INFORMATION THEORETIC SECRECY FOR SOME
MULTIUSER WIRELESS COMMUNICATION CHANNELS

A Dissertation in
Electrical Engineering
by
Ender Tekin

© 2008 Ender Tekin

Submitted in Partial Fulfillment
of the Requirements
for the Degree of

Doctor of Philosophy

August 2008
The dissertation of Ender Tekin was reviewed and approved* by the following:

Aylin Yener  
Associate Professor of Electrical Engineering  
Dissertation Adviser  
Chair of Committee

David J. Miller  
Associate Professor of Electrical Engineering

John F. Doherty  
Professor of Electrical Engineering

Guohong Cao  
Associate Professor of Computer Science

W. Kenneth Jenkins  
Professor of Electrical Engineering  
Head of the Department of Electrical Engineering

*Signatures are on file in the Graduate School.
Abstract

The widespread use of multiuser wireless communications has been raising the demand for higher data rates and until now that has been the main design focus in wireless systems. This design focus, however, neglects the critical issue of communications security inherent in wireless systems that present a channel that is very easy for people of criminal intent to tap. Existing approaches leave this important issue to the higher layers of the protocol hierarchies, yet the need to deal with it in lower layers is imminent as the security of many cryptographic algorithms is hard to evaluate and has caused disappointment in the past. In addition, there is rising interest in large networks of low-complexity transmitters such as sensor nodes and RF-ID tags that do not have room for complicated and computationally intensive cryptographic algorithms. Historically, communication secrecy has been evaluated using one of two approaches: information theory or computational complexity. Throughout this thesis, we look at the information theoretic measures of secrecy to find provable secure communication schemes, and try to bring a joint approach to improve both security and throughput.

We start by examining the Gaussian Multiple-Access Wire-Tap Channel (GMAC-WT), and an eavesdropper who has access to a degraded version of the legitimate receiver’s signal. For this scenario, we first define two suitable secrecy measures, called “collective” and “individual” secrecy measures. We first look at coding schemes to achieve a given amount of secrecy in the presence of this eavesdropper. We find achievable secrecy rate regions for each constraint, and show that we can achieve the secrecy sum-capacity for this scenario. We then look at a more general scenario where the eavesdropper does not necessarily have a degraded version of the receiver’s signal. In this more general case, we consider the “collective” constraints, as this constraint allows the system to achieve a larger rate region by placing trust on all users; and the “perfect secrecy” case, since this is in general a more appropriate constraint for practical purposes. We find an achievable secrecy rate region, and the power allocations that maximize
the achievable perfect secrecy sum-rate. We also introduce a novel scheme, which we call “cooperative jamming”, where users whose signals are vulnerable to decoding by the eavesdropper jam the eavesdropper, achieving higher secrecy rates for the remaining users. We also find an outer bound on the achievable secrecy sum-rate, which is shown to coincide with the achievable secrecy sum-rate for the degraded scenario.

Next, we consider the Gaussian Two-Way Wire-Tap Channel (GTW-WT) and the Binary Additive Two-Way Wire-Tap Channel (BATW-WT). For these channels, we find achievable secrecy regions, and show that utilizing the same channel, in addition to the transmitters knowing their own self-interference, allows for higher secrecy sum-rates than the GMAC-WT. We also investigate cooperative jamming and find the optimum transmit/jam powers for the two users.

Finally, we examine the ergodic block-fading case for the two user GMAC-WT. We find the secrecy sum-rate maximizing power allocations under a long-term power constraint, and see that unlike the standard GMAC where it is optimal for only one user to be transmitting at any given time, in some cases it is better for both users to be transmitting. We also consider cooperative jamming for this scenario, and give numerical results showing the improvement achievable for the secrecy sum-rate.

