to 80% of the maximum R_2, which was attained in problem $\mathcal{P}_{R_2}$. Note that the threshold depends on the position of T_2. In other words, we ask how much R_1 can be increased if the secondary system reduces its rate by 20%. The results in Figure 3.14 are depicted for two problems, the first column is $\mathcal{P}_{R_1}(\bar{\beta})$ and the second column is $\mathcal{P}_{R_1}$. Note that we use the last row for depicting P_2 and $P_{2\mathrm{c}}$ for $\mathcal{P}_{R_1}(\bar{\beta})$ and $\mathcal{P}_{R_1}$, respectively. We have $P_{2\mathrm{c}} = 0$ for $\mathcal{P}_{R_1}(\bar{\beta})$, while $P_2 = 10$ everywhere for $\mathcal{P}_{R_1}$.

Interestingly, for $\mathcal{P}_{R_1}$, R_1 can be significantly increased if T_2 is close to U_1. In this case relaying is beneficial and becomes the predominant strategy. The 80% of R_2 are attained by a fraction $P_{2\mathrm{c}}$, so that the remaining power is used for relaying. In $\mathcal{P}_{R_1}(\bar{\beta})$, however, almost all the power was already used for relaying. Reducing R_2 frees only marginal amounts of power, and hence R_1 cannot be increased significantly.

If T_2 is close to U_2, the rate R_1 can only be increased marginally for both $\mathcal{P}_{R_1}(\bar{\beta})$ and $\mathcal{P}_{R_1}$. Less power is required for transmitting both the secondary and the common messages. Therefore, R_1 can be increased by jamming slightly more than for the problem $\mathcal{P}_{R_2}$. Again, our results show the importance of the common message strategy. Not only is the secondary rate R_2 higher; the strategy also permits to significantly increase the primary rate R_1, having R_2 reduced.

Secondary Power Minimization

To evaluate the power minimization problem, we calculate the rate regions for successive increase of P_2. We find the minimum P_2 such that the rate constraints are fulfilled. Like in previous simulations, R_2^{thr} is set at 80% of the maximum rate R_2 found by for the problems $\mathcal{P}_{R_2}(\bar{\beta})$ and $\mathcal{P}_{R_2}$, respectively. The result is depicted in Figure 3.15, structured similarly as before, except that the total power P_2 is

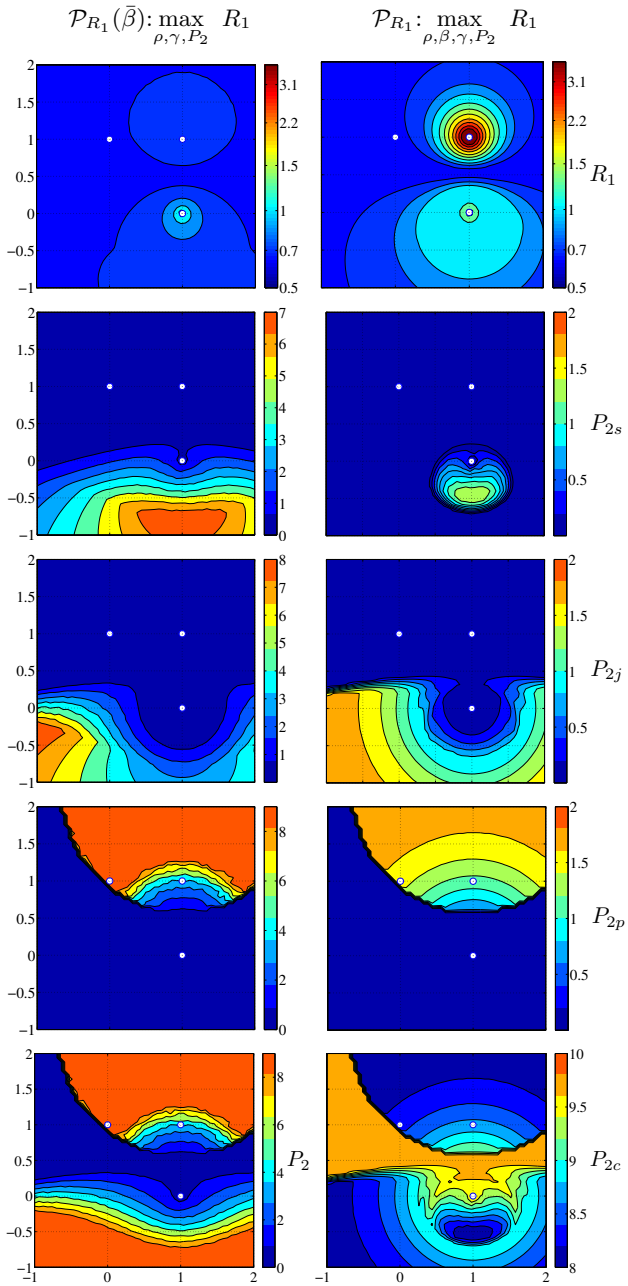


Figure 3.14: Operating primary rates and powers depending on the position of T_2 for $\mathcal{P}_{R_1}$.

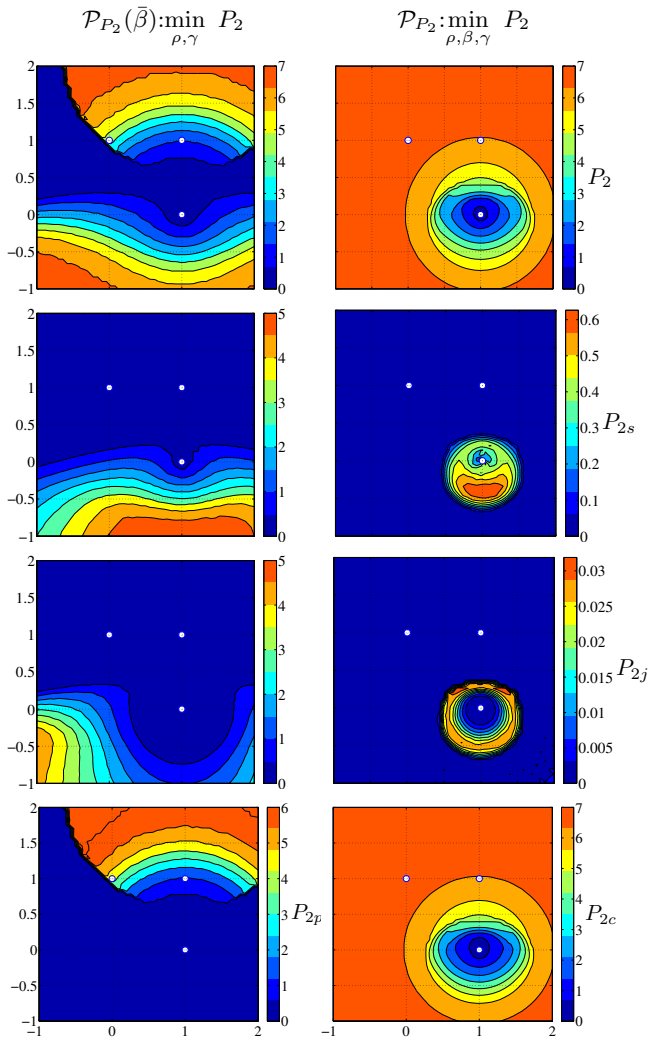


Figure 3.15: Operating powers depending on the position of T_2 for $\mathcal{P}_{P_2}$.

shown in the first row, while the other rows describe the power allocation strategies adopted by T_2.

First, we compare the corresponding values of P_2 in the last row and second and third column of Figure 3.13. We see that the overall power consumption has been significantly reduced compared to the rate maximization problems. The effect is the most significant for $\mathcal{P}_{P_2}$ since all available power P_2 was utilized for all locations of T_2 in the problem $\mathcal{P}_{R_2}$. Interestingly, the power saving opportunities are most prominent around the location of U_2.

We now visualize that the power allocation strategies depending on (x_{T_2}, y_{T_2}) are noticeably similar to the strategies adopted for the secondary rate maximizations depicted in Figure 3.13. In particular for $\mathcal{P}_{P_2}(\bar{\beta})$, in a large region between U_1 and U_2, T_2 does not transmit since no rate $R_2 > 0$ is achievable without hurting the primary system. When T_2 is close to U_2 on the opposite side of U_1, most of P_2 is allocated to T_2's own message; while when T_2 is closer to U_1 in the opposite side of U_2, the power is mainly allocated to relaying. Finally, we make the interesting observation that when T_2 is close enough to U_2 and common message is available, even power P_2 close to zero suffices to satisfy the rate constraints.

3.8 Conclusions

We summarize the chapter's contributions and we make some important remarks.

Summary In this chapter we investigated transmission strategies for the secondary transmitter in a cognitive radio channel to enhance the secrecy of the primary message. Based on achievable rate regions for two different cognitive scenarios, we defined three main optimization problems: the maximization of the secondary rate without decreasing the secrecy of the primary message, the maximization of the primary secrecy rate and the minimization of the secondary transmit power. We found solutions in closed-form for special cases of these optimizations.

We then assumed a more realistic cooperative scenario where we modeled the interaction between both transmitters as a Stackelberg competition. We derived the Stackelberg equilibrium for this game and analyzed its impact numerically in comparison to the fully cooperative case. While the secondary rate attained at the SE is lower than the maximum possible rate, the consumption of secondary power is much less. We observed this from the rate region for a specific topology as well as from our simulations of a varying topology, where we changed the position of the secondary transmitter T_2.

We also studied the optimization problems $\mathcal{P}_{R_2}$, $\mathcal{P}_{P_2}$ and $\mathcal{P}_{R_1}$ in our geometrical setup. We showed that the transmission of a common message, which can be decoded by both receivers, is a powerful strategy. We then reduced the rate R_2 by 20% and examined how this increased the primary rate R_1 or decreased the secondary power P_2 in $\mathcal{P}_{R_1}$ and $\mathcal{P}_{P_2}$, respectively. While T_2 being located close to U_1 is optimal for maximizing R_1, the opportunity for reducing the power P_2 is largest if T_2 is close to U_2. This is due to the possibility of effective relaying in the first case, and of transmitting the secondary message, in the other case.

Concluding Remarks The network model investigated in this chapter can be used as a starting framework to investigate more complicated cognitive radio networks with secrecy constraints, e.g., with multiple secondary transmitters as in Chapter 5. While cognitive radio networks are usually more complex than the 4-node network studied in this chapter due their *ad hoc* nature, we believe that the insight provided in this chapter on the impact of the transmission strategies on the achievable rates is important to the understanding of secrecy mechanisms in CRN.

However several simplifying assumptions made in the chapter should be further discussed. First, while the scenario $\mathcal{S}_2$ where T_2 has non-causal knowledge of the primary message can be justified, e.g., if there is a phase where T_2 learns w_1 before the transmission studied in this chapter occurs, this learning phase should have in general an impact on the secrecy of w_1. Therefore this problem of interest in investigated in Chapter 4. Secondly, if U_1 does not have multi-user decoding capabilities, the transmission scheme employed by the secondary transmitter should be adapted; and this modification will also be studied in Chapter 4.

3.A Proof of Theorem 3.1

Proof. First, the primary receiver can either perform joint decoding or separate decoding for w_1 and the common message. In particular, all rates in the joint decoding MAC region $\mathcal{R}_{1,\mathrm{MAC}}$ given by:

$$R_1 < \frac{1}{2}\log\left(1+\frac{P_1}{1+c_{21}P_{2\mathrm{s}}+c_{21}P_{2\mathrm{j}}}\right) \tag{3.45}$$

$$R_{2\mathrm{c}} < \frac{1}{2}\log\left(1+\frac{c_{21}P_{2\mathrm{c}}}{1+c_{21}P_{2\mathrm{s}}+c_{21}P_{2\mathrm{j}}}\right) \tag{3.46}$$

$$R_1+R_{2\mathrm{c}} < \frac{1}{2}\log\left(1+\frac{P_1+c_{21}P_{2\mathrm{c}}}{1+c_{21}P_{2\mathrm{s}}+c_{21}P_{2\mathrm{j}}}\right) \tag{3.47}$$

are achievable. We observe that in $\mathcal{R}_{1,\mathrm{MAC}}$, the secondary message and the jamming signal are treated as interference by the primary receiver. Similarly, the secondary receiver can perform joint decoding or separate decoding for its own message w_2 and the common message. In particular, all the rates in the MAC $\mathcal{R}_{2,\mathrm{MAC}}$ region are achievable:

$$R_{2\mathrm{s}} < \frac{1}{2}\log\left(1+\frac{c_{22}P_{2\mathrm{s}}}{1+c_{12}P_1+c_{22}P_{2\mathrm{j}}}\right) \tag{3.48}$$

$$R_{2\mathrm{c}}+R_{2\mathrm{s}} < \frac{1}{2}\log\left(1+\frac{c_{22}P_{2\mathrm{c}}+c_{22}P_{2\mathrm{s}}}{1+c_{12}P_1+c_{22}P_{2\mathrm{j}}}\right), \tag{3.49}$$

where the constraint on $R_{2\mathrm{c}}$ was redundant, and the primary message and the jamming signal are viewed as interference.
From the eavesdropper's (i.e., U_2) point of view, the rate pair has to be in the $\mathcal{R}_{e,\mathrm{MAC}}$ *or* the $\mathcal{R}_{e,\mathrm{SD}}$ region to be decodable. $\mathcal{R}_{e,\mathrm{MAC}}$ is defined by:

$$\begin{aligned}
R_1 &< \frac{1}{2}\log\left(1+c_{12}\frac{P_1}{1+c_{22}P_{2\mathrm{j}}}\right)\\
R_2 &< \frac{1}{2}\log\left(1+\frac{c_{22}P_{2\mathrm{c}}+c_{22}P_{2\mathrm{s}}}{1+c_{22}P_{2\mathrm{j}}}\right)\\
R_1+R_2 &< \frac{1}{2}\log\left(1+\frac{c_{12}P_1+c_{22}P_{2\mathrm{c}}+c_{22}P_{2\mathrm{s}}}{1+c_{22}P_{2\mathrm{j}}}\right),
\end{aligned}$$

while $\mathcal{R}_{e,\mathrm{SD}}$ is defined by

$$\begin{aligned}
R_1 &< \frac{1}{2}\log\left(1+\frac{c_{12}P_1}{1+c_{22}P_2}\right)\\
R_2 &> \frac{1}{2}\log\left(1+\frac{c_{22}P_{2\mathrm{c}}+c_{22}P_{2\mathrm{s}}}{1+c_{22}P_{2\mathrm{j}}}\right).
\end{aligned}$$

Finally the rate pair (R_1, R_2) is achievable if $R_1 = R_{1,p} - R_{1,e}$, $(R_{1,p}, R_2) \in (\mathcal{R}_{1,\mathrm{MAC}} \cap \mathcal{R}_{2,\mathrm{MAC}})$ and $(R_{1,e}, R_2) \notin (\mathcal{R}_{e,\mathrm{MAC}} \cup \mathcal{R}_{e,\mathrm{SD}})$. $R_{1,e}$ is a parameter of

the wiretap code used by T_p and it represents the amount of rate that T_p has to sacrifice in order to confuse the eavesdropper. Therefore, the "useful" rate for the primary message becomes $R_{1,p} - R_{1,e}$, where $R_{1,p}$ was achievable without secrecy constraints.

Choosing $R_{1,e} = \log\left(1 + \frac{c_{12}P_1}{1+c_{22}P_{2\mathrm{j}}}\right)$, we notice that $\forall R_2$, $(R_{1,e}, R_2) \notin \mathcal{R}_{e,\mathrm{MAC}} \cup \mathcal{R}_{e,\mathrm{SD}}$. We then obtain the achievable region $\mathcal{R}_1$ by replacing R_1 by $R_1 + R_{1,e}$ in (3.45) and (3.47) and after some manipulations on the inequalities. ■

3.B Proof of Proposition 3.1

Proof. The rate region $\mathcal{S}_{1,\mathrm{SD}}$ for $\gamma = 0$ is given by equations (3.13a) and (3.13b). First, consider that R_1 increases with increasing ρ, whereas R_2 decreases with decreasing ρ due to (3.13a) and (3.13b). Hence, any change of parameters that increases R_1 is also decreasing R_2. Therefore, the maximum R_2 will be attained for $R_1 = R_1^{\mathrm{WT}}$. We solve

$$\mathcal{C}\left(\frac{P_1}{1+c_{21}P_2}\right) - \mathcal{C}\left(\frac{c_{12}P_1}{1+c_{22}\rho P_2}\right) = \mathcal{C}(P_1) - \mathcal{C}(c_{12}P_1),$$

which yields

$$\rho^\star = \frac{c_{21}(1+c_{12}P_1)}{c_{22}\left[c_{12}(1+P_1) - c_{21}P_2(1-c_{12})\right]}. \tag{3.50}$$

Plugging $\rho^\star$ into (3.13b) yields

$$2^{2R_2^\star} = \frac{[c_{12}(1+P_1) - (1-c_{12})c_{21}P_2](1+c_{12}P_1+c_{22}P_2)}{c_{12}(1+c_{12}P_1)(1+P_1+c_{21}P_2)}$$

for the maximum achievable secondary rate $R_2^\star$. Maximizing 2^{2R_2} is equivalent to maximizing R_2, since $R_2 \geq 0$. We realize that $R_2^\star$ is not necessarily maximized by using all the available secondary power $P_2 = P_2^{\mathrm{thr}}$. The condition for an extremum in P_2, $\frac{\partial 2^{2R_2}}{\partial P_2} = 0$ reduces to

$$a_{R_2}P_2^2 + b_{R_2}P_2 + c_{R_2} = 0, \tag{3.51}$$

with

$$a_{R_2} \triangleq (1-c_{12})c_{21}^2c_{22}, \tag{3.52}$$

$$b_{R_2} \triangleq 2(1-c_{12})c_{21}c_{22}(1+P_1), \tag{3.53}$$

$$c_{R_2} \triangleq (1+P_1)[c_{21}(1+c_{12}P_1) - c_{12}c_{22}(1+P_1)]. \tag{3.54}$$

In order for R_1^{WT} to be positive, we require $c_{12} < 1$. This yields $a_{R_2} > 0$ and $b_{R_2} > 0$; hence, there exists at most one positive extremum

$$P_2^{\mathrm{crit}} = \frac{1}{2a_{R_2}}\left(\sqrt{b_{R_2}^2 - 4a_{R_2}c_{R_2}} - b_{R_2}\right). \tag{3.55}$$

The second derivative $\frac{\partial^2 2^{2R_2}}{\partial {P_2}^2}$ at $P_2 = P_2^{\text{crit}}$ is negative, which means that P_2^{crit} is the maximum we were seeking for. In the degraded scenario in which $P_2^{\text{crit}} < P_2^{\text{thr}}$, R_2 is decreasing for $P_2 > 0$. Furthermore, if $P_2^{\text{crit}} > P_2^{\text{thr}}$, the maximum feasible R_2 is attained at $P_2 = P_2^{\text{thr}}$. Finally,

$$P_2^\star = \min\left((P_2^{\text{crit}})^+, P_2^{\text{thr}}\right). \tag{3.56}$$

To calculate the corresponding $R_2^\star$, we plug $P_2^\star$ into (3.50); then we plug both values into (3.13b). We notice that the maximum R_2 is limited by the secrecy constraint which causes the limited feasible values of P_2 and the corresponding parameters. ■

3.C Proof of Proposition 3.2

Proof. Being in general non-convex, the problem can be simplified by reformulating the rate constraints into constraints on the secondary power. We solve both constraints (3.20b) and (3.20c) for P_2. The first constraint (3.20b) yields:

$$P_2^2 x_{P_2} + P_2 y_{P_2} \geq 0 \tag{3.57}$$

with

$$x_{P_2} \triangleq c_{21}c_{22}\left(\rho - \hat{R}_1\left(\rho + \gamma(1-\gamma)(1-\rho)^2\right)\right), \tag{3.58a}$$

$$\begin{aligned} y_{P_2} \triangleq\ & c_{21} + (1+P_1)c_{22}\rho - \hat{R}_1 c_{22}(\gamma + \rho - \gamma\rho) \\ & - \hat{R}_1 c_{21}(1 + c_{12}P_1)(1 - \gamma + \gamma\rho). \end{aligned} \tag{3.58b}$$

where we used the expressions (3.4) and (3.14) for R_1^{WT} and R_1, respectively. We also introduced the short-hand notation $\hat{R}_1 = 2^{2R_1^{\text{WT}}}$. Since $\hat{R}_1 > 1$, we have $x_{P_2} < 0$, hence, (3.57) yields

$$P_2 \leq -\frac{y_{P_2}}{x_{P_2}} = P_2^{\star(1)}. \tag{3.59}$$

Similarly, with $\hat{R}_2 = 2^{2R_2^{\text{thr}}}$, the secondary rate constraint (3.20c) in conjunction with (3.15) yields:

$$\frac{c_{22}P_2(1-\rho)(1-\gamma)}{1 + c_{12}P_1 + c_{22}P_2(\rho + \gamma - \rho\gamma)} \geq \hat{R}_2 - 1. \tag{3.60}$$

To solve for P_2 we transform the above equation to

$$c_{22}P_2(1 - \hat{R}_2(\rho + \gamma - \rho\gamma)) \geq (\hat{R}_2 - 1)(1 + c_{12}P_1). \tag{3.61}$$

We see that for $\hat{R}_2(\rho + \gamma - \rho\gamma) < 1$ we get the constraint

$$P_2 \geq \frac{(\hat{R}_2 - 1)(1 + c_{12}P_1)}{c_{22}(1 - \hat{R}_2(\rho + \gamma - \rho\gamma))} = P_2^{\star(2)}, \tag{3.62}$$

whereas for $\hat{R}_2(\rho+\gamma-\rho\gamma) \geq 1$, there is no solution to (3.61).

Accordingly, the feasible set for the optimization of P_2 is defined by $P_2^{\star(1)} \geq P_2^{\star(2)}$ when $\hat{R}_2(\rho+\gamma-\rho\gamma) < 1$. We see that $P_2^{\star(2)}$ is increasing in both γ and ρ, so the optimal P_2 lies in the intersection $P_2^{\star(1)} = P_2^{\star(2)}$ to get the minimum value. However, if there is no intersection of $P_2^{\star(1)}$ and $P_2^{\star(2)}$, there are two possible cases. First, $P_2^{\star(1)} \geq P_2^{\star(2)}$ everywhere, i.e., all values of ρ and γ are feasible. Second, $P_2^{\star(1)} < P_2^{\star(2)}$ everywhere, i.e., no feasible ρ or γ, which cannot apply. We easily see that the first case cannot apply either: at $\rho = \gamma = 0$, T_2 uses all its power to transmit its own secondary message. Hence, for any $P_2 > 0$, we have $R_1 < R_1^{\mathrm{WT}}$. This means that we cannot have $R_2 > 0$ at this point, which violates any reasonable constraint $R_2 \geq R_2^{\mathrm{thr}}$. With the two cases excluded, the smallest feasible value for P_2 has to lie in this intersection. Hence, the previous problem simplifies to

$$\min_{\gamma,\rho} \; P_2^{\star(2)} \tag{3.63a}$$

$$\text{s.t. } P_2^{\star(1)} = P_2^{\star(2)} \quad \text{and} \quad \rho+\gamma-\rho\gamma < 1/\hat{R}_2. \tag{3.63b}$$

In the following, we consider the optimization for $\rho = 0$ and $\gamma = 0$ separately; i.e., T_2 either acts as a deaf helper or has access to w_1 and cooperates actively.

Closed-form Expression for $\mathcal{P}_{P_2}(\bar{\beta},\bar{\gamma})$ For $\gamma = 0$, i.e., for the oblivious cooperation scenario, $P_2^{\star(1)} = P_2^{\star(2)}$ yields

$$\rho^2 a_{P_2} + \rho b_{P_2} + c_{P_2} = 0 \tag{3.64}$$

with

$$a_{P_2} \triangleq \hat{R}_2 c_{22}(1+P_1-\hat{R}_1), \tag{3.65}$$

$$b_{P_2} \triangleq c_{21}(\hat{R}_1-1)(\hat{R}_2-1)(1+c_{12}P_1) - c_{22}(1+P_1-\hat{R}_1) - c_{21}P_1\hat{R}_2, \tag{3.66}$$

$$c_{P_2} \triangleq c_{21}P_1. \tag{3.67}$$

Note that a_{P_2}, b_{P_2} and c_{P_2} are constants and $a_{P_2} > 0$. Hence, the only positive solution for ρ is

$$\rho^\star = \frac{1}{2a_{P_2}}\left(\sqrt{b_{P_2}^2 - 4a_{P_2}c_{P_2}} - b_{P_2}\right). \tag{3.68}$$

The solution is feasible if $\rho^\star < 1/\hat{R}_2$, otherwise there exists no solution.

Closed-form Expression for $\mathcal{P}_{P_2}(\bar{\beta},\bar{\rho})$ For $\rho = 0$, i.e., with message knowledge, $P_2^{\star(1)} = P_2^{\star(2)}$ yields

$$\gamma^2 d_{P_2} + \gamma e_{P_2} + f_{P_2} = 0 \tag{3.69}$$

with

$$d_{P_2} \triangleq c_{21}(1+P_1) - c_{22}\hat{R}_1\hat{R}_2, \tag{3.70}$$

$$e_{P_2} \triangleq c_{22}\hat{R}_1 - c_{21}(2(1+P_1) - P_1\hat{R}_2), \tag{3.71}$$

$$f_{P_2} \triangleq c_{21}P_1. \tag{3.72}$$

(3.69) has two solutions

$$\gamma^{\star,1} \triangleq \frac{1}{2d_{P_2}}\left(\sqrt{e_{P_2}^2 - 4d_{P_2}f_{P_2}c'} - e_{P_2}\right), \tag{3.73a}$$

$$\gamma^{\star,2} \triangleq \frac{1}{2d_{P_2}}\left(-\sqrt{e_{P_2}^2 - 4d_{P_2}f_{P_2}} - e_{P_2}\right). \tag{3.73b}$$

In order to be feasible, the solutions need to lie within the interval $(0, 1/\hat{R}_2)$. The optimum $\gamma^\star$ is the minimum of the feasible solutions, because $P_2^{\star(2)}$ is increasing in γ. ■

3.D Proof of Proposition 3.3

Proof. From equation (3.13a) we see that R_1 increases with ρ. If we plug (3.13b) into the constraint (3.21b), we see that R_2 decreases with ρ. Hence, the maximum R_1 will be attained for $R_2 = R_2^{\text{thr}}$, which we solve for $\rho^\star$ as

$$\rho^\star = \frac{c_{22}P_2 - (\hat{R}_2 - 1)(1 + c_{12}P_1)}{c_{22}P_2\hat{R}_2}, \tag{3.74}$$

in which $\hat{R}_2 = 2^{2R_2^{\text{thr}}}$. By plugging (3.74) into (3.13a), we get the following expression for the maximum rate $R_1^\star$,

$$2^{2R_1^\star} = \frac{(1 + P_1 + c_{21}P_2)(1 + c_{12}P_1 + c_{22}P_2 - c_{12}P_1\hat{R}_2)}{(1 + c_{12}P_1)(1 + c_{12}P_1 + c_{22}P_2)}. \tag{3.75}$$

The expression, and thus $R_1^\star$, is not necessarily maximized by using all secondary power $P_2 = P_2^{\text{thr}}$. So we solve $\frac{\partial 2^{2R_1^\star}}{\partial P_2} = 0$, which is reduced to

$$a_{R_1}P_2^2 + b_{R_1}P_2 + c_{R_1} = 0, \tag{3.76}$$

with

$$a_{R_1} \triangleq c_{21}c_{22}(c_{12}c_{21}\hat{R}_2 - c_{22}), \tag{3.77}$$

$$b_{R_1} \triangleq 2c_{21}c_{22}(\hat{R}_2 - 1 - c_{12}P_1), \tag{3.78}$$

$$c_{R_1} \triangleq c_{12}c_{22}\hat{R}_2(1 + P_1) + c_{21}(1 + c_{12}P_1)(c_{12}P_1(\hat{R}_2 - 1) - 1). \tag{3.79}$$

The two solutions of the quadratic equation

$$P_2^{\text{crit},1} \triangleq \frac{1}{2a_{R_1}}\left(\sqrt{b_{R_1}^2 - 4a_{R_1}c_{R_1}} - b_{R_1}\right), \tag{3.80a}$$

$$P_2^{\mathrm{crit},2} \triangleq \frac{1}{2a_{R_1}} \left(-\sqrt{b_{R_1}^2 - 4a_{R_1}c_{R_1}} - b_{R_1} \right), \tag{3.80b}$$

are candidates for the rate maximizing power P_2. We find the maximum R_1 by plugging the two values $P_2^{\star,1} = \min\left((P_2^{\mathrm{crit},1})^+, P_2^{\mathrm{thr}}\right)$ and $P_2^{\star,2} = \min\left((P_2^{\mathrm{crit},2})^+, P_2^{\mathrm{thr}}\right)$ into (3.75) and and selecting the one that maximizes (3.75). ■

Chapter 4

Clean Relaying for Cognitive Radio Channels with Secrecy

In this chapter we investigate clean relaying for secrecy in cognitive radio channels. First, we present the list of the chapter's goals.

Objectives of the Chapter.

- Extend the results of Chapter 3 in three directions:
  1. by investigating the impact of the learning phase at the secondary transmitter for the primary message;
  2. by considering a more realistic cognitive scenario where the primary user does not have multi-user decoding capabilities;
  3. by using a stronger secrecy measure for the primary message.
- Introduce the clean relaying (CR) scheme for our cognitive radio scenario with secrecy constraints.
- Derive the achievable rate region for the multi-phase CR scheme investigated in this chapter and compare this scheme to other signalling strategies, namely dirty paper coding (DPC), cooperative jamming (CJ) and interference neutralization (IN).
- Use the geometrical model developed in previous chapters to numerically compare the secrecy performance of the schemes.

Organization of the Chapter This chapter is organized as follows. In Section 4.1 we motivate the study in this chapter. In Section 4.2 we define our system

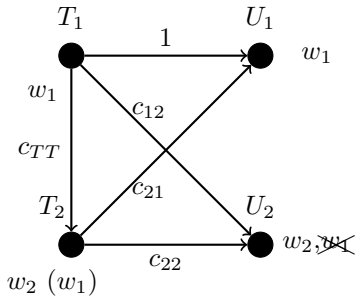
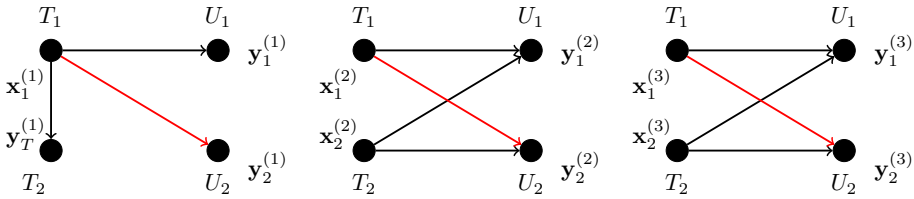


Figure 4.1: Cognitive channel with secrecy constraints.

model. In Section 4.3 we establish our main result and we formulate our optimization problem investigated throughout the chapter. In Section 4.4 we describe the transmission schemes and derive the achievable secrecy rates for different signalling strategies. Our theoretical results are investigated through numerical simulations in Section 4.5. Finally, Section 4.6 concludes this chapter.

4.1 Introduction and Motivation

In this chapter we generalize the model in Chapter 3 to a scenario with a stronger secrecy measure for the primary message. More specifically, the variational distance between the joint distribution and the product of marginal distributions of the message and Eve's received signal is considered, which is stronger than the commonly used weak secrecy [BL13]. In addition, the secondary transmitter uses multi-phase signalling. As in the original model in Chapter 3, we assume that the secondary receiver U_2 is treated as a potential eavesdropper with respect to the primary transmission. However in Chapter 3 it is assumed that the second transmitter has the knowledge of the primary message before the transmission occurs, which is a simplistic assumption. In our multi-phase signalling scheme, T_2 learns the primary message w_1 in the first phase. After successfully decoding w_1, T_2 implements two types of cooperation as introduced in Chapter 2, namely cooperative jamming and relaying of the primary message. Moreover, we use the clean relaying scheme introduced in [LLSH12], where the secondary transmitter splits its transmission into the third phase in which its own message is not broadcasted (thus, the term "clean") to increase the efficiency of relaying/cooperative jamming. We also derive the achievable rate of T_2 under the same constraint for several other schemes, such as the interference neutralization scheme [HJG13], the dirty paper coding scheme in addition to clean relaying, and a pure cooperative jamming scheme.



(a) First Phase (b) Second Phase (c) Third Phase

Figure 4.2: Multi-phase transmission scheme.

4.2 System Model

In this section we introduce our system model, i.e., the network and transmission model, as well as the notation used throughout this chapter.

4.2.1 Network Model

In this chapter we investigate the cognitive radio network described in Figure 4.1. The cognitive radio network consists of the following single antenna nodes: a primary transmitter T_1, a cognitive secondary transmitter T_2, a primary receiver U_1 and a secondary receiver U_2. T_1 wishes to transmit the secret message w_1 to U_1, which should be kept secret from U_2. Meanwhile, T_2 wants to transmit the message w_2 (without secrecy constraints) to the secondary receiver U_2. As in the previous chapters, we assume that all nodes operate in half-duplex mode. We also assume all channels are complex and static within a codeword length. We assume T_1 transmits at the rate equal to the wiretap channel capacity, where the wiretap channel is formed by T_1 (Alice), U_1 (Bob), and U_2 (Eve). This is due to the single user decoder assumption at U_1, similar to [JV09][1]. We assume that T_1 perfectly knows the channels from T_1 to U_1 and from T_1 to U_2, while T_2 knows all channels. All the channel gains in Figure 4.1 take complex values, which generalizes the assumption of real-valued channels made in Chapter 3.

4.2.2 Transmission Model, Schemes, and Notations

In this chapter we consider the following three-phase transmission scheme for the secondary user depicted in Figure 4.2. The ratios of the interval of each phase to a codeword are defined as η_1, η_2, and η_3, respectively. Assume the time index $t \in \mathbb{N}$. We define the corresponding intervals of the three phases as the following three sets

$$\mathsf{T}_1 = \{t : 1 \leq t \leq \lfloor \eta_1 n \rfloor\},$$

[1] In [JV09], the considered primary channel is only a point to point channel. But here it is a wiretap channel due to the secrecy requirement.

$$\mathsf{T}_2 = \{t : \lfloor \eta_1 n \rfloor + 1 \leq t \leq \lfloor (\eta_1 + \eta_2) n \rfloor\},$$
$$\mathsf{T}_3 = \{t : \lfloor (\eta_1 + \eta_2) n \rfloor + 1 \leq t \leq n\}.$$

Note that these ratios are fixed before each transmission according to the optimization results. We want to design T_2's transmit signal $\mathbf{x}_2$ with T_1's signal $\mathbf{x}_1$ left unchanged. For the ease of derivation, according to these phases we can divide the signal transmitted by T_1 into $\mathbf{x}_1 = [\mathbf{x}_1^{(1)} \mathbf{x}_1^{(2)} \mathbf{x}_1^{(3)}]$ where $\mathbf{x}_1^{(k)}$ corresponds to the fraction of a codeword in the kth phase. This representation is also valid for the received signals $\mathbf{y}_i$ and the noises $\mathbf{n}_i$. Recall that $x_1(t)$ and $x_2(t)$ are the signals transmitted by T_1 and T_2, respectively, at the t-th symbol. The CR scheme employs three phases of transmission that occupy a total of n channel uses, as described below.

Phase 1: For $t \in \mathsf{T}_1$, only T_1 broadcasts $\mathbf{x}_1^{(1)}$ while T_2 remains silent (i.e., $x_2(t) = 0$ due to the half-duplex assumption) and attempts to decode T_1's message w_1 from the overheard signal $y_T(t)$. The duration of Phase 1 is chosen adaptively to ensure that T_2 successfully decodes the T_1's message. If $\eta_1 \geq 1$, we can resort to jamming but not to relaying in order to keep the primary user's secrecy rate unchanged. This is quite different to the case without secrecy, in which if w_1 cannot be decoded within n channel uses, then Phases 2 and 3 cannot be employed since primary user's rate cannot be maintained under secondary user's transmission in which case the secondary user's achievable rate R_2 is zero [LLSH12]. The received signals at U_1, U_2, and T_2 within Phase 1 can be respectively described by

$$\mathbf{y}_1^{(1)} = \mathbf{x}_1^{(1)} + \mathbf{n}_1^{(1)}, \tag{4.1}$$
$$\mathbf{y}_2^{(1)} = c_{12} \mathbf{x}_1^{(1)} + \mathbf{n}_2^{(1)}, \tag{4.2}$$
$$\mathbf{y}_T^{(1)} = c_{TT} \mathbf{x}_1^{(1)} + \mathbf{n}_T^{(1)}. \tag{4.3}$$

Without loss of generality, we assume that the noises $n_1(t)$, $n_2(t)$, and $n_T(t)$ at the nodes U_1, U_2, and T_1, respectively, are independent and identically distributed circularly symmetric complex additive white Gaussian noises with zero mean and unit variance and are mutually independent for all t.

Phase 2: For $t \in \mathsf{T}_2$, T_2 splits its power $P_2^{(2)}$ in Phase 2 into three parts:

1. **Jamming:** The jamming signal is encoded into $j_2(t)$ with power $P_{2j}^{(2)} = \rho_2 P_2^{(2)}$ to confuse the eavesdropping secondary user U_2. The parameter $\rho_2 \in [0, 1)$ denotes the fraction of the power used for jamming.

2. **Relaying of the primary message:** For T_2 to be able to successfully decode message w_1 in Phase 1, the following *decodability constraint* must be satisfied

$$|c_{TT}| > 1. \tag{4.4}$$

   Then T_2 may help to forward the second part of node 1's codeword $\mathbf{x}_1^{(2)}$ in Phase 2 while simultaneously transmitting its own message w_2. The constraint (4.4) being satisfied guarantees that the channel capacity between T_1

and T_2 is large enough for T_2 to successfully decode all codewords in T_1's codebook, as U_1 does. We assume that T_2 knows T_1's codebook and w_1 is encoded into $\mathbf{v}_1^{(2)}$ with power $P_{2,1}^{(2)} = \gamma(1-\rho_2)P_2^{(2)}$. The message w_1 is to be decoded only by the primary receiver U_1, where γ is the ratio of the remained power for relaying.

3. **Transmission of the secondary message:** w_2 is encoded into $\mathbf{v}_2^{(2)}$ with power $P_{2,2}^{(2)} = (1-\gamma)(1-\rho_2)P_2^{(2)}$ to be decoded by the secondary user U_2 only.

Specifically, in Phase 2 node T_2 transmits

$$x_2(t) = v_2(t) + \sqrt{\frac{P_{2,1}^{(2)}}{P_1}} e^{-j\phi_{21}} x_1(t) + j_2^{(2)}(t) \triangleq v_2(t) + v_1^{(2)}(t) + j_2^{(2)}(t), \tag{4.5}$$

where ϕ_{21} is the phase of c_{21}; $v_2(t)$ is the t-th code symbol of the codeword encoding T_2's message w_2, and the received signals at U_1 and U_2 in this phase can be respectively described by

$$\mathbf{y}_1^{(2)} = \mathbf{x}_1^{(2)} + c_{21}\mathbf{x}_2^{(2)} + \mathbf{n}_1^{(2)}, \tag{4.6}$$

$$\mathbf{y}_2^{(2)} = c_{12}\mathbf{x}_1^{(2)} + c_{22}\mathbf{x}_2^{(2)} + \mathbf{n}_2^{(2)}. \tag{4.7}$$

Phase 3: For $t \in \mathsf{T}_3$, node T_2 performs clean relaying by transmitting the third part of T_1's codeword $\{x_1(t)\}_{t\in\mathsf{T}_3}$ with power $P_{2,1}^{(3)}$ and the jamming signal with power $P_{2j}^{(3)}$, but without super-imposing its own signal $v_2(t)$. The signal transmitted by T_2 can be written as

$$x_2(t) = \sqrt{\frac{P_{2,1}^{(3)}}{P_1}} e^{-j\phi_{21}} x_1(t) + j_2^{(3)}(t) \triangleq v_1^{(3)}(t) + j_2^{(3)}(t), \tag{4.8}$$

where $\{X_1(t)\}_{t\in\mathsf{T}_3}$ is the third part of the codeword transmitted by T_1. The received signals at U_1 and U_2 in this phase are

$$\mathbf{y}_1^{(3)} = \mathbf{x}_1^{(3)} + c_{21}\mathbf{x}_2^{(3)} + \mathbf{n}_1^{(3)}, \tag{4.9}$$

$$\mathbf{y}_2^{(3)} = c_{12}\mathbf{x}_1^{(3)} + c_{22}\mathbf{x}_2^{(3)} + \mathbf{n}_2^{(3)}, \tag{4.10}$$

respectively.