This thesis is among the first to point out the advantages that the wireless medium brings to securing information transfer at the physical layer. In particular, the multiple access nature of the communication models considered reveals that allowing confidence in the secrecy of other users, it is possible to achieve secrecy as long as we can put the overall system at an advantage compared to the eavesdropper, rather than needing each user to achieve secrecy for itself. In addition, for certain channels such as the two-way wire-tap channel, each user’s transmission can act as a key, providing an additional advantage over the eavesdropper and allowing improvements over the achievable single-user secrecy rates. Furthermore fading, together with cooperative jamming, provides another dimension to exploit when trying to create an advantage over the eavesdropper. In short, multiple-access nature of the wireless environment becomes a resource for security purposes.
# Table of Contents

List of Figures .................................................. viii

Acknowledgments .................................................. x

Chapter 1. Introduction .......................................... 1
  1.1 Wire-Tap Channels ........................................... 2
  1.2 GMAC-WT ...................................................... 4
  1.3 TW-WT .......................................................... 6
  1.4 Road Map ...................................................... 7
  1.5 Notation ....................................................... 8

Chapter 2. The Degraded Gaussian Multi-Access Wire-Tap Channel .......... 9
  2.1 Introduction ................................................... 9
  2.2 System Model and Problem Statement .......................... 11
    2.2.1 The Secrecy Measures .................................... 13
      2.2.1.1 Individual Secrecy .................................. 14
      2.2.1.2 Collective Secrecy .................................. 15
    2.2.2 The $\delta$-secrecy Capacity Region ...................... 16
    2.2.3 Some Preliminary Definitions .............................. 16
  2.3 Achievable $\delta$-Secrecy Rate Regions ...................... 17
    2.3.1 Individual Secrecy ...................................... 17
    2.3.2 Collective Secrecy ...................................... 21
    2.3.3 Time-Division Multiple Access .......................... 24
  2.4 $\delta$-Secrecy Sum Capacity ................................ 29
  2.5 Numerical Results and Observations ........................... 32
  2.6 Conclusions and Future Work ................................ 37
Chapter 3. The General Gaussian Multi-Access Wire-Tap Channel .......................... 38
  3.1 Introduction ................................................. 38
  3.2 System Model and Problem Statement .................................. 41
    3.2.1 Preliminary Definitions ................................. 43
  3.3 Achievable Secrecy Rate Regions .................................. 46
  3.4 Maximization of Sum Rate ......................................... 51
  3.5 Secrecy Through Cooperative Jamming ............................... 55
  3.6 Upper Bound on the Secrecy Sum-Rate for GGMAC-WT .................. 61
  3.7 Numerical Results and Observations .................................. 67
  3.8 Conclusions and Future Work ...................................... 68

Chapter 4. The Gaussian and Binary Additive Two-Way Wire-Tap Channels ................. 75
  4.1 Introduction ................................................. 75
  4.2 GTW-WT System Model ......................................... 77
  4.3 GTW-WT Achievable Rates ...................................... 79
  4.4 Sum-Rate Maximization for GTW-WT ................................. 86
  4.5 Secrecy Through Cooperative Jamming ............................... 88
  4.6 The BATW-WT System Model .................................... 92
  4.7 BATW-WT Achievable Rates ................................... 93
  4.8 Numerical Results and Observations .................................. 95
  4.9 Conclusions and Future Work ...................................... 96

Chapter 5. The Fading Gaussian Multi-Access Wire-Tap Channel .............................. 100
  5.1 Introduction ................................................. 100
  5.2 System Model and Problem Statement .................................. 101
  5.3 Sum-Rates with Ergodic Fading ................................... 103
  5.4 Sum Rate Maximization ......................................... 108
    5.4.1 \( h_M^1 - h_W^1 \leq \lambda_1, h_M^2 - h_W^2 \leq \lambda_2 \) ...................... 111
    5.4.2 \( h_M^1 - h_W^1 > \lambda_1, h_M^2 - h_W^2 \leq \lambda_2 \) ..................... 112
5.4.3  \( h_1^M - h_4^W \leq \lambda_1, h_2^M - h_2^W > \lambda_2 \) ........................................ 112

5.4.4  \( h_1^M - h_4^W > \lambda_1, h_2^M - h_2^W > \lambda_2 \) ........................................ 113

5.4.4.1  \( (h_1^M - h_1^W)/\lambda_1 \geq (h_2^M - h_2^W)/\lambda_2 \) ...................................... 113

5.4.4.2  \( (h_1^M - h_1^W)/\lambda_1 < (h_2^M - h_2^W)/\lambda_2 \) ...................................... 114

5.5  Sum Rate Maximization with Cooperative Jamming ........................................... 118

5.6  Numerical Results and Observations ................................................................. 122

5.7  Conclusions ........................................................................................................ 123