Note that the signal-to-interference-plus-noise ratio (SINR) at U_1 changes in each phase. The average transmit power constraints for both transmitters are considered

$$\frac{1}{n}\sum_{k=1}^{n} |x_i(k)|^2 \le P_i \quad \text{for} \quad i \in \{1,2\}. \tag{4.11}$$

More specifically, at T_2 we require the transmit power constraint

$$\eta_2 P_2^{(2)} + \eta_3 P_2^{(3)} \leq P_2. \tag{4.12}$$

A rate pair (R_1, R_2) for the messages w_1 and w_2 is achievable, if for $n \to \infty$, $P_{e,1} \triangleq P\{\hat{w}_1 \neq w_1\}$ and $P_{e,2} \triangleq P\{\hat{w}_2 \neq w_2\}$ can be made arbitrarily small, while the message w_1 stays secure from the secondary receiver, i.e.,

$$\max\{P_{e,1}, P_{e,2}\} \leq \varepsilon \quad \text{(Reliability)}, \tag{4.13a}$$
$$\sup |P_{W\mathbf{y}_2} - P_W P_{\mathbf{y}_2}| \leq \varepsilon \quad \text{(Secrecy)}, \tag{4.13b}$$

for arbitrarily small $\varepsilon > 0$. Note that the secrecy metric in (4.13b) is the *variational distance* or total variation distance [BL13], which is stronger than the commonly used weak secrecy constraint $\lim_{n\to\infty} \frac{1}{n} I(w_1; \mathbf{y}_2) \leq \varepsilon$. For the detailed characterization of different secure measures, please refer to [BL13, Proposition 1]. Note also that when only weak secrecy is considered, we may degenerate the fast fading wiretap channel with full channel state information at the transmitter (CSIT) [LPS08] to a fading channel with only three states corresponding to the three phases, to derive the capacity of the primary user. When T_2 does not transmit, the maximum achievable rate R_1^{WT} for which both the reliability and secrecy conditions are fulfilled is known as the secrecy capacity of the wiretap channel given by $R_1^{\mathrm{WT}} = \big(\mathcal{C}(P_1) - \mathcal{C}(c_{12}^2 P_1)\big)^+$.

4.3 Main Result and Optimization Problem

In this section we establish our main result. We show the discrete memoryless secrecy capacity of the wiretap channel formed by T_1 (Alice), U_1 (Bob), and U_2 (Eve) with the multi-phase transmission under the variational distance secrecy constraint. In particular we specialize the result from Bloch and Laneman in [BL13] to the considered case with three phases and average power constraint in Section 4.3.1. In Section 4.3.2 we formulate the optimization problem investigated in this chapter.

4.3.1 Main Result

Theorem 4.1.

For the 3-phase transmission, the memoryless secrecy capacity of the wire-tap channel formed by T_1, U_1, and U_2 can be represented as

$$C_s = \sup_{(\mathbf{V}_1,\mathbf{X}_1)\in P} \sum_{k=1}^{3} \eta_k \left\{ I(V_1^{(k)}; Y_1^{(k)}) - I(V_1^{(k)}; Y_2^{(k)}) \right\}, \tag{4.14}$$

where $\eta_1 + \eta_2 + \eta_3 = 1$, $\eta_k \geq 0$ and $P \triangleq \{(\mathbf{V}_1, \mathbf{X}_1) : \mathbf{V}_1 - \mathbf{X}_1 - \mathbf{Y}_1\mathbf{Y}_2$ forms a Markov chain and $\frac{1}{n}\Sigma_{j=1}^{n} X_j^2 \leq P\}$.

Proof. The proof of Theorem 4.1 is given in Appendix 4.A. Note that the result of Theorem 4.1 is also valid for finite alphabet input as proven in the Appendix. The finite alphabet case is important especially for the statistical CSIT case. In [LYT10] it was found that when the transmitter only knows the CSI of the main channel but there is only statistical CSI of Eve's channel, then finite alphabet signalling will outperform the Gaussian signalling. ■

Remark 4.1.

We can also prove the same result as Theorem 4.1 using [PC94], which had been applied to the problem of Gaussian Gelfand-Pinsker coding under non-stationary and non-ergodic channels and states in [YSJ+01]. However, according to [Tan14] we know that there are two caveats of using the non-information-spectrum method:

1. The weak typicality is used; i.e., the sample entropy is close to the entropy rate, which is hard to derive for the more general representation in (4.39).
2. The general asymptotic equipartition property in [PC94] is derived based on the Gaussian distribution and cannot be extended to the expression of (4.39), which is valid for general distribution.

Remark 4.2.

The proof of [PC94] is based on the fact that for a Gaussian process the difference between the empirical and the true entropy rates is a scaled chi-square distribution with parameters independent of the particular covariance matrices. Thus when it converges to zero as the block size goes to infinity, it does not rely on the stationarity or ergodicity of the Gaussian process.

4.3.2 Optimization Problem

In this chapter we aim at maximizing the secondary user's rate R_2 using different transmission schemes under the constraint that the primary user's secrecy rate R_1 when T_2 is transmitting is no lower than the target secrecy rate R_1^{WT}, and with an average power constraint P_2 at the secondary transmitter. We formulate the optimization problem in the following definition.

Definition 4.1.

The optimization problem $\mathcal{P}_{R_{2m}}$ investigated in this chapter is defined as

$$\max_{\eta_1,\eta_2,\rho_2,\rho_3,\gamma,P_2^{(2)},P_2^{(3)}} R_2 \tag{4.15}$$

$$\text{s. t. } R_1 \geq R_1^{\mathrm{WT}} \tag{4.16}$$

$$\eta_2 P_2^{(2)} + \eta_3 P_2^{(3)} \leq P_2. \tag{4.17}$$

We assume that the strategy employed by T_2 is known to T_1 before the transmission occurs such that T_1 designs its wiretap code according to the wiretap channel where the point-to-point capacity from T_1 to T_2 is now given as

$$C_b = \sup_{(\mathbf{V}_1,\mathbf{X}_1)\in P} \sum_{k=1}^{3} \eta_k I(V_1^{(k)}; Y_1^{(k)}),$$

instead of $\mathcal{C}(P_1)$ when T_2 does not transmit. If we consider the more stringent cognitive model where it is required that the wiretap coding at T_1 stays unchanged, as investigated in [LGT+14b], the additional constraint (4.18) is added to the optimization problem $\mathcal{P}_{R_{2m}}$:

$$\sum_{k=1}^{3} \eta_k I(V_1^{(k)}; Y_1^{(k)}) = \mathcal{C}(P_1). \tag{4.18}$$

4.4 Transmission Schemes and Achievable Rate Regions

In the following we will discuss different transmission schemes and the corresponding achievable rate pairs under AWGN channels. In Section 4.4.1 we consider our proposed scheme, clean relaying, combined with cooperative jamming. In Section 4.4.2 we consider CR, combined this time with dirty paper coding in addition to cooperative jamming. In order to evaluate the performance of our scheme, we propose several other transmission strategies, which will be compared to CR in Section 4.5. In particular we derive the achievable rate region for pure cooperative jamming in Section 4.4.3, which acts as a benchmark for the comparison. Finally in Section 4.4.4 we consider the interference neutralization scheme considered in [HJG13].

4.4.1 Clean Relaying with Cooperative Jamming

In this section we consider the clean relaying scheme combined with cooperative jamming as described in Section 4.2.2. For T_2 to be able to relay T_1's signal in the second phase using decode and forward relaying, the decodability constraint (4.4) must be satisfied. Therefore in this scenario, η_1 is set as

$$\eta_1 = \frac{\mathcal{C}(P_1)}{\mathcal{C}(|c_{TT}|^2 P_1)}, \tag{4.19}$$

and w_1 is re-encoded using the same codebook as shown in (4.5) and (4.8), respectively:

$$x_2^{(2)}(t) = v_2(t) + \sqrt{\frac{P_{2,1}^{(2)}}{P_1}} e^{-j\phi_{21}} x_1(t) + j_2^{(2)}(t),$$
$$x_2^{(3)}(t) = \sqrt{\frac{P_{2,1}^{(3)}}{P_1}} e^{-j\phi_{21}} x_1(t) + j_2^{(3)}(t).$$

We give in the following proposition the achievable rate region using the CR scheme combined with CJ.

Proposition 4.1.

The achievable rate pair (R_1, R_2) for the clean relaying scheme with cooperative jamming is given by the following region $\mathcal{R}_{\mathrm{CR}}$:

$$
\begin{aligned}
R_1 < \Bigg(& \eta_1 R_1^{\mathrm{WT}} \\
& \eta_2 \left\{ \mathcal{C}\left(\frac{\left| \sqrt{P_1} + |c_{21}| \sqrt{(1-\rho_2)\gamma P_2^{(2)}} \right|^2}{1 + c_{21}^2 (1 - \gamma + \gamma\rho_2) P_2^{(2)}} \right) \right. \\
& \left. - \mathcal{C}\left(\frac{\left| c_{12}\sqrt{P_1} + c_{22} e^{-j\phi_{21}} \sqrt{(1-\rho_2)\gamma P_2^{(2)}} \right|^2}{1 + c_{22}^2 \rho_2 P_2^{(2)}} \right) \right\} \\
& + \eta_3 \left\{ \mathcal{C}\left(\frac{\left| \sqrt{P_1} + |c_{21}| \sqrt{(1-\rho_3) P_2^{(3)}} \right|^2}{1 + c_{21}^2 \rho_3 P_2^{(3)}} \right) \right. \\
& \left. - \mathcal{C}\left(\frac{\left| c_{12}\sqrt{P_1} + c_{22} e^{-j\phi_{21}} \sqrt{(1-\rho_3) P_2^{(3)}} \right|^2}{1 + c_{22}^2 \rho_3 P_2^{(3)}} \right) \right\} \Bigg)^+ , \qquad (4.20)
\end{aligned}
$$

$$
R_2 < \eta_2 \, \mathcal{C}\left(\frac{c_{22}^2 (1-\rho_2)(1-\gamma) P_2^{(2)}}{1 + c_{22}^2 \rho_2 P_2^{(2)} + \left| c_{22} e^{-j\phi_{21}} \sqrt{\gamma(1-\rho_2) P_2^{(2)}} + c_{12}\sqrt{P_1} \right|^2} \right). \qquad (4.21)
$$

Proof. The rate region defined by (4.20) and (4.21) can be obtained based on the capacity expression (4.14), the signalling schemes introduced in the previous section, and the selection $\mathbf{V}_1 = \mathbf{X}_1$. The proof of Proposition 4.1 is given in Appendix 4.B. ■

4.4.2 Clean Relaying with Cooperative Jamming and Dirty Paper Coding

In this section we discuss the case where T_2 implements dirty paper coding. In this scenario, we need to take into account the information leakage due to DPC. After considering this leakage effect, the DPC assisted cognitive radio is not a trivial extension of the interference mitigating CR in [JV09]. Note that here we consider the weak secrecy constraint instead of the total variation distance constraint as in the previous section. To have a fair and feasible comparison, we may first consider Theorem 4.1 with weak secrecy constraint, since the achievable rate in Equation (4.14) is still valid under a weak secrecy constraint due to the expression in (4.39) being valid for several secrecy levels where the most stringent level is the total variation distance. In other terms, a stronger secrecy measure does not come at an extra cost. We first prove that when T_2 uses DPC, T_1 cannot use the usual transmission rate $I(V_1;Y_1) - I(V_1;Y_2)$ and the corresponding coding scheme since this choice of rate cannot guarantee perfect secrecy.

Proposition 4.2.

When T_2 uses DPC, the original rate $I(V_1;Y_1) - I(V_1;Y_2)$ used at T_1 cannot guarantee perfect secrecy.

Proof. The proof of Proposition 4.2 is given in Appendix 4.C. ■

To guarantee the perfect secrecy of primary user's transmission when T_2 exploits DPC, we may specialize the broadcast channel with confidential messages (BC-CM) in [LMSY08], i.e., both receivers have their own secret message to be kept unknown to each other, into the case that only one user requires secret transmission and the other does not. This specialization is feasible since the latter is a special case of the former. There we may consider the achievable rate region of the discrete memoryless channel [2] as

$$R_1 \leq I(V_1;Y_1) - I(V_1;Y_2|V_2) - I(V_1;V_2), \tag{4.22}$$

$$R_2 \leq I(V_2;Y_2) - I(V_1;V_2). \tag{4.23}$$

Note that in the original BC-CM model, $I(V_1;Y_2|V_2)$ needs to be subtracted from R_2 additionally. Note also that, even if T_1 does not use DPC, the term $-I(V_1;V_2)$ must be taken into account as the information leakage due to DPC being used by T_2, the same as in the original BC-CM model.

[2] For DMCs, the authors in [LMSY08] do not prove the capacity since a tight upper bound is missing. However for AWGN channels, the capacity can be proved by substituting the Gaussian signalling into the DMC capacity formula.

Transmission Model The received signals at U_1 and U_2 at time $t \in \mathsf{T}_2$ are given as

$$y_1(t) = x_1(t) + c_{21}x_2(t) + n_1(t) = x_1(t) + c_{21}(v_{1,r}(t) + u_2(t) + j_2(t)) + n_1(t) \tag{4.24}$$

$$= \left(1 + c_{21}e^{-j\phi_{21}}\sqrt{\frac{(1-\rho_2)\gamma P_2^{(2)}}{P_1}}\right) x_1(t) + c_{21}(u_2(t) + j_2(t)) + n_1(t),$$

$$y_2(t) = c_{22}x_2(t) + c_{12}x_1(t) + n_2(t)$$

$$= \left(c_{22}e^{-j\phi_{21}}\sqrt{\frac{(1-\rho_2)\gamma P_2^{(2)}}{P_1}} + c_{12}\right) x_1(t) + c_{22}(u_2(t) + j_2(t)) + n_2(t), \tag{4.25}$$

where $x_2(t) = v_{1,r}(t) + u_2(t) + j_2(t)$, $v_{1,r}(t) \triangleq e^{-j\phi_{21}}\sqrt{\frac{(1-\rho_2)\gamma P_2^{(2)}}{P_1}}x_1(t)$ is T_1's signal relayed by T_2, $j_2 \sim \mathcal{N}\left(0, \rho_2 P_2^{(2)}\right)$ is the cooperative jamming term. More specifically, on the design of the DPC, if we use the original notation in Costa's paper [Cos83] we let $V_2 = U_2 + \alpha U_1'$, where

$$U_1' = \left(c_{12} + c_{22}e^{-j\phi_{21}}\sqrt{\frac{(1-\rho_2)\gamma P_2^{(2)}}{P_1}}\right) V_1,$$

and where $V_1 = X_1$, $X_1 \sim N(0, P_1)$, $U_2 \sim \mathcal{N}\left(0, (1-\rho_2)(1-\gamma)P_2^{(2)}\right)$. With this choice of random variables, V_1 is independent of V_2, and there is a Markov chain $V_1 - V_2 - Y_2$. Finally in the third phase T_2 uses the same signalling as in the previous scheme, i.e.,

$$x_2(t)^{(3)} = \sqrt{\frac{P_{2,1}^{(3)}}{P_1}}e^{-j\phi_{21}}x_1(t) + j_2^{(3)}(t).$$

The achievable rate region using this CR scheme combined with DPC is given in the following proposition.

Proposition 4.3.

The achievable rate pair (R_1, R_2) for the CR with DPC scheme is given by the region $\mathcal{R}_{\mathrm{DPC}}$ defined as:

$$\begin{aligned} R_1 \leq & \eta_1 R_1^{WT} + \\ & \eta_2 \left\{ \mathcal{C}\left(\frac{|\sqrt{P_1} + |c_{21}|\sqrt{(1-\rho_2)\gamma P_2^{(2)}}|^2}{1 + |c_{21}|^2(1-\gamma+\rho_2\gamma)P_2^{(2)}} \right) \right. \\ & \left. -\mathcal{C}\left(\frac{|c_{12}\sqrt{P_1} + c_{22}e^{-j\phi_{21}}\sqrt{(1-\rho_2)\gamma P_2^{(2)}}|^2}{1 + |c_{22}|^2(1-\gamma+\rho_2\gamma)P_2^{(2)}} \right) \right\} \\ & + \eta_3 \left\{ \mathcal{C}\left(\frac{\left|\sqrt{P_1} + |c_{21}|\sqrt{(1-\rho_3)P_2^{(3)}}\right|^2}{1 + c_{21}^2\rho_3 P_2^{(3)}} \right) \right. \\ & \left. -\mathcal{C}\left(\frac{\left|c_{12}\sqrt{P_1} + c_{22}e^{-j\phi_{21}}\sqrt{(1-\rho_3)P_2^{(3)}}\right|^2}{1 + c_{22}^2\rho_3 P_2^{(3)}} \right) \right\}, \end{aligned} \tag{4.26}$$

$$R_2 \leq \eta_2 \mathcal{C}\left(\frac{|c_{22}|^2(1-\rho_2)(1-\gamma)P_2^{(2)}}{1 + |c_{22}|^2\rho_2 P_2^{(2)}} \right). \tag{4.27}$$

Proof. We refer to Appendix 4.D for the proof of Proposition 4.3. ■

4.4.3 Pure Cooperative Jamming

In this section we use a simple cooperative jamming scheme as a benchmark to compare with the performance of the clean relaying scheme. In particular if the constraint (4.4) is violated, then the constraint (4.16) cannot be satisfied by relaying under the assumption that the primary channel is fully loaded. Therefore, we implement cooperative jamming as follows. Since in this case T_2 does not need to listen and decode w_1, the signalling in the new phases 1 and 2 is modified respectively as

$$x_2^{(1)}(t) = v_2^{(1)}(t) + j_2^{(1)}(t), \text{ and } x_2^{(2)}(t) = v_2^{(2)}(t) + j_2^{(2)}(t).$$

Note that phases 1 and 2 in the cooperative jamming scheme are not aligned to those in the previous scheme. The durations of these two phases here are to be

solved according to the optimization problem in Definition 4.1. We parameterize the power allocated to jamming and T_2's own message transmission as $P_{2j}^{(2)} = \rho_2 P_2^{(2)}$, and $P_{2,2} = (1-\rho_2)P_2^{(2)}$, respectively, where $\rho_2 \in [0,1]$ denotes the fraction of the power used for jamming. In the third phase, we only transmit the jamming signal as

$$x_2^{(3)}(t) = j_2^{(3)}(t). \tag{4.28}$$

Proposition 4.4.

The achievable rate pair (R_1, R_2) for the CJ scheme is given by the region $\mathcal{R}_{\mathrm{CJ}}$ defined as:

$$R_1 < \left(\eta_1 R_1^{\mathrm{WT}} + \eta_2 \left\{ \mathcal{C}\left(\frac{P_1}{1+|c_{21}|^2 P_2^{(2)}}\right) - \mathcal{C}\left(\frac{|c_{12}|^2 P_1}{1+|c_{22}|^2 \rho_2 P_2^{(2)}}\right)\right\} + \eta_3 \left\{ \mathcal{C}\left(\frac{P_1}{1+|c_{21}|^2 P_2^{(3)}}\right) - \mathcal{C}\left(\frac{c_{12}^2 P_1}{1+|c_{22}|^2 P_2^{(3)}}\right)\right\}\right)^+, \tag{4.29}$$

$$R_2 < \eta_2\, \mathcal{C}\left(\frac{|c_{22}|^2(1-\rho_2)P_2^{(2)}}{1+|c_{12}|^2 P_1 + |c_{22}|^2 \rho_2 P_2^{(2)}}\right). \tag{4.30}$$

4.4.4 Interference Neutralization

In this section we consider an interference neutralization (IN) strategy as a transmission scheme for T_2. The idea of interference neutralization is to nullify the interference signal received from T_1 at U_2. In our scenario, this strategy could potentially yield to two beneficial effects: the leakage of the primary message to the secondary user is eliminated, while at the same time the quality of the secondary transmission could be improved since there is no more primary interference. The signalling in the first phase is the same as for the relaying schemes, since T_2 needs to decode w_1 in the first phase. Therefore the constraint (4.4) must be satisfied and η_1 is set as $\mathcal{C}(P_1)/\mathcal{C}(|c_{TT}|^2 P_1)$. In the second phase T_2 transmits:

$$x_2^{(2)}(t) = v_2^{(2)}(t) - \frac{c_{12}}{c_{22}} x_1^{(2)}(t). \tag{4.31}$$

The received signals in the second phase are given by:

$$\mathbf{y}_1^{(2)} = \mathbf{x}_1^{(2)} + c_{21}\mathbf{x}_2^{(2)} + \mathbf{n}_1^{(2)}, \tag{4.32}$$

$$\mathbf{y}_2^{(2)} = c_{12}\mathbf{x}_1^{(2)} + c_{22}\mathbf{x}_2^{(2)} + \mathbf{n}_2^{(2)}, \tag{4.33}$$

which simplifies to

$$\mathbf{y}_1^{(2)} = \left(1 - \frac{c_{12}c_{21}}{c_{22}}\right)\mathbf{x}_1^{(2)} + c_{21}\mathbf{v}_2^{(2)} + \mathbf{n}_1^{(2)}, \tag{4.34}$$

$$\mathbf{y}_2^{(2)} = c_{22}\mathbf{v}_2^{(2)} + \mathbf{n}_2^{(2)}. \tag{4.35}$$

Note that if $|c_{12}|$ is too large and/or $|c_{22}|$ is too small such that

$$\eta_2 |\frac{c_{12}}{c_{22}}|^2 P_1 > P_2, \tag{4.36}$$

then T_2 may not have enough power to neutralize the interference and therefore IN cannot be implemented. Based on this signalling, we obtain easily the achievable rate region as follows.

Proposition 4.5.

The achievable rate pair (R_1, R_2) for IN is given by the region $\mathcal{R}_{\text{IN}}$ defined as:

$$R_1 < \eta_1 R_1^{\text{WT}} + \eta_2\, \mathcal{C}\left(\frac{P_1|1 - \frac{c_{12}c_{21}}{c_{22}}|^2}{1 + |c_{21}|^2(P_2^{(2)} - |\frac{c_{12}}{c_{22}}|^2 P_1)}\right), \tag{4.37}$$

$$R_2 < \eta_2\, \mathcal{C}\left(|c_{22}|^2\left(P_2^{(2)} - \left|\frac{c_{12}}{c_{22}}\right|^2 P_1\right)\right). \tag{4.38}$$

4.5 Numerical Illustrations

In this section we present the numerical results and related discussions. We will compare the rate performance of the proposed clean relaying with cooperative jamming, pure cooperative jamming, and the relaying without the additional phase, with respect to the particular topology of interest. In particular, we are interested in how the system behaves for different locations of the secondary transmitter. We will also show how the relaying and time splitting of different strategies are affected by the relative positions of nodes.

In our simulation, we fix the locations of the primary transmitter T_1 and receiver U_1 at the coordinates $(0, 0)$ and $(1, 0)$, respectively. The secondary receiver is fixed at $(1, -1)$. We assume a path-loss model with path-loss exponent $\alpha = 3$, i.e., $c_{ij} = d_{ij}^{-3}$. The power constraints at both transmitters are $P_1^{\max} = P_2^{\max} = 10$ dB. We scan the parameters $(\rho_2, \rho_3, \gamma, \eta_1, \eta_2, P_2^{(2)}, P_2^{(3)})$ over a sufficiently fine grid and take the maximum achievable rate over all corresponding rates. Note that we also include power control as a possible strategy for T_2; i.e., the transmission power utilized is not necessarily fixed to its maximum $P_2^{\max} = 10$ dB.

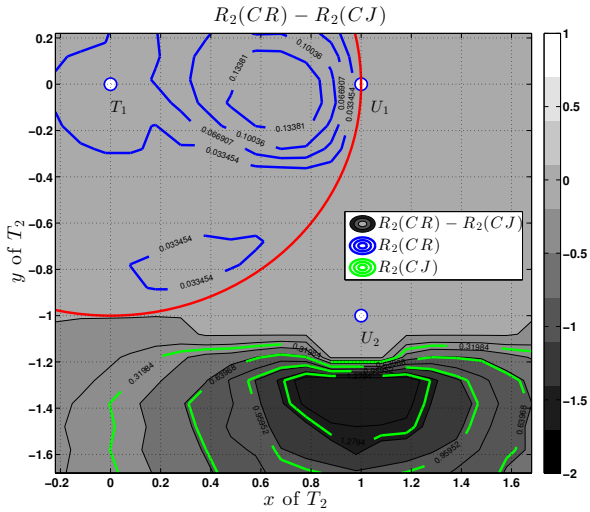


Figure 4.3: Difference $R_2(\mathrm{CR}) - R_2(\mathrm{CJ})$ depending on the location of T_2.

Comparison with Pure Cooperative Jamming In Figure 4.3 we depict the difference in terms of maximal achievable rates between the clean relaying with cooperative jamming strategy and the pure cooperative jamming strategy. The red line represents the coarse boundary under which the clean relaying results in $R_2 = 0$, since the decodability constraint is not satisfied for T_2 located outside this decodability circle. In the region below the red line, pure CJ is efficient while above the red line, the pure CJ strategy yields to $R_2 = 0$. As discussed in the previous chapter, the explanations of this phenomenon are two-fold: first, if T_2 is above this region, pure jamming may degrade the main channel more than Eve's channel. Therefore relaying is necessary while jamming is hurtful. Secondly, because T_2 is much closer to U_2 than to U_1 when T_2 is below the red line, the relaying contributes more to the numerator of the second term in the bracket multiplied by η_2 in (4.20), which degrades the primary user's secrecy rate. The achievable rates by clean relaying and CJ are also labeled in the figure by blue and green lines, respectively. From Figure 4.3 we observe that pure CJ and CR are achieving strictly positive secondary rates in different regions, and their performance is not comparable for a fixed location of T_2. Thus in the following we restrict our comparison with the other schemes, namely CR with DPC and IN. This observation also leads to the idea of an hybrid scheme where T_2 either uses one of the strategies where X_1's knowledge is necessary, or resorts to jamming if X_1 is not decodable, i.e., outside the decodability region.

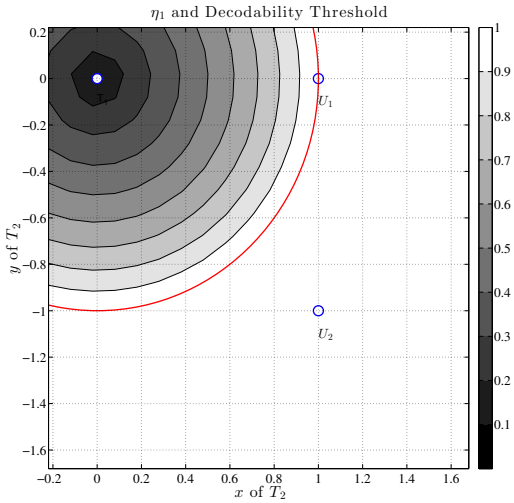


Figure 4.4: Illustration of the existence of a region where w_1 is decodable by T_2.

Clean Relaying: Signalling Parameters In Figure 4.4 we show the relation between the relative position of T_2 to other nodes and the necessary interval η_1 for T_2 to successfully decode w_1. It is intuitive that when T_2 is much further away from T_1, η_1 becomes larger. There exists a threshold over which T_1 is unable to successfully decode w_1 within a codeword, in which case the relaying scheme can not be used.

In Figure 4.5 we show the relation between the location of T_2 and the time splitting parameters η_3 for T_2 to implement clean relaying/cooperative jamming in the third phase. The figure shows that the third phase, specific to the clean relaying scheme, is used by the secondary transmitter, which shows the relevance of considering the CR scheme for our cognitive model. We observe that η_3 decreases with the increasing distance between T_2 to T_1. One possible explanation to this observation is that since η_1 becomes larger as T_2 gets further away from T_1, as shown in Figure 4.4, there is less time allowed for clean relaying to be implemented in the third phase. The interesting behavior in the middle-left area can be tentatively explained using the observations from Figures 4.8a and 4.8b. In this particular area, the third phase is solely for CJ instead of relaying the message, which possibly explains the difference in behavior as the aim of the third phase is changed.

In Figure 4.6 we depict how the secondary power in the second phase $P_2^{(2)}$ is distributed depending on the location of T_2. This transmission power is constituted of three parts: the power allocated to the primary message, the jamming power, and the power allocated to the secondary message. According to numerical results not depicted here we made the following observations:

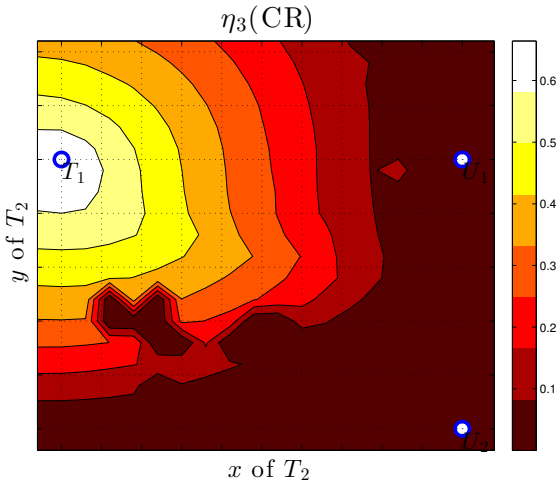


Figure 4.5: Distribution of η_3 depending on the location of T_2.

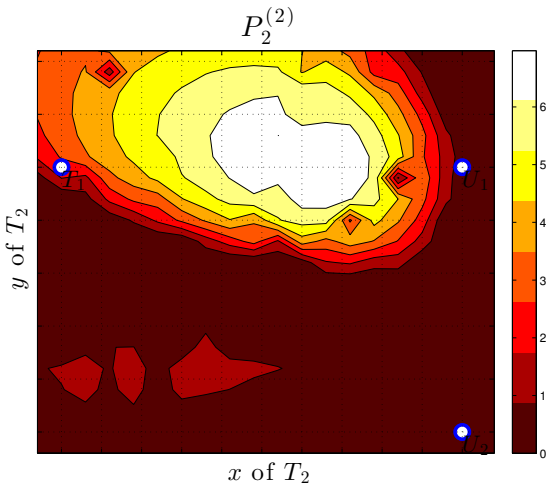


Figure 4.6: Transmission power $P_2^{(2)}$ in the second phase for the CR scheme depending on the location of T_2.

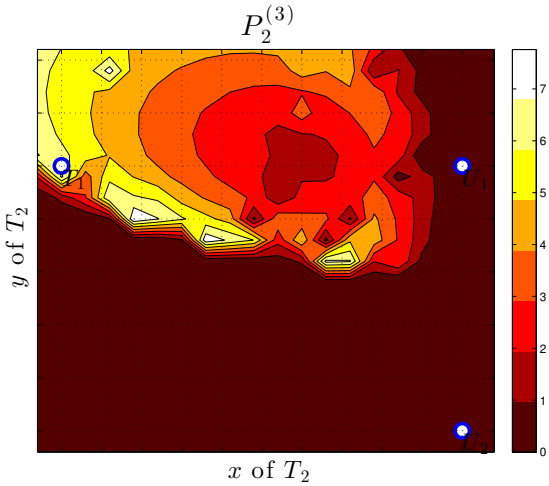


Figure 4.7: Transmission power $P_2^{(3)}$ in the third phase for the CR scheme depending on the location of T_2.

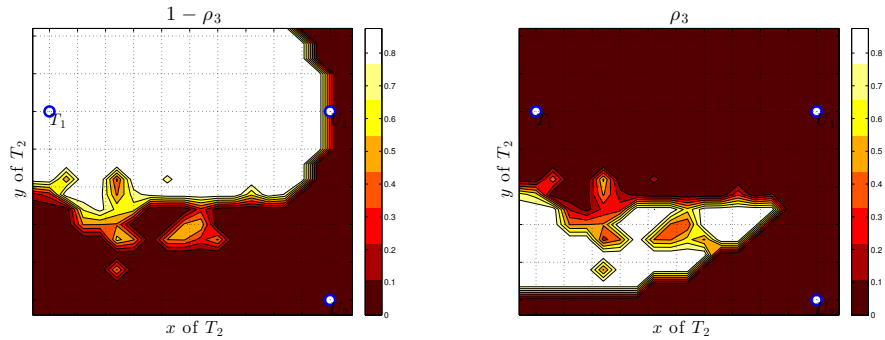
1. Most of the transmission power used in the second phase is allocated to the transmission of the secondary message, i.e., the term $(1-\gamma)(1-\rho)P_2^{(2)}$.

2. No power is allocated to the relaying of the primary message in the second phase, i.e., $\gamma = 0$. Instead the power allocated to relaying is concentrated in the third phase, as highlighted in Figure 4.8a.

3. There exists a region where some jamming power is allocated, namely the region inside the decodability circle which is the closest to U_2, since CJ is efficient in this location.

In Figure 4.7 we show how the secondary power in the third phase $P_2^{(3)}$ is distributed depending on the location of T_2. By comparing Figure 4.7 with Figure 4.6 we observe that T_2 is allocating power to the third phase whenever there is still power available after the second phase, since we observe some complementarity in the region of interest between the two plots. However one aspect of the third phase transmission is not visible in Figure 4.7: the power allocated to jamming in the lower left part of the figure. This is due to the amount of power needed for CJ in this area being negligible compared to the power allocated to relaying in the upper part of the figure.

In order to highlight the existence of an area where jamming is used in the third phase we represent the power splitting parameter ρ_3 for CJ and $(1-\rho_3)$ for relaying in Figure 4.8. The figure shows that clean relaying of the primary message is implemented when T_2 is between T_1 and U_1, as intuitively expected,



(a) Fraction $(1-\rho_3)$ of power allocated to relaying. (b) Fraction ρ_3 of power allocated to CJ.

Figure 4.8: Power splitting for the third phase for the CR scheme depending on the location of T_2.

while jamming is preferred in the region where T_2 is closer to U_2. However due to the decodability constraint on η_1, T_2 cannot be located in the most efficient position for CJ, i.e., extremely close to U_2.

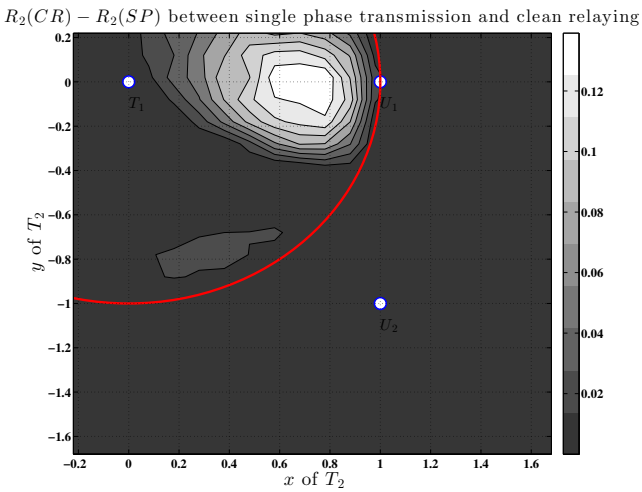


Figure 4.9: Difference $R_2(\mathrm{CR}) - R_2(\mathrm{SP})$ using clean relaying and without clean relaying depending on the location of T_2.

In Figure 4.9 we compare the achievable secondary rates $R_2(\mathrm{CR})$ and $R_2(\mathrm{SP})$

where $R_2(\text{SP})$ denotes the rate R_2 by the transmission scheme without the third phase. Since the transmission without the clean relaying phase is a special case of the multi-phase scheme, we expect therefore the existence of a third phase to perform at worst the same as without clean phase, and potentially improve the secondary rate performance. We can observe that clean relaying indeed outperforms the one without clean phase, especially when T_2 is close to U_1 and further away from U_2. This is consistent to the intuition in the sense that, when T_2 is at such location, the clean relaying is highly efficient: it will boost the SINR of $I(V_1; Y_1^{(3)})$ much faster than Phase 2 due to T_2 is close to U_1. Meanwhile the increment on the SINR of $I(V_1; Y_2^{(3)})$ is kept limited due to T_2 being far from U_2. Another small region around the point $(0.4, 0.8)$ shows an improvement compared to the single phase transmission, which corresponds to the area where T_2 implements CJ in the third phase.

Combining Clean Relaying with DPC We now investigate the improvement in performance due to the use of DPC in addition to clean relaying with cooperative jamming by T_2. We should first note that, even if an improvement in terms of achievable rates is to be expected, there is some drawback to the implementation of DPC. First the rate expression in (4.22) relies on the use of double binning scheme which is different to the single binning one originally used by T_1. Thus when the secondary user starts to transmit with DPC, there must exist a protocol to acknowledge the primary user to change the coding scheme accordingly. Further we consider the weak secrecy constraint instead of the total variation distance; in other terms, the secrecy requirements for the use of the DPC scheme are lowered compared to the CR scheme without DPC.

In Figure 4.10 we illustrate the achievable secondary rate for the CR scheme with DPC while in Figure 4.11 we depict the improvement in performance in terms of secondary rate obtained by implementing DPC in addition to the CR scheme. We notice two distinct regions for which DPC improves the performance of the CR scheme: when T_2 is between T_1 and U_1, and in the area where CJ was used for the CR scheme. In order to understand the reasons of this increase in performance we investigate the power and time splitting parameters for the DPC based scheme.

First we compare in Figure 4.12 the importance of the second phase with and without DPC by depicting the value of η_2 for both schemes. We observe that for the DPC scheme the length of the second phase is higher than for the simple CR scheme. This difference indicates that the DPC encoding in the second phase yields to a performance improvement or that the use of a third relaying phase is not crucial any longer with DPC. The latter reason would explain the decrease of the third phase length and hence the increase of η_2.

In Figure 4.13 we complement the previous observation by showing the powers $P_2^{(2)}(\text{DPC})$ and $P_2^{(3)}(\text{DPC})$ used by T_2 in the second and third phase, respectively. The phenomenon is confirmed as most of the transmission power of the secondary transmitter is allocated to the second phase while some power, albeit at most only

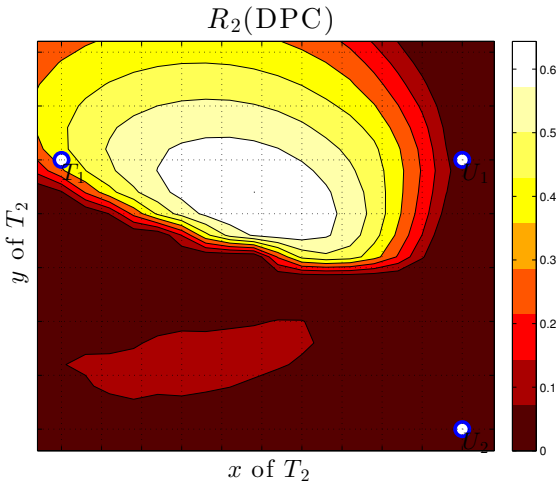


Figure 4.10: Achievable secondary rate R_2(DPC) using CR with DPC depending on the location of T_2.