Chapter 6  Conclusion .............................................................................................. 125

6.1  Thesis Summary .................................................................................................. 125

6.2  Future Work ....................................................................................................... 127

References ............................................................................................................... 128
## List of Figures

1.1 Secrecy system model .................................................. 2

2.1 Equivalent GMAC-WT System Model for the degraded case. ............. 13
2.2 Regions for $P_1 = 10$, $P_2 = 5$, $\delta = \{0.01, 0.5, 1\}$ and $h = 0.1$ ................. 34
2.3 Regions for $P_1 = 10$, $P_2 = 5$, $\delta = \{0.01, 0.5, 1\}$ and $h = 0.5$ ................. 35
2.4 Regions for $P_1 = 10$, $P_2 = 5$, $\delta = \{0.01, 0.5, 1\}$ and $h = 0.9$ ................. 36

3.1 The standardized GMAC-WT system model. .......................... 42
3.2 GGMAC-WT achievable regions for different channel parameters, $G_{\text{MA}}^{(4, 2)}$. ........... 69
3.3 GGMAC-WT achievable secrecy region when $\bar{P}_1 = 4$, $\bar{P}_2 = 4$, $h_1 = .1$, $h_2 = .3$. 70
3.4 GGMAC-WT cooperative jamming secrecy sum-rate as a function of $P_2$ with different $h_1$ for $\bar{P}_1 = \bar{P}_2 = 2$, $h_2 = 1.4$. ................................. 71
3.5 GGMAC-WT cooperative jamming secrecy sum-rate as a function of $P_2$ with different $h_1$ for $\bar{P}_1 = \bar{P}_2 = 100$, $h_2 = 1.4$. ................................. 72
3.6 GGMAC-WT cooperative jamming example. .......................... 73

4.1 The standardized GTW-WT system model. .......................... 78
4.2 GTW-WT achievable regions for different channel parameters, $G_{\text{TW}}^{(4, 2)}$. ........... 84
4.3 GTW-WT achievable secrecy region when $\bar{P}_1 = 4$, $\bar{P}_2 = 2$, $h_1 = .3$, $h_2 = .7$. 85
4.4 BATW-WT system model. ................................................ 92
4.5 GTW-WT cooperative jamming secrecy sum-rate as a function of $P_2$ with different $h_1$ for $\bar{P}_1 = \bar{P}_2 = 2$, $h_2 = 4.2$. ................................. 97
4.6 GTW-WT cooperative jamming example. .......................... 98

5.1 Two-user general Gaussian Multiple-Access Wire-Tap Channel (GGMAC-WT) system model. 102
5.2 Achievable secrecy sum-rate and upper bound as a function of mean eavesdropper channel gain $h_{W}$. 

124
Finally, it seems I have reached the end of my long career as a student. I would like to extend my thanks and appreciation to those who have been instrumental in me reaching this point.

I would like to especially thank my advisor Prof. Aylin Yener for her guidance and mentorship throughout my graduate studies. I have greatly benefited from her advice in both academic and personal areas, and her motivation and support of my work has been crucial in me accomplishing what I have. I greatly appreciate getting the chance to be part of the Wireless Communications and Networking Laboratory, where I had the opportunity to work with and befriend some great people.

I would also like to express my sincere gratitude to the members of my dissertation committee, Prof. David Miller, Prof. John Doherty and Prof. Guohong Cao, for their valuable time and contributions to this dissertation.

There are too many people, whose support and help I have counted on during my time at Penn State, to name here - colleagues from WCAN, friends, roommates... Thank you all for having been part of my life.

Finally, but most of all, I would like to thank my family and my dear wife, Larissa, for all their love and support. None of this would have happened without you.
Chapter 1

Introduction

Telecommunications, especially wireless networking, is a booming industry. The recent launch of 3G mobile networks and 4G already looming on the horizon prove once again that people are asking to be able to do more and more using their communication devices. However, e-crimes such as identity theft and credit card fraud are also at an all time high. To be able to offer newer and better services while preserving security of information is becoming ever more challenging yet essential.

The existing approaches to tackling the security problem leave this issue to the higher layers of the communication protocol hierarchies. However, there is a usually overlooked need to include security measures in lower levels. This kind of approach can serve as both a final lock on valuable information, and as the easiest method to implement for cheap and computationally limited nodes such as sensors or RF-ID tags.

Claude Shannon’s ground-breaking work on developing a measure of ‘information’ [1] and his follow-up paper applying this new concept to what he called ‘secrecy systems’ [2] paved the way for analyzing the security of communication systems on an absolute basis. In the latter paper, Shannon gave a brief overview of secrecy systems, and examined two ways of evaluating the value of a system, looking either at the mathematical complexity, or looking at the entropy of the information available to the eavesdropper to try to design systems with “perfect secrecy”.

The computational complexity approach has one shortcoming - the security claim is hard to analyze and prove mathematically. Also, increases in computational power over time have traditionally been underestimated, resulting in easily breakable encryption schemes [3]. Most notable of these are the breaking of the A3/A8 authentication and key generation algorithms that use COMP128 in GSM, [4], and the revelation that a modern PC could be used to produce effective attacks on the A5/1 voice encryption algorithm, again used in GSM [5]. These, in addition
to others such as the insecurity of CMEA which is used to secure control channel information by many U.S. based digital cellular companies, [6], and the cracking of the then cryptographically standard DES algorithm by a joint effort led by the Electronic Frontier Foundation, [7], has shaken the trust placed upon algorithms that solely rely on computational complexity. As a result, it is of theoretical and practical interest to examine “provably secure” systems.

1.1 Wire-Tap Channels

The information theoretic approach to secrecy started with Shannon, who, in [2], analyzed secrecy systems in communications which is modeled in Figure 1.1. He showed that to achieve perfect secrecy of communications, we must have the conditional probability of the message given the cryptogram independent of the actual transmitted message, i.e., \( P\{M|E\} = P\{M\} \).

![Secrecy system model, [2].](image)

In [8], Wyner applied this concept to the discrete memoryless channel, with a wire-tapper who has access to a degraded version of the intended receiver’s signal. He measured the amount of “secrecy” using the conditional entropy \( \Delta \), the conditional entropy of the transmitted message
given the received signal at the wire-tapper. In this work, the region of all possible \( (R, \Delta) \) pairs was determined, and the existence of a secrecy capacity, \( C_s \), below which it is possible to limit the rate of information leaked to the wire-tapper to arbitrarily small values, was shown. In this analysis, no assumption was made as to the capabilities of the eavesdropper. In other words, in this model, the eavesdropper is assumed to have knowledge of the codewords, transmission scheme used, and has no restrictions on computational power. There is also no “shared secret” between the transmitters and the legitimate receiver.

Carleial and Hellman, in [9], showed that it is possible to send several low-rate messages, each completely protected from the wire-tapper individually, and use the channel at close to capacity. The drawback is, in this case, if any of the messages are revealed to the wire-tapper, the others might also be compromised. In [10], the authors extended Wyner’s results to Gaussian channels and also showed that Carleial and Hellman’s results in [9] also held for the Gaussian channel [10]. Csiszár and Körner, in [11], showed that Wyner’s results can be extended to weaker, so called “less noisy” and “more capable” channels. Furthermore, they analyzed the more general case of sending common information to both the receiver and the wire-tapper, and private information to the receiver only.

Later, the closely related problem of common randomness and secret key generation also gathered attention. Maurer and Wolf, [12], and Bennett et. al., [13], have focused on the process of “distilling” a secret key between two parties in the presence of a wire-tapper, all of whom have partial information about a random variable. Reference [13] breaks this down into three main steps: (i) advantage distillation: where the two parties have zero wiretap capacity and need to find some way of creating an advantage over the wire-tapper, (ii) information reconciliation: where the secret key decided by one of the partners is communicated to the other partner and the wire-tapper is still left with only partial information about it, (iii) privacy amplification: where a new secret key is generated from the previous one about which the wire-tapper has negligible information. In [12], it was shown that for the case when the wire-tap channel capacity is zero between two users, the existence of a “public” feedback channel that the wire-tapper can also observe can nevertheless enable the two parties to be able to generate a secret key with perfect
secrecy. This discussion was then furthered by [14] and [15] where the secrecy key capacities and common randomness capacities, the maximum rates of common randomness that can be generated by two terminals, were developed for several models.