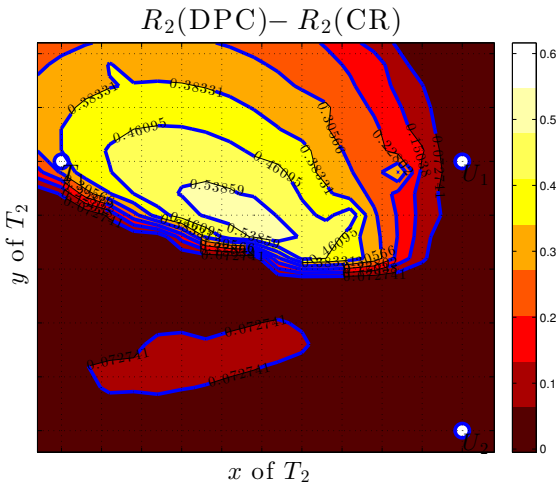
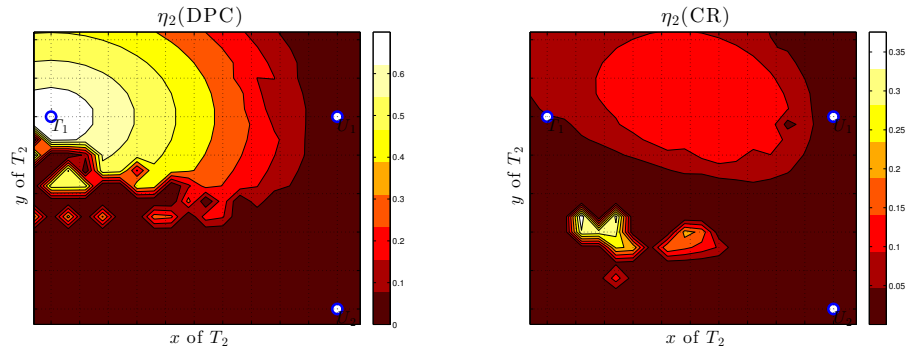
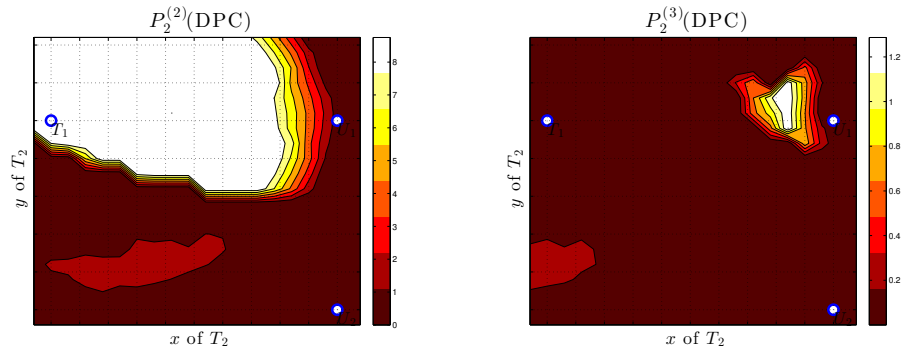


Figure 4.11: Difference R_2(DPC) $-$ R_2(CR) using CR with and without DPC depending on the location of T_2.



(a) η_2(DPC). (b) η_2(CR).

Figure 4.12: Comparison of the length of the second phase η_2 for the CR scheme with and without DPC with depending on the location of T_2.



(a) $P_2^{(2)}$(DPC) in the second phase. (b) $P_2^{(3)}$(DPC) in the third phase.

Figure 4.13: Transmission power for the CR scheme with DPC depending on the location of T_2.

20% of the maximum transmission power, is allocated to third phase when T_2 is located close to U_1. Before analyzing this efficient power splitting in the second phase we will look at the power splitting in the third phase in Figure 4.14.

As expected we observe in Figure 4.14 a similar area where some power $\rho_3 P_2^{(3)}$ is allocated to CJ as for the CR scheme without DPC. Combining this observation with the power splitting from Figure 4.13b we can deduce that relaying in the third phase is only implemented in a smaller region near U_1 compared to the first CR

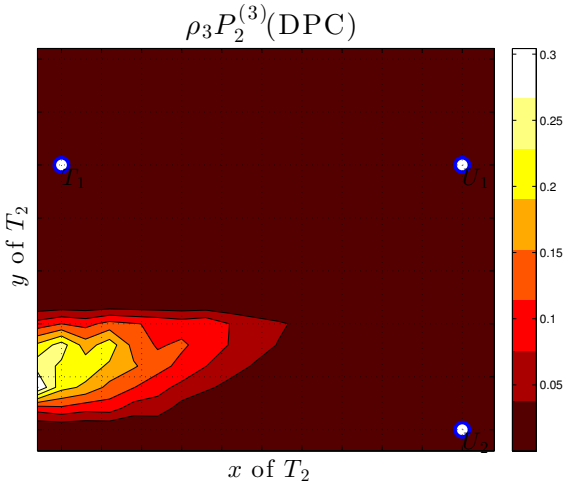


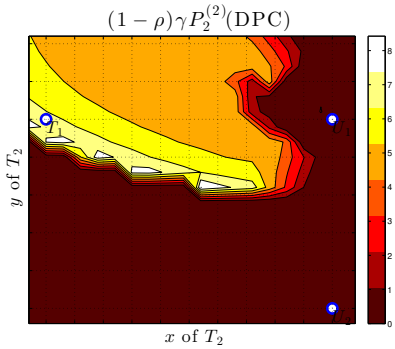
Figure 4.14: Power $\rho_3 P_2^{(3)}$(DPC) allocated to CJ in the third phase.

scheme.

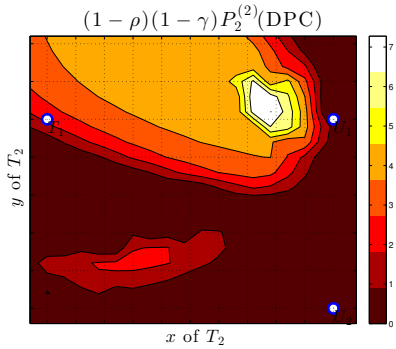
In Figure 4.15 we represent the power splitting during the second phase. In particular Figure 4.15a depicts the power allocated to relaying the primary message while Figure 4.15b shows the power allocated to w_2. We see that in contrast to the CR scheme without DPC, an important fraction of the transmission power is allocated to relaying w_1 thus explaining that the third phase is less used compared to the CR scheme.

Comparison with Interference Neutralization We now illustrate the performance of the IN scheme. First in Figure 4.16 we depict the secondary rate achievable using interference neutralization. We observe two separate regions where IN achieves strictly positive secondary rates. First when T_2 is located close to U_2, yet still in the decodability region since X_1 needs to be known by T_2 for the implementation of the scheme, we observe that IN performs well. This is expected since T_2 can neutralize the interference caused by X_1 transmitted by T_1 efficiently. The IN scheme being efficient when T_2 is close to U_1 is surprising however and it can be explained as follows. Since c_{21} is large for that scenario, the negative part of X_1 adding itself to the received signal at U_1 becomes large enough so that the amplitude of the received signal in X_1, is higher than without the interference caused by T_2. Thus T_2 is effectively relaying X_1 to U_1 in that region.

Finally in Figure 4.17 we compare CR and IN in terms of achievable secondary rates. We observe that in the region between T_1 and U_1, CR outperforms IN. However in the lower part of the plane, IN outperforms CR, which highlights that IN is more effective than jamming, i.e., that cancelling the signal X_1 at U_2 is preferable



(a) $(1-\rho)\gamma P_2^{(2)}$(DPC) allocated to w_1.



(b) $(1-\rho)(1-\gamma)P_2^{(2)}$(DPC) allocated to w_2.

Figure 4.15: Power splitting in the second phase for the CR scheme with DPC depending on the location of T_2.

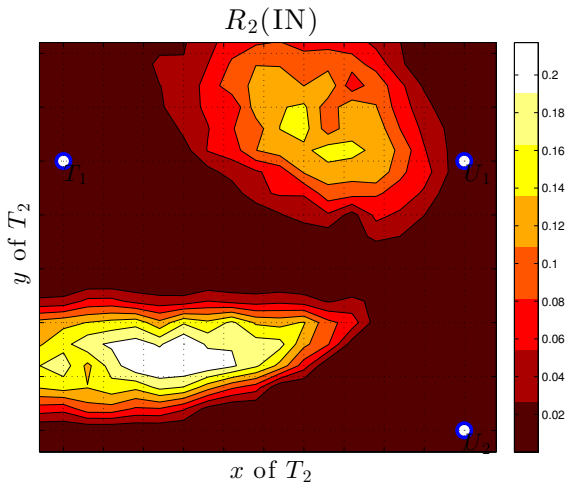


Figure 4.16: Achievable secondary rate R_2(IN) using IN depending on the location of T_2.

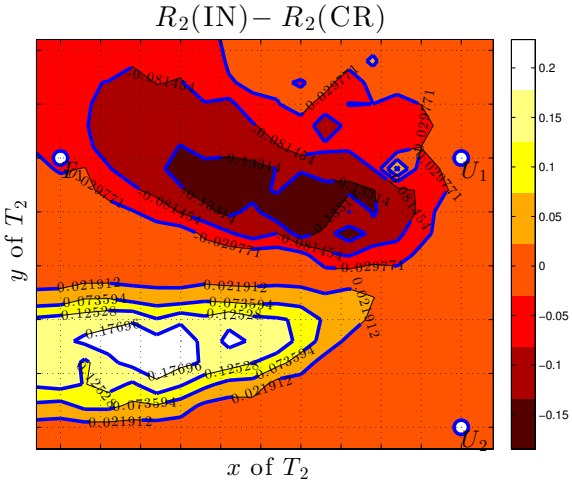


Figure 4.17: Difference $R_2(\mathrm{IN}) - R_2(\mathrm{CR})$ between the CR and IN schemes depending on the location of T_2.

to exhausting the decoding capabilities of U_2 by jamming using Gaussian signals. However we should note that the IN strategy necessitates a precise knowledge of the channels' CSI to be implemented, while the CJ scheme does not rely on the knowledge of the signal coefficients for its signalling.

4.6 Conclusions

In this chapter we investigated the cognitive channel introduced in Chapter 3 where the secondary receiver is a potential eavesdropper with respect to the primary transmission. To efficiently allow the secondary system to operate simultaneously with the primary system while leaving the primary user's secrecy rate unchanged, we introduced clean relaying combined with cooperative jamming and dirty paper coding. The main contributions of this chapter can be summarized as follows:

- We introduced the clean relaying scheme for the cognitive radio channel with a stronger secrecy constraint than the weak secrecy, which generalizes the results in Chapter 3. Furthermore the model analyzed in this chapter considered the impact of the message-learning phase at T_2 in contrast with the ideal assumption in Chapter 3. Using the multi-phase clean relaying scheme, we derived the achievable secrecy rate of the considered channel via specializing the result from the information spectrum method [BL13].

- We investigated the optimization of the secondary user's rate under the constraint of non-degradation of the primary user's secrecy rate, over the power splitting and time splitting arguments.

- We considered several signalling strategies for the secondary transmitter and in particular we analyzed T_2's achievable rate when dirty paper coding with clean relaying or interference neutralization is used to compare with the performance of clean relaying with cooperative jamming.

- Finally we illustrated our results through numerical examples based on a geometrical setup, which emphasized the impact of the node geometry on the achievable rates and on the optimal power allocation and time splitting of the secondary transmitter. We also compared the performance of the CR scheme with the other signalling strategies in our setup.

Our results showed the impact of the primary message-learning phase on the system's performance as well as the role of the third phase for the clean relaying of the primary message, which confirmed the importance of the study in this chapter. Furthermore our study demonstrated how the signalling strategies can outperform each other depending on the relative location of the nodes. We conclude from this observation that the position of the users must be taken into account for the design of secure transmissions in cognitive radio networks.
Since secondary networks in CRNs usually consist of more than a single transmitter-receiver pair, the results of this chapter suggest that the primary network could choose which secondary transmitter is allowed to access the spectrum, depending on the users' location and their impact on the achievable secrecy rates. This leads to the study in the following chapter, where we will analyze the spectrum sharing mechanisms for cognitive radio networks with multiple secondary pairs.

4.A Proof of Theorem 4.1

Proof. The secrecy capacity of a general wiretap channel can be restated as the following from [BL13, Corollary 1]

$$C_s = \sup_{(\mathbf{V}_1,\mathbf{X}_1)\in P} \left(p\text{-}\liminf_{n\to\infty} \frac{1}{n} i(\mathbf{V}_1;\mathbf{Y}_1) - p\text{-}\limsup_{n\to\infty} \frac{1}{n} i(\mathbf{V}_1;\mathbf{Y}_2) \right), \tag{4.39}$$

where $P \triangleq \Big\{ \{\mathbf{V}_1\mathbf{X}_1\}_{n\geq 1} : \forall\, n \in \mathbb{N},\ \mathbf{V}_1 - \mathbf{X}_1 - \mathbf{Y}_1\mathbf{Y}_2$ forms a Markov chain and $\frac{1}{n} c_n(\mathbf{X}_1) \leq P$ with probability $1\Big\}$, $\{c_n\}_{n\geq 1}$ is a sequence of cost functions with $c_n : \mathcal{X} \to \mathbb{R}^+$, and

$$p\text{-}\liminf_{n\to\infty} \frac{1}{n} i(\mathbf{X};\mathbf{Y}) \triangleq \sup \left\{ \alpha : \lim_{n\to\infty} P\left(\frac{1}{n} i(\mathbf{X};\mathbf{Y}) < \alpha \right) = 0 \right\},$$
$$p\text{-}\limsup_{n\to\infty} \frac{1}{n} i(\mathbf{X};\mathbf{Y}) \triangleq \inf \left\{ \alpha : \lim_{n\to\infty} P\left(\frac{1}{n} i(\mathbf{X};\mathbf{Y}) > \alpha \right) = 0 \right\},$$

and $i(\mathbf{X};\mathbf{Y}) = \ln \frac{p(\mathbf{X},\mathbf{Y})}{p(\mathbf{X})p(\mathbf{Y})}$ is the information density. Since the whole channel is memoryless and for each phase the channel is stationary, we can rewrite the right-hand side (RHS) of (4.39) as follows

$$\begin{aligned}
C_s &\overset{(a)}{=} \sup_{(\mathbf{V}_1,\mathbf{X}_1)\in P} \Bigg(p\text{-}\liminf_{n\to\infty} \frac{1}{n} \left\{ i(\mathbf{V}_1^{(1)};\mathbf{Y}_1^{(1)}) + i(\mathbf{V}_1^{(2)};\mathbf{Y}_1^{(2)}) + i(\mathbf{V}_1^{(3)};\mathbf{Y}_1^{(3)}) \right\} - \\
&\qquad p\text{-}\limsup_{n\to\infty} \frac{1}{n} \left\{ i(\mathbf{V}_1^{(1)};\mathbf{Y}_2^{(1)}) + i(\mathbf{V}_1^{(2)};\mathbf{Y}_2^{(2)}) + i(\mathbf{V}_1^{(3)};\mathbf{Y}_2^{(3)}) \right\} \Bigg) \\
&\overset{(b)}{=} \sup_{(\mathbf{V}_1,\mathbf{X}_1)\in P} \Bigg(p\text{-}\liminf_{n\to\infty} \frac{1}{n} \left\{ \sum_{j=1}^{n_1} i(V_{1j}^{(1)};Y_{1j}^{(1)}) + \sum_{j=1}^{n_2} i(V_{1j}^{(2)};Y_{1j}^{(2)}) + \sum_{j=1}^{n_3} i(V_{1j}^{(3)};Y_{1j}^{(3)}) \right\} - \\
&\qquad p\text{-}\limsup_{n\to\infty} \frac{1}{n} \left\{ \sum_{j=1}^{n_1} i(V_{1j}^{(1)};Y_{2j}^{(1)}) + \sum_{j=1}^{n_2} i(V_{1j}^{(2)};Y_{2j}^{(2)}) + \sum_{j=1}^{n_3} i(V_{1j}^{(3)};Y_{2j}^{(3)}) \right\} \Bigg) \\
&\overset{(c)}{=} \sup_{(\mathbf{V}_1,\mathbf{X}_1)\in P} \Bigg(p\text{-}\liminf_{n\to\infty} \left\{ \frac{n_1}{n} \frac{1}{n_1} \sum_{j=1}^{n_1} i(V_{1j}^{(1)};Y_{1j}^{(1)}) + \frac{n_2}{n} \frac{1}{n_2} \sum_{j=1}^{n_2} i(V_{1j}^{(2)};Y_{1j}^{(2)}) \right. \\
&\qquad \left. + \frac{n_3}{n} \frac{1}{n_3} \sum_{j=1}^{n_3} i(V_{1j}^{(3)};Y_{1j}^{(3)}) \right\} - \\
&\qquad p\text{-}\limsup_{n\to\infty} \left\{ \frac{n_1}{n} \frac{1}{n_1} \sum_{j=1}^{n_1} i(V_{1j}^{(1)};Y_{2j}^{(1)}) + \frac{n_2}{n} \frac{1}{n_2} \sum_{j=1}^{n_2} i(V_{1j}^{(2)};Y_{2j}^{(2)}) \right. \\
&\qquad \left. + \frac{n_3}{n} \frac{1}{n_3} \sum_{j=1}^{n_3} i(V_{1j}^{(3)};Y_{2j}^{(3)}) \right\} \Bigg) \\
&\overset{(d)}{=} \sup_{(\mathbf{V}_1,\mathbf{X}_1)\in P} \Bigg(p\text{-}\liminf_{n\to\infty} \left\{ \frac{n_1}{n} I(V_1^{(1)};Y_1^{(1)}) + \frac{n_2}{n} I(V_1^{(2)};Y_1^{(2)}) + \frac{n_3}{n} I(V_1^{(3)};Y_1^{(3)}) \right\} - \\
&\qquad p\text{-}\limsup_{n\to\infty} \left\{ \frac{n_1}{n} I(V_1^{(1)};Y_2^{(1)}) + \frac{n_2}{n} I(V_1^{(2)};Y_2^{(2)}) + \frac{n_3}{n} I(V_1^{(3)};Y_2^{(3)}) \right\} \Bigg)
\end{aligned}$$

$$\overset{(e)}{=} \sup_{(\mathbf{V}_1,\mathbf{X}_1)\in P} \Big(\Big\{ \eta_1 I(V_1^{(1)};Y_1^{(1)}) + \eta_2 I(V_1^{(2)};Y_1^{(2)}) + \eta_3 I(V_1^{(3)};Y_1^{(3)}) \Big\} - \Big\{ \eta_1 I(V_1^{(1)};Y_2^{(1)}) + \eta_2 I(V_1^{(2)};Y_2^{(2)}) + \eta_3 I(V_1^{(3)};Y_2^{(3)}) \Big\} \Big)$$

where in

(a) we use the fact that there are three non-overlapping phases and these phases are memoryless and independent;

(b) we use the memoryless property $p_{\mathbf{Y}_1\mathbf{Y}_2|\mathbf{V}_1}(y_1^n, y_2^n|u^n) = \Pi_{i=1}^n p_{Y_1Y_2|X_1}(y_{1i}, y_{2i}|x_{1i}) \cdot p_{X_1|V_1}(x_{1i}|u_i)$, and the fact that in each phase the distribution is independent and identically distributed;

(c) we introduce n_k/n_k for each phase for the ease of the expression in average mutual information in the next step;

(d) we apply the law of large numbers: $\frac{1}{n_k} i(\mathbf{V}_1^{(k)};\mathbf{Y}_l^{(k)}) = \frac{1}{n_k}\sum_{j=1}^{n_k} i(V_{1j}^{(k)};Y_{lj}^{(k)}) \to I(V_1^{(k)};Y_l^{(k)})$ a.s. as $n_k \to \infty$, $k = \{1,2,3\}$ and $l = \{1,2\}$;

(e) we first define $\eta_k \triangleq n_k/n$, $k = \{1,2,3\}$, which are fixed. After substituting η_k, the RHS of (d) is independent of n and we can remove the p-$\liminf$ and the p-$\limsup$ operations.

For the power constraint, we can follow steps in [BL13, Theorem 3] with discrete approximations to have the average power constraint. This completes the proof. ■

4.B Proof of Proposition 4.1

Proof of Equation (4.20)

Proof. Using (4.14) in Theorem 4.1, the following secrecy rate is achievable for the primary user

$$R_1 = \sum_{k=1}^{3} \eta_k \left(I(V_1^{(k)};Y_1^{(k)}) - I(V_1^{(k)};Y_2^{(k)}) \right). \tag{4.40}$$

By the selection $\mathbf{V}_1 = \mathbf{X}_1$, we have

$$R_1 = \sum_{k=1}^{3} \eta_k \left(I(X_1^{(k)};Y_1^{(k)}) - I(X_1^{(k)};Y_2^{(k)}) \right). \tag{4.41}$$

Since T_2 is silent during the first phase, the normalized secrecy rate in this phase is $\eta_1 R_1^{\mathrm{WT}}$. To derive the normalized secrecy rate in the second phase, after substituting $x_2(t) = v_2(t) + \sqrt{\frac{P_{2,1}^{(2)}}{P_1}} e^{-j\phi_{21}} x_1(t) + a_2^{(2)}(t)$ where $c_{21} = |c_{21}|e^{j\phi_{21}}$ into (4.41),

we have

$$
\begin{aligned}
I\left(\mathbf{x}_1^{(2)};\mathbf{y}_1^{(2)}\right) &= I\left(\mathbf{x}_1^{(2)};\left(1+|c_{21}|\sqrt{\frac{P_{2,1}^{(2)}}{P_1}}\right)\mathbf{x}_1^{(2)}+c_{21}e^{j\phi_{21}}(\mathbf{v}_2^{(2)}+\mathbf{a}_2^{(2)})+\mathbf{n}_1^{(2)}\right)\\
&= h\left(\left(1+|c_{21}|\sqrt{\frac{P_{2,1}^{(2)}}{P_1}}\right)\mathbf{x}_1^{(2)}+c_{21}e^{j\phi_{21}}(\mathbf{v}_2^{(2)}+\mathbf{a}_2^{(2)})+\mathbf{n}_1^{(2)}\right)\\
&\quad - h\left(\left(1+|c_{21}|\sqrt{\frac{P_{2,1}^{(2)}}{P_1}}\right)\mathbf{x}_1^{(2)}+c_{21}e^{j\phi_{21}}(\mathbf{v}_2^{(2)}+\mathbf{a}_2^{(2)})+\mathbf{n}_1^{(2)}|\mathbf{x}_1^{(2)}\right)\\
&= \frac{1}{2}\log\left(1+\frac{P_1\left(1+|c_{21}|\sqrt{\frac{P_{2,1}^{(2)}}{P_1}}\right)^2}{1+|c_{21}|^2((1-\gamma)(1-\rho_2)+\rho_2)P_2^{(2)}}\right)\\
&= \mathcal{C}\left(\frac{\left|\sqrt{P_1}+|c_{21}|\sqrt{(1-\rho_2)\gamma P_2^{(2)}}\right|^2}{1+|c_{21}|^2(1-\gamma+\gamma\rho_2)P_2^{(2)}}\right)
\end{aligned}
$$

with $P_{2,1}^{(2)}=\gamma(1-\rho_2)P_2^{(2)}$ and

$$
\begin{aligned}
I(\mathbf{x}_1^{(2)};\mathbf{y}_2^{(2)}) &\le I(\mathbf{x}_1^{(2)};\mathbf{y}_2^{(2)}|\mathbf{v}_2^{(2)})\\
&= I\left(\mathbf{x}_1^{(2)};\left(c_{21}+c_{22}e^{-j\phi_{21}}\sqrt{\frac{P_{2,1}^{(2)}}{P_1}}\right)\mathbf{x}_1^{(2)}+c_{22}(\mathbf{v}_2^{(2)}+\mathbf{a}_2^{(2)})+\mathbf{n}_2^{(2)}|\mathbf{v}_2^{(2)}\right)\\
&= h\left(\left(c_{21}+c_{22}e^{-j\phi_{21}}\sqrt{\frac{P_{2,1}^{(2)}}{P_1}}\right)\mathbf{x}_1^{(2)}+c_{22}(\mathbf{v}_2^{(2)}+\mathbf{a}_2^{(2)})+\mathbf{n}_2^{(2)}|\mathbf{v}_2^{(2)}\right)\\
&\quad - h\left(\left(c_{21}+c_{22}e^{-j\phi_{21}}\sqrt{\frac{P_{2,1}^{(2)}}{P_1}}\right)\mathbf{x}_1^{(2)}+c_{22}(\mathbf{v}_2^{(2)}+\mathbf{a}_2^{(2)})+\mathbf{n}_2^{(2)}|\mathbf{x}_1^{(2)},\mathbf{v}_2^{(2)}\right)\\
&= \mathcal{C}\left(\frac{\left|c_{12}\sqrt{P_1}+c_{22}e^{-j\phi_{21}}\sqrt{(1-\rho_2)\gamma P_2^{(2)}}\right|^2}{1+c_{22}^2\rho_2 P_2^{(2)}}\right).
\end{aligned}
$$

Note that in the second term inside the bracket multiplied to η_2 on the RHS of (4.20), the denominator includes only the power from jamming but no power

from $v_2(t)$. This considers the worst case for T_1 that U_2 can decode w_2 and subtract $v_2(t)$ first, then the channel between T_1 and U_2 is not interfered by the signal $v_2(t)$, translated by the upper bounding of the leakage term in the proof $I(\mathbf{x}_1^{(2)};\mathbf{y}_2^{(2)}) \leq I(\mathbf{x}_1^{(2)};\mathbf{y}_2^{(2)}|\mathbf{v}_2^{(2)})$. Finally the normalized secrecy rate in the third phase $\eta_3 \left(I(X_1^{(3)};Y_1^{(3)}) - I(X_1^{(3)};Y_2^{(3)}) \right)$ is immediately obtained from the proof of the second term by setting $\gamma = 1$. ■

Proof of Equation (4.21)

Proof. For the secondary user, the power used for the transmission of w_2, which only happens in phase 2, is $P_{2,2}^{(2)} = (1-\rho_2)(1-\gamma)P_2^{(2)}$. In addition, the single letter expression rate should be scaled by η_2 since only phase 2 is used to transmit, then we have

$$\begin{aligned} R_2 &\leq \eta_2 I(\mathbf{v}_2^{(2)};\mathbf{y}_2^{(2)}) \\ &= I\left(\mathbf{v}_2^{(2)}; \left(c_{21} + c_{22}e^{-j\phi_{21}}\sqrt{\frac{P_{2,1}^{(2)}}{P_1}}\right)\mathbf{x}_1^{(2)} + c_{22}(\mathbf{v}_2^{(2)} + \mathbf{a}_2^{(2)}) + \mathbf{n}_2^{(2)}\right) \\ &= \mathcal{C}\left(\frac{c_{22}^2(1-\rho_2)(1-\gamma)P_2^{(2)}}{1 + c_{22}^2\rho_2 P_2^{(2)} + \left|c_{22}e^{-j\phi_{21}}\sqrt{\gamma(1-\rho_2)P_2^{(2)}} + c_{12}\sqrt{P_1}\right|^2}\right). \end{aligned}$$

The achievable rate region is proven. ■

4.C Proof of Proposition 4.2

Proof. To prove Proposition 4.2, we show that there exists a gap which cannot be made arbitrarily close to zero between the equivocation rate $H(w_1|\mathbf{Y}_2)$ and $H(w_1)$. First we know that

$$\begin{aligned} H(w_1|\mathbf{Y}_2) &\overset{(a)}{\geq} H(\mathbf{V}_1|\mathbf{V}_2) - H(\mathbf{V}_1|\mathbf{V}_2,\mathbf{Y}_2,w_1) - I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2) \\ &\overset{(b)}{\geq} (H(\mathbf{V}_1) - nI(V_1;V_2)) - n\varepsilon_2 - nI(V_1;Y_2|V_2), \end{aligned} \tag{4.42}$$

where (a) is from [LMSY08, (68)]; the expansion of the last two terms in (b) are from Lemma 2 and Lemma 3 in [LMSY08], respectively. For the original T_1, $H(\mathbf{V}_1) = n(R_1 + I(V_1;Y_2))$. After substituting it into (4.42), we have

$$H(w_1|\mathbf{Y}_2) \geq n(R_1 + I(V_1;Y_2) - I(V_1;V_2) - I(V_1;Y_2|V_2) - \varepsilon_2), \tag{4.43}$$

which can be further rearranged as

$$\frac{1}{n}I(w_1;\mathbf{Y}_2) \leq I(V_1;V_2Y_2) - I(V_1;Y_2) + \varepsilon_2 = I(V_1;V_2|Y_2) + \varepsilon_2. \tag{4.44}$$

Since there is no Markov chain as $V_1 - Y_2 - V_2$, from [Yeu08, Th. 2.34], we know that $I(V_1; V_2|Y_2) \neq 0$. Thus the weak secrecy constraint can not be guaranteed. ■

4.D Proof of Proposition 4.3

Proof. We first calculate the first term of (4.22):

$$\begin{aligned} I(V_1; Y_1) &= h(Y_1) - h(Y_1|V_1) \\ &= h(y_1) - h(c_{21}u_2 + c_{21}j_2 + n_1) \\ &= \log\left(1 + \frac{\left|1 + |c_{21}|\sqrt{\frac{(1-\rho_2)\gamma P_2^{(2)}}{P_1}}\right|^2 P_1}{1 + |c_{21}|^2(1-\gamma+\rho_2\gamma)P_2^{(2)}}\right) \\ &= \mathcal{C}\left(\frac{\left|\sqrt{P_1} + |c_{21}|\sqrt{(1-\rho_2)\gamma P_2^{(2)}}\right|^2}{1 + |c_{21}|^2(1-\gamma+\rho_2\gamma)P_2^{(2)}}\right). \end{aligned} \tag{4.45}$$

Then we calculate the summation of the remaining terms:

$$\begin{aligned} &I(V_1; Y_2|V_2) + I(V_1; V_2) = I(V_1, V_2; Y_2) - (I(V_2; Y_2) - I(V_1; V_2)) \\ &= \log\left(\frac{1 + \left|c_{22}e^{-j\phi_{21}}\sqrt{\frac{(1-\rho_2)\gamma P_2^{(2)}}{P_1}} + c_{12}\right|^2 P_1 + |c_{22}|^2(1-\gamma+\rho_2\gamma)P_2^{(2)}}{1 + |c_{22}|^2\rho_2 P_2^{(2)}}\right) \\ &\quad - (I(V_2; Y_2) - I(V_1; V_2)) \\ &= \log\left(\frac{1 + |c_{22}e^{-j\phi_{21}}\sqrt{(1-\rho_2)\gamma P_2^{(2)}} + c_{12}\sqrt{P_1}|^2 + |c_{22}|^2(1-\gamma+\rho_2\gamma)P_2^{(2)}}{1 + |c_{22}|^2\rho_2 P_2^{(2)}}\right) \\ &\quad - \log\left(\frac{1 + |c_{22}|^2(1-\gamma+\rho_2\gamma)P_2^{(2)}}{1 + |c_{22}|^2\rho_2 P_2^{(2)}}\right) \qquad (4.46) \\ &= \mathcal{C}\left(\frac{\left|c_{22}e^{-j\phi_{21}}\sqrt{(1-\rho_2)\gamma P_2^{(2)}} + c_{12}\sqrt{P_1}\right|^2}{1 + |c_{22}|^2(1-\gamma+\rho_2\gamma)P_2^{(2)}}\right) \qquad (4.47) \end{aligned}$$

where (4.46) results from the DPC capacity being the same as that of the interference free channel and here the powers of the signal and the equivalent additive

noise are $|c_{22}|^2(1-\gamma)(1-\rho_2)P_2^{(2)}$ and $1+|c_{22}|^2\rho_2 P_2^{(2)}$, respectively. After combining (4.45) and (4.47), we have (4.26). Finally R_2 is obtained from the usual achievable secondary rate expression for DPC transmission. This completes the proof of Proposition 4.3. ■

Chapter 5

Secrecy Games in CRNs with Multiple Secondary Users

In this chapter we investigate secrecy games in CRNs with multiple secondary pairs and secrecy constraints. First, we present the list of the chapter's goals.

Objectives of the Chapter.

- Extend the cognitive channel model from previous chapters to larger cognitive radio networks with multiple secondary pairs.
- Define the new network model and achievable rate regions when secondary pairs are allowed to use the channel simultaneously.
- Investigate the spectrum sharing mechanisms using several game theoretic models, namely:
  1. A single-leader multiple-follower Stackelberg game with T_1 as the leader and the secondary transmitters as followers.
  2. A non-cooperative power control game between the secondary transmitters if they can access the channel simultaneously.
  3. An auction between a primary auctioneer and secondary bidders which allows the primary transmitter to exploit the competitive interaction between the secondary transmitters.
- Illustrate through numerical simulations the equilibrium outcomes of the analyzed games and the impact of the competition between the secondary transmitters on the secrecy performance of the primary transmission in the cognitive radio network.

Organization of the Chapter This chapter consists of 6 sections. In Section 5.1 we motivate the study in this chapter and introduce some background on auction theory in cognitive radio networks. In Section 5.2 we describe our new system model. In Section 5.3 we investigate Stackelberg games between primary and secondary transmitters. In Section 5.4 we analyze the case where multiple secondary transmitters are allowed to transmit simultaneously through a Nash power control game. In Section 5.5 we describe and study the interaction between the primary transmitter and the secondary transmitters as a Vickrey auction. Further we illustrate numerically the outcome of the auction game and compare it to the Stackelberg games. Finally Section 5.6 concludes this chapter.

5.1 Introduction and Motivation

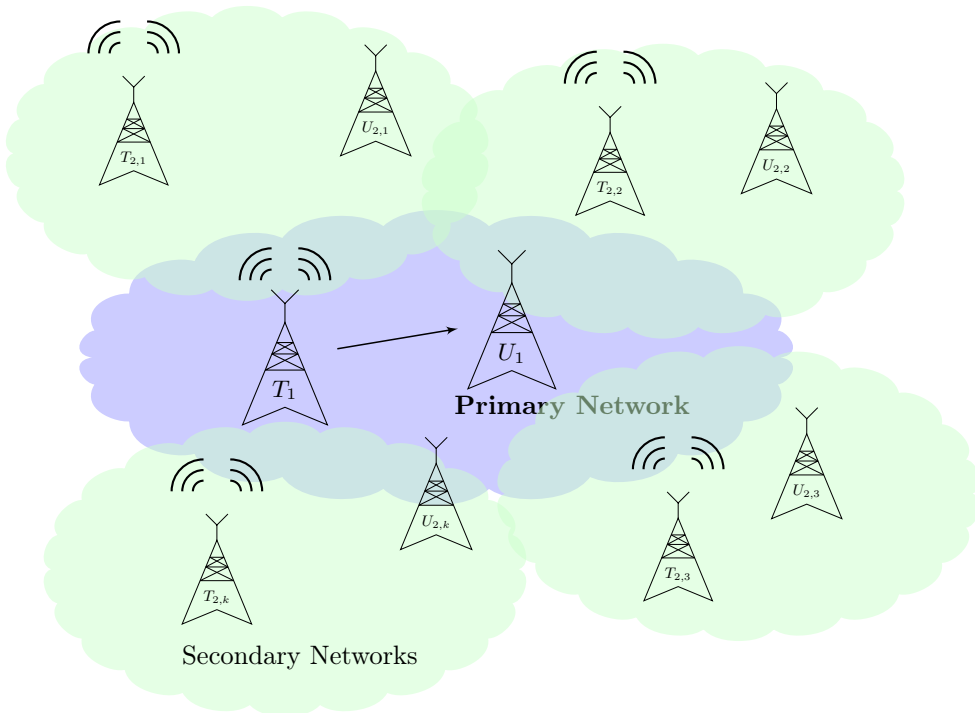


Figure 5.1: Cognitive radio network with multiple secondary pairs.

In this chapter we investigate the scenario described in Figure 5.1. As in the previous chapters, we consider a cognitive radio scenario, however in this chapter, we look at the novel case where multiple secondary transmitter-receiver pairs wish to access the spectrum. In this scenario, the primary network can either grant a share

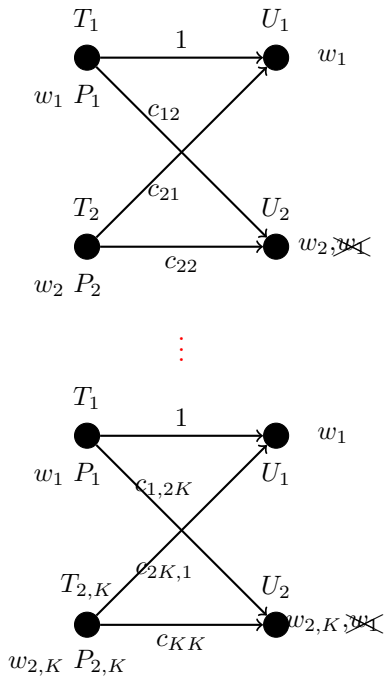


Figure 5.2: Equivalent orthogonal cognitive channels with secrecy constraints.

of the spectrum access to one secondary pair, which reduces to the cognitive channel investigated in the previous chapters, or it can allow multiple secondary pairs to access the spectrum. In the latter case, the transmission occurs simultaneously. As in Chapter 3 and Chapter 4 we investigate cooperation for secrecy in cognitive radio networks where the secondary receiver(s) are treated as potential eavesdropper(s) with respect to the primary transmission. We now explore the case where any secondary receiver $U_{2,k}$ which has been allowed to access the spectrum is treated as a potential eavesdropper with respect to the primary transmission. In this context, the primary transmitter T_1 is assisted by the trustworthy secondary transmitters T_{2k}'s if the cooperation could improve the secrecy performance, while the secondary transmitters benefit as they are awarded a share of the spectrum for their own data transmission. Therefore this chapter is a natural extension of our previous model to the more general network containing K secondary pairs in the network.

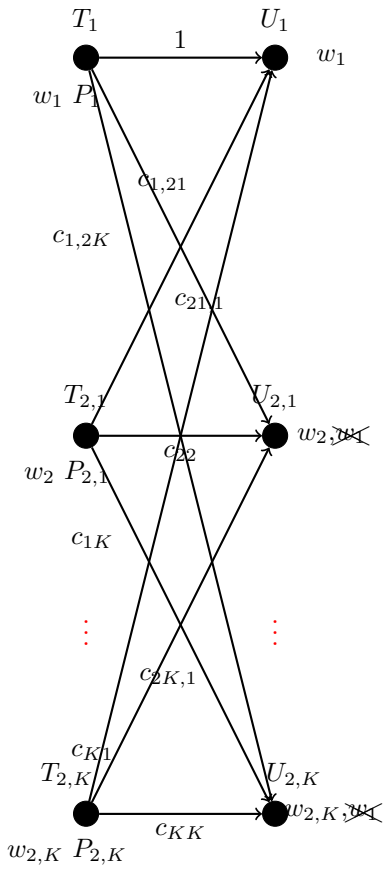


Figure 5.3: Cognitive channel with secrecy constraints and multiple secondary simultaneous transmissions.

5.2 System Model

In this section we define the model investigated throughout this chapter and we describe the different transmission scenarios considered.

5.2.1 Network Model

In this chapter we investigate the cognitive radio network described in Figure 5.1. The cognitive radio network consists of the following single antenna nodes: a primary transmitter T_1, a primary receiver U_1, and K potential cognitive secondary transmitter-receiver pairs $(T_{2,k}, U_{2,k})$, with $k \in [|1, K|]$. T_1 wishes to transmit the

secret message w_1, which is intended to U_1, and which should be kept secret from allowed secondary receivers $U_{2,k}$ with $k \in \mathcal{T}$ where $\mathcal{T}$ denotes the subset of secondary pairs allowed to use the spectrum. Simultaneously, $T_{2,k}$ wants to transmit the message $w_{2,k}$ (without secrecy constraints) to the secondary receiver $U_{2,k}$. We consider in particular two scenarios:

Single Secondary Pair: In this scenario $\mathcal{S}_s$, the primary network only allows one secondary transmitter-receiver pair to access the spectrum and transmit. This scenario can therefore be described as K orthogonal cognitive radio channels with secrecy where only one channel is active. This model is depicted in Figure 5.2.

Multiple Secondary Pairs: In this scenario $\mathcal{S}_m$, the primary network allows a subset $\mathcal{T} \subseteq \{1, \ldots, K\}$ to access the spectrum. Therefore several secondary transmitters are transmitting simultaneously, potentially increasing the benefit of cooperation. However, this leads to more secondary receivers being allowed to sense the spectrum and listen to the transmissions, thus potentially eavesdropping the primary message. This model is depicted in Figure 5.3.

5.2.2 Channel Model and Notations

In this section we describe the channel model corresponding to either scenario.

Single Secondary Pair Scenario $\mathcal{S}_s$: This corresponds to the cognitive scenario investigated in the previous chapters. We remind the AWGN channel model

$$\mathbf{y}_1 = \mathbf{x}_1 + \sqrt{c_{2i,1}}\mathbf{x}_2 + n_1, \tag{5.1}$$

$$\mathbf{y}_{2,i} = \sqrt{c_{1,2i}}\mathbf{x}_1 + \sqrt{c_{ii}}\mathbf{x}_2 + n_{2,i}, \tag{5.2}$$

where the noises $n_1, n_{2,i}$ are real-valued Gaussian distributed with unit variance, i.e., $n_1, n_{2,i} \sim \mathcal{N}(0,1)$ and

$$\frac{1}{n}\sum_{k=1}^{n} |x_{i,k}|^2 \leq P_i \quad \text{for} \quad i \in \{1,2\}. \tag{5.3}$$

A rate pair $(R_1, R_{2,i})$ for the messages w_1 and $w_{2,i}$ is then achievable, if $P_{e,1} \triangleq \Pr\{\hat{w}_1 \neq w_1\}$ and $P_{e,2} \triangleq \Pr\{\hat{w}_{2,i} \neq w_{2,i}\}$ can be made arbitrarily small, while the message w_1 stays secure from the secondary receiver, i.e.:

$$\max\{P_{e,1}, P_{e,2}\} \leq \varepsilon, \tag{5.4a}$$

$$I(w_1; \mathbf{y}_{2,i}) \leq n\varepsilon. \tag{5.4b}$$

When $T_{2,i}$ does not transmit, the maximum achievable rate R_1^{WT} such that both the reliability and secrecy conditions are fulfilled is known as the secrecy capacity of the wiretap channel given by $R_1^{\mathrm{WT}} = (\mathcal{C}(P_1) - \mathcal{C}(c_{1,2i}P_1))^+$.