It was argued in [16], that the secrecy constraint developed by Wyner and later utilized by Csiszár and Körner was “weak” since it only constrained the rate of information leaked to the wire-tapper, rather than the total information. It was shown that Wyner’s scenario could be extended to “strong” secrecy for discrete channels with no loss in achievable rates, where the secrecy constraint is placed on the total information obtained by the wire-tapper, as the information of interest might be in the small amount leaked. Maurer then examined the case of active adversaries, where the wire-tapper has read/write access to the channel in [17]– [19]. Venkatesan and Anantharam examined the cases where the two terminals generating common randomness were connected by different DMC’s in [20] and later generalized this to a network of DMC’s connecting any finite number of terminals in [21]. Csiszár and Narayan extended Ahlswede and Csiszár’s previous work to multiple-terminals by looking at what a helper terminal can contribute in [22], and the case of multiple terminals where an arbitrary number of terminals are trying to distill a secret key and a subset of these terminals can act as helper terminals to the rest in [23].

Recently, there has been a resurgence of interest in wire-tap channels. Secrecy for parallel channels, [24,25], relay channels, [26], and fading channels, [27,28] were also examined. Fading and parallel channels were examined together in [29,30]. Broadcast and interference channels with confidential messages were considered in [31]. References [32,33] examined the multiple access channel with confidential messages where two transmitters try to keep their messages secret from each other while communicating with a common receiver.

1.2 GMAC-WT

The Gaussian Multiple-Access Channel (GMAC) model is an uplink communications scenario where multiple users communicate with a receiver, e.g. a base station, over a common band and in the presence of additive white Gaussian noise (AWGN), [34,35]. We consider the
Gaussian Multiple Access Wire-Tap Channel (GMAC-WT) where multiple users are transmitt-}

ing to a base station in the presence of AWGN, and a wiretapper also receives a noisy version of

the signal received at the base station. We define two separate secrecy constraints, which we call

the individual and collective secrecy constraints. These are (i) the normalized entropy of any

set of messages conditioned on the transmitted codewords of the other users and the received

signal at the wire-tapper, and (ii) the normalized entropy of any set of messages conditioned

on the wire-tapper’s received signal. The first set of constraints is more conservative to ensure

secrecy of any subset of users even when the remaining users are compromised. The second

set of constraints ensures the collective secrecy of any set of users, utilizing the secrecy of the

remaining users. We consider the case where a pre-determined level of secrecy, measured by

$0 \leq \delta \leq 1$, is to be achieved, where $\delta = 0$ corresponds to no secrecy constraint, and $\delta = 1$

corresponds to “perfect secrecy”. Using random Gaussian codebooks and superposition coding,

we find achievable secrecy rate regions for each constraint, where users can communicate with

arbitrarily small probability of error with the intended receiver, while the wire-tapper is kept

ignorant to a pre-determined level. We show that this scheme achieves secrecy sum capacity

for collective constraints. We also find a secrecy rate region using the results of [10] for the

single-user case and TDMA. This scheme achieves secrecy sum capacity for both constraints,

but is smaller than the region for collective constraints. When individual constraints are con-

sidered, the achievable region is the convex hull of the union of the superposition coding and

TDMA regions. In practical situations, we can think of this as the wire-tapper being outside of a

controlled indoor environment, such as in [36] or just being able to wire-tap the receiver rather

than receive the signals itself.

Then, we consider the general case where the signal received by the eavesdropper is not

necessarily degraded. Rather, we assume the eavesdropper also receives the signals through a

different GMAC. We utilize the “collective” secrecy constraints, and perfect secrecy of the trans-

mited messages. We find an achievable secrecy rate region, where users can communicate with

arbitrarily small probability of error with the intended receiver under perfect secrecy from the

eavesdropper. We also find an outer bound on the achievable secrecy sum rate. For the special
case of the degraded GGMAC-WT, this is shown to achieve the secrecy sum-capacity. We then find the secrecy sum-rate maximizing power allocations. It is seen that as long as the users are not *single-user decodable at the eavesdropper*, a secrecy-rate trade off is possible between the users. Next, we show that a non-transmitting user can help increase the secrecy capacity for a transmitting user by effectively “jamming” the eavesdropper, or even enable secret communications that would not be possible in a single-user scenario. We term this new scheme *cooperative jamming*. We find the optimum transmit/jamming power allocations that maximize the achievable secrecy sum-rate for this scheme, and show that significant increases in the secrecy sum-rate are possible.

Finally, we look at the block-fading Gaussian multiple-access wire-tap channel. We give an achievable secrecy rate region, and find the secrecy sum-rate maximizing power allocation. We then examine how cooperative jamming can improve the secrecy sum-rate. We see that utilizing cooperative jamming allows us to achieve a secrecy-sum rate close to the outer bound.

We note that we generally find *achievable rate regions* using Gaussian codebooks, and the capacity regions for the channels considered are currently open problems. Gaussian codebooks are shown achieve sum-capacity for the degraded case, but the general description of the rate regions are still unknown.

### 1.3 TW-WT

We also consider the two-way channel where two nodes communicate with each other over a common medium, first defined in [37]. We introduce the two-way wire-tap (TW-WT) channel where an external *eavesdropper* receives the transmitters’ signals through a MAC. In particular, we consider the Gaussian Two-Way Wire-Tap Channel (GTW-WT), and the Binary Additive Two-Way Wire-Tap Channel (BATW-WT). We utilize, as our secrecy constraint, the normalized conditional entropy of the transmitted secret messages given the eavesdropper’s signal, termed “collective secrecy” in [38]. We show that satisfying this constraint implies the secrecy of the messages for both users. For both scenarios, we find an achievable *secrecy rate*
region, where users can communicate with arbitrarily small probability of error with the intended receiver under perfect secrecy from the eavesdropper.

We also show that in cases where a user is not able to achieve secrecy, that user may help the other user increase its secrecy rate or achieve secrecy if it was not possible before, by jamming the eavesdropper. Thus, similar to the Gaussian multiple-access wire-tap channel, cooperative jamming helps increase the secrecy rate. The GTW-WT is shown to be especially useful for secret communications, as the multiple-access nature of the channel hurts the eavesdropper without affecting the communication rate. This is due to the fact that the transmitted messages of each user essentially help hide the other user’s secret messages, and reduce the extra randomness needed in wire-tap channels to confuse the eavesdropper.

We note that our results give an achievable secrecy rate region for each channel model considered, and not the capacity region, which is still an open problem.

1.4 Road Map

We first look at the degraded Gaussian Multi-Access Wire-Tap Channel in Chapter 2. We then look at the general Gaussian Multi-Access Wire-Tap Channel in Chapter 3. Next, we consider achievable rates for the Gaussian Two-Way and Binary Additive Two-Way Channels in Chapter 4. After that, Chapter 5 examines the ergodic block-fading case for the GMAC-WT. We provide the conclusion and future directions in Chapter 6.

Most of the results in this thesis were presented at conferences, and also submitted for publication as journal papers. In particular, Chapter 2 includes results from [39, 40], and was submitted for publication [38]. Results in Chapter 3 were presented in [41, 42] and accepted for publication [43]. Chapter 4 contains work presented in [44], and partially included in [43]. Finally, Chapter 5 was presented in [45].

We begin each chapter with a detailed introduction to the system we are considering, which is followed by a model of the system. We then present our results, discussion and future directions for each chapter. We hope that this will make each chapter a self-contained unit.
1.5 Notation

Throughout this dissertation, we use $H(X)$ to refer to discrete entropy, $h(X)$ to refer to differential entropy, and $I(X;Y)$ to refer to the mutual information, as defined in [35]. All logarithms, unless otherwise stated, are taken to the base 2, such that these quantities are given in \textit{bits}. We also use bold font to refer to vectors and matrices, or collections of variables, and script font to refer to sets.
Chapter 2

The Degraded Gaussian Multi-Access Wire-Tap Channel

2.1 Introduction

Shannon, in [2], showed that to achieve perfect secrecy in communications the \textit{a posteriori} probability of a message must be equivalent to its \textit{a priori} probability. This concept was applied to the discrete memoryless channel by Wyner in [8]. Wyner defined the \textit{wire-tap channel}, where there is a wire-tapper who has access to a degraded version of the intended receiver’s signal. Wyner found the region of all possible rate/equivocation, \((R, \Delta)\), pairs. He showed the existence of a positive \textit{secrecy capacity}, \(C_s\), the rate up to which it is possible to limit the information leaked to the wire-tapper to arbitrarily small values. Carleial and Hellman, in [9], showed that it is possible to send several low-rate messages, each completely protected from the wire-tapper individually, and use the channel at close to capacity. At the same time, reference [10] extended this result to Gaussian channels. In this work, the authors showed that Later, Csiszár and Körner, [11], generalized Wyner’s results to channels satisfying some weaker conditions than degradedness.