Multiple Secondary Pairs Scenario $\mathcal{S}_m$: In this scenario described in Figure 5.3 the primary and secondary receiver k now receive:

$$\mathbf{y}_1 = \mathbf{x}_1 + \sum_{k\in\mathcal{T}} \sqrt{c_{2k,1}}\mathbf{x}_{2k} + n_1, \tag{5.5}$$

$$\mathbf{y}_{2,k} = \sqrt{c_{kk}}\mathbf{x}_{2k} + \sqrt{c_{1,2k}}\mathbf{x}_1 + \sum_{j\in\mathcal{T},j\neq k} \sqrt{c_{jk}}\mathbf{x}_j + n_{2,k}. \tag{5.6}$$

For the message w_1 to stay perfectly secure from the secondary receivers, the constraint (5.4b) now becomes

$$I(w_1; Y_{2,k}) \leq n\varepsilon \; \forall k \in \mathcal{T}, \tag{5.7}$$

for every $\varepsilon > 0$ and a sufficiently large n. Finally, without the cognitive transmitters $T_{2,k}$ the worst-case achievable secrecy rate assuming that all secondary receivers are potentially eavesdropping is given by:

$$R_{1,\mathrm{WC}}^{\mathrm{WT}} = \min_{k\in[|1,K|]} \left(\mathcal{C}(P_1) - \mathcal{C}(c_{1,2k}P_1)\right)^+. \tag{5.8}$$

5.2.3 Achievable Rate Regions

In this section we give the achievable rate regions depending on the scenario considered. Throughout this chapter, we assume the underlay scenario of Chapter 3 where the secondary transmitters do not have the knowledge of w_1. Thus, only the cooperative jamming strategy is available at $T_{2,k}$.

Single Secondary Pair Scenario $\mathcal{S}_s$ We parameterize the power fraction devoted to jamming by the transmitting user $T_{2,i}$ as $P_{2j,i} = \rho P_{2,i}$, where the parameter $\rho \in [0,1]$ denotes the fraction of the power used for jamming. The achievable rate region $\mathcal{R}_{\mathrm{jam},s}$ is given by:

$$R_1 < \left(\mathcal{C}\left(\frac{P_1}{1+c_{2i,1}P_{2,i}}\right) - \mathcal{C}\left(\frac{c_{1,2i}P_1}{1+c_{ii}\rho P_{2,i}}\right)\right)^+, \tag{5.9}$$

$$R_{2,i} < \mathcal{C}\left(\frac{c_{ii}(1-\rho)P_{2,i}}{1+c_{1,2i}P_1+c_{ii}P_{2,i}\rho}\right). \tag{5.10}$$

Multiple Secondary Pairs Scenario $\mathcal{S}_m$ Each secondary transmitter $T_{2,k} \in \mathcal{T}$ splits its available power $P_{2,k}$ into two parts: $P_{2\mathrm{s},k}$ for its own message $w_{2,k}$, and $P_{2\mathrm{j},k}$ for the jamming signal, such that $P_{2\mathrm{j},k} = \rho_k P_{2,k}$. In the following proposition we give the achievable rate region $\mathcal{R}_{\mathrm{jam},m}$ for this scenario.

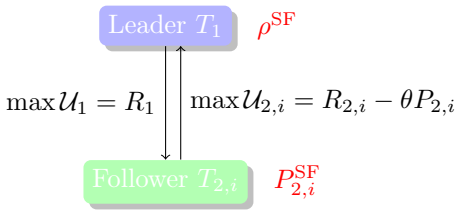


Figure 5.4: Single secondary user Stackelberg game (SF-SG) between T_1 and $T_{2,i}$.

Proposition 5.1.

The achievable rate region $\mathcal{R}_{\mathrm{jam},m}$ is given by:

$$R_1 < \left(\mathcal{C}\left(\frac{P_1}{1+\sum_k c_{2k,1} P_{2,k}} \right) - \max_{k\in\mathcal{T}} \mathcal{C}\left(\frac{c_{1,2k} P_1}{1 + c_{kk}\rho_k P_{2,k} + \sum\limits_{j\in\mathcal{T}, j\neq k} c_{j,k} P_{2,j}} \right) \right)^+ ,$$

$$R_{2,k} < \mathcal{C}\left(\frac{c_{kk}(1-\rho_k) P_{2,k}}{1 + c_{1,2k} P_1 + c_{kk}\rho_k P_{2,k} + \sum_{j\in\mathcal{T}, j\neq k} c_{j,k} P_{2,j}} \right),$$

where $k \in \mathcal{T}$.

In the following sections we will investigate different types of games between the primary transmitter T_1 and the secondary transmitters $T_{2,k}$ in order to predict the behavior of the users in this large cognitive radio network.

5.3 Stackelberg Games

In this section we investigate an important Stackelberg game between the primary transmitter T_1 and the secondary transmitters $T_{2,k}$. The Stackelberg model studied in this section constitutes the reference scenario upon which we will build the auction analysis in Section 5.5.

5.3.1 Single Follower Stackelberg Game

The single follower Stackelberg game (SF-SG) is depicted in Figure 5.4. We consider the case where there is a single secondary transmitter $T_{2,i}$, which corresponds to the cognitive channel model investigated in the previous chapters. This case represents

the communication scenario $\mathcal{S}_s$ when T_1 has already chosen the secondary pair according to some mechanism which will be described later on. As discussed in Chapter 3, a Stackelberg game between T_1 and $T_{2,i}$ is a common model to represent the conditional cooperation between both transmitters. Naturally, we consider the primary transmitter T_1, which is the owner of the spectrum, as the game leader selling some fraction of its spectrum to $T_{2,i}$ and, thus, $T_{2,i}$ as the follower being awarded a share of the spectrum for its cooperation.

Secondary Follower Utility $T_{2,i}$ is modeled as a buyer of the resource from the primary system which wants to maximize its achievable rate minus the cost of the power:

$$\mathcal{U}_{2,i}(\rho, P_{2,i}) = R_{2,i} - \theta P_{2,i},$$

where θ represents the fixed price per unit power for $T_{2,i}$ who solves:

$$\max_{P_{2,i}} \mathcal{U}_{2,i}(\rho, P_{2,i}).$$

Primary Leader Utility In this chapter we consider a different utility function for T_1 compared to Chapter 3, as an emphasis is placed on the secrecy performance of the primary network, and thus the payment $\theta P_{2,i}$ from $T_{2,i}$ for the power used is not taken into account in the primary utility; i.e., we have:

$$\mathcal{U}_1(\rho, P_{2,i}) = R_1,$$

and T_1 solves:

$$\max_{\rho} \mathcal{U}_1(\rho, P_{2,i}).$$

In the following theorem we derive the Stackelberg equilibrium of the (SF-SG) game defined above.

Theorem 5.1.

The Stackelberg equilibrium of the (SF-SG) game is given by $(P_{2,i}^{\mathrm{SF}}, \rho^{\mathrm{SF}})$, where

$$P_{2,i}^{\mathrm{SF}}(\rho) = \arg\max_{P_{2,i}} \mathcal{U}_{2,i}(\rho, P_{2,i}),$$
$$\rho^{\mathrm{SF}} = \arg\max_{\rho} \mathcal{U}_1(\rho, P_{2,i}^{\mathrm{SF}}).$$

The optimal power allocation $P_{2,i}^{\mathrm{SF}}$ is given by

$$P_{2,i}^{\mathrm{SF}}(\rho) = \left[\frac{\sqrt{(1-\rho)c_{\mathrm{SF}}\left[(1-\rho)b_{\mathrm{SF}}c_{\mathrm{SF}} + 2\rho a_{\mathrm{SF}}\right]}}{\rho a_{\mathrm{SF}}\sqrt{b_{\mathrm{SF}}}} - \frac{(1+\rho)c_{\mathrm{SF}}}{\rho a_{\mathrm{SF}}} \right]_0^{P_{2,i}^{\max}},$$

where $a_{\mathrm{SF}} \triangleq 2c_{ii}$, $b_{\mathrm{SF}} \triangleq 2\ln 2\theta$, $c_{\mathrm{SF}} \triangleq 1 + c_{1,2i}P_1$ and $[x]_{x_{\min}}^{x_{\max}} \triangleq \min\{x_{\min}, \max\{x_{\max}, x\}\}$. The corresponding equilibrium utilities are $(\mathcal{U}_1(\rho^{\mathrm{SF}}, P_{2,i}^{\mathrm{SF}}(\rho^{\mathrm{SF}})), \mathcal{U}_{2,i}(\rho^{\mathrm{SF}}, P_{2,i}^{\mathrm{SF}}(\rho^{\mathrm{SF}})))$ where T_1 first computes the optimal:

$$\rho^{\mathrm{SF}} = \arg\max_{0\le\rho\le 1} \mathcal{U}_1(P_{2,i}^{\mathrm{SF}}(\rho), \rho).$$

Finally ρ^{SF} is plugged into (5.1) to obtain the optimal power level of the secondary transmitter $P_{2,i}^{\mathrm{SF}}(\rho^{\mathrm{SF}})$.

Proof. Theorem 5.1 is obtained by first noticing that $\forall\rho \in [0,1]$ we have

$$\frac{\partial^2 \mathcal{U}_{2,i}(\rho, P_{2,i})}{\partial P_{2,i}^2} < 0.$$

Therefore the optimal power $P_{2,i}^{\mathrm{SF}}(\rho)$ is found by solving

$$\frac{\partial \mathcal{U}_{2,i}(\rho, P_{2,i})}{\partial P_{2,i}} = 0.$$

The result in the theorem follows by standard calculations. ■

Remark 5.1.

A condition for the participation of the secondary transmitter $T_{2,i}$ is obtained by noticing that if

$$\frac{\partial \mathcal{U}_{2,i}(\rho, P_{2,i}=0)}{\partial P_{2,i}} < 0 \tag{5.12}$$

then $\mathcal{U}_{2,i}$ is maximized for $P_{2,i} = 0$; i.e., the secondary transmitter does not cooperate with the primary transmitter. After calculations we obtain that Equation (5.12) is equivalent to

$$c_{ii}(1-\rho) - b_{\mathrm{SF}}\theta c_{\mathrm{SF}} < 0. \tag{5.13}$$

We can formulate a quantitative interpretation of this condition. Since $f(\rho,\theta) \triangleq c_{ii}(1-\rho) - b_{\mathrm{SF}}\theta c_{\mathrm{SF}}$ is a decreasing function in both ρ and θ, if those parameters are getting too large, then the secondary transmitter will not participate. This is intuitively reasonable, since if the price of the power is too high, or if most of the transmitting power is allocated to jamming, then the secondary transmitter is not interested in cooperating.

Illustration of the (SF-SG) Game In this section we illustrate the single follower Stackelberg game and its Stackelberg equilibrium using the geometrical model from previous chapters. The locations of the primary transmitter T_1 and receiver U_1 are still fixed at the coordinates $(0,0)$ and $(1,0)$, respectively while the secondary receiver is fixed at $(1,-1)$. We assume a path-loss model with path-loss exponent $\alpha = 3$, i.e., $c_{ij} = d_{ij}^{-3}$. The power constraints at both transmitters are $P_1^{\max} = P_{2,k}^{\max} = 10$ dB. In our example depicted in Figure 5.5, $T_{2,k}$ is located in $(1,-0.8)$.

In the figure we represent $\mathcal{U}_2(\rho, P_{2,k})$ as the red surface while $-\mathcal{U}_1(\rho, P_{2,k})$ is the blue surface. Note that we choose to represent the opposite of the primary utility for better readability of the figure, as both utilities would overlap otherwise. The Stackelberg game (SF-SG) can be explained as follows. For each possible strategy of T_1, $T_{2,k}$ finds the transmission power maximizing its utility; i.e., $T_{2,k}$ derives the function $P_{2,k}^{\mathrm{SF}}(\rho)$. In the figure $P_{2,k}^{\mathrm{SF}}(\rho)$ is depicted as the black line superimposed to the secondary utility. T_1, as the leader of the (SF-SG) game, is aware of $T_{2,k}$'s strategy and chooses accordingly the jamming fraction ρ^{SF} maximizing its own utility (i.e., minimizing $-\mathcal{U}_1(\rho, P_{2,k}^{\mathrm{SF}})$ in Figure 5.5). ρ^{SF} is represented as a green dot in the figure. Finally we note that the utility achieved in the SE of the (SF-SG) game is given by $\mathcal{U}_{2,i}(\rho^{\mathrm{SF}}, P_{2,i}^{\mathrm{SF}}(\rho^{\mathrm{SF}}))$ which is evaluated numerically as $\mathcal{U}_{2,i}(\rho^{\mathrm{SF}}, P_{2,i}^{\mathrm{SF}}(\rho^{\mathrm{SF}})) \approx 0.05$. We remark that $T_{2,k}$'s utility in the SE is significantly lower than its maximum utility, which is due to $T_{2,k}$ being the follower in

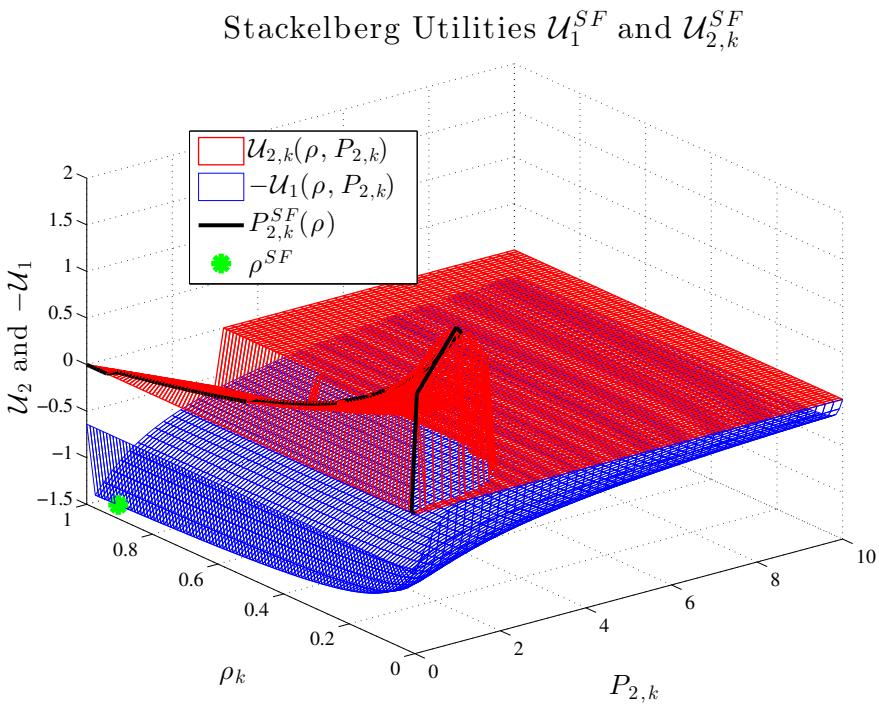


Figure 5.5: Illustration of the Stackelberg equilibrium mechanism for the (SF-SG) game.

the Stackelberg game model.

5.3.2 Multi-Follower Stackelberg Game

In this section we explain how to reduce the general framework of multiple secondary transmitters to the single follower analysis of Section 5.3.1. As described in Figure 5.3, the network can be decoupled into K possible 4-node channels with a single secondary transmitter. Therefore, T_1 can choose among K possible followers. For every possible follower $T_{2,i}$, it solves the corresponding (SF-SG) game as described in Section 5.3.1. T_1 then chooses the secondary pair which maximizes its utility $\mathcal{U}_1$.

The corresponding multi-follower Stackelberg game (MF-SG) is depicted in Figure 5.6. Formally the Stackelberg game framework described in Section 5.3.1 is changed as follows. The SE strategy of T_1 is now the jamming power and the

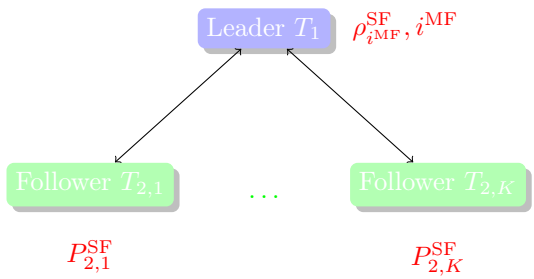


Figure 5.6: Multi-follower Stackelberg game (MF-SG) between T_1 and $T_{2,i}$ in Scenario $\mathcal{S}_s$.

indice i of the chosen secondary transmitter, such that

$$i^{\mathrm{MF}} = \arg\max_i \mathcal{U}_1(\rho_i^{\mathrm{SF}}, P_{2,i}^{\mathrm{SF}}),$$

where $(\rho_i^{\mathrm{SF}}, P_{2,i}^{\mathrm{SF}})$ are the corresponding Stackelberg equilibrium strategies of the single-follower Stackelberg game between T_1 and $T_{2,i}$. The primary transmitter SE utility is then given by $\mathcal{U}_1(\rho_i^{\mathrm{SF}}, P_{2,i}^{\mathrm{SF}})$, while only the secondary transmitter $T_{2,i^{\mathrm{MF}}}$ achieves a non-zero utility $\mathcal{U}_2(\rho_i^{\mathrm{SF}}, P_{2,i}^{\mathrm{SF}})$ among the secondary transmitters.
However, this Stackelberg game approach does not exploit fully the rational and competitive behavior of the secondary transmitters, as they are maximizing their utilities in the Stackelberg framework without taking into consideration the other secondary transmitters' strategies. This observation leads to the auction scenario which will be investigated in Section 5.5.

5.4 Power Control Game

In this section we consider the case where the secondary transmitters are allowed to transmit simultaneously, i.e., Scenario $\mathcal{S}_m$. For this scenario, we recall that the achievable rate region is given by Proposition 5.1.

5.4.1 Game Definition

We consider the Stackelberg framework from the previous section where T_1 is the leader of the game and the secondary transmitters $T_{2,k}$ are the followers. However there is now a fundamental difference with the model of the previous section since the strategy chosen by a secondary transmitter has an influence over the others' utilities due to the rate expressions in Proposition 5.1. Therefore we are now

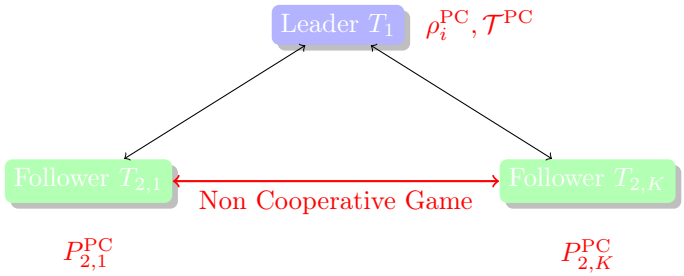


Figure 5.7: Multiple-user Stackelberg game between T_1 and $T_{2,i}$ in Scenario $\mathcal{S}_m$.

considering a 2-stage game as described in Figure 5.7. This power control game (PC-G) can be explained by the following steps.

1. For a given ρ_i and a given set of active secondary transmitters $\mathcal{T}$, each jammer i determines its transmitter power $P_{2,i}^{\mathrm{PC}}$ according to the Nash equilibrium of the non-cooperative game between the secondary transmitters.

2. T_1, as the leader of the Stackelberg game, accordingly chooses $\mathcal{T}^{\mathrm{PC}}$ and the corresponding ρ_i^{PC}'s of the secondary transmitters belonging to that set, i.e., with $i \in \mathcal{T}^{\mathrm{PC}}$, maximizing its utility.

5.4.2 Nash Equilibrium and Power Control Game Outcomes

In this section we establish the solution of the two-stage game between T_1 and the competing secondary transmitters. First, we characterize the outcome of the (PC-G) game in the following theorem.

Theorem 5.2.

The equilibrium outcome of the power control game (PC-G) between T_1 and the K secondary transmitters $T_{2,i}$ is given by the parameters $(P_{2,i}^{\mathrm{PC}}, \rho_i^{\mathrm{PC}}, \mathcal{T}^{\mathrm{PC}})$, $\forall i \in \mathcal{T}^{\mathrm{PC}}$ such that:

$$(\rho_i^{\mathrm{PC}}, \mathcal{T}^{\mathrm{PC}}) = \arg\max_{\rho} \mathcal{U}_1(\rho, , \mathcal{T}, P_{2,i}^{\mathrm{PC}}(\rho_i, \mathcal{T})), \tag{5.14}$$

with $\mathcal{T} \subseteq \{1, \ldots, K\}$ and where $P_{2,i}^{\mathrm{PC}}$ is the Nash equilibrium of the non-cooperative game between the secondary transmitters, i.e.

$$\mathcal{U}_{2,i}(\rho_i, \mathcal{T}, P_{2,i}^{\mathrm{PC}}, \mathbf{P}_{2,k}^{\mathrm{PC}}) \geq \mathcal{U}_{2,i}(\rho_i, \mathcal{T}, P_{2,i}, \mathbf{P}_{2,k}^{\mathrm{PC}}),\ \forall\, P_{2,i}, \tag{5.15}$$

where $(\rho_i, \mathcal{T})$ are fixed and $\mathbf{P}_{2,k}^{\mathrm{PC}}$ represents the vector of $P_{2,k}^{\mathrm{PC}}$, $\forall k \in \mathcal{T}$ with $k \neq i$.

Furthermore we are able to derive the transmission power of the secondary transmitters in the equilibrium outcome as given by the following proposition.

Proposition 5.2.

The Nash equilibrium strategy $P_{2,i}^{\mathrm{PC}}(\rho_i, \mathcal{T})$ for transmitter i of the non-cooperative game between the secondary transmitters is given by

$$P_{2,i}^{\mathrm{PC}}(\rho_i, \mathcal{T}) = \left[\frac{\sqrt{(1-\rho)c_{\mathrm{PC}}\left[(1-\rho)b_{\mathrm{PC}}c_{\mathrm{PC}} + 2\rho a_{\mathrm{PC}}\right]}}{\rho a_{\mathrm{PC}}\sqrt{b_{\mathrm{PC}}}} - \frac{(1+\rho)c_{\mathrm{PC}}}{\rho a_{\mathrm{PC}}} \right]_0^{P_{2,i}^{\max}}, \tag{5.16}$$

where $a_{\mathrm{PC}} \triangleq 2c_{ii}$, $b_{\mathrm{PC}} \triangleq 2\ln 2\theta$, $c_{\mathrm{PC}} \triangleq 1 + c_{1,2i}P_1 + \sum_{j\in\mathcal{T}, j\neq i} c_{j,i}P_{2,j}^{\mathrm{PC}}$.

Proof. Proposition 5.2 is obtained by solving

$$P_{2,i}^{\mathrm{PC}}(\rho_i, \mathcal{T}) \triangleq \frac{\partial \mathcal{U}_{2,i}(\rho_i, \mathcal{T})}{\partial P_{2,i}} = 0,$$

with $P_{2,j} = P_{2,j}^{\mathrm{PC}}$, $\forall j \in \mathcal{T}$, $j \neq i$. The proposition follows from standard calculations. ■

5.5 Auction Games

In this section we analyze the spectrum sharing mechanism from an auction perspective. In contrast to the Stackelberg game (MF-SG) investigated in Section 5.3,

the auction game model takes advantage of the competitive interaction between the secondary users for spectrum access. First we define the Vickrey auction considered in Section 5.5.1. We then investigate the outcome of the auction in Section 5.5.2.

5.5.1 Vickrey Auction Between T_1 and Secondary Bidders

In this section we consider the Vickrey auction defined as follows.

Definition 5.1.

- The auctioneer is the primary transmitter T_1, with utility $\mathcal{U}_1$ defined in Equation (5.3.1).
- The bidders are the secondary transmitters $T_{2,k}$. Bidder k's strategy is its transmission power $P_{2,k}$ and its utility is $\mathcal{U}_{2,k}$ is defined in Equation (5.3.1).
- The bids are given by $\mathcal{U}_1(\rho, P_{2,k})$ for ρ fixed, with the minimal bid being set as $R_{1,\mathrm{WC}}^{\mathrm{WT}}$; i.e., the primary transmitter only accepts bids higher than its worst-case achievable secrecy rate without the participation of the secondary transmitters.

Bidders are incentivized to bid their true value for second-price auction such as Vickrey auctions. This means formally that since truthful bidding is a dominant strategy, the outcome of Vickrey auctions is the dominant strategy equilibrium where every participant bids according to its dominant strategy defined as follows.

Definition 5.2 (Dominant strategy equilibrium)**.**

A dominant strategy equilibrium of a non cooperative game $\mathcal{G} = (\mathcal{N}, (\mathcal{S}_i)_{i\in\mathcal{N}}, (\mathcal{U}_i)_{i\in\mathcal{N}})$ is a strategy profile $s^{\mathrm{DS}} \in \mathcal{S}$, such that $\forall i \in \mathcal{N}$, we have:

$$\mathcal{U}_i(s_i^{\mathrm{DS}}, s_{-i}) \geq \mathcal{U}_i(s_i, s_{-i}) \qquad \forall s_i \in \mathcal{S}_i. \tag{5.17}$$

We denote here the winning bidder of the auction, i.e., the highest bidder, by

$$k^*(\rho) \triangleq \arg \max_{k\in[|1,K|]} \mathcal{U}_1(\rho, P_{2,k}^{\mathrm{DS}}(\rho)), \tag{5.18}$$

for a given ρ. Finally we denote the second highest bid, i.e., the minimum price that the auction winner has to pay, by

$$\mathcal{U}_1^{(2)}(\rho) \triangleq \max_{k\in[|1,K|],k\neq k^*} \mathcal{U}_1(\rho, P_{2,k}^{\mathrm{DS}}(\rho)). \tag{5.19}$$

As explained in [SY13], a winning bidder can possibly have an incentive to bid a larger amount than $\mathcal{U}_1^{(2)}(\rho)$, if for instance its utility is increased by doing so, and therefore we allow in the following the winning secondary transmitter to make a payment higher than the second-best price since this modification does not harm any user's utility.

Before analyzing the Vickrey auction defined above, we make the following remark.

Remark 5.2.

The Vickrey auction model chosen in this section is not the only possible way to analyze the competitive interaction between secondary transmitters from an auction perspective. An alternative auction scheme could be based on traditional ascending clock auctions, where T_1 is now changing the price θ assumed that is fixed in the Vickrey auction. The utility function of $T_{2,k}$ is still $\mathcal{U}_{2,k}(\rho, \theta, P_{2,k}) = R_{2,k} - \theta P_{2,k}$ and the utility function of T_1 is now $U_1(\rho, \theta, P_{2,k}) = R_1 - R_1^{\mathrm{WT}}$. Note how the wiretap rate is subtracted from the utility of the auctioneer in order to fix the reserve price such that T_1 does not participate in the auction if he does not provide the performance achieved without the presence of the secondary transmitters.

1. Start with T_1 setting $\theta_0 = 0$, and solve $P_{2,k}^*(\theta_0) = \arg\max_{P_{2,k}} \mathcal{U}_{2,k}(\theta_0, P_{2,k})$, $\forall k$.
2. If $\mathcal{U}_1(\rho, \theta_0, P_{2,k}(0)) \leq 0$ (alternatively $\max_\rho \mathcal{U}_1(\rho, \theta_0, P_{2,k}(0)) \leq 0$), the primary transmitter does not participate in the trade.
3. While $\sum_k P_{2,k} \geq P_2^{\max}$, $\theta_t = \theta_{t-1} + \varepsilon$, and continue the auction.

After the auction has finished, T_1 is then maximizing its utility over ρ, as in the Stackelberg framework for the Vickrey auction.

5.5.2 Auction Analysis

In this section we investigate the outcome of the sealed-bid second-price auction defined in Section 5.5.1. First we derive the secondary transmission power $P_{2,k}^M$ which maximizes the primary utility in the following proposition.

Proposition 5.3.

Assuming that ρ is fixed, the function $\mathcal{U}_1(\rho, P_{2,k})$ is quasi-concave in $P_{2,k}$ with a maximum for $P_{2,k}^M \triangleq \arg\max_{P_{2,k}\in[0,P_{2,k}^{max}]} \mathcal{U}_1(\rho, P_{2,k})$ given by

$$P_{2,k}^M = \left[\frac{d_M + \sqrt{d_M^2 - (b_M - c_M)(a_M(b_M c_{1,2k} - c_{2k,1}) + c_M)}}{b_M - c_M} \right]_0^{P_{2,k}^{\max}}, \tag{5.20}$$

if the following condition is satisfied:

$$\frac{b_M c_{1,2k}}{1 + c_{1,2k} P_1} > \frac{c_{2k,1}}{a_M}, \tag{5.21}$$

with $a_M \triangleq 1 + P_1$, $b_M \triangleq c_{kk}\rho$, $c_M \triangleq c_{1,2k}c_{2k,1}$, and $d_M \triangleq c_{1,2k} - 1$.

Proof. The proof of Proposition 5.3 is given in Appendix 5.A. ■

Using the previous result, we give in the following proposition the dominant strategy for secondary transmitter $T_{2,k}$ in the dominant strategy equilibrium.

Proposition 5.4.

The dominant strategy $P_{2,k}^{\mathrm{DS}}(\rho)$ for secondary transmitter $T_{2,k}$ for a fixed ρ is given by

$$P_{2,k}^{\mathrm{DS}}(\rho) = \min(P_{2,k}^M, P_{2,k}^{\max}). \tag{5.22}$$

where $P_{2,k}^{max}$ is the maximum available transmission power and $P_{2,k}^M$ is given in Proposition 5.3.

Proof. The proof of Proposition 5.4 is obtained immediately from the following observations:

1. $T_{2,k}$'s dominant strategy is to maximize its chance of winning the auction, which is independent from the other transmitter's bids. Therefore $T_{2,k}$ aims at maximizing $\mathcal{U}_1$; i.e., $T_{2,k}$ bids $P_{2,k}^M$.

2. The bidding amount must be within the transmission power range; i.e. $P_{2,k}^{\mathrm{DS}}(\rho)$ is limited by $P_{2,k}^{\max}$.

■

Finally we give in the following theorem the outcome of the Vickrey auction between T_1 and the secondary transmitters $T_{2,k}$.

Theorem 5.3.

Let $T_{2,k^*(\rho)}$ be the winner of the Vickrey auction between T_1 and the secondary transmitters $T_{2,k}$. The transmission power $P_{2,k^*(\rho)}(\rho)$ chosen by $T_{2,k^*(\rho)}$ is given by

$$P^{\mathrm{VA}}_{2,k^*(\rho)}(\rho) = \begin{cases} P_{2,\mathrm{r1}} & \text{if } P^{\mathrm{SF}}_{2,k^*(\rho)}(\rho) > P_{2,\mathrm{r1}}, \\ P_{2,\mathrm{r2}} & \text{if } P^{\mathrm{SF}}_{2,k^*(\rho)}(\rho) < P_{2,\mathrm{r2}}, \\ P^{\mathrm{SF}}_{2,k^*(\rho)}(\rho) & \text{if } P_{2,\mathrm{r2}} \leq P^{\mathrm{SF}}_{2,k^*(\rho)}(\rho) \leq P_{2,\mathrm{r1}}, \end{cases}$$

where we define $P_{2,\mathrm{r1}}$ and $P_{2,\mathrm{r2}}$, with $P_{2,\mathrm{r1}} > P_{2,\mathrm{r2}}$, as the roots of the second-price constraint:

$$\mathcal{U}_1(\rho, P_{2,k^*(\rho)}(\rho)) = \mathcal{U}_1^{(2)}(\rho), \tag{5.23}$$

and where $P^{\mathrm{SF}}_{2,k^*(\rho)}(\rho)$ is defined in Theorem 5.1.
Finally, as the leader of the resulting Stackelberg game in which the auction winner is the follower, T_1 determines its SE strategy as

$$\rho^{\mathrm{VA}} \triangleq \arg\max_{\rho} \mathcal{U}_1^{\mathrm{VA}}(\rho, P^{\mathrm{VA}}_{2,k^*(\rho)}(\rho)), \tag{5.24}$$

which leads to its SE utility $\mathcal{U}_1^{\mathrm{VA}}$.

Proof. Since $T_{2,k^*(\rho)}$ has won the auction, it should provide the auctioneer T_1 an utility at least equal to the second bid, i.e., such that

$$\mathcal{U}_1(\rho, P_{2,k^*(\rho)}(\rho)) \leq \mathcal{U}_1^{(2)}(\rho). \tag{5.25}$$

Since $\mathcal{U}_1$ is quasi-concave in P_2 and we assume that the condition (5.21) of Proposition 5.3 is fulfilled, there exists two roots $P_{2,\mathrm{r1}}$ and $P_{2,\mathrm{r2}}$ of Equation (5.23), and $T_{2,k^*(\rho)}$ can choose any transmission power in the interval $[P_{2,\mathrm{r2}}, P_{2,\mathrm{r1}}]$. Therefore $T_{2,k^*(\rho)}$ maximizes its utility $\mathcal{U}_{2,k^*(\rho)}$, under the constraint (5.25). This leads to three cases due to the quasi-concavity of $\mathcal{U}_{2,k^*(\rho)}$ in $P_{2,k^*(\rho)}$, depending on the relative order between $P^{\mathrm{SF}}_{2,k^*(\rho)}(\rho)$ which is the solution of the maximization of $\mathcal{U}_{2,k^*(\rho)}$ and the roots of Equation (5.23). This concludes the proof of the theorem. ■

5.5.3 Numerical Illustrations

In this section we illustrate and compare the multiple follower Stackelberg game (MF-SG) and the Vickrey auction (VA) using our geometrical model. We are now

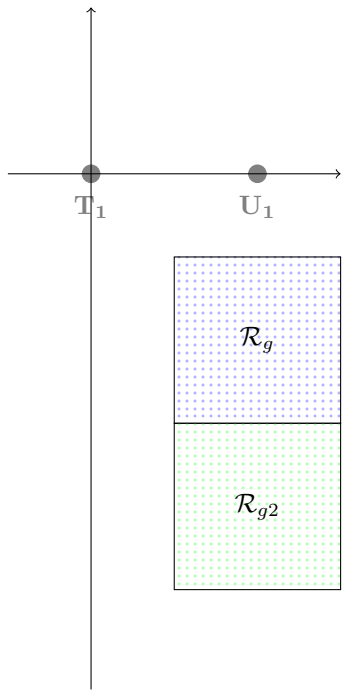


Figure 5.8: Topology of the cognitive radio network: $T_1 = (0, 0)$, $U_1 = (1, 0)$, and $(T_{2,k}, U_{2,k})$ in the rectangle $\mathcal{R}_g$ or the rectangle $\mathcal{R}_{g2}$.

interested in how the system behaves for different locations of the secondary pairs. In particular, we consider two regions of interest for the possible locations of the pairs $(T_{2,k}, U_{2,k})$ as shown in Figure 5.8. The cognitive pairs are located randomly inside a rectangle, either $\mathcal{R}_g$ or $\mathcal{R}_{g2}$. For each scenario we average our simulation results over 200 possible $(T_{2,k}, U_{2,k})$ coordinates. The locations of the primary transmitter T_1 and receiver U_1 are still fixed at the coordinates $(0, 0)$ and $(1, 0)$ while we assume as usual a path-loss model with path-loss exponent $\alpha = 3$ and power constraints at both transmitters as $P_1^{\max} = P_2^{\max} = 10$ dB.

In Figure 5.9 we show the average primary equilibrium utilities $\mathcal{U}_1^{\mathrm{MF}}$ and $\mathcal{U}_1^{\mathrm{VA}}$ for the multi-follower Stackelberg game (MF-SG) and the Vickrey auction, respectively, for cognitive pairs in $\mathcal{R}_g$ as a function of the number of potential transmitters $T_{2,k}$. We observe that the primary utility in the Vickrey auction equilibrium $\mathcal{U}_1^{\mathrm{VA}}$ are higher than those in the Stackelberg game $\mathcal{U}_1^{\mathrm{MF}}$, which shows that the auction exploits the competition between the secondary users to increase the auctioneer's, i.e. T_1's utility. Both utilities are increasing functions of the number of potential secondary transmitters, which is the expected behavior. Moreover by comparing the slope of the curves, we observe that each increment of the number of users has a

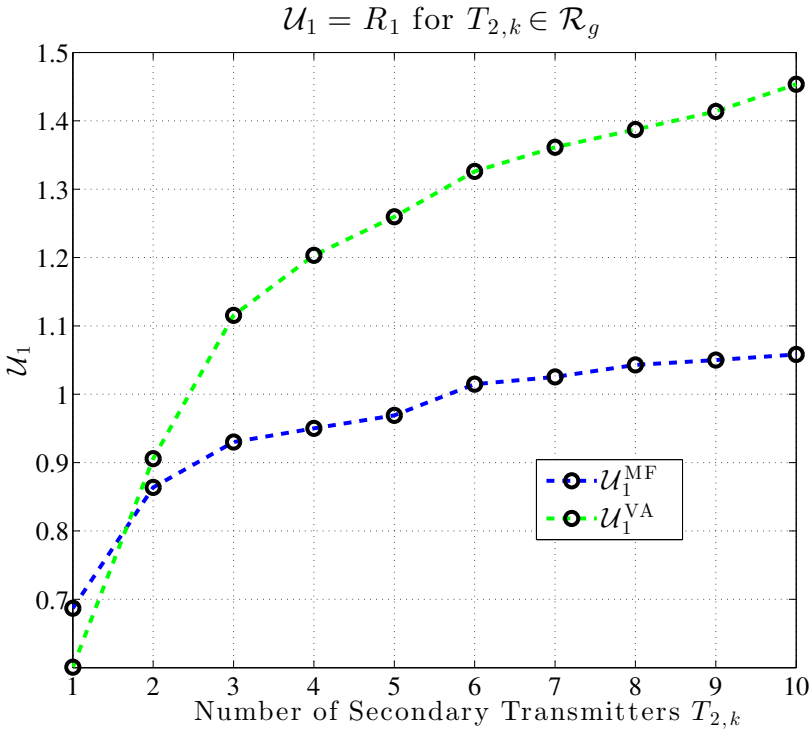


Figure 5.9: $\mathcal{U}_1^{\mathrm{MF}}$ and $\mathcal{U}_1^{\mathrm{VA}}$ for cognitive pairs in $\mathcal{R}_g$ as a function of the number of existing secondary transmitters.

bigger impact on the primary utility in the Vickrey auction than in the Stackelberg game. This is due to secondary users being in direct competition for the Vickrey auction, which leads to an increment of the bids (and thus, the primary utilities) for each new potential bidder. On the other hand, adding a new Stackelberg follower does not influence the other followers' strategies since the Stackelberg game is played between T_1 and the $T_{2,k}$'s, which justifies the smaller impact on the primary equilibrium utility. Finally when the number of secondary transmitter is equal to 1, $T_{2,k}$ simply needs to bid the wiretap rate to win the auction, which explains why the (MF-SG) game outperforms the Vickrey auction game in this case. We observe indeed in Figure 5.9 that for 1 secondary transmitter, the primary utility is 0.62 which is the average achievable wiretap rate with $U_{2,k}$ randomly located in $\mathcal{R}_g$.

The previous observations are verified in Figure 5.10 where we show the average primary equilibrium utilities $\mathcal{U}_1^{\mathrm{MF}}$ and $\mathcal{U}_1^{\mathrm{VA}}$, this time for cognitive pairs in $\mathcal{R}_{g2}$ as a function of the number of potential transmitters $T_{2,k}$. We note that for this

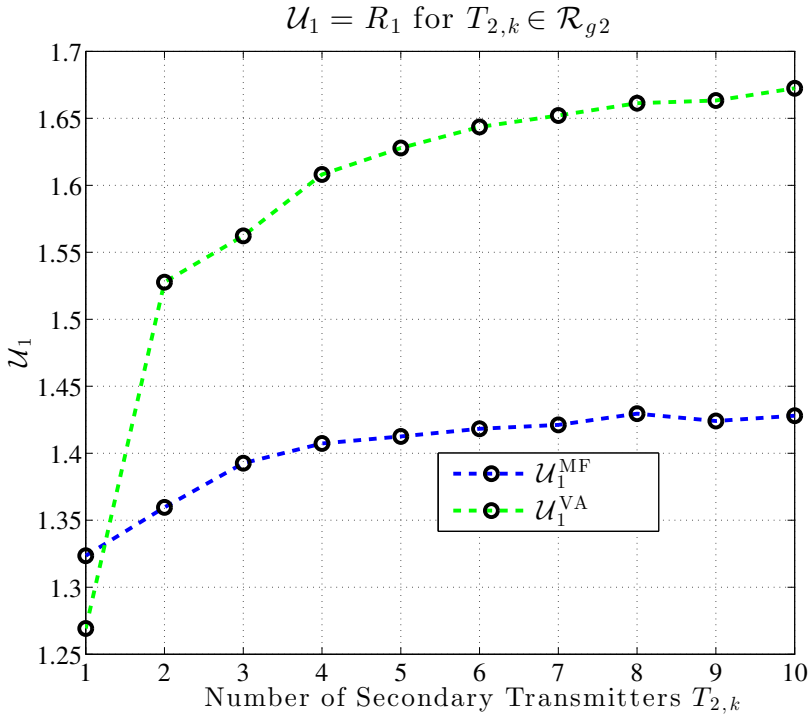


Figure 5.10: $\mathcal{U}_1^{\mathrm{MF}}$ and $\mathcal{U}_1^{\mathrm{VA}}$ for cognitive pairs in $\mathcal{R}_{g2}$ as a function of the number of existing secondary transmitters.

region of secondary networks, the primary utilities have higher values than in the previous case, since the potential eavesdroppers are located further away.

5.6 Conclusions

In this chapter we extended our cognitive channel model to larger cognitive radio networks with multiple secondary pairs. Based on this newly defined network model we investigated several spectrum sharing mechanisms using a game theoretic perspective to model the interactions between the secondary transmitters. In particular we analyzed:

- A single-leader multiple-follower Stackelberg game (MF-SG) with T_1 as the leader and the secondary transmitters as followers.
- A non-cooperative power control game (PC-G) between secondary transmitters accessing the channel simultaneously.
- A Vickrey auction (VA) between a primary auctioneer and secondary bidders which allows the primary transmitter to exploit the competitive interaction between the secondary transmitters.

We characterized the game theoretic equilibrium of each game, and we illustrated how the primary transmitter can exploit the competition between secondary transmitters via the Vickrey auction compared to the (MF-SG) game. Intuitively, we could have expected the secrecy performance to be negatively affected by the presence of multiple potential eavesdroppers in the cognitive radio network. Instead, our results highlight the fact that the primary network can exploit the competition between secondary users aiming at accessing the spectrum for their transmissions to increase its secrecy performance, even if the secondary transmitters are potentially eavesdropping the primary message.

Note that the study in this chapter can be pursued in several promising directions, such as:

- The use of other game theoretic concepts (e.g., social welfare maximization).
- The use of different auction mechanisms than Vickrey auction for spectrum sharing, (e.g., a share auction where multiple secondary transmitters can access the spectrum simultaneously).
- The perspective of cooperative game theory for the optimization of the secondary users' strategies.

5.A Proof of Proposition 5.3

Let $a_M \triangleq 1 + P_1$, $b_M \triangleq c_{kk}\rho$, $c_M \triangleq c_{1,2k}c_{2k,1}$, and $d_M \triangleq c_{1,2k} - 1$ as defined in Proposition 5.3. First we solve

$$\frac{\partial R_1}{\partial P_{2,k}}(P_{2,k} = 0) > 0, \tag{5.26}$$

with

$$R_1 = \mathcal{C}\left(\frac{P_1}{1 + c_{2k,1}P_{2,k}}\right) - \mathcal{C}\left(\frac{c_{1,2k}P_1}{1 + c_{kk}\rho P_{2,k}}\right). \tag{5.27}$$

Solving Equation (5.26) yields to the condition (5.21). Then, assuming the condition (5.21) is satisfied, we have

$$P_{2,k}^M \triangleq \arg \max_{P_{2,k} \in [0, P_{2,k}^{max}]} \mathcal{U}_1(\rho, P_{2,k}) \tag{5.28}$$

$$\implies P_{2,k}^M \in [0, P_{2,k}^{max}] \text{ and } \frac{\partial R_1}{\partial P_{2,k}}(P_{2,k} = P_{2,k}^M) = 0. \tag{5.29}$$

Proposition 5.3 follows from solving Equation (5.29), which reduces after standard calculations to solving a polynomial equation in $P_{2,k}^M$. This concludes the proof of the proposition.

Chapter 6

Energy Efficiency Analysis of Cognitive Radio Channels with Secrecy

In this chapter we investigate energy efficiency for cognitive radio channels with secrecy. First, we present the list of the chapter's goals.

Objectives of the Chapter.

- Introduce the energy efficiency (EE) performance measure for cognitive radio networks with secrecy constraints.
- Investigate the optimal power allocation and power splitting at the secondary transmitter for our cognitive model to maximize the secondary EE under secrecy constraints.
- Formulate and analyze an important EE Stackelberg game between the two transmitters aiming at maximizing their utilities.
- Illustrate the analytical results through our geometrical model highlighting the EE performance of the system as well as the role of the optimization parameters and the impact of the Stackelberg game on the performance.

Organization of the Chapter This chapter consists of 6 sections. In Section 6.1 we introduce the notion of energy efficiency and we motivate the study of this chapter. In Section 6.2 we recall our system model and we provide the necessary definitions for this chapter. In Section 6.3 we investigate and solve the maximization

of the secondary energy efficiency. In Section 6.4 we study a competitive interaction modeled as a Stackelberg game between both transmitters. In Section 6.5 we illustrate our results through numerical simulations which highlight the optimal parameters, the impact of the Stackelberg game and the energy efficiency performance of cooperation for secrecy in CRNs. Section 6.6 concludes this chapter.

6.1 Introduction on Energy Efficiency in Cognitive Radio Networks

Spectrum efficiency and energy efficiency (EE) are two fundamental issues for wireless communication networks. While cognitive radio is a promising paradigm to tackle the spectrum scarcity problem and thus improve the spectral efficiency of wireless networks, not much attention had been paid to the optimization of power consumption in cognitive radio networks until recently. Power consumption optimization, and hence energy efficient communication, is of crucial importance for CRNs as it reduces the environmental impact while simultaneously cutting deployment costs necessary to the development of green wireless networks [FJL+13]. The EE criterion has gained considerable attention lately, as highlighted by the publication of a recent special issue on energy efficient cognitive radio networks in the IEEE Communications Magazine [sur14], see references therein.

Several definitions of EE exist in the literature. The most common definition of the energy efficiency of a communication link is the benefit-cost ratio, where the benefit is the amount of data that can be reliably transmitted per unit of time while the cost is the resulting consumed energy per unit of time. It can therefore be seen as minimizing the energy consumption of the secondary users while guaranteeing QoS requirements, such as the secondary data rate R_2. An approach to energy efficient spectrum allocation in cognitive radio *ad hoc* networks is described in [YLH10] where the channel access problem is formulated as a joint power-rate control and channel optimization problem, with the objective to maximize the total capacity and minimize the power consumption of the system. In [LWM11] the problem of channel assignment in cognitive radio sensor networks is studied from an energy efficiency perspective as the sensor networks are energy constrained by nature. For further references on the spectrum allocation in cognitive radio networks with energy efficiency constraints, we refer the interested reader to [TZFS13] and references therein.

6.2 System Model, Transmission Schemes and Achievable Rate Regions

In this section we introduce the system model investigated in this chapter and we remind the achievable rate regions for the considered schemes in our scenario.

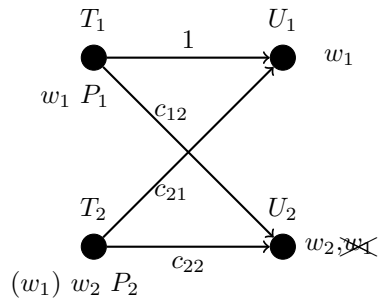


Figure 6.1: Cognitive channel with secrecy constraints.

6.2.1 Network Model

In this chapter we investigate the cognitive radio network defined in Chapter 3 and depicted in Figure 6.1. We remind the assumptions for the ease of the reader. The cognitive radio network consists of the following single antenna nodes: a primary transmitter T_1, a cognitive secondary transmitter T_2, a primary receiver U_1 and a secondary receiver U_2. T_1 wishes to transmit the secret message w_1, which is intended to U_1, and which should be kept secret from U_2, whereas T_2 wants to transmit the message w_2 (without secrecy constraints) to the secondary receiver U_2.

6.2.2 Transmission Model and Notations

We consider the following transmission scheme. T_1 encodes its message w_1 into $\mathbf{x_1}$ independently of the encoding at the secondary transmitter. T_2 encodes (w_1, w_2) into $\mathbf{x_2}$. We have:

$$\begin{aligned}\mathbf{y}_1 &= \mathbf{x}_1 + \sqrt{c_{21}}\mathbf{x}_2 + n_1,\\ \mathbf{y}_2 &= \sqrt{c_{12}}\mathbf{x}_1 + \sqrt{c_{22}}\mathbf{x}_2 + n_2,\end{aligned}$$

As in the previous chapters, a rate pair (R_1, R_2) for the messages w_1 and w_2 is achievable, if $P_{e,1} \triangleq P\{\hat{w}_1 \neq w_1\}$ and $P_{e,2} \triangleq P\{\hat{w}_2 \neq w_2\}$ can be made arbitrarily small, while the message w_1 stays secure from the secondary receiver, i.e.:

$$\max\{P_{e,1}, P_{e,2}\} \leq \varepsilon, \tag{6.1a}$$

$$I(w_1; \mathbf{y}_2) \leq n\varepsilon. \tag{6.1b}$$

When T_2 does not transmit, the maximum achievable rate R_1^{WT} such that both the reliability and secrecy conditions are fulfilled is known as the secrecy capacity of the wiretap channel and is given by $R_1^{\mathrm{WT}} = (\mathcal{C}(P_1) - \mathcal{C}(c_{12}P_1))^+$.

6.2.3 Transmission Schemes and Achievable Rate Regions

In this section we remind the achievable rate region from Chapter 3 depending on the transmitting scheme of the secondary transmitter.

Without Knowledge of w_1 at T_2 This scenario will be our main case of study throughout the chapter. Only the cooperative jamming strategy is available at T_2 since the secondary transmitter cannot relay w_1. We parameterize the power fraction devoted to jamming as $P_{2j} = \rho P_2$, where the parameter $\rho \in [0, 1]$ denotes the fraction of the power used for jamming. The achievable rate region $\mathcal{R}_{\text{jam}}$ is given by:

$$R_1 < \left(\mathcal{C}\left(\frac{P_1}{1 + c_{21}P_2} \right) - \mathcal{C}\left(\frac{c_{12}P_1}{1 + c_{22}\rho P_2} \right) \right)^+, \tag{6.2}$$

$$R_2 < \mathcal{C}\left(\frac{c_{22}(1-\rho)P_2}{1 + c_{12}P_1 + c_{22}P_2\rho} \right). \tag{6.3}$$

With Knowledge of w_1 at T_2 The secondary transmitter T_2 knows the primary message w_1 perfectly in this scenario. This scenario will only be considered for numerical comparison purposes in Section 6.5, as the intractability of the rate region makes an analytical optimization of the EE over the transmission parameters difficult. With the knowledge of w_1, T_2 is encoding (w_1, w_2) into $\mathbf{x}_2$. In particular T_2 splits its available transmission power P_2 into three parts: w_2 encoded into V_2, the jamming signal encoded into J_2, and w_1 is encoded into V_1, to be decoded only by the primary user U_1. In other words, we have:

$$x_2(t) = V_2(t) + V_1(t) + J_2(t).$$

For convenience, we parameterize the power fractions devoted to jamming, relaying and own message as $P_{2j} = \rho P_2$, $P_{2,1} = \gamma(1-\rho)P_2$ and $P_{2,2} = (1-\gamma)(1-\rho)P_2$, respectively. We consider the scheme where w_1 is encoded into V_1 and independent of the other Gaussian random variables as considered in Chapter 3, and we refer the reader to this chapter for further details. The achievable rate region $\mathcal{R}_{rel}$ is given by:

$$R_1 < \left(\mathcal{C}\left(\frac{P_1 + c_{21}(1-\rho)\gamma P_2}{1 + c_{21}(1-\gamma+\gamma\rho)P_2} \right) - \mathcal{C}\left(\frac{c_{12}P_1 + c_{22}(1-\rho)\gamma P_2}{1 + c_{22}\rho P_2} \right) \right)^+, \tag{6.4}$$

$$R_2 < \mathcal{C}\left(\frac{c_{22}(1-\rho)(1-\gamma)P_2}{1 + c_{12}P_1 + c_{22}P_2(\rho + \gamma - \rho\gamma)} \right). \tag{6.5}$$

6.3 Optimization of the Secondary Energy Efficiency

In this section we investigate the optimization of the secondary user's energy efficiency for the underlay scenario where T_2 does not have the knowledge of the primary message.

6.3.1 Definitions and Optimization Problem

First, we give some necessary definitions for our system study.

Definition 6.1 (Secondary Energy Efficiency)**.**

We define the energy efficiency of the secondary user as:

$$EE_2 \triangleq \frac{R_2}{P_2 + P_c},$$

where P_c denotes the hardware-dissipated power at the secondary transmitter.

We then define the optimization problem investigated throughout the chapter.

Definition 6.2.

Considering the rate region $\mathcal{R}_{\text{jam}}$ defined by (6.2) and (6.3), we define the optimization problem $\mathcal{P}_{\mathcal{R}_{\text{jam}}}(EE_2)$ as

$$\mathcal{P}_{\mathcal{R}_{\text{jam}}}(EE_2) \triangleq \max_{\rho, P_2} EE_2$$
$$\text{s.t. } R_1 \geq R_1^{\text{WT}} \quad \text{and} \quad P_2 \leq P_2^{\max}.$$

6.3.2 Main Result

In this section we derive our main result, stated in the following theorem.

Theorem 6.1.

There exists a unique power allocation $P_2^\star$ and a unique corresponding power splitting $\rho^\star$ which are the solution of the optimization problem $\mathcal{P}_{\mathcal{R}_{\text{jam}}}(EE_2)$, i.e.,

$$(\rho^\star, P_2^\star) \triangleq \arg\max_{\rho, P_2} \; EE_2, \tag{6.7}$$

assuming that the following constraint is satisfied:

$$\frac{c_{21}(1 + c_{12}P_1)}{c_{22}c_{12}(1 + P_1)} < 1. \tag{6.8}$$

Proof. The proof of Theorem 6.1 is given in Appendix 6.A. ■

We can make the following interesting remark.

Remark 6.1.

We notice that the necessary condition (6.8) (i.e., $\rho^\star(0) \in [0; 1]$, see Appendix 6.A) implies that

$$\frac{c_{21}(1 + c_{12}P_1)}{c_{22}c_{12}(1 + P_1)} < 1 \xrightarrow[P_1 \to \infty]{} \frac{c_{21}}{c_{22}} < 1. \tag{6.9}$$

That is, with unlimited power available at the primary transmitter, the necessary condition for the existence of an optimal power splitting for the energy efficiency is to have a better channel from T_2 to U_2 than to U_1 which is intuitively correct since it means that the jamming is more hurtful to the eavesdropper than the legitimate receiver of the protected message.

6.3.3 Numerical Evaluation of $P_2^\star$

While Theorem 6.1 guarantees the existence of an optimal power allocation $P_2^\star$ under certain constraints, it does not provide an efficient way to obtain the optimal value numerically. In this section we introduce an algorithm adapted to this challenge.

The energy efficiency is defined as in Definition 6.1 by

$$EE_2 = \frac{R_2}{P_2 + P_c}\,, \tag{6.10}$$

wherein P_2 and P_c denote the transmit power and hardware-dissipated power, respectively. Given the fractional nature of (6.10), it is clear that a key tool in the

analysis and optimization of energy efficiency is fractional programming, a mathematical technique which provides a framework for the optimization of fractional functions [Sch83]. We give in the following the results from fractional programming theory which will be used in the numerical simulations.

In its more general form, a fractional problem can be defined as follows.

Definition 6.3.

Let $\mathcal{C} \subseteq \mathbb{R}^n$ be a convex set and consider the functions, $f : \mathcal{C} \to \mathbb{R}_0^+$ and $g : \mathcal{C} \to \mathbb{R}^+$. A fractional program is the optimization problem

$$\begin{cases} \max\limits_{\mathbf{x}} \dfrac{f(\mathbf{x})}{g(\mathbf{x})} \\ \text{s.t. } \mathbf{x} \in \mathcal{C} \end{cases} \tag{6.11}$$

A fundamental result of fractional programming relates the solution of (6.11) to the auxiliary function $F(\lambda) = \max\{f(\mathbf{x}) - \lambda g(\mathbf{x}) \ : \ \mathbf{x} \in \mathcal{C}\}$.

Proposition 6.1.

Consider Problem (6.11) and the auxiliary function $F(\lambda)$. An $\mathbf{x}^\star \in \mathcal{C}$ solves (6.11) if and only if $\mathbf{x}^\star = \arg\max\{f(\mathbf{x}) - \lambda^\star g(\mathbf{x}) \ : \ \mathbf{x} \in \mathcal{C}\}$, with $\lambda^\star$ the unique zero of $F(\lambda)$.

Proof. The result has first been proved in [Jag66, Din67] with additional assumptions on $f(\mathbf{x})$ and $g(\mathbf{x})$ and then extended to general fractional programs in [RLV99]. ■

Proposition 6.1 implies that we can solve (6.11) by finding the zero of $F(\lambda)$ and then solving the associated auxiliary problem. An algorithm to do so is Dinkelbach's algorithm [Din67].

Algorithm 1 Dinkelbach's Algorithm

Set $\varepsilon > 0$; $\lambda = 0$;
repeat
  $\mathbf{x}^\star = \arg\max\{f(\mathbf{x}) - \lambda g(\mathbf{x}) \ : \ \mathbf{x} \in \mathcal{C}\}$
  $F = f(\mathbf{x}^\star) - \lambda g(\mathbf{x}^\star)$;
  $\lambda = \dfrac{f(\mathbf{x}^\star)}{g(\mathbf{x}^\star)}$;
until $F \leq \varepsilon$

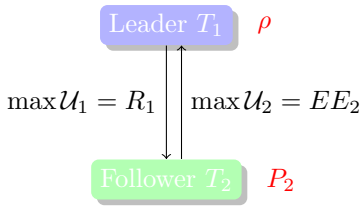


Figure 6.2: Stackelberg game between T_1 and T_2.

If we assume that $f(\mathbf{x})$ and $g(\mathbf{x})$ are concave and convex, respectively, then in each iteration we need to solve a convex problem, which means that we can solve (6.11) by solving a sequence of convex problems. Moreover, it is known that Dinkelbach's algorithm converges with a super-linear rate.

6.4 Game Theoretic Analysis: a Stackelberg Game Perspective

In this section we consider a more realistic cooperation between both transmitters as a non-cooperative Stackelberg game, represented in Figure 6.2. Indeed since T_1 and T_2 have their own interests and do not cooperate unconditionally, and T_1 is the legacy owner of the spectrum, the Stackelberg game is a natural approach to model their competitive interaction.

Definition of the Stackelberg Game

As in the previous section, T_2 aims at maximizing its energy efficiency. Therefore its utility function is defined as

$$\mathcal{U}_2(\rho, P_2) = EE_2, \tag{6.12}$$

T_2 intends to maximize its utility, i.e., to solve the following maximization problem:

$$\max_{P_2} \mathcal{U}_2(\rho, P_2). \tag{6.13}$$

However, unlike in the previous section where T_1 was satisfied with $R_1 > R_1^{\mathrm{WT}}$, in the Stackelberg model, T_1 aims at maximizing its achievable secrecy rate by adapting the jamming power provided by the secondary transmitter. We define its utility function as

$$\mathcal{U}_1(\rho, P_2) = R_1 - \theta\rho P_2, \tag{6.14}$$

where θ represents the cost paid by T_1 for the jamming power. We will elaborate on the role of the penalty $-\theta\rho P_2$ in Section 6.5. Similarly, T_1 wants to maximize

its utility; i.e., it wants to solve:

$$\max_{\rho} \mathcal{U}_1(\rho, P_2). \tag{6.15}$$

The SE of the game is then given by

$$P_2^*(\rho) = \arg\max_{P_2} \mathcal{U}_2(\rho, P_2), \tag{6.16a}$$

$$\rho^* = \arg\max_{\rho} \mathcal{U}_1(\rho, P_2^*). \tag{6.16b}$$

The corresponding equilibrium utilities are $(\mathcal{U}_1^{\mathrm{SE}}(\rho^*, P_2^*(\rho^*)), \mathcal{U}_2^{\mathrm{SE}}(\rho^*, P_2^*(\rho^*)))$.

T_1, as a leader, sets some value to the parameter ρ, which T_2, as a follower, takes into account. The secondary transmitter then optimizes P_2 to maximize its own utility $\mathcal{U}_2(\rho, P_2)$. As shown in the proof in Appendix 6.A, we have that $EE_2(\rho, P_2)$ is a concave function of P_2 and therefore, the optimal power as a function of the jamming power fraction is found by setting the derivative $\frac{\partial}{\partial P_2}\mathcal{U}_2(\rho, P_2)$ to zero. The optimal power allocation is then given by $P_2^*(\rho)$. Numerically, we can find the optimal power allocation $P_2^*(\rho)$ using Algorithm 1.

T_1 can then compute the optimal jamming fraction ρ^* maximizing its own utility function $\mathcal{U}_1(\rho, P_2^*)$:

$$\rho^* = \arg\max_{0 \le \rho \le 1} \mathcal{U}_1(\rho, P_2^*(\rho)). \tag{6.17}$$

The optimal jamming fraction ρ^* is then plugged into $P_2^*(\rho)$ to obtain the optimal power level of the secondary transmitter $P_2^*(\rho^*)$. Thus, a pair $(\rho^*, P_2^*(\rho^*))$ determines the Stackelberg equilibrium for the game, i.e., the optimal power allocation for the secondary user.

6.5 Numerical Results

In this section we present numerical results and related discussions. We will illustrate the energy efficiency and corresponding rate results, as well as the power splitting and power consumption using a specific topology of interest. In particular, we are interested in how the system behaves for different locations of the secondary transmitter. The region of interest for the possible locations of T_2 is shrinked compared to the previous chapters as represented in Figure 6.3. From Chapter 3 we know that CJ performs better when T_2 is located close to U_2 and therefore we reduce the possible locations of T_2 to the rectangle $\mathcal{R}_{EE}$ compared to the illustrative examples in previous chapters. The locations of the primary transmitter T_1 and receiver U_1 are still fixed at the coordinates $(0, 0)$ and $(1, 0)$, respectively while the secondary receiver is fixed at $(1, -1)$. We assume a path-loss model with path-loss exponent $\alpha = 3$, i.e., $c_{ij} = d_{ij}^{-3}$. The power constraints at both transmitters are $P_1^{\max} = P_2^{\max} = 10$ dB. In every figure in this section the x-axis represents the x coordinate of T_2 inside $\mathcal{R}_{EE}$, i.e., varying from $x = 0.5$ to $x = 1.1$ while the y-axis of each plot represents the y coordinate of T_2 inside $\mathcal{R}_{EE}$, i.e. for $y \in [-1.1, 0.1]$.

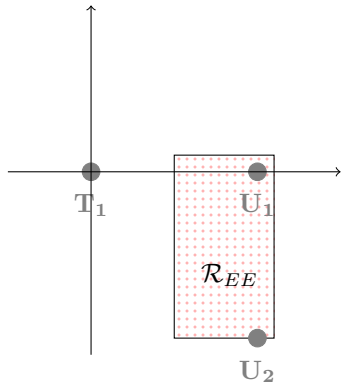


Figure 6.3: Topology of the cognitive radio channel: $T_1 = (0,0)$, $U_1 = (1,0)$, $U_2 = (1,-1)$ and T_2 in the rectangle $\mathcal{R}_{EE}$.

6.5.1 Energy Efficiency Optimization

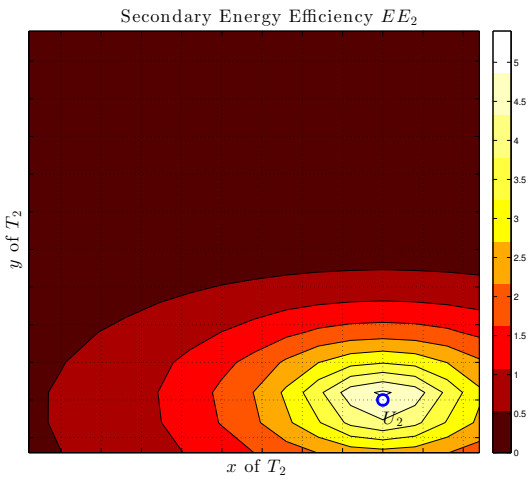


Figure 6.4: Secondary energy efficiency depending on the position of T_2.

First we illustrate the secondary energy efficiency performance of our scheme in Figure 6.4. A darker coordinate (x_{T_2}, y_{T_2}) in the figure represents a low value for EE_2 while lighter colors represent higher energy efficiencies. We observe, as expected, that the secondary energy efficiency is the highest for T_2 being located

close to U_2. This is due to several reasons.

1. The secondary transmitter needs to use less transmission power when it is located close to its receiver for its own message. Thus the denominator in the expression of EE_2 is reduced.

2. Similarly R_2 is increased when T_2 is close to U_2, which increases EE_2.

3. Jamming is more efficient when the target of the jamming is located closer to the source of the interference.

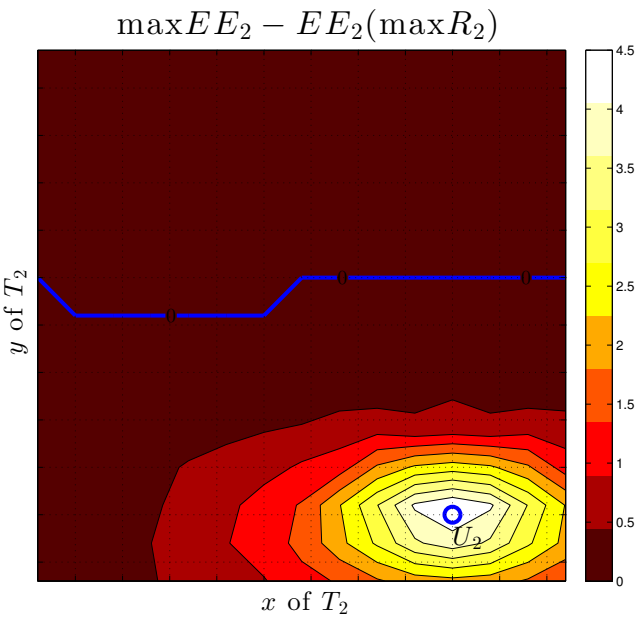


Figure 6.5: Comparison of the energy efficiency EE_2 obtained for the optimizations $\mathcal{P}_{\mathcal{R}_{\text{jam}}}(EE_2)$ and $\max R_2$.

In Figure 6.5 we compare the energy efficiency EE_2 obtained for the optimizations $\mathcal{P}_{\mathcal{R}_{\text{jam}}}(EE_2)$ and when T_2 maximizes its achievable rate, i.e., solves $\max R_2$. For the region located above the blue line, both energy efficiencies are zero. For the region under this line, we observe that as T_2 gets closer to U_2, there is a considerable improvement of the energy efficiency performance when T_2 maximizes EE_2 instead of R_2, which shows that some power P_2 is wasted when T_2 aims at maximizing its rate instead of considering $\mathcal{P}_{\mathcal{R}_{\text{jam}}}(EE_2)$.

6.5.2 Power Allocation and Power Splitting

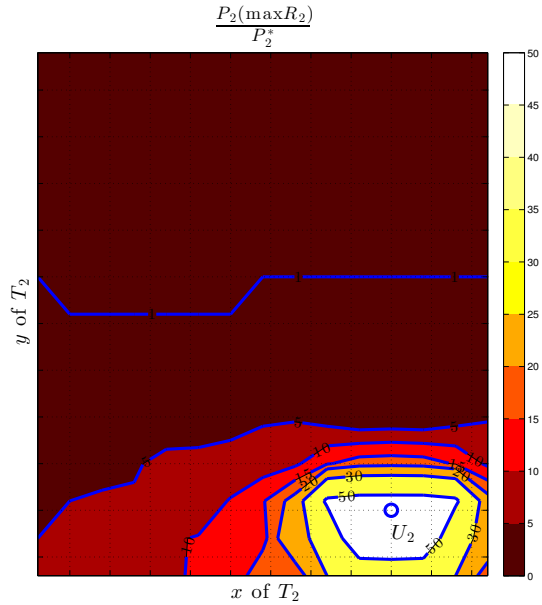


Figure 6.6: Comparison of the power consumption of T_2 for the optimizations $\mathcal{P}_{\mathcal{R}_{\text{jam}}}(EE_2)$ and $\max R_2$.

In Figure 6.6 we illustrate our previous observation by representing the ratio $\frac{P_2(\max R_2)}{P_2^\star}$ of the transmission power of the secondary transmitter used to maximize R_2 over the transmission power maximizing the secondary energy efficiency. We observe that the largest savings are obtained when T_2 is located close to its receiver, as the power ratio goes up to 50 in an area around U_2.

In Figure 6.7 we show the optimal jamming power which maximizes EE_2 for the optimization problem $\mathcal{P}_{\mathcal{R}_{\text{jam}}}(EE_2)$. First, as depicted in the previous figures, no $EE_2 > 0$ is achievable for locations of T_2 in the upper part of the rectangle $\mathcal{R}_{EE}$, which explains the zero power allocated to jamming in that region. Further we observe that in the relevant region, the power allocated to jamming decreases as T_2 gets closer to U_2. This can be explained by two main reasons.

1. The total power consumed by T_2 decreases as T_2 gets closer to U_2 when $\mathcal{P}_{\mathcal{R}_{\text{jam}}}(EE_2)$ is considered, and thus, even if the power splitting parameters ρ is kept constant, the total power allocated to CJ is decreased.

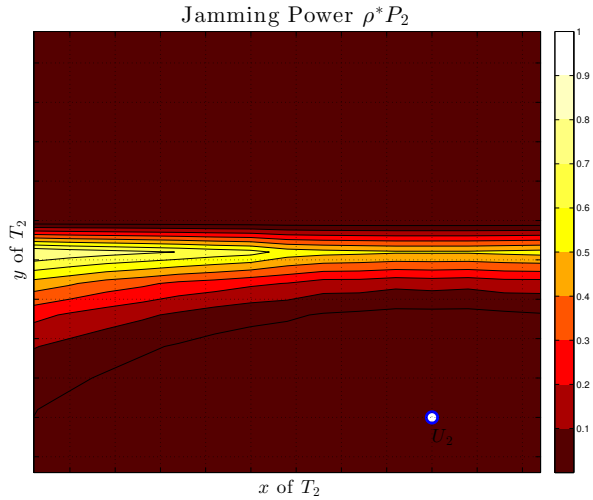


Figure 6.7: Optimal power splitting $\rho^\star$ for $\mathcal{P}_{\mathcal{R}_{\text{jam}}}(EE_2)$.

2. As T_2 approaches U_2, jamming becomes more efficient, and thus the proportion of jamming needed to efficiently confuse U_2 about the primary message is decreased.

6.5.3 Impact of the Stackelberg Game

In this section we evaluate the influence of the competitive interaction between T_1 and T_2, modeled as a Stackelberg game, on the energy efficiency performance of the system. We evaluate first the impact of the game on the primary performance. Since T_1 is the leader of the Stackelberg, and now aims at maximizing its utility $\mathcal{U}_1$ instead of only requiring the constraint $R_1 \geq R_1^{\text{WT}}$ to be satisfied, we expect its performance to be improved in the Stackelberg game. We first consider the case where $\theta = 0$. From Equation (6.14) we have $\mathcal{U}_1 = R_1$ and T_1 does not pay any price for the jamming power. This is therefore the best case scenario for T_1 which is the leader of the Stackelberg game and maximizes its achievable secrecy rate without any penalty for the jamming power sacrificed by T_2.

In Figure 6.8 we plot the difference between the utility $\mathcal{U}_1^{\text{SE}} = R_1^{\text{SE}}$ of T_1 in the Stackelberg equilibrium and R_1^{WT} which can be referred to as its utility without the Stackelberg competition. We observe a large increase of the SE utility $\mathcal{U}_1^{\text{SE}}$ as T_2 gets closer to U_2. This is due to the fact that T_1 is maximizing its utility over the jamming power ρ and can thus set a large proportion of the secondary power to be allocated to jamming as T_2 approaches U_2 leading to a higher primary

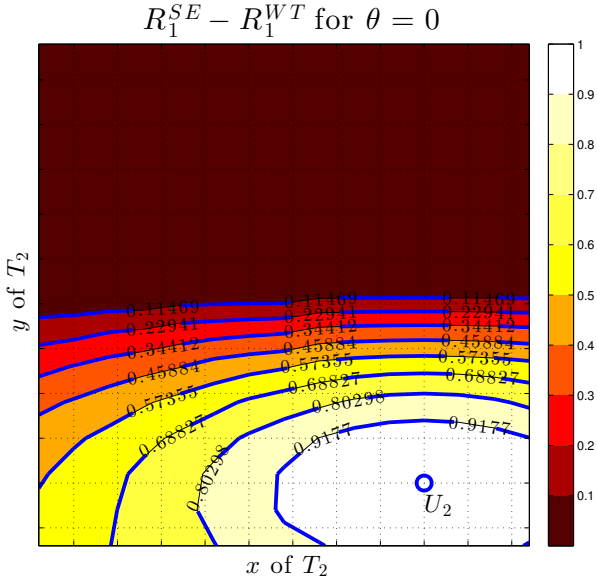


Figure 6.8: Difference between $\mathcal{U}_1^{\mathrm{SE}} = R_1^{\mathrm{SE}}$ in the Stackelberg equilibrium and R_1^{WT}.

utility defined as the secrecy rate. We should expect this to affect the secondary energy efficiency EE_2 in the Stackelberg equilibrium, as the power splitting are now singularly different than for $\mathcal{P}_{\mathcal{R}_{\mathrm{jam}}}(EE_2)$.

In order to confirm our previous observation, we represent in Figure 6.9 the difference between the secondary energy efficiency obtained previously for $\mathcal{P}_{\mathcal{R}_{\mathrm{jam}}}(EE_2)$ and the energy efficiency $EE_2^{\mathrm{SE}} = \mathcal{U}_2^{\mathrm{SE}}$ in the Stackelberg equilibrium. We observe a large decrease of EE_2 in the SE compared to the maximized secondary energy efficiency. The decrease gets more significant as T_2 gets closer to U_2. In fact, by comparing the values of the difference $\max EE_2 - EE_2^{\mathrm{SE}}$ with $\max EE_2$ in Figure 6.4, we notice that EE_2 is almost zero everywhere in the Stackelberg equilibrium, which is a consequence of T_1 being the leader of the game choosing ρ to maximize its own utility. However this model does not take account the penalty $-\theta\rho P_2$ on the primary utility for the jamming power as $\theta = 0$, i.e., we considered the most optimistic scenario for T_1.

A fairer Stackelberg model is investigated in the following as we consider $\theta = 0.9$. Due to the penalty introduced for the jamming power, we should expect a decrease in the utility performance of T_1. To verify this expected behavior, we represent in Figure 6.10 the difference between $\mathcal{U}_1^{\mathrm{SE}}(\theta = 0.9)$ and $\mathcal{U}_1^{\mathrm{SE}}(\theta = 0)$. First we note that in the upper part of the plane we had $\mathcal{U}_1^{\mathrm{SE}}(\theta = 0) = R_1^{\mathrm{SE}} = R_1^{\mathrm{WT}}$, i.e., the achievable secrecy rate in the Stackelberg equilibrium was unchanged and equal to

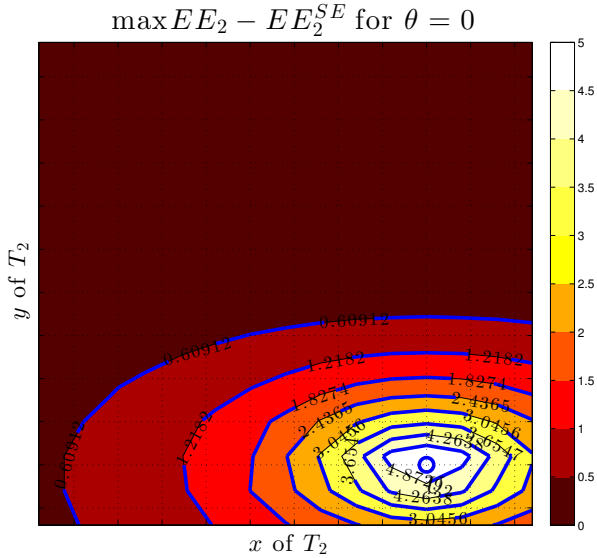


Figure 6.9: Difference between EE_2 for $\mathcal{P}_{\mathcal{R}_{\text{jam}}}(EE_2)$ and $\mathcal{U}_2^{\text{SE}} \triangleq EE_2^{\text{SE}}$ in the Stackelberg equilibrium.

the wiretap rate. As a consequence, we also have $\mathcal{U}_1^{\text{SE}}(\theta = 0.9) = R_1^{\text{WT}}$ since T_1 will not buy any jamming power when it is not for free if it already did not buy any jamming power when the cost was $\theta = 0$, i.e., for "free". Therefore in the upper part of the rectangle $\mathcal{R}_{EE}$ we have:

$$\mathcal{U}_1^{\text{SE}}(\theta = 0.9) - \mathcal{U}_1^{\text{SE}}(\theta = 0) = R_1^{\text{WT}} - R_1^{\text{WT}} = 0. \tag{6.18}$$

In the lower part of the plot we observe that the difference is always negative which was the predicted behavior. The magnitude of the difference grows as T_2 goes further away from U_2. A possible explanation of this result is that when T_2 is further away from U_2, the "value" of the jamming power decreases as the cooperative jamming is less efficient. Therefore, since T_1 is paying for the jamming power for a fixed cost θ regardless of the efficiency of jamming, its utility in the Stackelberg equilibrium decreases as the influence of ρ on R_1 decreases since $\mathcal{U}_1(\rho, P_2) = R_1 - \theta\rho P_2$. In addition to this explanation, we should also note that since less jamming power is needed when T_2 is close to U_2, (see, e.g., Figure 6.7,) then the value of the penalty $-\theta\rho P_2$ decreases in the area around U_2 and thus the difference between $\mathcal{U}_1^{\text{SE}}(\theta = 0.9)$ and $\mathcal{U}_1^{\text{SE}}(\theta = 0)$ is reduced.

Finally we depict in Figure 6.11 the influence of the penalty applied on $\mathcal{U}_1$ over the energy efficiency performance of the secondary user. As remarked from

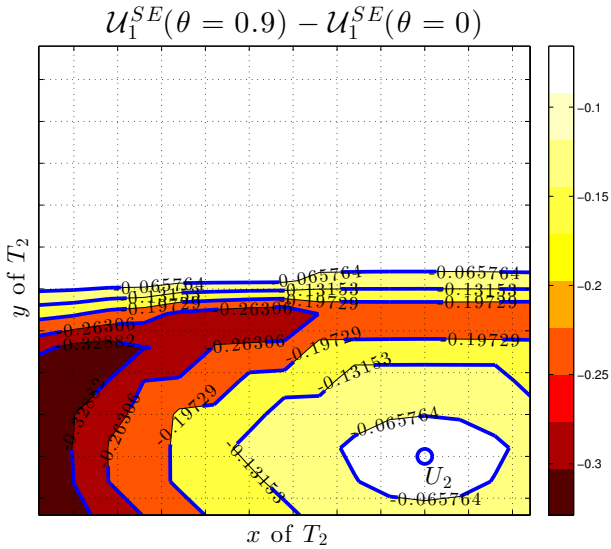


Figure 6.10: Difference between $\mathcal{U}_1^{\mathrm{SE}}(\theta = 0.9)$ and $\mathcal{U}_1^{\mathrm{SE}}(\theta = 0)$.

combining the observations from Figure 6.4 and Figure 6.9, $EE_2 = 0$ everywhere in the Stackelberg equilibrium when $\theta = 0$. However when we have $\theta = 0.9$ we observe that the secondary user's performance increases as there now exists an area around U_2 for which $EE_2 > 0$ with increasing values as T_2 gets closer to U_2. By comparing the numerical values with those in Figure 6.4, we observe that EE_2^{SE} is roughly half of EE_2 for $\mathcal{P}_{\mathcal{R}_{\mathrm{jam}}}(EE_2)$, while EE_2 increases from around 0 when $\theta = 0$ to 2.5 for its maximum value.