Later, Maurer and Wolf, [12], and Bennett et. al., [13], focused on the process of “distilling” a secret key between two parties who have partial information about a common random variable in the presence of a wire-tapper. In [12], it was shown that for the case when the wire-tap channel capacity is zero between two users, the existence of a “public” feedback channel can enable the two parties to generate a secret key with perfect secrecy. This is broken down into three main steps in reference [13]: (i) advantage distillation: the two parties with zero wiretap capacity need to find some way of creating an advantage over the wire-tapper, (ii) information reconciliation: the secret key decided by one of the partners is communicated to the other partner and the wire-tapper is left with only partial information about it, (iii) privacy amplification:
a new secret key is generated from the previous one about which the wire-tapper has negligible information. This discussion was then furthered by [14] and [15] where the secrecy key capacities and common randomness capacities, the maximum rates of common randomness that can be generated by two terminals, were developed.

More recently, the notion of the wire-tap channel has been extended to parallel channels, [24, 25], relay channels, [26], and fading channels, [27, 46]. References [29, 30] considered fading and parallel channels together. Broadcast and interference channels with confidential messages were examined in [31]. References [32, 33] examined the multiple access channel with confidential messages, where two transmitters want to ensure the secrecy of their messages from each other while communicating with a common receiver. In [32], an achievable region is found in general, and the capacity region is found for some special cases.

In this chapter, we consider the Gaussian Multiple Access Channel (GMAC) where multiple users are transmitting to a base station in the presence of AWGN, and a wiretapper also receives a noisy version of the signal received at the base station. We define two separate secrecy constraints, which we call the individual and collective secrecy constraints. These are (i) the normalized entropy of any set of messages conditioned on the transmitted codewords of the other users and the received signal at the wire-tapper, and (ii) the normalized entropy of any set of messages conditioned on the wire-tapper’s received signal. The first set of constraints is more conservative to ensure secrecy of any subset of users even when the remaining users are compromised. The second set of constraints ensures the collective secrecy of any set of users, utilizing the secrecy of the remaining users. We consider the case where a pre-determined level of secrecy, $0 \leq \delta \leq 1$ is to be provided for each set of users, where $\delta = 0$ corresponds to no secrecy constraint, and $\delta = 1$ corresponds to perfect secrecy. Using random Gaussian codebooks and superposition coding, we find achievable secrecy rate regions for each constraint, where users can communicate with arbitrarily small probability of error with the intended receiver, while the wire-tapper is kept ignorant to a pre-determined level. We show that this scheme achieves secrecy sum capacity for collective constraints. We also find a secrecy rate region using the results of [10] for the single-user case and TDMA. This scheme achieves secrecy sum capacity for both
constraints, but is smaller than the region for collective constraints. When individual constraints are considered, the achievable region is the convex hull of the union of the superposition coding and TDMA regions.

We next present the system model in section 2.2. We present achievable rates for each of our constraints in section 2.3, and an upper bound on the secrecy sum-rate for both constraints in section 2.4. We give numerical results and conclusions in sections 2.5 and 2.6.

### 2.2 System Model and Problem Statement

We consider $K$ users communicating with a receiver in the presence of a wire-tapper in a Gaussian channel. In general, transmitter $k \in \mathcal{K} \triangleq \{1, \ldots, K\}$ chooses a message $W_k$ from a set of equally likely messages $\mathcal{W}_k = \{1, \ldots, M_k\}$. The messages are encoded using $(2^nR_k, n)$ codes into $\{\tilde{X}_k^n(W_j)\}$, where $R_k = \frac{1}{n} \log_2 M_k$. The encoded messages $\{\tilde{X}_k\} = \{\tilde{X}_k^n\}$ are then transmitted, and the intended receiver and the wire-tapper get $\tilde{Y} = \tilde{Y}^n$ and $\tilde{Z} = \tilde{Z}^n$, respectively. The receiver decodes $\tilde{Y}$ to get an estimate of the transmitted messages, $\hat{W}$. We would like to communicate with the receiver with arbitrarily low probability of error, while maintaining secrecy to a pre-determined level $\delta$.