6.5.4 Comparison with the Overlay Scenario

In order to investigate the impact of message knowledge at T_2 in terms of energy efficiency, we consider here the rate region $\mathcal{R}_{rel}$ defined by (6.4) and (6.5).

1. Maximization of Secondary Energy Efficiency $\mathcal{P}_{\mathcal{R}_{rel}}(EE_2)$

$$\max_{\gamma,\rho,P_2} EE_2$$
$$\text{s.t. } R_1 \geq R_1^{\mathrm{WT}} \quad \text{and} \quad P_2 \leq P_2^{\max}.$$

Interestingly we obtained in our numerical simulations that

$$\max_{\gamma,\rho,P_2} EE_2(\mathcal{P}_{\mathcal{R}_{rel}}(EE_2)) = \max_{\rho,P_2} EE_2(\mathcal{P}_{\mathcal{R}_{\mathrm{jam}}}(EE_2)), \tag{6.20}$$

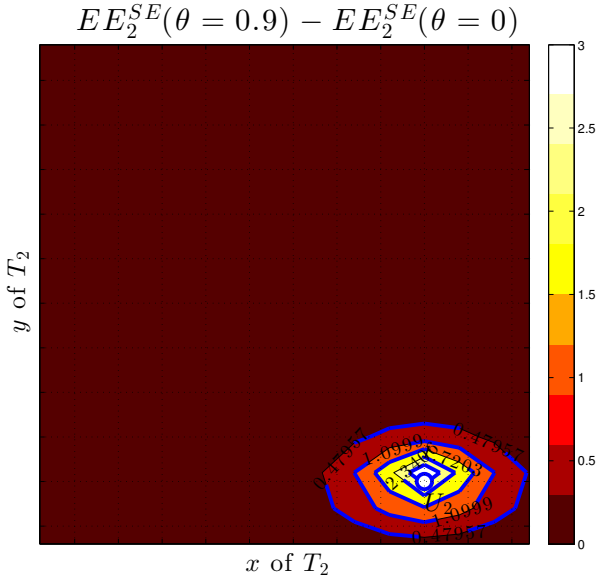


Figure 6.11: Difference between $EE_2^{\mathrm{SE}}(\theta = 0.9)$ and $EE_2^{\mathrm{SE}}(\theta = 0)$.

which means that the energy efficiency performance of the secondary network is not improved by having knowledge of the message w_1 at T_2. Furthermore we observed, as seen, e.g., in Chapter 3, that

$$\max_{\gamma,\rho,P_2} \; R_2(\mathcal{P}_{\mathcal{R}_{rel}}(R_2)) \geq \max_{\rho,P_2} \; R_2(\mathcal{P}_{\mathcal{R}_{\mathrm{jam}}}(R_2)), \tag{6.21}$$

which means that while having w_1 at T_2 benefits the secondary network in terms of achievable rate, this rate improvement is obtained at the cost of more transmission power being spent as the optimal energy efficiency EE_2 stays unchanged.

6.6 Conclusions

In this chapter we investigated our cognitive radio scenario with secrecy constraints from the perspective of energy efficiency, which is a fundamental criterion for the design of power efficient wireless networks. We investigate and solved the maximization of the secondary energy efficiency EE_2 under the constraint that the secrecy rate of the primary user should stay unchanged. Furthermore we studied the optimization problem using a Stackelberg game model between both transmitters where the primary transmitter aims at maximizing its secrecy rate while the secondary transmitters utility is the energy efficiency. We illustrated our results by using our geometrical model, and highlighted with these numerical examples several aspects of our study, such as

- the energy efficiency performance of the system,
- the optimal parameters and the power savings induced by the energy efficiency maximization,
- the impact of the Stackelberg game on the primary and the secondary utilities defined as the secrecy rate and the energy efficiency, respectively,
- the impact of the cost of the jamming power on the Stackelberg equilibrium outcome.

In previous chapters, we showed that the primary users could benefit from the cooperation of secondary users in order to improve, or at least preserve, their secrecy performance while the secondary users achieved positive rates for their own messages. The results in this chapter show that if the secondary network aims at maximizing its energy efficiency instead of its achievable rate, i.e., the important criterion of power consumption is taken into account by T_2, then a cooperation between primary and secondary network is still advantageous to both networks. Indeed, assuming the secondary users are located close enough to each other, the secondary network achieves strictly positive energy efficiency while the primary secrecy rate is kept unchanged; and the secrecy performance is even increased if a Stackelberg competition is considered between both networks.

6.A Proof of Theorem 6.1

Proof. Since EE_2 is a decreasing function of ρ, we find first the jamming threshold which satisfies the wiretap constraint, i.e., $R_1 \geq R_1^{\mathrm{WT}}$. We have

$$\begin{aligned} R_1 \geq R_1^{\mathrm{WT}} &\Leftrightarrow \mathcal{C}\left(\frac{P_1}{1+c_{21}P_2}\right) - \mathcal{C}\left(\frac{c_{12}P_1}{1+c_{22}\rho P_2}\right) \geq \left(\mathcal{C}(P_1) - \mathcal{C}(c_{12}P_1)\right)^+ \\ &\Leftrightarrow \rho \geq \rho^\star \triangleq \frac{c_{21}(1+c_{12}P_1)}{c_{22}\left(c_{12}(1+P_1) - c_{21}P_2(1-c_{12})\right)} \in [0;1] \end{aligned}$$

Defining $a \triangleq \frac{(1+c_{12}P_1)}{c_{22}}$, $b \triangleq c_{12}(1+P_1)$, and $c \triangleq c_{21}(1-c_{12})$ with $a, b, c > 0$ we have

$$\rho^\star = \frac{c_{21}a}{b - cP_2} \tag{6.22}$$

$$R_2 = \mathcal{C}\left(\frac{(1-\rho)P_2}{a + P_2\rho}\right) = \mathcal{C}\left(\frac{-cP_2^2 + (b - c_{21}a)P_2}{ab - (ac - ac_{21})P_2}\right) \tag{6.23}$$

From (6.22), we have that $\rho^\star(P_2) \in [0; +\infty[\Rightarrow P_2 \leq P_2^{\max} = \frac{b}{c}$.

Furthermore, we notice that $\rho^\star(P_2)$ is a positive increasing function of $P_2 \in [0; P_2^{\max}]$. If $\rho^\star(0) = \frac{c_{21}a}{b} > 1$, then the maximization problem is infeasible. Therefore in the following, we assume that $\rho^\star(0) \in [0;1]$ i.e., $b - c_{21}a \geq 0$.

We now solve

$$\rho^*(P_2) = 1 \Leftrightarrow P_2 = \frac{b - c_{21}a}{c} \triangleq P_2^{thr}.$$

The previous steps of the proof are illustrated in Figure 6.12. We then analyze the rate expression in (6.23) for $P_2 \in [0; P_2^{thr}]$. By defining $t \triangleq b - c_{21}a > 0$ and $d \triangleq c_{21}c_{12} > 0$, we can analyze equivalently the function defined as

$$f(P_2) = \frac{-cP_2^2 + tP_2}{b + dP_2}.$$

We easily calculate that

$$\frac{\partial^2 f(P_2)}{\partial P_2^2} < 0, \tag{6.24}$$

$$\frac{\partial f(P_2 = 0)}{\partial P_2} > 0, \tag{6.25}$$

$$\frac{\partial f(P_2 = P_2^{thr})}{\partial P_2} < 0. \tag{6.26}$$

Therefore f has a unique maximum for $P_2 \in [0; P_2^{thr}]$, attained for (after derivations)

$$P_2^{opt} = \frac{\sqrt{bc(bc+td)} - bc}{cd}. \tag{6.27}$$

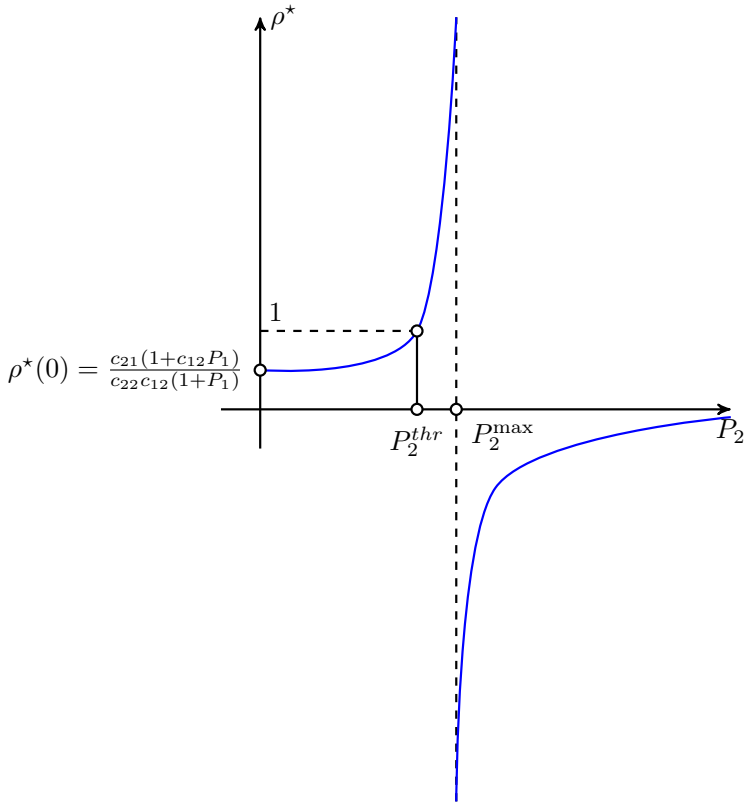


Figure 6.12: Illustration of P_2^{thr} and $\rho^\star$.

We now come back to our energy efficiency maximization:

$$\max_{\rho,P_2,R_1\geq R_1^{\mathrm{WT}}} EE_2 \Leftrightarrow \max_{\rho=\rho^\star(P_2),P_2} EE_2 \Leftrightarrow \max_{\rho=\rho^\star(P_2),P_2} \frac{R_2}{P_2+P_e}.$$

Similarly, we calculate:

$$\frac{\partial^2 EE_2}{\partial P_2^2} = (P_c+P_2)\frac{\partial^2 R_2}{\partial P_2^2} < 0, \tag{6.28}$$

$$\frac{\partial EE_2(P_2=0)}{\partial P_2} > 0, \tag{6.29}$$

$$\frac{\partial EE_2(P_2=P_2^{thr})}{\partial P_2} < 0. \tag{6.30}$$

Therefore, there is a unique $P_2^\star$ s.t. $\frac{\partial EE_2}{\partial P_2}(P_2 = P_2^\star) = 0$ and $\frac{\partial^2 EE_2}{\partial P_2^2} < 0$. Consequently, there exists a unique power allocation and power splitting maximizing the energy efficiency of the secondary transmitter, assuming Equation (6.8) is satisfied. This proves the theorem. ■

Chapter 7

A Key Agreement Perspective on Secrecy in Wireless Networks

In this chapter we investigate information theoretic secrecy using key agreement techniques in wireless networks. We present first the list of the chapter's goals.

Objectives of the Chapter.

- Motivate the study of the pairwise secret key agreement schemes and establish the connection with the focus of this thesis, i.e., secure communications in CRNs.
- Derive achievable secret key rate regions for two different key agreement schemes in Gaussian channels using several transmission strategies such as power control and cooperative jamming.
- Analyze the complex interaction between both transmitting users from a game theoretic perspective using non-cooperative games.
- Illustrate our results to characterize the performance of the key agreement schemes and to evaluate the impact of the game between both users.

Organization of the Chapter The chapter is organized as follows. In Section 7.1 we introduce the concept of secret key agreement and give motivations to complement the results obtained in this thesis by a study on key agreement schemes in wireless networks. In Section 7.2 we present the system model and the discrete memoryless results for the pairwise key agreement over the noisy channel. In Section 7.3 we consider Gaussian channels and we derive our main results, i.e., the

achievable rate regions for both schemes in the Gaussian setup and we illustrate the achievable key rate performance by using both schemes through numerical simulations. In Section 7.4 we study the interaction between the transmitting users from a game theoretic approach. We conclude the chapter in Section 7.5.

7.1 Introduction to Secret Key Agreement and Motivation for CRNs

In this section we introduce the concept of secret key agreement in communication networks and we explain the motivations behind the study in this chapter under the scope of the thesis.

A Case for Secret Key Agreement The physical layer approach of exploiting the inherent randomness of wireless channels to generate secret keys has gained considerable interest in recent years. One reason for this interest resides in the information theoretic security level attained by this technique compared to crypto schemes for which the security level depends on assumptions on the intractability of mathematical problems. Furthermore usual cryptography techniques rely on secure distribution of keys through noiseless links, which is not well adapted to decentralized networks. Moreover, generating secret keys at the physical layer provides two advantages over classical cryptographic methods:

- The keys are already shared during the key agreement process, which solves or at least simplifies the difficult challenge of key distribution and management in networks.
- The keys are generated dynamically as users join the network and as channels vary over time.

In Figure 7.1, adapted from [BB11], we illustrate how information theoretic secrecy techniques can be integrated into the security architecture of wireless devices and networks in combination to existing techniques at the above layers. In other terms, the approach of using the randomness of wireless channels can be deployed in combination with existing security encryptions. While transmitting secure messages using secure codes can be viewed as an independent security feature, key-agreement is a technique which can be combined with the classic cryptographic schemes as the secret keys generated using the channel transmissions can be passed to above layers as described in Figure 7.1.

For these reasons we consider in this chapter the information theoretic approach to secret key agreement/generation as a system aspect complement to the study in this thesis. We refer the interested reader to the fundamental works [AC93], [Mau93] and [CN00] for further details on information theoretic models for key sharing.

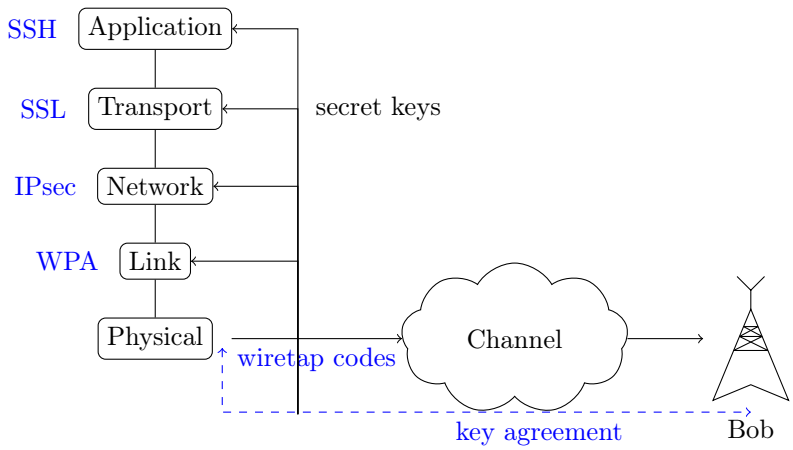


Figure 7.1: Information theoretic secrecy integration into wireless networks' architecture. Table adapted from [BB11].

Background on Secret Key Agreement in Wireless Networks In recent years, the problem of secret key sharing in wireless networks has been investigated from an information theoretic point of view in different scenarios. Ahlswede and Csiszár [AC93] and Maurer [Mau93] considered the problem of secret key sharing in a basic network of three users where two legitimate users intended to share a secret key in the presence of an eavesdropper. The two legitimate users exploited source or channel common randomness to share the key where a noiseless public channel with unlimited capacity is available for communications between the two legitimate users through which all communications can be overheard by the eavesdropper. Thereafter secret key sharing has been investigated in different scenarios in [CN00], [YN05], [SSAG11], [SSSA12] and [SGS14]. Among these works, [SSSA12] and [SGS14] consider pairwise key sharing in a network, i.e., each pair of the users intends to agree on a key hidden from the remaining users. This provides a high level of security since it facilitates secure communication between each pair of the users. The pairwise key sharing in the physical layer is a promising technique that eliminates the need to symmetric key infrastructure and public key infrastructure which impose high burden to the network and are based on unproven mathematical assumptions. In [SSSA12], pairwise key sharing is considered in a network of 3 users who access to correlated sources while in [SGS14] pairwise key sharing is performed through a noisy channel.

Channel Model for Secret Key Agreement Secret key agreement in the channel model is depicted in Figure 7.2. In addition to the classic channel defined by the transition probabilities $p(y, z|x)$, there exists a public authenticated channel of

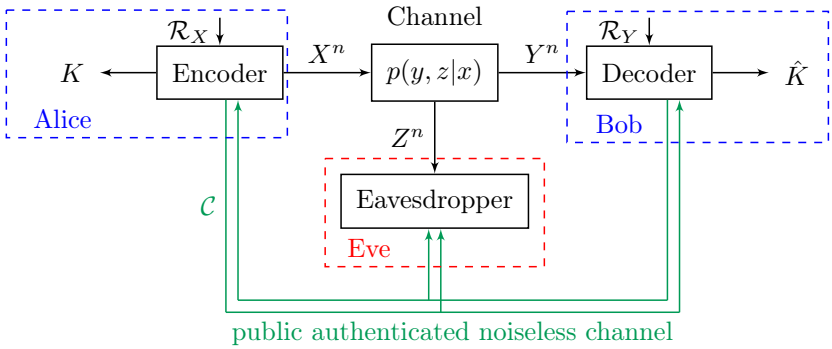


Figure 7.2: Channel model for secret key agreement.

unlimited capacity. Note that this channel does not provide any additional secrecy since Eve can intercept all messages transmitted over this channel. The goal for Alice and Bob is to use their transmission over the noisy channels to agree on a secret key K. This key could then be used by Alice and Bob e.g., on above layers for cryptographic applications as explained previously. We define the following secrecy measures for secret key agreement.

Definition 7.1.

The three concepts for security measures in secret key agreement problems are reliability, information leakage, and uniformity defined as:

Reliability:

$$P_e^{(n)} = P\{\hat{K} \neq K\},$$

Information Leakage:

$$L^{(n)} = I(K; Z^n, \mathcal{C}),$$

Uniformity:

$$U^{(n)} = \log(2^{nR}) - H(K),$$

respectively.

Based on those secrecy measures, we are able to define achievability for secret key rates.

Definition 7.2.

A secret key rate R is achievable if

$$P_e^{(n)} \xrightarrow[n\to\infty]{} 0 \qquad \text{(Reliability)}$$
$$\frac{1}{n}L^{(n)} \xrightarrow[n\to\infty]{} 0 \qquad \text{(Secrecy)}$$
$$\frac{1}{n}U^{(n)} \xrightarrow[n\to\infty]{} 0 \qquad \text{(Uniformity)}$$

Our Contribution In this chapter we consider two pairwise key sharing schemes in a 3-user network where the users communicate through a generalized multiple access channel. In the first scheme, namely pre-generated keys scheme, the channel inputs are stochastic functions of pre-generated keys. In the second scheme, namely generalized scheme, the channel inputs are functions of not only pre-generated keys but also the previous channel outputs. In particular we investigate the important practical case where the channels between the three users are AWGN channels. We derive achievable secret key rate regions for both encoding schemes by specifying the corresponding auxiliary random variables. These new results allow us to design adapted transmission strategies for Users 1 and 2 to maximize the achievable secret key rates and give us a good insight on the achievable rates and the transmission schemes. We propose in particular two different strategies of power splitting, one based on power control at Users 1 and 2, and the second including a cooperative jamming part in the input signals. The rate regions of different schemes and power splitting strategies are compared through numeric examples. Furthermore we consider the interaction between User 1 and User 2 in the pre-generated keys scheme where both users aim at maximizing their utilities, defined for each of them as the sum of their own achievable secret key rates. This competitive interaction between both users is naturally analyzed using a non-cooperative game perspective, as this tool which analyzes the competitive interaction between selfish players is particularly adapted to networks with secrecy constraints. We analyze the Nash equilibrium of the game and we furthermore illustrate our results using numerical simulations.

Application to Cognitive Radio Networks While the network model investigated in this chapter is different than the cognitive radio network analyzed throughout this thesis, we can actually justify that this 3-user network is indeed particularly relevant to our model of interest. The key agreement setup for the 3-node network investigated in this chapter can be viewed as a canonical example for larger networks, e.g., cognitive radio networks. For instance, User 1 and User 2 could represent a secondary transmitter/receiver pair (T_2, U_2) from the previous

chapters wanting to use the spectrum of a primary user T_1 which is represented by User 3. Thus, they need to agree on a secret key- which can be used as well at upper layers- with User 1 in order to be allowed to access the spectrum. Moreover, they agree on a secret key for their own transmission to be hidden from the primary network, as well as the potential other secondary users due to the broadcast nature of larger cognitive radio networks. This application highlights the advantages of key sharing using information theoretic techniques in dynamic networks such as the cognitive radio networks studied in this thesis.

7.2 Key Agreement Schemes and Main Results

In this section we introduce the system model of the pairwise key sharing in the general case of discrete memoryless case. In particular, two pairwise key agreement schemes, namely the pre-generated keys scheme and the generalized scheme are described along with the achievable secret key rate regions for both schemes. In both of the schemes, each pair of the three users intends to share a secret key while keeping it concealed from the remaining user. There is a generalized multiple access channel with probability distribution $P_{Y_1,Y_2,Y_3|X_1,X_2}$, where Users 1 and 2 govern the inputs X_1 and X_2 and then the outputs Y_1, Y_2 and Y_3 are received by Users 1, 2, and 3 respectively.

7.2.1 Pre-Generated Keys Scheme

In the pre-generated keys scheme, each of the Users 1 and 2 generates two secret keys to share with the other two users and sends the required information through the generalized multiple access channel as shown in Figure 7.3. In this scheme, secret key sharing is performed as follows:

Step 1: n uses of the generalized multiple access channel: Keys K_{12} and K_{13} are randomly generated by User 1 to be shared with Users 2 and 3, respectively. Then, the ith channel input $X_{1,i}$ is generated as stochastic function of keys K_{12} and K_{13} by User 1. Similarly, User 2 generates keys K_{21} and K_{23}, to be shared with User 1 and 3, respectively, and then $X_{2,i}$ as the ith channel input for $i = 1, 2, ..., n$. The outputs $Y_{1,i}, Y_{2,i}$ and $Y_{3,i}$ are then observed by Users 1, 2, and 3, respectively.

Step 2: Decoding of the corresponding keys: User 3 makes estimates $\hat{K}_{13}$ and $\hat{K}_{23}$ as a deterministic function of Y_3^n. Also, estimates $\hat{K}_{21}$ and $\hat{K}_{12}$ are made by Users 1 and 2, respectively, as stochastic functions of Y_1^n and Y_2^n.

After these two steps, the key pair $K_{1,2} = (K_{12}, K_{21})$ is shared between User l and User 2, K_{13} between User 1 and User 3, and K_{23} between User 2 and User 3. All the above keys take values in some finite sets. Now, we state the conditions that should be met in the described secret key sharing framework.

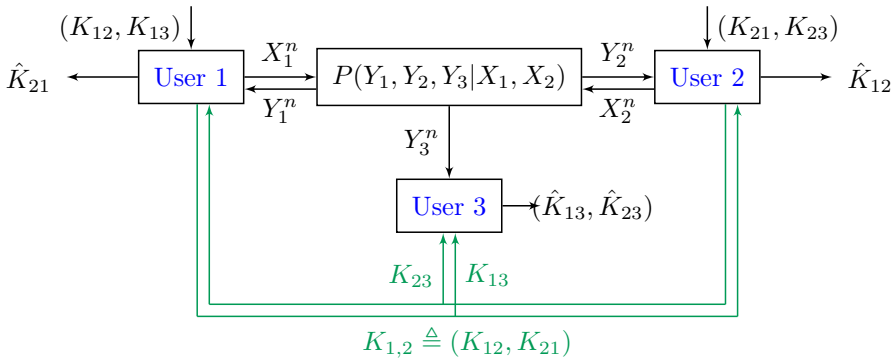


Figure 7.3: Pairwise key sharing over the generalized multiple access channel.

Definition 7.3.

In the pairwise secret key sharing of the proposed model, the rate triple (R_{12}, R_{13}, R_{23}) is an achievable key rate triple if for every $\varepsilon > 0$ and sufficiently large n, we have:

$$\begin{cases} \frac{1}{n}H(K_{1,2}) = \frac{1}{n}H(K_{12}, K_{21}) > R_{12} - \varepsilon, \\ \frac{1}{n}H(K_{13}) > R_{13} - \varepsilon, \\ \frac{1}{n}H(K_{23}) > R_{23} - \varepsilon \end{cases} \tag{7.1}$$

$$\begin{cases} P\{(K_{12}, K_{21}) \neq (\hat{K}_{12}, \hat{K}_{21})\} < \varepsilon, \\ P\{K_{13} \neq \hat{K}_{13}\} < \varepsilon, \\ P\{K_{23} \neq \hat{K}_{23}\} < \varepsilon \end{cases} \tag{7.2}$$

$$\begin{cases} \\ \frac{1}{n}I(K_{12}, K_{21}; Y_3^n) < \varepsilon, \\ \frac{1}{n}I(K_{13}; X_2^n, Y_2^n) < \varepsilon, \\ \frac{1}{n}I(K_{23}; X_1^n, Y_1^n) < \varepsilon \end{cases} \tag{7.3}$$

Equations (7.1) mean that the rates R_{12}, R_{13} and R_{23} are the rates of the secret keys between Users 1 and 2, Users 1 and 3, and users 2 and 3, respectively. Equations (7.2) mean that each user can correctly estimate the related keys. Equations (7.3) mean that each user effectively has no information about the remaining users' secret key.

Definition 7.4.

The region containing all the achievable secret key rate triples (R_{12}, R_{13}, R_{23}) is the secret key capacity region.

In the following, we give an achievable secret key rate region for the pre-generated keys scheme.

We first define the following rates:

$$r_{12} = [I(S_{12}; X_2, Y_2|S_{23}) - I(S_{12}; Y_3, S_{13}|S_{23})]^+, \tag{7.4}$$
$$r_{21} = [I(S_{21}; X_1, Y_1|S_{13}) - I(S_{21}; Y_3, S_{23}|S_{13})]^+, \tag{7.5}$$
$$I_{12} = I(S_{12}; S_{21}|Y_3, S_{13}, S_{23}), \tag{7.6}$$
$$r_{13} = [I(S_{13}; Y_3|S_{23}) - I(S_{13}; X_2, Y_2, S_{12}|S_{23})]^+, \tag{7.7}$$
$$r_{23} = [I(S_{23}; Y_3|S_{13}) - I(S_{23}; X_1, Y_1, S_{21}|S_{13})]^+, \tag{7.8}$$
$$I_3 = I(S_{13}; S_{23}|Y_3) \tag{7.9}$$

Theorem 7.1.

In the described setup, the closure of the convex hull of the set of all key rate triples (R_{12}, R_{13}, R_{23}) that satisfy the following region is achievable [SGS14]:

$$R_{12} \geq 0, R_{13} \geq 0, R_{23} \geq 0, \tag{7.10}$$
$$R_{12} \leq r_{12}+r_{21} - I_{12}, \tag{7.11}$$
$$R_{13} \leq r_{13}, \tag{7.12}$$
$$R_{23} \leq r_{23}, \tag{7.13}$$
$$R_{13} + R_{23} \leq r_{13}+r_{23} - I_3, \tag{7.14}$$

for random variables taking values in finite sets according to a distribution of the form: $p(s_{12},s_{13},s_{21},s_{23},x_1,x_2,y_1,y_2,y_3) = p(s_{12},s_{13})p(s_{21},s_{23})p(x_1|s_{12},s_{13})p(x_2|s_{21},s_{23})p(y_1,y_2,y_3|x_1,x_2)$.

Proof. The proof of Theorem 7.1 is given in [SGS14]. ■

7.2.2 Generalized Scheme

In the generalized key sharing scheme, the channel outputs as induced sources are involved in key generation. In contrast to the pre-generated keys scheme, the channel outputs are used at Users 1 and 2 as inputs to encoders and hence, the channel

inputs are functions of not only pre-generated keys but also the previous channel outputs. We describe the corresponding steps of key sharing in the following.

Step 1: n uses of the generalized multiple access channel: The i-th channel input $X_{1,i}$ is generated as stochastic function of the previous channel outputs Y_1^{i-1} by User 1. User 2 similarly generates $X_{2,i}$ for $i = 1, 2, ..., n$. Subsequently, the outputs $Y_{1,i}, Y_{2,i}$ and $Y_{3,i}$ are observed by Users 1, 2, and 3, respectively.

Step 2: Decoding of the corresponding keys: User 3 makes estimates $\hat{K}_{13}$ and $\hat{K}_{23}$ as a deterministic function of Y_3^n. Also, estimates $\hat{K}_{21}$ and $\hat{K}_{12}$ are made by Users 1 and 2, respectively, as stochastic functions of X_1^n, Y_1^n and X_2^n, Y_2^n.

After these steps, the key pair K_{12} is shared between User l and User 2, K_{13} between User 1 and User 3, and K_{23} between User 2 and User 3. All the above keys take values in some finite sets. In the pairwise secret key sharing of the generalized scheme, the rate triple (R_{12}, R_{13}, R_{23}) is an achievable key rate triple if Equations (7.1)-(7.3) in Definition 7.3 are satisfied and the secret key capacity region is defined the same as in Definition 7.4. In the following, we give an achievable secret key rate region for the generalized scheme.

We define the following rates:

$$r_{12,p} = [I(S_{12}; X_2, Y_2) - I(S_{12}; Y_3, S_{13}, S_{23}, T_{13}, T_{23})]^+, \tag{7.15}$$
$$r_{21,p} = [I(S_{21}; X_1, Y_1) - I(S_{21}; Y_3, S_{13}, S_{23}, T_{13}, T_{23})]^+, \tag{7.16}$$
$$I_{12,p} = I(S_{12}; S_{21}|Y_3, S_{13}, S_{23}, T_{13}, T_{23}), \tag{7.17}$$
$$r_{13,p} = [I(S_{13}; Y_3|S_{23}) - I(S_{13}; X_2, Y_2, S_{12}, T_{12}|S_{23})]^+, \tag{7.18}$$
$$r_{23,p} = [I(S_{23}; Y_3|S_{13}) - I(S_{23}; X_1, Y_1, S_{21}, T_{21}|S_{13})]^+, \tag{7.19}$$
$$I_{3,p} = I(S_{13}; S_{23}|Y_3) \tag{7.20}$$
$$r_{12,s} = [I(T_{12}; X_2, Y_2|S_{12}, S_{21}) - I(T_{12}; Y_3, S_{13}, S_{23}, T_{13}, T_{23}|S_{12}, S_{21})]^+, \tag{7.21}$$
$$r_{21,s} = [I(T_{21}; X_1, Y_1|S_{12}, S_{21}) - I(T_{21}; Y_3, S_{13}, S_{23}, T_{13}, T_{23}|S_{12}, S_{21})]^+, \tag{7.22}$$
$$I_{12,s} = I(T_{12}; T_{21}|Y_3, S_{13}, S_{23}, T_{13}, T_{23}, S_{12}, S_{21}), \tag{7.23}$$
$$r_{13,s} = [I(T_{13}; Y_3|S_{13}, S_{23}, T_{23}) - I(T_{13}; X_2, Y_2, S_{12}, T_{12}|S_{13}, S_{23}, T_{23})]^+, \tag{7.24}$$
$$r_{23,s} = [I(T_{23}; Y_3|S_{13}, T_{13}, S_{23}) - I(T_{23}; X_1, Y_1, S_{21}, T_{21}|S_{13}, T_{13}, S_{23})]^+, \tag{7.25}$$
$$I_{3,s} = I(T_{13}; T_{23}|Y_3, S_{13}, S_{23}) \tag{7.26}$$

Theorem 7.2.

In the generalized scheme of the pairwise secret key sharing, all rate triples in the closure of the convex hull of the set of all key rate triples (R_{12}, R_{13}, R_{23}) that satisfy the following conditions are achievable:

$$R_{12} \geq 0, R_{13} \geq 0, R_{23} \geq 0, \tag{7.27}$$

$$R_{12} \leq [r_{12,p} + r_{21,p} - I_{12,p}]^+ + [r_{12,s} + r_{21,s} - I_{12,s}]^+, \tag{7.28}$$

$$R_{13} \leq r_{13,p} + r_{13,s}, \tag{7.29}$$

$$R_{23} \leq r_{23,p} + r_{23,s}, \tag{7.30}$$

$$R_{13} + R_{23} \leq [r_{13,p}+r_{23,p} - I_{3,p}]^+ + [r_{13,s}+r_{23,s} - I_{3,s}]^+, \tag{7.31}$$

for random variables taking values in finite sets according to a distribution of the form: $p(s_{12},s_{13},s_{21},s_{23},t_{12},t_{13},t_{21},t_{23},x_1,x_2,y_1,y_2,y_3) = p(s_{12})p(s_{13})p(s_{21})p(s_{23})p(x_1|s_{12},s_{13})p(x_2|s_{21},s_{23})p(y_1,y_2,y_3|x_1,x_2)$ $p(t_{12}|x_1,y_1,s_{12})p(t_{13}|x_1,y_1,s_{13})p(t_{21}|x_2,y_2,s_{21})p(t_{23}|x_2,y_2,s_{23})$.
and subject to the constraints:

$$I(T_{12}; X_1, Y_1|X_2, Y_2, S_{12}, S_{21}, S_{23}) \leq I(S_{12}; X_2, Y_2), \tag{7.32}$$

$$I(T_{13}; X_1, Y_1|Y_3, S_{13}, S_{23}, T_{23}) \leq I(S_{13}; Y_3|S_{23}), \tag{7.33}$$

$$I(T_{21}; X_2, Y_2|X_1, Y_1, S_{12}, S_{21}, S_{13}) \leq I(S_{21}; X_1, Y_1), \tag{7.34}$$

$$I(T_{23}; X_2, Y_2|Y_3, S_{13}, S_{23}, T_{13}) \leq I(S_{23}; Y_3|S_{13}), \tag{7.35}$$

$$I(T_{13}, T_{23}; X_1, Y_1, X_2, Y_2|Y_3, S_{13}, S_{23}) \leq I(S_{13}, S_{23}; Y_3). \tag{7.36}$$

Proof. The proof of Theorem 7.2 is given in [SGS14]. ■

The achievability of the rate region in Theorem 7.2 is based on two-stage key generation; the first parts of the keys are randomly generated and the required information is sent through the channel as in the pre-generated keys scheme and the second parts are shared between the users considering the channel outputs as correlated sources. Each individual rate bound in Theorem 7.2 consists of two parts; the primary part and the secondary part, denoted by subscripts 'p' and 's', respectively. The primary parts are associated with the pre-generated keys randomly generated and sent by Users 1 and 2 through the channel and are justified as in Theorem 7.1. The secondary parts are generated by Users 1 and 2 after receiving the channel outputs. In fact, the received outputs at the users are exploited as induced sources to generate keys in addition to the pre-generated keys. This procedure is performed in multiple blocks. At each block, by n uses of the channel, Users 1 and 2 encode the pre-generated keys and send them over the channel and then, exploiting the channel outputs received at the end of the block, they generate the

second parts of the keys where the required information is sent over the channel in the next block. In particular, T_{12} and T_{13} are the auxiliary random variables associated with the secondary keys generated by User 1 to be shared with Users 2 and 3, respectively. Symmetrically, T_{21} and T_{23} are the auxiliary random variables related to the secondary keys generated by User 2 to be shared with Users 1 and 3, respectively.

7.3 Main Results for Gaussian Channels

In this section we describe our Gaussian setup and we then derive the achievable secret key rate regions for Gaussian channels. We consider AWGN channels in which the relationships between the channel inputs and outputs are given by

$$\begin{aligned} Y_1 &= X_1 + \sqrt{c_{21}}X_2 + N_1, \\ Y_2 &= \sqrt{c_{12}}X_1 + X_2 + N_2, \\ Y_3 &= \sqrt{c_{13}}X_1 + \sqrt{c_{23}}X_2 + N_3. \end{aligned}$$

The additive noise N_i at user $i = 1, 2, 3$ is zero-mean unit-variance white Gaussian. We denote by P_i the transmission power of User i such that $\mathbb{E}[|X_i|^2] \leq P_i$, $\forall i \in \{1, 2\}$. By standard arguments corresponding to the discrete channel arguments, the results in Theorem 7.1 and 7.2 can be extended to the Gaussian case. In the following, we describe how the auxiliary random variables in these theorems are substituted to obtain the obtain Gaussian rate regions. The key rate regions for the pre-generated keys scheme and the generalized scheme are derived in Section 7.3.1 and Section 7.3.2, respectively.

7.3.1 Pre-Generated Keys Scheme

We investigate first the pre-generated keys scheme. For this scheme, we consider two strategies, namely power control and cooperative jamming.

Power Control

User 1 and User 2 transmit

$$\begin{aligned} X_1 &= S_{12} + S_{13}, \\ X_2 &= S_{21} + S_{23}, \end{aligned}$$

where $S_{12} \sim \mathcal{N}(0, P_{12})$, $S_{13} \sim \mathcal{N}(0, P_{13})$, $S_{21} \sim \mathcal{N}(0, P_{21})$ and $S_{23} \sim \mathcal{N}(0, P_{23})$. Power allocation parameters α and β and power control parameters γ_1 and γ_2 are defined as

$$\begin{aligned} \alpha \triangleq \frac{P_{12}}{P_1},\ \beta \triangleq \frac{P_{21}}{P_2}, \\ \gamma_1 \triangleq \frac{P_1}{P},\ \gamma_2 \triangleq \frac{P_2}{P}, \end{aligned}$$

where P_1 and P_2 are the consumed powers at Users 1 and 2, respectively, and P is the fixed available power for each transmitter. Substituting the auxiliary random variables of Theorem 7.1 as above, we obtain the following result.

Theorem 7.3.

The achievable secret key rate region of the pre-generated keys scheme for the power control strategy is given as:

$$R_{12} \geq 0,\ \ R_{13} \geq 0,\ \ R_{23} \geq 0,$$

$$R_{12} \leq r_{12} + r_{21} - \left(\mathcal{C}(c_{13}\alpha\gamma_1 P) - \mathcal{C}\left(\frac{c_{13}\alpha\gamma_1 P}{1 + c_{23}\beta\gamma_2 P}\right)\right),$$

$$R_{13} \leq r_{13},\ \ R_{23} \leq r_{23},$$

$$R_{13} + R_{23} \leq r_{13} + r_{23} - \mathcal{C}\left(\frac{c_{13}(1-\alpha)\gamma_1 P}{1+c_{13}\alpha\gamma_1 P + c_{23}\beta\gamma_2 P}\right) + \mathcal{C}\left(\frac{c_{13}(1-\alpha)\gamma_1 P}{1+c_{13}\alpha\gamma_1 P + c_{23}\gamma_2 P}\right)$$

where

$$r_{12} \triangleq \left(\mathcal{C}\left(\frac{c_{12}\alpha\gamma_1 P}{1 + c_{12}(1-\alpha)\gamma_1 P}\right) - \mathcal{C}\left(\frac{c_{13}\alpha\gamma_1 P}{1 + c_{23}\beta\gamma_2 P}\right)\right)^+,$$

$$r_{21} \triangleq \left(\mathcal{C}\left(\frac{c_{12}\beta\gamma_2 P}{1 + c_{12}(1-\beta)\gamma_2 P}\right) - \mathcal{C}\left(\frac{c_{23}\beta\gamma_2 P}{1 + c_{13}\alpha\gamma_1 P}\right)\right)^+,$$

$$r_{13} \triangleq \left(\mathcal{C}\left(\frac{c_{13}(1-\alpha)\gamma_1 P}{1+c_{13}\alpha\gamma_1 P + c_{23}\beta\gamma_2 P}\right) - \mathcal{C}\left(c_{12}(1-\alpha)\gamma_1 P\right)\right)^+,$$

$$r_{23} \triangleq \left(\mathcal{C}\left(\frac{c_{23}(1-\beta)\gamma_2 P}{1+c_{23}\beta\gamma_2 P + c_{13}\alpha\gamma_1 P}\right) - \mathcal{C}\left(c_{12}(1-\beta)\gamma_2 P\right)\right)^+.$$

Proof. The proof of Theorem 7.3 is included in the proof of Theorem 7.4 in Appendix 7.A, as the power control scheme is included in the cooperative jamming scheme, by setting the power allocated to CJ as $\eta_1 = \eta_2 = 0$. ■

Cooperative Jamming

For this strategy, Users 1 and 2 implement cooperative jamming, i.e., they also transmit the Gaussian jamming signals J_1 and J_2 to increase the rate of the key between themselves by confusing the eavesdropping node, i.e., User 3. In fact, there is a two-way channel between Users 1 and 2 while User 3 acts as an eavesdropper. Cooperative jamming involves splitting of the transmission power of the transmitters into two parts; the first is allocated to encode the keys with the other two users and the other part is used as artificial noise to confuse User 3 in order to

achieve higher key rate with other transmitter. Then, $X_1 = S_{12} + S_{13} + J_1$ where $S_{12} \sim \mathcal{N}(0, (1-\eta_1)\alpha P_1)$, $S_{13} \sim \mathcal{N}(0, (1-\eta_1)(1-\alpha)P_1)$ and $J_1 \sim \mathcal{N}(0, \eta_1 P_1)$ and $X_2 = S_{21} + S_{23} + J_2$ where $S_{21} \sim \mathcal{N}(0, (1-\eta_2)\beta P_2)$, $S_{23} \sim \mathcal{N}(0, (1-\eta_2)(1-\beta)P_2)$ and $J_2 \sim \mathcal{N}(0, \eta_2 P_2)$.

Theorem 7.4.

The achievable secret key rate region of the pre-generated keys scheme for the cooperative jamming strategy is given as:

$$R_{12} \geq 0, \quad R_{13} \geq 0, \quad R_{23} \geq 0,$$

$$R_{12} \leq r_{12} + r_{21}$$

$$-\mathcal{C}\left(\frac{c_{13}(1-\eta_1)\alpha P_1}{1 + c_{13}\eta_1 P_1 + c_{23}\eta_2 P_2}\right) + \mathcal{C}\left(\frac{c_{13}(1-\eta_1)\alpha P_1}{1 + c_{13}\eta_1 P_1 + c_{23}(\eta_2 P_2 + (1-\eta_2)\beta P_2)}\right), \tag{7.37}$$

$$R_{13} \leq r_{13},$$

$$R_{23} \leq r_{23},$$

$$R_{13} + R_{23} \leq r_{13} + r_{23}$$

$$+\mathcal{C}\left(\frac{c_{13}(1-\alpha)(1-\eta_1)P_1}{1 + c_{13} g_{P_1}(\eta_1, \alpha) + c_{23} P_2}\right) - \mathcal{C}\left(\frac{c_{13}(1-\alpha)(1-\eta_1)P_1}{1 + c_{13} g_{P_1}(\eta_1, \alpha) + c_{23} g_{P_2}(\eta_2, \beta)}\right), \tag{7.38}$$

where

$$r_{12} \triangleq \mathcal{C}\left(\frac{c_{12}(1-\eta_1)\alpha P_1}{1 + c_{12} g_{P_1}(\eta_1, 1-\alpha)}\right) - \mathcal{C}\left(\frac{c_{13}(1-\eta_1)\alpha P_1}{1 + c_{13}\eta_1 P_1 + c_{23} g_{P_2}(\eta_2, \beta)}\right)^+, \tag{7.39}$$

$$r_{21} \triangleq \mathcal{C}\left(\frac{c_{12}(1-\eta_2)\beta P_2}{1 + c_{12} g_{P_2}(\eta_2, 1-\beta)}\right) - \mathcal{C}\left(\frac{c_{23}(1-\eta_2)\beta P_2}{1 + c_{23}\eta_2 P_2 + c_{13} g_{P_1}(\eta_1, \alpha)}\right)^+, \tag{7.40}$$

$$r_{13} \triangleq \mathcal{C}\left(\frac{c_{13}(1-\alpha)(1-\eta_1)P_1}{1 + c_{13} g_{P_1}(\eta_1, \alpha) + c_{23} g_{P_2}(\eta_2, \beta)}\right) - \mathcal{C}\left(\frac{c_{12}(1-\alpha)(1-\eta_1)P_1}{1 + c_{12}\eta_1 P_1}\right)^+, \tag{7.41}$$

$$r_{23} \triangleq \mathcal{C}\left(\frac{c_{23}(1-\beta)(1-\eta_2)P_2}{1 + c_{13} g_{P_1}(\eta_1, \alpha) + c_{23} g_{P_2}(\eta_2, \beta)}\right) - \mathcal{C}\left(\frac{c_{12}(1-\beta)(1-\eta_2)P_2}{1 + c_{12}\eta_2 P_2}\right)^+, \tag{7.42}$$

in which $g_{P_i}(\eta_i, x) = P_i(\eta_i + (1-\eta_i)x)$ for $i \in \{1, 2\}$.

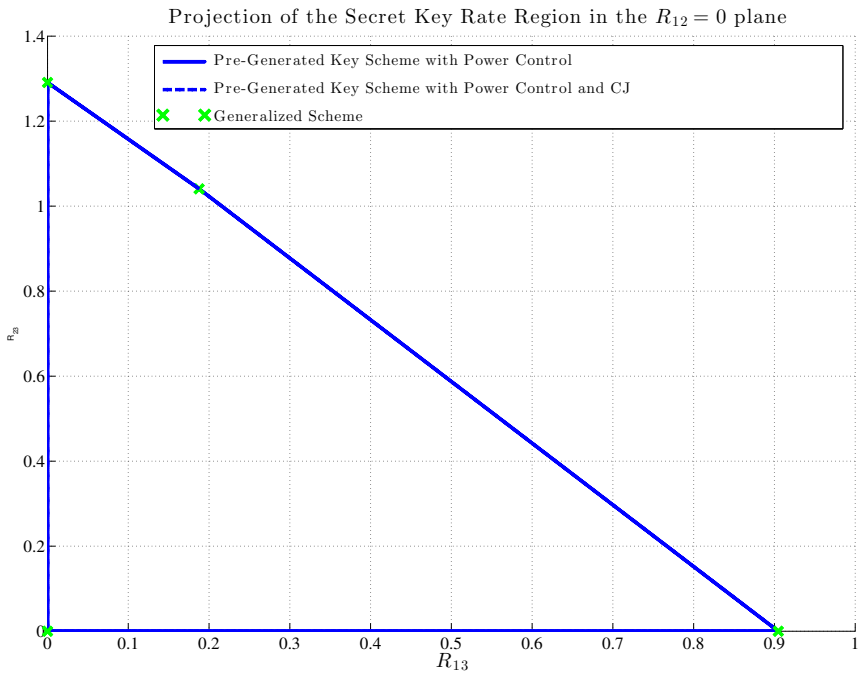


Figure 7.4: Comparison of the three schemes for User 3 in $(0.55, 0)$ in the $R_{12} = 0$ plane.

Proof. The proof of Theorem 7.4 is given in Appendix 7.A. ■

7.3.2 Generalized Scheme

In this section we consider the generalized scheme described in Section 7.2.2. For this scheme, Users 1 and 2 need to implement cooperative jamming since the part of the power dedicated to cooperative jamming is used as a source of secrecy generation. Using the main result in Theorem 7.2, we obtain the following achievable rate region.

Theorem 7.5.

The achievable secret key rate region of the generalized scheme for the cooperative jamming strategy is given as:

$$
\begin{aligned}
&R_{12} \geq 0, \quad R_{13} \geq 0, \quad R_{23} \geq 0, \\
&R_{12} \leq r_{12} + r_{21} + r_{s12} \\
&\quad -\mathcal{C}\left(\frac{c_{13}(1-\eta_1)\alpha P_1}{1 + c_{13}\eta_1 P_1 + c_{23}\eta_2 P_2}\right) + \mathcal{C}\left(\frac{c_{13}(1-\eta_1)\alpha P_1}{1 + c_{13}\eta_1 P_1 + c_{23}(g_{P_2}(\eta_2,\beta))}\right), \\
&R_{13} \leq r_{13}, \\
&R_{23} \leq r_{23}, \\
&R_{13} + R_{23} \leq r_{13} + r_{23} \\
&\quad +\mathcal{C}\left(\frac{c_{13}(1-\alpha)(1-\eta_1)P_1}{1 + c_{13}g_{P_1}(\eta_1,\alpha) + c_{23}P_2}\right) - \mathcal{C}\left(\frac{c_{13}(1-\alpha)(1-\eta_1)P_1}{1 + c_{13}g_{P_1}(\eta_1,\alpha) + c_{23}g_{P_2}(\eta_2,\beta)}\right),
\end{aligned}
$$

where

$$
\begin{aligned}
r_{s12} &= \mathcal{C}\left(\frac{c_{12}P'_{12}\eta_2 P_2}{(c_{12}(g_{P_2}(\eta_2, 1-\beta)) + 1)^2 - c_{12}P'_{12}\eta_2 P_2}\right) \\
&\quad + \mathcal{C}\left(\frac{c_{12}P'_{21}\eta_1 P_1}{(c_{12}(g_{P_1}(\eta_1, 1-\alpha)) + 1)^2 - c_{12}P'_{21}\eta_1 P_1}\right) \\
&\quad - \log\left(\frac{P'_{21}P'_{12}(1 + c_{23}\eta_2 P_2 + c_{13}\eta_1 P_1)}{\det(M)}\right), \qquad (7.43)
\end{aligned}
$$

$$
M \triangleq \begin{bmatrix}
P'_{12} & 0 & \frac{\sqrt{c_{12}c_{23}}(1-\eta_2)(1-\beta)P_2 P'_{12}}{c_{12}(g_{P_2}(\eta_2,1-\beta))+1} \\
0 & P'_{21} & \frac{\sqrt{c_{12}c_{13}}(1-\eta_1)(1-\alpha)P_1 P'_{21}}{c_{12}(g_{P_1}(\eta_1,1-\alpha))+1} \\
\frac{\sqrt{c_{12}c_{23}}(1-\eta_2)(1-\beta)P_2 P'_{12}}{c_{12}(g_{P_2}(\eta_2,1-\beta))+1} & \frac{\sqrt{c_{12}c_{13}}(1-\eta_1)(1-\alpha)P_1 P'_{21}}{c_{12}(g_{P_1}(\eta_1,1-\alpha))+1} & 1 + c_{23}\eta_2 P_2 + c_{13}\eta_1 P_1
\end{bmatrix}
$$

with the power constraints

$$
\begin{aligned}
P'_{12} &\leq \frac{(1-\eta_1)\alpha P_1 (c_{12}(g_{P_2}(\eta_2, 1-\beta)) + 1)^2}{(1-\eta_1)\alpha P_1 (c_{12}(g_{P_2}(\eta_2, 1-\beta)) + 1) + 1 + c_{12}(g_{P_1}(\eta_1, 1-\alpha))}, \\
P'_{21} &\leq \frac{(1-\eta_2)\beta P_2 (c_{12}(g_{P_1}(\eta_1, 1-\alpha)) + 1)^2}{(1-\eta_2)\beta P_2 (c_{12}(g_{P_1}(\eta_1, 1-\alpha)) + 1) + 1 + c_{12}(g_{P_2}(\eta_2, 1-\beta))},
\end{aligned}
$$

and r_{12}, r_{21}, r_{13}, and r_{23} are given by Equations (7.39), (7.40), (7.41) and (7.42), respectively.

The above rate region is obtained by substituting $X_1 = S_{12} + S_{13} + J_1$, $X_2 = S_{21} + S_{23} + J_2$ and $T_{13} = T_{23} = \emptyset$ in Theorem 7.2. Users 1 and 2, respectively, dedicate powers P'_{12} and P'_{21} from the received output powers to the auxiliary random variables T_{12} and T_{21}.

Proof. The proof of Theorem 7.5 is given in Appendix 7.B. ■

7.3.3 Numerical Illustration

In this section we illustrate how different encoding schemes and power allocation strategies in Sections 7.3.1 and 7.3.2 affect the key rate region. For this analysis, two different cases of users' physical location are considered. First we consider the case where User 3 is located between the two transmitters, i.e., User 1 and User 2. Then, we analyze the rate region in the opposite scenario where User 3 is further away from the two transmitters. We use the path-loss model $\sqrt{c_{ij}} = |h_{ij}| = 1/d_{ij}^{\alpha}$, where α represents the path-loss exponent and d_{ij} is the Euclidian distance between node i and node j. In our setup, Users 1 and 2 are located, respectively, in $(0, 0)$ and $(1, 0)$. The maximum transmitting powers are fixed as $P_1 = P_2 = 10$ dB.

User 3 between User 1 and User 2

In this case, we assume User 3 is located in $(0.55, 0)$. Since User 3 is located between User 1 and User 2, we intuitively expect R_{13} and R_{23} to be strictly positive while $R_{12} = 0$. For better visibility of the results, we choose to illustrate the achievable secret key rate region by projecting the 3D rate region into the planes $R_{12} = 0$ and $R_{23} = 0$ in Figure 7.4 and Figure 7.5, respectively, since depicting the 3D rate region in an informative way was not possible in a satisfying manner. We also omit the projection into the $R_{13} = 0$ as it provides the same information as the projection in the $R_{23} = 0$ plane. First we observe in Figure 7.4 that in the (R_{13}, R_{23}) plane, the three encoding schemes and power allocation strategies result in the same performance, i.e., neither cooperative jamming nor the generalized scheme improves the rate of the secret keys with User 3. This is expected since in the pre-generated keys scheme with cooperative jamming, Users 1 and 2 sacrifice a part of power to increase the rate of the key shared between themselves and not with User 3. For the generalized scheme, as described in Section 7.3.2, we need to use cooperative jamming as the power allocation strategy and we choose $T_{13} = T_{23} = \emptyset$. This explains why the three rate regions in Figure 7.4 are the same. Figure 7.5 depicts the projection of the key rate region in $R_{23} = 0$ plane. We observe that using the pre-generated keys scheme with power control results in $R_{12} = 0$ which is due to the fact that User 3 is between Users 1 and 2 and hence, they can not agree on a secret key hidden from User 3. On the other hand, using cooperative jamming, one or both of Users 1 and 2 dedicate a part of power to confuse User 3 and therefore, they can share a secret key even though User 3 is between them. In the generalized scheme, the part of power dedicated to cooperative jamming increase the rate of

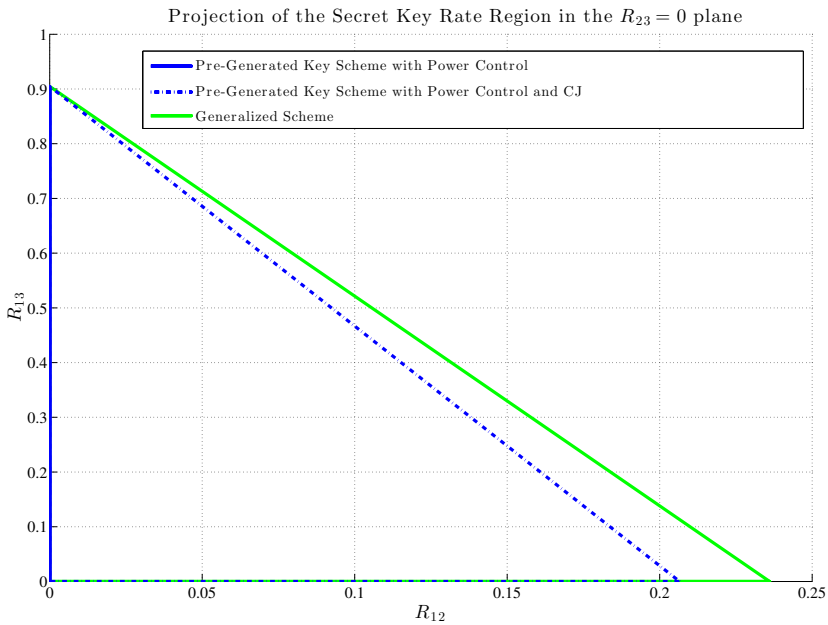


Figure 7.5: Comparison of the three schemes for User 3 in $(0.55, 0)$ in the $R_{23} = 0$ plane.

the secret key between Users 1 and 2 by creating correlation between the channel outputs at Users 1 and 2.

User 2 between User 1 and User 3 and User 3 in $(1.6, 0)$

In this case, we assume User 3 is located in $(1.6, 0)$. This case is fundamentally different than the previous one, since User 2 is now located between User 1 and User 3, and it is expected that no strictly positive R_{13} can be achieved. Furthermore, the cooperative jamming strategy in both of the pre-generated keys and the generalized schemes is aimed at increasing the rate of the key between Users 1 and 2 and hence, does not increase R_{13}. Thus, in all the three rate regions we have $R_{13} = 0$. In Figure 7.6 the 3D-plot is reduced into a 2D-plot in the $R_{13} = 0$ plane. It is observed that there is a significant performance improvement in terms of R_{12} by applying the generalized scheme instead of the pre-generated keys scheme. Furthermore, the figure shows the importance of allocating some power to the transmission of a jamming signal, since the pre-generated keys scheme with cooperative jamming outperforms the one with only the power control strategy available.

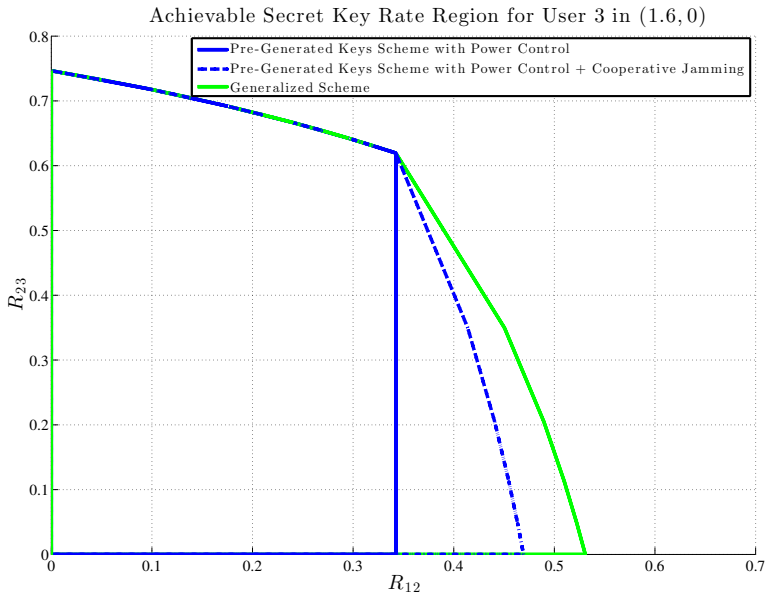


Figure 7.6: Comparison of the three schemes for User 3 in $(1.6, 0)$.

7.4 Game Theoretic Analysis with Numerical Illustrations

In this section we consider a non-cooperative game between both transmitting users, i.e., User 1 and User 2. Due to the similarity of the analysis, we only consider the pre-generated keys scheme, for which both the power control and cooperative jamming strategies are investigated. We should note that a similar game theoretical analysis could be performed for the generalized scheme.

In all scenarios, each of the Users 1 and 2 splits its available power such that their own total key rate is maximized. To analyze the interaction between the users, we formally define a non-cooperative game between User 1 and User 2 with respective utility functions [HNS+12]:

$$\mathcal{U}_1 \triangleq R_{12} + R_{13}, \tag{7.44}$$

$$\mathcal{U}_2 \triangleq R_{12} + R_{23}. \tag{7.45}$$

Definition 7.5.

The non-cooperative game in strategic form is then formally defined as the triplet $\mathcal{G} = (\mathcal{N}, (\mathcal{S}_i)_{i\in\mathcal{N}}, (\mathcal{U}_i)_{i\in\mathcal{N}})$ where:

- $\mathcal{N}$ is the set of players. Here, $\mathcal{N} \triangleq \{\text{User1}, \text{User2}\}$.
- $\mathcal{S}_i$ is the set of available strategies for player i.
- $\mathcal{U}_i : \mathcal{S} \to \mathbb{R}$ is the utility function of User i, with $\mathcal{S} \triangleq \mathcal{S}_1 \times \mathcal{S}_2$. Here $\mathcal{U}_1 \triangleq R_{12} + R_{13}$ and $\mathcal{U}_2 \triangleq R_{12} + R_{23}$.

7.4.1 Power Control Game

The set of available strategies for each player is such that $S_1 \triangleq (\alpha, \gamma_1)$ with $(\alpha, \gamma_1) \in [0,1]^2$, and $S_2 \triangleq (\beta, \gamma_2)$ with $(\beta, \gamma_2) \in [0,1]^2$. We then define the Nash equilibrium (NE) of this game, which is the most accepted solution for non-cooperative games.

Definition 7.6.

The Nash equilibrium of the game $\mathcal{G}_\mathcal{P}$ is given by the strategy profile $((\alpha^*, \gamma_1^*), (\beta^*, \gamma_2^*)) \in \mathcal{S}_\mathcal{P}$, such that we have:

$$\begin{aligned}\mathcal{U}_1((\alpha^*, \gamma_1^*), (\beta^*, \gamma_2^*)) \geq &\mathcal{U}_1((\alpha, \gamma_1), (\beta^*, \gamma_2^*)) \ \ \forall(\alpha, \gamma_1) \in S_1,\\ \mathcal{U}_2((\alpha^*, \gamma_1^*), (\beta^*, \gamma_2^*)) \geq &\mathcal{U}_2((\alpha^*, \gamma_1^*), (\beta, \gamma_2)) \ \ \forall(\beta, \gamma_2) \in S_2.\end{aligned}$$

The Nash equilibrium of the power control game $\mathcal{G}_\mathcal{P}$ is found as follows. For all $P_1 \in [0, P]$ and $P_2 \in [0, P]$, we denote $(\alpha^*_{P_1,P_2}, \beta^*_{P_1,P_2})$ as the NE of the fixed power game, i.e., the NE of the subgame where User 1 and User 2 transmit with respective fixed powers P_1 and P_2, that is:

$$\begin{aligned}\alpha^*_{P_1,P_2} &= \arg\max_{\alpha\in[0,1]} \mathcal{U}_1(\alpha, \beta^*_{P_1,P_2}),\\ \beta^*_{P_1,P_2} &= \arg\max_{\beta\in[0,1]} \mathcal{U}_2(\alpha^*_{P_1,P_2}, \beta).\end{aligned}$$

Then we define the best response power functions as

$$\begin{aligned}P_1^*(P_2) &= \arg\max_{P_1\in[0,P]} \mathcal{U}_1(\alpha^*_{P_1,P_2}, \beta^*_{P_1,P_2}),\\ P_2^*(P_1) &= \arg\max_{P_2\in[0,P]} \mathcal{U}_2(\alpha^*_{P_1,P_2}, \beta^*_{P_1,P_2}).\end{aligned}$$

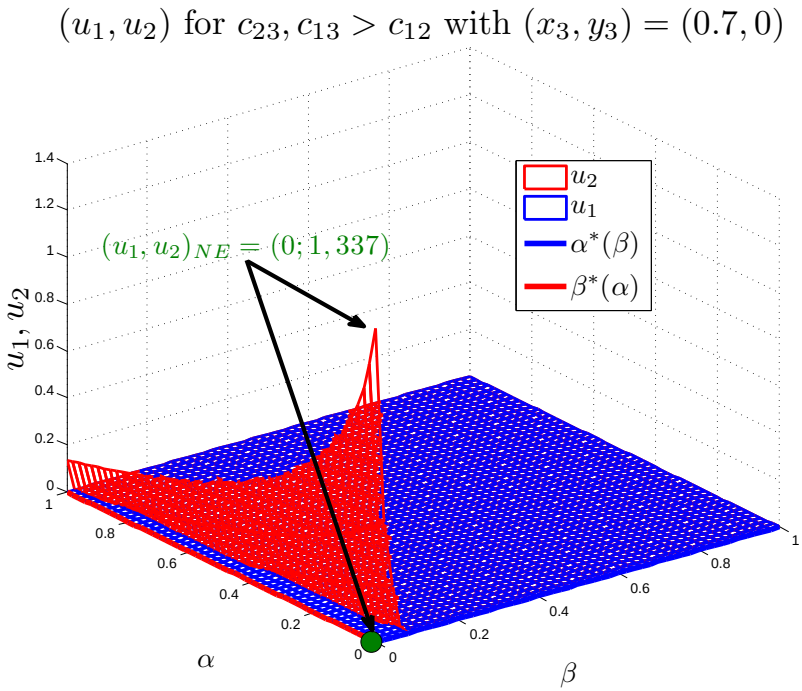


Figure 7.7: Fixed power subgame $(x_1, y_1) = (0, 0), (x_2, y_2) = (1, 0)$, $P_1 = P_2 = 10$ dB.

The NE of the game $\mathcal{G}_{\mathcal{P}}$ is then $((\alpha^*, \gamma_1^*), (\beta^*, \gamma_2^*))$ with $\gamma_1^* \triangleq \frac{P_1^*(P_2^*)}{P}$, $\gamma_2^* \triangleq \frac{P_2^*(P_1^*)}{P}$, $\alpha^* \triangleq \alpha^*_{P_1^*(P_2^*), P_2^*(P_1^*)}$ and $\beta^* \triangleq \beta^*_{P_1^*(P_2^*), P_2^*(P_1^*)}$.

In our setup, Users 1, 2 and 3 are located respectively in $(0, 0)$, $(1, 0)$ and $(0.7, 0)$. We illustrate how to find the Nash equilibrium in Figure 7.8. In the figure, we represent the NE utility outcomes $\mathcal{U}_1(\alpha^*_{P_1,P_2}, \beta^*_{P_1,P_2})$ and $\mathcal{U}_2(\alpha^*_{P_1,P_2}, \beta^*_{P_1,P_2})$ for all powers $(P_1, P_2) \in [0.5, 10]$. Note that in all figures in this chapter, the notation u_i is used for the utility of User i.

First, in order to clarify how to find the NE utility outcomes in the subgame where both users transmit with fixed powers P_1 and P_2, we illustrate the fixed-power subgame in Figure 7.7. We choose the transmitting powers as $P_1 = P_2 = 10$ dB, i.e., we consider the case without power control at Users 1 and 2. In this subgame denoted by $\mathcal{G}$, the NE is given by the strategy profile $(\alpha^*, \beta^*) \in \mathcal{S}$, such

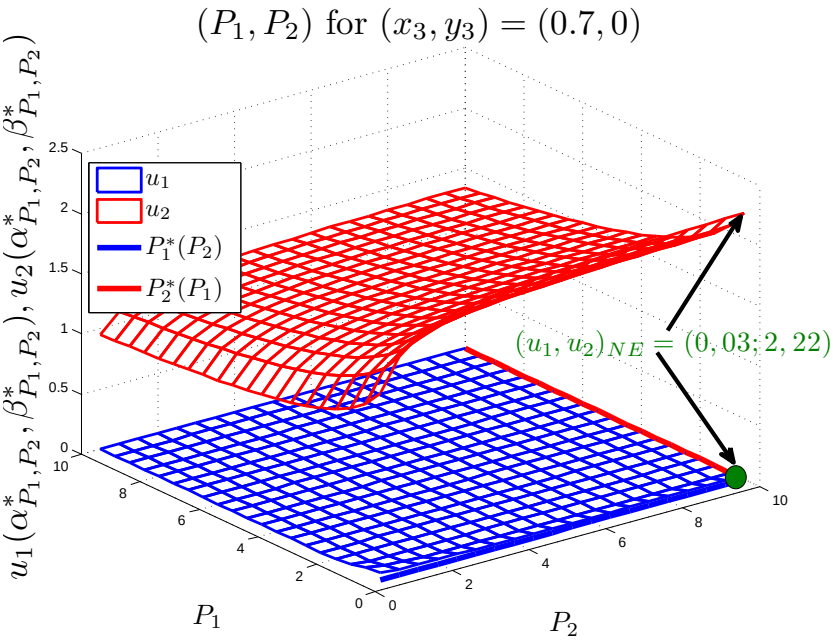


Figure 7.8: Power control game $(x_1, y_1) = (0, 0), (x_2, y_2) = (1, 0)$.

that we have:

$$\begin{aligned} \mathcal{U}_1(\alpha^*, \beta^*) \geq & \mathcal{U}_1(\alpha, \beta^*) \quad \forall \alpha \in [0, 1], \\ \mathcal{U}_2(\alpha^*, \beta^*) \geq & \mathcal{U}_2(\alpha^*, \beta) \quad \forall \beta \in [0, 1]. \end{aligned}$$

The best response function $\beta^*(\alpha)$, respectively $\beta^*(\alpha)$, is represented in red, respectively blue, in the plane $z = 0$. We find from the figure that $(\alpha^*, \beta^*) = (0, 0)$ which leads to NE utility outcomes $(0, 1.337)$.

The next step is to compute the NE utility outcomes for every possible transmitting powers P_1 and P_2, as shown in Figure 7.8. We impose a minimal transmit power of 0.5 (since the grid step for the power allocation is 0.5 in our numerical simulations) in our example since we want to consider a system model where both User 1 and User 2 are transmitting, i.e., they cannot be silent. The best response functions for the powers $P_1^*(P_2)$, respectively $P_1^*(P_2)$, is represented in blue, respectively red, in the plane $z = 0$. The best response functions cross in $(P_1^*(P_2^*), P_2^*(P_1^*))$, which is the NE of the game represented with a green circle.

In Figure 7.8 it is observed that using all the available power (i.e., $P_1 = P_2 = 10$) is a suboptimal strategy in this case, as $\mathcal{U}_1$ and $\mathcal{U}_2$ are decreasing functions of P_1.

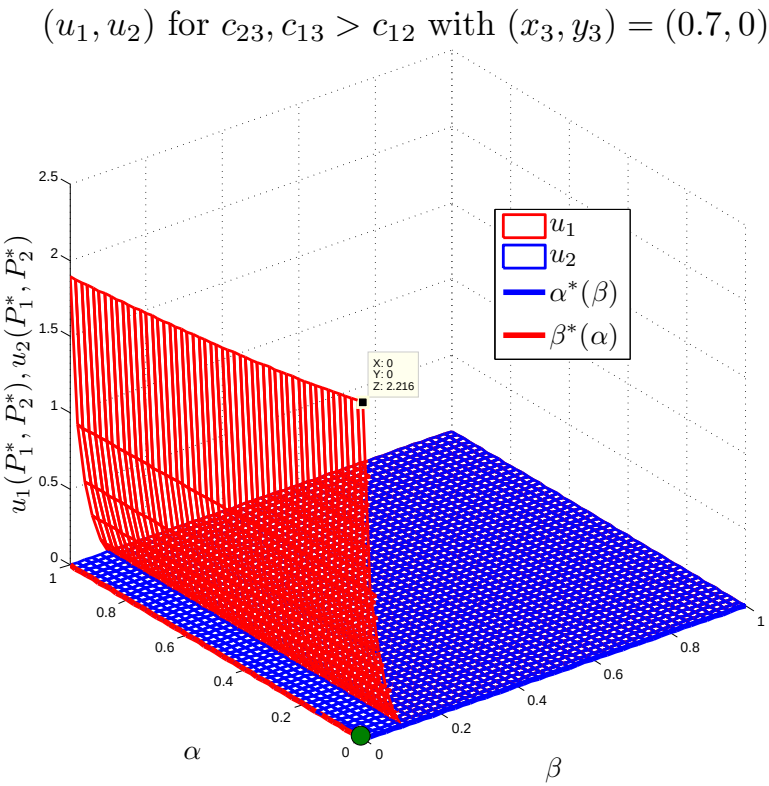


Figure 7.9: Power control game $(x_1, y_1) = (0, 0), (x_2, y_2) = (1, 0)$.

Moreover, we observe in Figure 7.8 that $(P_1, P_2) = (0.5, 10)$ yields to the highest utilities. Thus $(P_1^*, P_2^*) = (0.5, 10)$ is the NE of the game, i.e., $(\gamma_1^*, \gamma_2^*) = (0.05, 1)$ with NE outcomes $(\mathcal{U}_1, \mathcal{U}_2)_{\text{NE}} = (0.03, 2.22)$, which is strictly better than without power control as observed in Figure 7.7. This behavior is in accordance with the intuition since User 3 is in the middle of the other two users and closer to User 2.

Finally, for completeness, we represent in Figure 7.9 the corresponding utility outcomes region depending on the power allocations parameters α and β for $(P_1^*, P_2^*) = (0.5, 10)$. We observe that α^* and β^* are unchanged compared to the fixed power scenario, i.e., $\alpha^* = \beta^* = 0$.

7.4.2 Cooperative Jamming Game

Similarly, we could analyze the cooperative jamming (CJ) game where the strategies of the users are defined by $S_{1,\text{CJ}} \triangleq (\alpha, \eta_1)$ with $(\alpha, \eta_1) \in [0, 1]^2$, and $S_{2,\text{CJ}} \triangleq (\beta, \eta_2)$

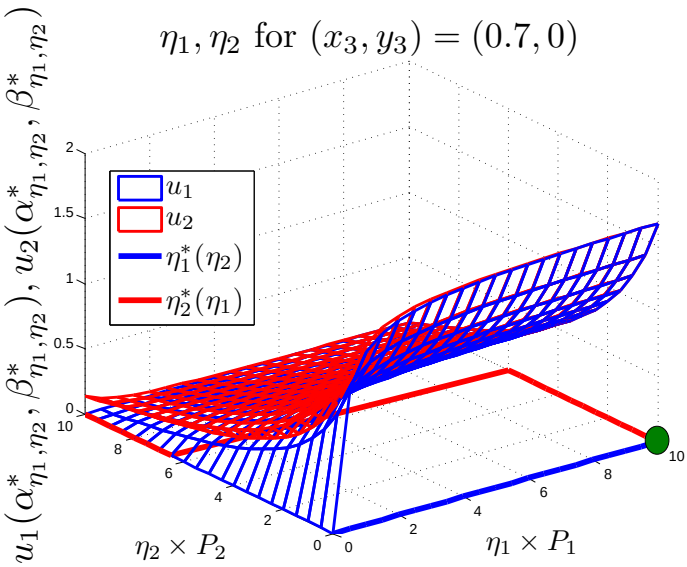


Figure 7.10: Cooperative jamming game $(x_1, y_1) = (0, 0), (x_2, y_2) = (1, 0)$.

with $(\beta, \eta_2) \in [0, 1]^2$. For simplicity, we restrict ourselves to an illustration of the Nash equilibrium of the cooperative jamming game in the same geographical setup of users as in the power control game in Figure 7.10 where $(\mathcal{U}_1, \mathcal{U}_2)_{\text{NE}} = (1.68, 1.68)$. In the Nash equilibrium, User 1 allocates all its available power to cooperative jamming, while User 2 allocates none of its power to cooperative jamming. We observe that cooperative jamming leads to higher utilities for User 1, as well as higher sum rates, in the Nash equilibrium in our setup compared to the power control solution, at the price of a higher power consumption. It should be noted that our setup illustrates one particular example of node geometry, and therefore the NE strategies would be changed depending if the nodes were located differently in the space.

7.5 Conclusions

In this chapter after introducing the secret key agreement concept in wireless networks and justifying its relevance for the network model considered in this thesis, we investigated a Gaussian generalized multiple access channel with three users where each pair of the users intends to share a secret key hidden from the remaining user. We summarize our contributions:

- We derived achievable secret key rate regions for different coding schemes and power allocation strategies where the rate regions were compared through numerical simulations.
- We modeled the competitive interaction between the two transmitting users as a non-cooperative game, in which both users intend to maximize their secret key sum rates and we analyzed the Nash equilibrium of this game.
- We illustrated the non-cooperative game through numerical examples and we also investigated the impact of a power control game on the Nash equilibrium secret key rates outcomes as well as a cooperative jamming game. In particular we showed how both strategies can potentially lead to higher utilities depending on the geometry of the nodes.

Our results show that strictly positive secret key rates are achievable for various topologies of the 3-node network investigated in this chapter. This network can be viewed as a canonical example for larger networks, e.g., the cognitive radio network studied in the thesis where User 1 and User 2 represent the secondary pair (T_2, U_2) and the primary transmitter T_1 is represented by User 3. T_2 and U_2 need to agree with T_1 on a secret key, which can additionally be used at the above layers, in order to be allowed to access the spectrum. Moreover, T_2 and U_2 agree on a secret key for their own transmission to be hidden from the primary network, as well as the other secondary pairs $(T_{2,k}, U_{2,k})$ if we consider the larger cognitive radio networks of Chapter 5. Therefore the results in this chapter highlight the possibility of successfully implementing a key agreement scheme to increase the secrecy of cognitive radio networks in addition to using the secrecy transmission schemes investigated in the previous chapters.

7.A Proof of Theorem 7.4

Proof. We prove the expressions for r_{12}, r_{13}, I_{12}, and I_3 in Theorem 7.4. The expressions of r_{21} and r_{23} follow from r_{12} and r_{13} by exchanging all subscripts 1 and 2 in the proof.

1. r_{12}: We have $r_{12} = [I(S_{12}; X_2, Y_2|S_{23}) - I(S_{12}; Y_3, S_{13}|S_{23})]^+$.

   For the first term:

$$\begin{aligned} I(S_{12}; X_2, Y_2|S_{23}) &= I(S_{12}; X_2|S_{23}) + I(S_{12}; Y_2|S_{23}, X_2) \\ &\overset{(a)}{=} I(S_{12}; Y_2|S_{23}, X_2) \\ &= h(Y_2|S_{23}, X_2) - h(Y_2|S_{23}, X_2, S_{12}). \end{aligned}$$

   in which (a) is deduced from the random variables' distributions.

   With $X_2 = S_{21} + S_{23} + J_2$, $X_1 = S_{12} + S_{13} + J_1$, $Y_2 = \sqrt{c_{12}}X_1 + X_2 + N_2$ and $Y_3 = \sqrt{c_{13}}X_1 + \sqrt{c_{23}}X_2 + N_3$, where $S_{12} \sim \mathcal{N}(0, (1-\eta_1)\alpha P_1)$, $S_{13} \sim \mathcal{N}(0, (1-\eta_1)(1-\alpha)P_1)$, $J_1 \sim \mathcal{N}(0, \eta_1 P_1)$ and $S_{21} \sim \mathcal{N}(0, (1-\eta_2)\beta P_2)$, $S_{23} \sim \mathcal{N}(0, (1-\eta_2)(1-\beta)P_2)$, $J_2 \sim \mathcal{N}(0, \eta_2 P_2)$, we have

$$\begin{aligned} I(S_{12}; X_2, Y_2|S_{23}) &= h(\sqrt{c_{12}}X_1 + N_2) - h(\sqrt{c_{12}}(S_{13} + J_1) + X_2 + N_2) \\ &= \mathcal{C}\left(\frac{c_{12}(1-\eta_1)\alpha P_1}{1 + c_{12} g_{P_1}(\eta_1, 1-\alpha)}\right). \end{aligned}$$

   where $g_{P_i}(\eta_i, x) \triangleq P_i(\eta_i + (1-\eta_i)x)$.

   For the second term:

$$\begin{aligned} I(S_{12}; Y_3, S_{13}|S_{23}) &= I(S_{12}; S_{13}|S_{23}) + I(S_{12}; Y_3|S_{23}, S_{13}) \\ &\overset{(b)}{=} I(S_{12}; Y_3|S_{23}, S_{13}) \\ &= h(Y_3|S_{23}, S_{13}) - h(Y_3|S_{23}, S_{13}, S_{12}). \\ &= \mathcal{C}\left(\frac{c_{13}(1-\eta_1)\alpha P_1}{1 + c_{13}\eta_1 P_1 + c_{23} g_{P_2}(\eta_2, \beta)}\right), \end{aligned}$$

   in which (b) is deduced from the random variables' distributions.

2. I_{12}: We have

$$\begin{aligned} I_{12} &= I(S_{12}; S_{21}|Y_3, S_{13}, S_{23}) \\ &= I(S_{12}; S_{21}, Y_3|S_{13}, S_{23}) - I(S_{12}; Y_3|S_{13}, S_{23}) \\ &= I(S_{12}; Y_3|S_{13}, S_{23}, S_{21}) - I(S_{12}; Y_3|S_{13}, S_{23}) \\ &= h(Y_3|S_{13}, S_{23}, S_{21}) - h(Y_3|S_{13}, S_{23}, S_{21}, S_{12}) \\ &\quad - (h(Y_3|S_{13}, S_{23}) - h(Y_3|S_{13}, S_{23}, S_{12})) \\ &= \mathcal{C}\left(\frac{c_{13}(1-\eta_1)\alpha P_1}{1 + c_{13}\eta_1 P_1 + c_{23}\eta_2 P_2}\right) - \mathcal{C}\left(\frac{c_{13}(1-\eta_1)\alpha P_1}{1 + c_{13}\eta_1 P_1 + c_{23}(\eta_2 P_2 + (1-\eta_2)\beta P_2)}\right) \end{aligned}$$

3. r_{13}: We have

$$\begin{aligned} r_{13} &= [I(S_{13};Y_3|S_{23}) - I(S_{13};X_2,Y_2,S_{12}|S_{23})] \\ &= [(h(Y_3|S_{23}) - h(Y_3|S_{23},S_{13})) \\ &- (h(Y_2|S_{23},X_2,S_{12}) - h(Y_2|S_{23},X_2,S_{12},S_{13}))] \\ &= [h(\sqrt{c_{13}}X_1 + \sqrt{c_{23}}(S_{21}+J_2) + N_3) \\ &- h(\sqrt{c_{13}}(S_{12}+J_1) + \sqrt{c_{23}}(S_{21}+J_2) + N_3)] \\ &- (h(\sqrt{c_{12}}(S_{13}+J_1) + N_2) - h(\sqrt{c_{12}}J_1 + N_2)] \\ &= \mathcal{C}\left(\frac{c_{13}(1-\alpha)(1-\eta_1)P_1}{1+c_{13}g_{P_1}(\eta_1,\alpha)+c_{23}g_{P_2}(\eta_2,\beta)}\right) - \mathcal{C}\left(\frac{c_{12}(1-\alpha)(1-\eta_1)P_1}{1+c_{12}\eta_1 P_1}\right). \end{aligned}$$

4. I_3: We have

$$\begin{aligned} I_3 &= I(S_{13};S_{23}|Y_3) = I(S_{13};S_{23},Y_3) - I(S_{13};Y_3) = I(S_{13};Y_3|S_{23}) - I(S_{13};Y_3) \\ &= h(Y_3|S_{23}) - h(Y_3|S_{23},S_{13}) - (h(Y_3) - h(Y_3|S_{13})) \\ &= \mathcal{C}\left(\frac{c_{13}(1-\alpha)(1-\eta_1)P_1}{1+c_{13}g_{P_1}(\eta_1,\alpha)+c_{23}g_{P_2}(\eta_2,\beta)}\right) - \mathcal{C}\left(\frac{c_{13}(1-\alpha)(1-\eta_1)P_1}{1+c_{13}g_{P_1}(\eta_1,\alpha)+c_{23}P_2}\right). \end{aligned}$$

This concludes the proof of Theorem 7.4. Note that the achievable region of Theorem 7.3 is also proven by canceling the cooperative jamming, i.e., setting $\eta_1 = \eta_2 = 0$. ■

7.B Proof of Theorem 7.5

Proof. First we notice that since $T_{13} = T_{23} = \emptyset$, we have immediately $r_{13,s} = r_{23,s} = I_{3,s} = 0$. Furthermore we observe that $r_{13,p} = r_{13}$, $r_{23,p} = r_{23}$ and $I_{3,p} = I_3$ from the pre-generated keys scheme. Therefore the rate expressions for R_{13} and R_{23} are the same as those in Theorem 7.4.

We need to prove the first inequality for R_{12}. We equivalently show that $r_{12,p} + r_{21,p} - I_{12,p} = r_{12} + r_{21} - I_{12}$, where r_{12}, r_{21} and I_{12} are defined in Theorem 7.1. Since $T_{13} = T_{23} = \emptyset$ we have clearly $I_{12,p} = I_{12}$.

Furthermore, we have:

$$\begin{aligned} r_{12,p} &= [I(S_{12};X_2,Y_2) - I(S_{12};Y_3,S_{13},S_{23})]^+ \\ &= [I(S_{12};X_2,Y_2|S_{23}) - I(S_{12};Y_3,S_{13}|S_{23})]^+ \\ &= r_{12}, \end{aligned}$$

where $I(S_{12};X_2,Y_2) = I(S_{12};X_2,Y_2|S_{23})$ due to S_{12} and S_{23} being mutually independent given Y_2 *and* X_2 and $I(S_{12};Y_3,S_{13},S_{23}) = I(S_{12};Y_3,S_{13}|S_{23})$ due to chain rule and S_{12} and S_{23} being mutually independent. By symmetry, the result is similar for $r_{21,p}$ and therefore $r_{12,p} + r_{21,p} - I_{12,p} = r_{12} + r_{21} - I_{12}$. We then replace the random variables in $X_1 = S_{12} + S_{13} + J_3$ and $X_2 = S_{21} + S_{23} + J_2$

with $S_{12} \sim \mathcal{N}(0,(1-\eta_1)\alpha P_1)$, $S_{13} \sim \mathcal{N}(0,(1-\eta_1)(1-\alpha)P_1)$, $J_1 \sim \mathcal{N}(0,\eta_1 P_1)$, $S_{21} \sim \mathcal{N}(0,(1-\eta_2)\beta P_2)$, $S_{23} \sim \mathcal{N}(0,(1-\eta_2)(1-\beta)P_2)$, and $J_2 \sim \mathcal{N}(0,\eta_2 P_2)$. According to the generalized scheme, User 1 and User 2 compute

$$Y_1^{'} = Y_1 - X_1 - \sqrt{c_{21}}S_{21} = \sqrt{c_{21}}(S_{23}+J_2) + N_1 \triangleq T_{12} + D_{12},$$
$$Y_2^{'} = Y_2 - X_2 - \sqrt{c_{12}}S_{12} = \sqrt{c_{12}}(S_{13}+J_1) + N_2 \triangleq T_{21} + D_{21},$$

respectively. The powers P'_{12} and P'_{21} are then allocated for T_{12} and T_{21} respectively while $T_{13} = T_{23} = \emptyset$. We obtain after manipulations:

$$I_{12,s} = I(T_{12};T_{21}|Y_3,S_{13},S_{23},S_{12},S_{21}) \tag{7.46}$$
$$= \log\left(\frac{P'_{21}P'_{12}(1+c_{23}\eta_2 P_2 + c_{13}\eta_1 P_1)}{\det(M)}\right), \tag{7.47}$$

and

$$r_{12,s} = I(T_{12};X_2,Y_2|S_{12},S_{21}) - I(T_{12};Y_3,S_{13},S_{23}|S_{12},S_{21}) \tag{7.48}$$
$$= \mathcal{C}\left(\frac{c_{12}P'_{12}\eta_2 P_2}{(c_{12}((1-\eta_2)(1-\beta)P_2+\eta_2 P_2)+1)^2 - c_{12}P'_{12}\eta_2 P_2}\right), \tag{7.49}$$

which proves that $r_{12,s} + r_{21,s} - I_{12,s} = r_{s12}$ since $r_{21,s}$ is obtained in the same way as $r_{12,s}$ by symmetry. To conclude the proof of Theorem 7.5, we need to express the constraint (7.36) in Theorem 7.2. The second, fourth and fifth inequalities disappear since $T_{13} = T_{23} = \emptyset$. The first inequality becomes the first power constraint in Theorem 7.5 by expressing the mutual information with the Gaussian random variable and tediously manipulating the resulting inequality. Finally the fifth inequality in (7.36) is equivalent to the second power constraint by symmetry of the subscripts 1 and 2. This concludes the proof of Theorem 7.5. ■

Chapter 8

Conclusions

In this chapter we summarize the main contributions of the thesis in Section 8.1. We then suggest future promising research directions in Section 8.2.

8.1 Summary of Contributions and Conclusions

In this thesis we studied cooperation between users in cognitive radio networks to enhance the secrecy of communications in the scenario where the secondary receiver is treated as potential eavesdropper to the primary transmission. Cooperation between the primary and secondary transmitters was shown to improve the primary secrecy performance, while the secondary transmitter benefited from using the spectrum for its own data transmission. We investigated this scenario from multiple perspectives throughout this thesis. In Figure 8.1 we provide an overview of the key questions investigated in the thesis and the different methods utilized to answer those questions using a chronological chart. In addition to this illustrative representation of our contribution, we summarize each chapter's contributions in the following.

Chapter 2: We gave a thorough review of the fundamentals needed for the understanding of this thesis and we investigated a case study of cooperation for secrecy in wireless networks which allowed us to motivate the network model considered in this thesis.

Chapter 3: We introduced and analyzed the cognitive radio channel with secrecy constraints investigated in this thesis. In particular we derived the achievable rate regions for the AWGN cognitive radio channel model with and without primary message knowledge. We formulated and solved three relevant power allocation problems: the maximization of the primary and the secondary rates, and the minimization of the transmitting powers. We illustrated our results through numerical examples based on a geometrical setup, highlighting the impact of the node geometry on the achievable rates and on the optimal

strategy of the secondary transmitter and compared those results to the game theoretic interaction between transmitters.

Chapter 4: We introduced the clean relaying scheme for secrecy in cognitive radio channels, generalizing the results of Chapter 3 in several ways. We derived the achievable rate region for the multi-phase scheme investigated in this chapter as well as for other signalling schemes. We then compared the secrecy performance of the schemes numerically.

Chapter 5: We extended the cognitive channel model from previous chapters to larger cognitive radio networks with multiple secondary transmitter-receiver pairs. We investigated spectrum sharing mechanisms using several game theoretic models, such as, single-leader multiple-follower Stackelberg games, non-cooperative power control games, and auction games. We illustrated the equilibrium outcomes of the analyzed games and the impact of the competitive interaction between the secondary transmitters through numerical simulations.

Chapter 6: We investigated cognitive radio channels with secrecy from the important aspect of energy efficiency. In particular we analyzed the optimal power allocation and power splitting at the secondary transmitter in terms of energy efficiency. We compared these results to the outcomes of the Stackelberg game between the two transmitters aiming at maximizing their utilities.

Chapter 7: We introduced system aspects of secrecy in wireless networks by discussing secret key agreement in wireless networks. In particular we derived achievable secret key rate regions for two different key agreement schemes in Gaussian channels using several transmission strategies such as power control and cooperative jamming. We then analyzed the interactions between users from a non-cooperative Nash game perspective.

8.2 Future Research Directions

In this section we first present the main topics of interest for future research. These topics can be viewed as natural extensions of the work presented in the thesis. We then discuss several other potential topics of investigation.

MIMO Techniques for Secrecy in Wireless Networks In this thesis we assumed that the users in the networks were equipped with single antenna nodes, i.e., that they could not benefit from the advantages of multi-antenna transmission. MIMO communications, such as multi-user MIMO and massive MIMO, have gained considerable interest in recent years, both within the research community and within industry. As a consequence of security issues becoming increasingly important in wireless communications, many works have been focusing in the last

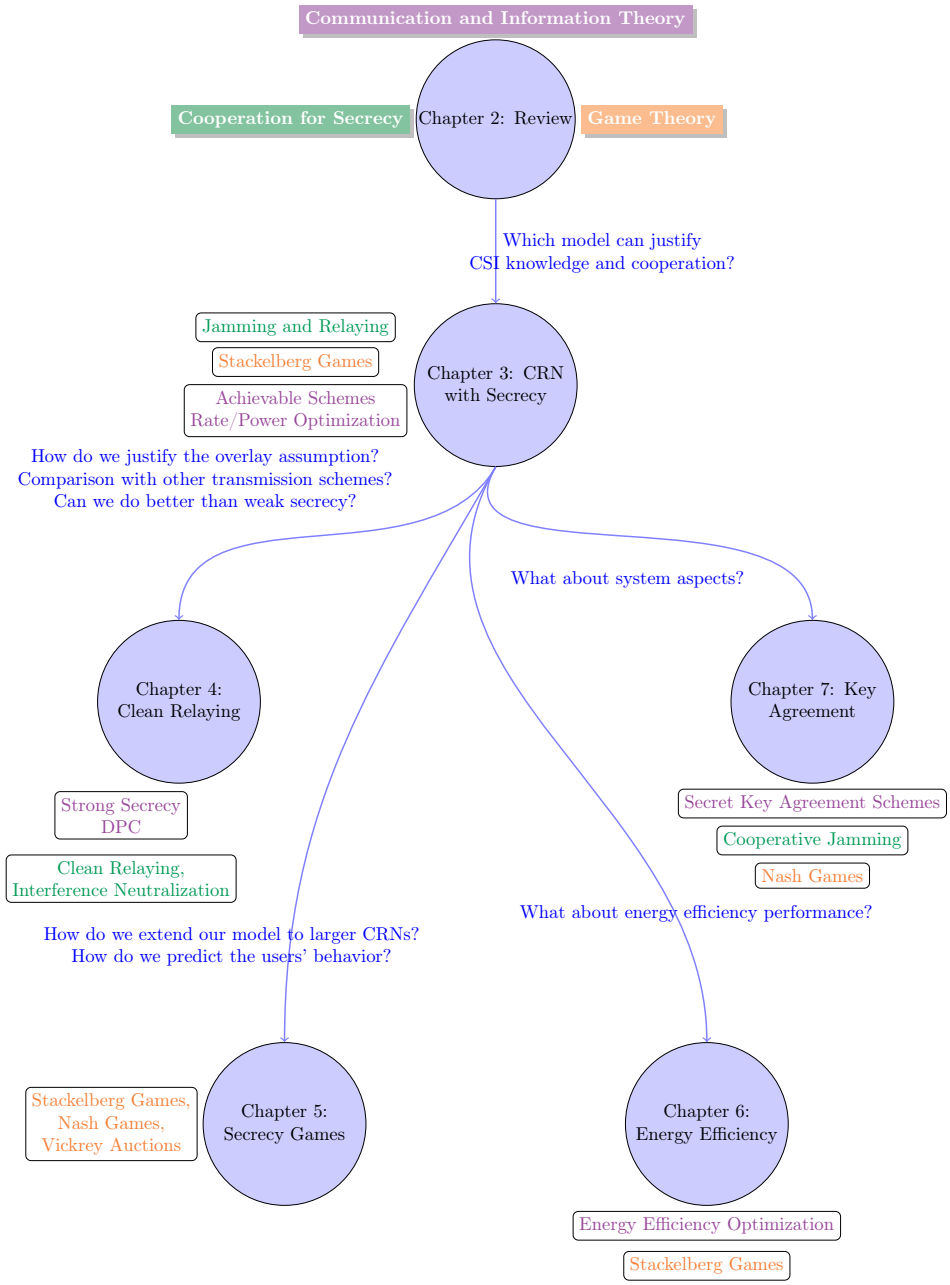


Figure 8.1: A chart representation of the key questions and the solution concepts investigated in the thesis.

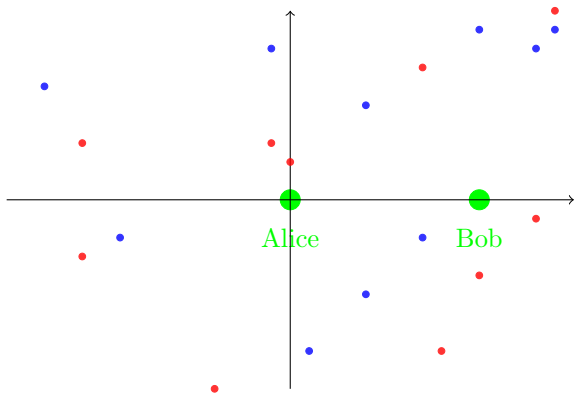


Figure 8.2: Potential helpers and eavesdroppers in a large-scale network.

years in the applications of MIMO techniques to information theoretic secrecy. In particular, the secrecy capacity of the MIMO wiretap channel has been characterized in [KW10], [LS09], [SLU09], and [OH08]. Many powerful tools exist to analyze the performance of large MIMO communication systems, e.g., large-system analysis as investigated in [Gir14]. Therefore, a natural extension to the work in this thesis is the study of MIMO cognitive radio networks, in which the users are equipped with multiple antennas, and hence can benefit from the advantages of multi-antenna transmission for secrecy purposes.

Cooperation Against an Active Eavesdropper In this thesis we assumed a particular attacker model, namely that the eavesdropper was passive in the system; i.e., Eve did not attempt with the communications channels for instance via jamming. This assumption is evidently restrictive and a generalization to an active eavesdropper model is both of theoretical and practical interest.

Cooperative Game Theory for Networks with Secrecy Constraints In this thesis we have focused on tools from non-cooperative game theory to analyze the interaction between the competing transmitters in the system. However another promising direction is to investigate their competitive interaction from a cooperative game theory perspective, which is especially suitable for the cognitive radio networks studied throughout the thesis. Coalitional game theory has already been successfully used as a powerful tool for modeling cooperative behavior in many wireless communications applications related to those investigated in this thesis, such as cognitive radio networks, cooperative communications, and information theoretic secrecy [SHD+09].

Secrecy in a Network of Nodes with Random Topology A fundamental limitation of the literature in the field of information theoretic secrecy is that it has mostly considered scenarios with a small number of nodes. Consequently, recent works have developed a framework based on secrecy graphs to account for large-scale networks composed of multiple legitimate and eavesdropper nodes, e.g., in [PBW12] and references therein. Using a similar approach, the cognitive radio networks investigated in this thesis can be extended to larger networks, consisting of multiple potential secondary helpers and eavesdroppers, as depicted in Figure 8.2. In this model, the primary network, or Alice and Bob, try to communicate secretly while multiple secondary nodes are present in the network and can be viewed as potential helpers or eavesdroppers due to the broadcast nature of the wireless network. Again, a game theoretical approach is the natural way to analyze the behavior of these nodes and coalitional game theory, as discussed in the previous paragraph, could be used as an analysis tool. This extension would constitute a general framework for the analysis of the complex interaction between cooperation and secrecy in large wireless networks with multiple nodes. It would as well generalize the works on cooperation with an untrusted helper, e.g., in[HY10].

Other Topics of Interest Albeit information theoretic secrecy has been extensively studied in numerous ways in the last years, many questions, both theoretical and practical, remain open in this area. Multi-user networks with secrecy constraints, similar to the cognitive radio networks investigated in this thesis, are of particular theoretical interest and an overview of the significant amount of possible research directions for the secrecy of multi-user systems can be found in [LPSS09]. Integration of information theoretic secrecy techniques into the architecture of wireless networks also remains an important challenge, as today's communication networks still rely heavily on cryptography-based security implemented at higher layers; see e.g., [BB11] for a related detailed discussion on practical implementations of information theoretic secrecy.

List of Figures

Bibliography

[AB11] T. Alpcan and T. Basar. *Network Security: A Decision and Game Theoretic Approach*. Cambridge University Press, 2011.

[AC93] R. Ahlswede and I. Csiszár. Common randomness in information theory and cryptography, part I: Secret sharing. *IEEE Transactions on Information Theory*, 39(4):1121–1132, July 1993.

[ALVM06] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty. NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Computer Networks*, 50:2127–2159, Sep. 2006.

[Ama09] G. Amariucai. *Physical security in wireless networks: Intelligent jamming and eavesdropping*. PhD thesis, Louisiana State University, USA, May 2009.

[And14] M. Andersson. *Coding and Transmission Strategies for Secrecy*. PhD thesis, KTH, Royal Institute of Technology, April 2014.

[ATV+12] A. Attar, H. Tang, A. Vasilakos, F. R. Yu, and V. Leung. A survey of security challenges in cognitive radio networks: Solutions and future research directions. *Proceedings of the IEEE*, 100(12):3172–3186, December 2012.

[BB11] M. Bloch and J. Barros. *Physical-Layer Security*. Cambridge University Press, 2011.

[BBRM08] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin. Wireless information-theoretic security. *IEEE Transactions on Information Theory*, 54(6):2515–2534, June 2008.

[BBVM10] M. Bloch, J. Barros, J. Vilela, and S. W. McLaughlin. Friendly jamming for wireless secrecy. In *Proc. IEEE International Conference on Communications (ICC)*, June 2010.

[BL13] M. Bloch and J. N. Laneman. Strong secrecy from channel resolvability. *IEEE Transactions on Information Theory*, 59(12):8077–8098, December 2013.

[BO99] T. Basar and G. J. Olsder. *Dynamic Non-Cooperative Game Theory.* SIAM Series in Classics in Applied Mathematics. Society for Industrial and Applied Mathematics, 1999.

[BSSA10] H. G. Bafghi, S. Salimi, B. Seyfe, and M. Aref. Cognitive interference channel with two confidential messages. In *Proc. IEEE International Symposium on Information Theory and its Applications (ISITA)*, October 2010.

[BU12] R. Bassily and S. Ulukus. Secure communication in multiple relay networks though decode-and-forward strategies. *Journal of Communications and Networks*, 14(4):353–363, August 2012.

[BU13] R. Bassily and S. Ulukus. Deaf cooperation and relay selection strategies for secure communication in multiple relay networks. *IEEE Transactions on Signal Processing*, 61(6):1544–1554, March 2013.

[CEG79] T. Cover and A. El Gamal. Capacity theorems for the relay channel. *IEEE Transactions on Information Theory*, 25(5):572–584, September 1979.

[CK78] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, May 1978.

[CN00] I. Csiszár and P. Narayan. Common randomness and secret key generation with a helper. *IEEE Transactions on Information Theory*, 46(2):344–366, March 2000.

[Cos83] M. H. M. Costa. Writing on dirty paper. *IEEE Transactions on Information Theory*, 29(3):439–441, May 1983.

[CT06] T. Cover and J. Thomas. *Elements of Information Theory.* John Wiley, New York, 2006.

[DHPP10] L. Dong, Z. Han, A. Petropulu, and H. V. Poor. Improving wireless physical layer security via cooperating relays. *IEEE Transactions on Signal Processing*, 58(3):1875–1888, March 2010.

[Din67] W. Dinkelbach. On nonlinear fractional programming. *Management Science*, 13(7):492–498, March 1967.

[EGK12] A. El Gamal and Y.-H. Kim. *Network Information Theory.* Cambridge, January 2012.

[EGMZ06] A. El Gamal, M. Mohseni, and S. Zahedi. Bounds on capacity and minimum energy-per-bit for AWGN relay channels. *IEEE Transactions on Information Theory*, 52(4):1545–1561, April 2006.

[EHT+13] E. Ekrem, X. He, E. Tekin, J. Xie, M. Bloch, S. Ulukus, and A. Yener. Cooperative security at the physical layer: A summary of recent advances. *IEEE Signal Processing Magazine*, 30(5):16–28, September 2013.

[EU11] E. Ekrem and S. Ulukus. Secrecy in cooperative relay broadcast channels. *IEEE Transactions on Information Theory*, 57(1):137 – 155, January 2011.

[FJL+13] D. Feng, C. Jiang, G. Lim, J. Cimini, G. Feng, and G. Li. A survey of energy-efficient wireless communications. *IEEE Communications Surveys and Tutorials*, 15(1):167–178, January 2013.

[GA11] G. Gür and F. Alagöz. Green wireless communications via cognitive dimension: an overview. *IEEE Network*, 25(2):50–56, March-April 2011.

[Gab12] F. Gabry. *Cooperation for Secrecy in Wireless Networks*. Licentiate thesis, KTH, Royal Institute of Technology, September 2012.

[GBGO14] O. Goubet, G. Baudic, F. Gabry, and T. J. Oechtering. Low complexity scalable iterative algorithms for IEEE 802.11p receivers. *IEEE Transactions on Vehicular Technology*, accepted for publication, 2014.

[GGM+13a] M. Girnyk, F. Gabry, V. M., L. K. Rasmussen, and M. Skoglund. On the transmit beamforming for MIMO wiretap channels: Large-system analysis. In *Proc. IEEE International Conference on Information Theoretic Security*, November 2013.

[GGM+13b] M. M. Girnyk, F. Gabry, V. M., L. K. Rasmussen, and M. Skoglund. Large-system analysis of MIMO wire-tap channels with randomly located eavesdroppers. In *Proc. IEEE International Symposium on Wireless Communication Systems*, August 2013.

[GGV+15] M. Girnyk, F. Gabry, M. Vehkaperä, R. L. K., and M. Skoglund. MIMO wiretap channels with randomly located eavesdroppers: Large-system analysis. In *submitted to IEEE International Conference of Communications (ICC)*, 2015.

[Gir14] M. Girnyk. *A Statistical-Physics Approach to the Analysis of Wireless Communication Systems*. PhD thesis, KTH, Royal Institute of Technology, September 2014.

[GJMS09] A. Goldsmith, S. Jafar, I. Maric, and S. Srinivasa. Breaking spectrum gridlock with cognitive radios: An information theoretic perspective. *Proceedings of the IEEE*, 97(5):894–914, May 2009.

[GLG+14] F. Gabry, N. Li, M. Girnyk, N. Schrammar, L. K. Rasmussen, and M. Skoglund. On the optimization of the secondary transmitter's strategy in cognitive radio channels with secrecy. *IEEE Journal on Selected Areas in Communications*, 32(3):451 – 463, March 2014.

[GLS+12] F. Gabry, N. Li, N. Schrammar, M. Girnyk, E. Karipidis, R. Thobaben, L. K. Rasmussen, and M. Skoglund. Secure broadcasting in cooperative cognitive radio networks. In *Proc. Future Networking and Mobile Summit (FNMS)*, July 2012.

[GSG+12] F. Gabry, N. Schrammar, M. Girnyk, N. Li, R. Thobaben, and L. K. Rasmussen. Cooperation for secure broadcasting in cognitive radio networks. In *Proc. IEEE International Conference of Communications (ICC)*, June 2012.

[GSJ12] S. Gerbracht, C. Scheunert, and E. Jorswieck. Secrecy outage in MISO systems with partial state information. *IEEE Transactions on Information Forensics and Security*, 7(2):704–716, April 2012.

[GSTS13] F. Gabry, S. Salimi, R. Thobaben, and M. Skoglund. High SNR performance of amplify-and-forward relaying in Rayleigh fading wiretap channels. In *Proc. Iran Workshop on Communication and Information Theory (IWCIT)*, May 2013.

[GTS11a] F. Gabry, R. Thobaben, and M. Skoglund. Cooperation for secrecy in presence of an active eavesdropper: A game-theoretic perspective. In *Proc. IEEE International Symposium on Wireless Communication Systems (ISWCS)*, November 2011.

[GTS11b] F. Gabry, R. Thobaben, and M. Skoglund. Outage performance and power allocation for decode-and-forward relaying and cooperative jamming for the wiretap channel. In *Proc. IEEE International Conference on Communications Workshops, ICC Workshops*, June 2011.

[GTS11c] F. Gabry, R. Thobaben, and M. Skoglund. Outage performance for amplify-and-forward, decode-and-forward and cooperative jamming strategies for the wiretap channel. In *Proc. IEEE Wireless Communications & Networking Conference (WCNC)*, March 2011.

[GTS14] F. Gabry, R. Thobaben, and M. Skoglund. Secrecy games in cognitive radio networks with multiple secondary users. *Submitted to IEEE Transactions on Communications*, November 2014.

[GZJS14] F. Gabry, A. Zappone, E. Jorswieck, and M. Skoglund. Energy efficiency analysis of cognitive radio networks with secrecy constraints. *Submitted to IEEE Communications Letters*, 2014.

[HA03] M. Hasna and M. Alouini. End-to-end performance of transmission systems with relays over Rayleigh-fading channels. *IEEE Transactions on Wireless Communications*, 52(1):1126–1131, January 2003.

[HHCP08] J. Huang, Z. Han, M. Chiang, and H. V. Poor. Auction-based resource allocation for cooperative communications. *IEEE Journal on Selected Areas in Communications*, 26(7):1226–1237, Sep. 2008.

[HJG13] Z. K. M. Ho, E. Jorswieck, and S. Gerbracht. Information leakage neutralization for the multi-antenna non-regenerative relay-assisted multi-carrier interference channel. *IEEE Journal on Selected Areas in Communications (JSAC)*, 31(9):1672–1686, September 2013.

[HK81] T. Han and K. Kobayashi. A new achievable rate region for the interference channel. *IEEE Transactions on Information Theory*, 27(1):19–31, January 1981.

[HL05] Z. Han and K. J. R. Liu. Non-cooperative power-control game and throughput game over wireless networks. *IEEE Transactions on Communications*, 53(10):1625–1629, October 2005.

[HL08] Z. Han and K. J. R. Liu. *Ressource Allocation for Wireless Networks: Basics, Techniques and Applications*. Cambridge University Press, 2008.

[HMZ05] A. Høst-Madsen and J. Zhang. Capacity bounds and power allocation for wireless relay channels. *IEEE Transactions on Information Theory*, 51(6):2020–2040, June 2005.

[HNS+12] Z. Han, D. Niyato, W. Saad, T. Basar, and A. Hjørungnes. *Game Theory in Wireless and Communication Networks*. Cambridge, 2012.

[HY10] X. He and A. Yener. Cooperation with an untrusted relay: A secrecy perspective. *IEEE Transactions on Information Theory*, 56(8):3807–3827, August 2010.

[Jag66] R. Jagannathan. On some properties of programming problems in parametric form pertaining to fractional programming. *Management Science*, 12(7), March 1966.

[JV09] A. Jovicic and P. Viswanath. Cognitive radio: an information-theoretic perspective. *IEEE Transactions on Information Theory*, 55(9):3945–3958, September 2009.

[KGG05] G. Kramer, M. Gastpar, and P. Gupta. Cooperative strategies and capacity theorems for relay networks. *IEEE Transactions on Information Theory*, 51(9):3037–3063, September 2005.

[KMY07] G. Kramer, I. Maric, and R. D. Yates. *Cooperative Communications*, volume 1. Now Publishers Inc., 2007.

[KP11] T. T. Kim and H. V. Poor. On the secure degrees of freedom of relaying with half-duplex feedback. *IEEE Transactions on Information Theory*, 57(1):291–302, January 2011.

[Kri10] V. Krishna. *Auction Theory*. Academic Press, 2010.

[KW10] A. Khisti and G. Wornell. Secure transmission with multiple antennas I: The MISOME wiretap channel. *IEEE Transactions on Information Theory*, 56(7):3088–3144, July 2010.

[LCK13] K. Lee, C.-B. Chae, and J. Kang. Spectrum leasing via cooperation for enhanced physical-layer secrecy. *IEEE Transactions on Vehicular Technology*, 62(9):4672–4678, November 2013.

[LEG08] L. Lai and H. El Gamal. The relay-eavesdropper channel: Cooperation for secrecy. *IEEE Transactions on Information Theory*, 54(9):4005–4019, September 2008.

[LGT+14a] P.-H. Lin, F. Gabry, R. Thobaben, E. Jorswieck, and M. Skoglund. Clean relaying in cognitive radio networks with variational distance secrecy constraint. In *Proc. IEEE Global Communications conference, GLOBECOM, to appear*, December 2014.

[LGT+14b] P.-H. Lin, F. Gabry, R. Thobaben, E. Jorswieck, and M. Skoglund. Clean relaying in cognitive radio networks with variational distance secrecy constraint. *Submitted to IEEE Transactions on Wireless Communications (TWC)*, November 2014.

[LLSH12] P.-H. Lin, S.-C. Lin, H.-J. Su, and Y.-W. Hong. Improved transmission strategies for cognitive radio under the coexistence constraint. *IEEE Transactions on Wireless Communications*, 11(11):4058 – 4073, November 2012.

[LMSY08] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Transactions on Information Theory*, 54(6):2493–2507, June 2008.

[LPS08] Y. Liang, H. V. Poor, and S. Shamai. Secure communication over fading channels. 54(6):2470–2492, June 2008.

[LPSS09] Y. Liang, H. V. Poor, and S. Shamai (Shitz). Information theoretic security. *Foundations and Trends in Communications and Information Theory*, 5:355–580, April 2009.

[LS09] T. Liu and S. Shamai. A note on the secrecy capacity of the multiple-antenna wiretap channel. *IEEE Transactions on Information Theory*, 55(6):2547–2553, June 2009.

[LSBP+09] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. S. Shamai, and S. Verdú. Capacity of cognitive interference channels with and without secrecy. *IEEE Transactions on Information Theory*, 55(2):604–619, February 2009.

[LT09] R. Liu and W. Trappe. *Securing Wireless Communications at the Physical Layer*. Springer Publishing Company, 2009.

[LTW04] J. Laneman, D. Tse, and G. Wornell. Cooperative diversity in wireless networks: Efficient protocols and outage behaviour. *IEEE Transactions on Information Theory*, 50(12):3063–3080, December 2004.

[LWM11] X. Li, D. Wang, and J. McNair. Residual energy aware channel assignment in cognitive radio sensor networks. In *Proc. IEEE Wireless Communications & Networking Conference (WCNC)*, April 2011.

[LYCH78] S. K. Leung-Yan-Cheong and M. E. Hellman. The Gaussian wire-tap channel. *IEEE Transactions on Information Theory*, 24(4):4687–4698, July 1978.

[LYT10] Z. Li, R. Yates, and W. Trappe. Achieving secret communication for fast Rayleigh fading channels. *IEEE Transactions on Wireless Communications*, 9(9):2792 – 2799, September 2010.

[Mau93] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733–742, May 1993.

[Mit00] J. Mitola. *Cognitive Radio: An integrated agent architecture for software defined radio*. PhD thesis, KTH, May 2000.

[MS10] A. Mukherjee and A. L. Swindlehurst. Equilibrium outcomes of dynamic games in MIMO channels with active eavesdroppers. In *Proc. IEEE International Conference on Communications (ICC)*, June 2010.

[MvOV96] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[Nas50] J. Nash. Equilibrium points in n-person games. *Proceedings of the National Academy of Sciences*, 36(1):48–49, 1950.

[NH08] D. Niyato and E. Hossain. Competitive pricing for spectrum sharing in cognitive radio networks: Dynamic game, inefficiency of Nash equilibrium, and collusion. *IEEE Journal on Selected Areas in Communications*, 26(1):192–202, Jan. 2008.

[OH08] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. In *Proc. IEEE International Symposium on Information Theory (ISIT)*, July 2008.

[PBW12] P. C. Pinto, J. Barros, and M. Z. Win. Secure communication in stochastic wireless networks part I: Connectivity. *IEEE Transactions on Information Forensics and Security*, 7(1):125–138, February 2012.

[PC94] S. Pombra and T. Cover. Non white Gaussian multiple access channels with feedback. 40(3):885–892, May 1994.

[PLZ+10] Y. Pei, Y.-C. Liang, L. Zhang, T. K. C., and K. H. Li. Secure communication over MISO cognitive radio channels. *IEEE Transactions on Wireless Communications*, 9(4):1494–1502, April 2010.

[RLV99] R. Ródenas, M. López, and D. Verastegui. Extensions of Dinkelbach's algorithm for solving non-linear fractional programming problems. *Springer Top: An Official Journal of the Spanish Society of Statistics and Operations Research*, 7(1):33 – 70, June 1999.

[RTD12] S. Rini, D. Tuninetti, and N. Devroye. Inner and outer bounds for the Gaussian cognitive interference channel and new capacity results. *IEEE Transactions on Information Theory*, 58(2):820–848, February 2012.

[SC73] M. Simaan and J. B. Cruz. On the Stackelberg strategy in non zero-sum games. *Journal of Optimization Theory and Applications*, 11(5):533–555, May 1973.

[Sch83] S. Schaible. Fractional programming. *Zeitschrift für Operations Theory and Applications*, 27(1):347–352, 1983.

[SGS13] S. Salimi, F. Gabry, and M. Skoglund. Pairwise key agreement over a generalized multiple access channel: Capacity bounds and game-theoretic analysis. In *Proc. IEEE International Symposium on Wireless Communication Systems (ISWCS)*, August 2013.

[SGS14] S. Salimi, F. Gabry, and M. Skoglund. Pairwise key agreement over a generalized multiple access channel. *To be submitted*, 2014.

[Sha48] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948.

[Sha49] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, 1949.

[SHD+09] W. Saad, Z. Han, M. Debbah, T. Basar, and A. Hjørungnes. Coalitional game theory for communication networks: A tutorial. *IEEE Signal Processing Magazine: Special issue on Game Theory in Signal Processing and Communcations*, 26:77–97, September 2009.

[SLU09] S. Shafiee, N. Liu, and S. Ulukus. Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel. *IEEE Transactions on Information Theory*, 55(9):4033–4039, September 2009.

[SQC13] Z. Shu, Y. Qian, and S. Ci. On physical layer security for cognitive radio networks. *IEEE Network*, 27(3):28–33, May-June 2013.

[SSAG11] S. Salimi, M. Salmasizadeh, M. R. Aref, and J. D. Golić. Key agreement over multiple access channel. *IEEE Transactions on Information Forensics and Security*, 6(3):775–790, September 2011.

[SSS+08] O. Simeone, I. Stanojev, S. Savazzi, Y. Bar-Ness, U. Spagnolini, and R. Pickholtz. Spectrum leasing to cooperating secondary ad hoc networks. *IEEE Journal on Selected Areas in Communications*, 26(1):203–213, January 2008.

[SSSA12] S. Salimi, M. Skoglund, M. Salmasizadeh, and M. R. Aref. Pairwise secret key agreement using the source common randomness. In *Proc. IEEE International Symposium on Wireless Communication Systems (ISWCS)*, August 2012.

[sur14] *IEEE Communications Magazine, Special Issue on Energy efficient cognitive radio networks*, July 2014.

[SY11] I. Stanojev and A. Yener. Cooperative jamming via spectrum leasing. In *Proc. IEEE International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)*, May 2011.

[SY13] I. Stanojev and A. Yener. Improving secrecy rates via spectrum leasing for friendly jamming. *IEEE Transactions on Wireless Communications*, 12(1):134–144, January 2013.

[Tan14] V. Y. F. Tan. A formula for the capacity of the general Gel'fand-Pinsker channel. 62(6):1857–1870, June 2014.

[TKEG10] E. Toher, O. O. Koyluoglu, and H. El Gamal. Secrecy games over the cognitive channel. In *Proc. IEEE International Symposium on Information Theory (ISIT)*, July 2010.

[TLSP11] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. Interference assisted secret communication. *IEEE Transactions on Information Theory*, 57(5):3153 – 3167, May 2011.

[TV10] D. Tse and P. Viswanath. *Fundamentals of Wireless Communications*. Cambridge University Press, 2010.

[TY08a] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. *IEEE Transactions on Information Theory*, 54(12):5747–5755, December 2008.

[TY08b] E. Tekin and A. Yener. The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Transactions on Information Theory*, 54(6):2735 –2751, June 2008.

[TZFS13] E. Z. Tragos, S. Zeadally, A. G. Fragkiadakis, and V. A. Siris. Spectrum assignment in cognitive radio networks: A comprehensive survey. *IEEE Communications Surveys and Tutorials*, 15(3):1108–1135, Third Quarter 2013.

[VBBM11] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin. Wireless secrecy regions with friendly jamming. *IEEE Transactions on Information Forensics and Security*, 6(2):256–266, June 2011.

[vdM71] E. C. van der Meulen. Three-terminal communication channels. *Advances in Applied Probability*, 3:120–154, 1971.

[WL11] Y. Wu and K. J. R. Liu. An information secrecy game in cognitive radio networks. *IEEE Transactions on Information Forensics and Security*, 6(3):831 – 842, September 2011.

[WLX+10] X. Wang, Z. Li, P. Xu, Y. Xu, X. Gao, and H.-H. Chen. Spectrum sharing in cognitive radio networks : an auction-based approach. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 40(3):587 – 596, Jun. 2010.

[WLZZ13] H. Wen, S. Li, X. Zhu, and L. Zhou. A framework of the PHY-layer approach to defense against security threats in cognitive radio networks. *IEEE Network*, 27(3):34–39, May-June 2013.

[WWL10] B. Wang, Y. Wu, and K. J. R. Liu. Game theory for cognitive radio networks: an overview. *Computer Networks*, 54:2537–2561, April 2010.

[Wyn75] A. Wyner. The wire-tap channel. *Bell Systems Technical Journal*, 54(8):1355–1387, October 1975.

[Yeu08] R. W. Yeung. *Information Theory and Network Coding*. Springer, 2008.

[YLE11] M. Yuksel, X. Liu, and E. Erkip. A secure communication game with a relay helping the eavesdropper. *IEEE Transactions on Information Forensics and Security*, 6(3):818 – 830, September 2011.

[YLH10] L. Yu, C. Liu, and W. Hu. Spectrum allocation algorithm in cognitive ad-hoc networks with high energy efficiency. In *Proc. International Conference on Green Circuits and Systems (ICGCS)*, June 2010.

[YN05] C. Ye and P. Narayan. The secret key-private key capacity region for three terminals. In *Proc. IEEE International Symposium on Information Theory (ISIT)*, September 2005.

[YSJ+01] W. Yu, A. Sutivong, D. Julian, T. Cover, and M. Chiang. Writing on colored paper. In *Proc. IEEE International Symposium on Information Theory (ISIT)*, July 2001.

[Yuk08] M. Yuksel. *Reliability, Rate and Security in Cooperative Networks*. PhD thesis, Polytechnic University, Brooklyn, U.S.A., January 2008.

[ZYC+09] P. Zhang, J. Yuan, J. Chen, J. Wang, and J. Yang. Analyzing amplify-and-forward and decode-and-forward cooperative strategies in Wyner's channel model. In *Proc. IEEE Wireless Communications & Networking Conference (WCNC)*, April 2009.