The signals at the intended receiver and the wiretapper for the GMAC-WT are given by

\[
\tilde{Y} = \sum_{k=1}^{K} \sqrt{h_k^M} \tilde{X}_k + \tilde{N}_M \\
\tilde{Z} = \sum_{k=1}^{K} \sqrt{h_k^W} \tilde{X}_k + \tilde{N}_W
\]  

(2.1a) 

(2.1b)

where $\tilde{N}_M, \tilde{N}_W$ are the AWGN at the intended receiver and eavesdropper, respectively. Each component of $\tilde{N}_M \sim \mathcal{N}\left(0, \sigma_M^2\right)$ and $\tilde{N}_W \sim \mathcal{N}\left(0, \sigma_W^2\right)$. We do not make any assumptions on noise correlations, since due to the broadcast nature of this channel, coupled with the fact that the intended receiver and the eavesdropper are assumed not to cooperate, the capacity will depend only on the marginal probabilities, and will be the same regardless of the noise correlations [35, 47]. The transmit power constraints are given by $\frac{1}{n} \sum_{i=1}^{n} \tilde{X}_{ki}^2 \leq \tilde{P}_k, \ k = 1, \ldots, K$. 


Faithful to Wyner’s terminology, we term this channel the Gaussian Multiple Access Wire-Tap Channel (GMAC-WT).

Similar to the scaling transformation to put an interference channel in standard form, [48], we can represent any GMAC-WT by an equivalent standard form, [40]:

\[
Y = \sum_{k=1}^{K} X_k + N_M \tag{2.2a}
\]

\[
Z = \sum_{k=1}^{K} \sqrt{h_k} X_k + N_W \tag{2.2b}
\]

where

- the codewords \(\{\tilde{X}\}\) are scaled to get \(X_k = \sqrt{\frac{h_k^M}{\sigma_M^2}} \tilde{X}_k\);
- the new power constraints are \(\bar{P}_k = \frac{h_k^M}{\sigma_M^2} \tilde{P}_k\);
- the new wiretapper channel gains are \(h_k = \frac{h_k^W \sigma_M^2}{h_k M \sigma_W^2}\);
- the AWGN are normalized by \(N_M = \frac{1}{\sigma_M^2} \tilde{N}_M\) and \(N_W = \frac{1}{\sigma_W^2} \tilde{N}_W\).

We shall examine the case where the wire-tapper receives a \textit{stochastically degraded} version of the signal received at the legitimate receiver, i.e., there exists a distribution \(\tilde{p}(z|y)\) such that we can write \(p(z|x_1, \ldots, x_K) = \int_{-\infty}^{\infty} p(y|x_1, \ldots, x_K) \tilde{p}(z|y) dy\). Similar to the broadcast channel, since the legitimate receiver and the eavesdropper do not cooperate, noise correlations do not play a role, and as a result, the capacity of the stochastically degraded wire-tap channel is the same as that of the \textit{physically degraded} wire-tap channel, where \(p(y, z|x_1, \ldots, x_K) = p(y|x_1, \ldots, x_K)p(z|y)\). It can easily be shown that the wire-tapper gets a stochastically degraded version of the receiver’s signal if \(h_1 = \ldots = h_K \equiv h < 1\). Since, as noted earlier, the noise correlations do no affect the capacity region, we equivalently consider the physically degraded case, where the wire-tapper’s received signal is a noisier version of the legitimate receiver’s scaled received signal, \(Z = \sqrt{h} Y + N_{MW}\), where \(N_{MW}\) has each component...
∼ \mathcal{N}(0, 1 - h)$ and is independent of $Y$. This model is illustrated in Figure 2.1. In practical situations, we can think of this as the wire-tapper being outside of a controlled indoor environment, such as in [36] or just being able to wire-tap the receiver rather than receive the signals itself.

![Fig. 2.1: Equivalent GMAC-WT System Model for the degraded case.](image)

2.2.1 The Secrecy Measures

Letting $\Delta_S$ be our secrecy constraint for any subset $S$ of users, we require that $\Delta_S \geq \delta - \epsilon$ for all sets $S \subseteq \mathcal{K}$, with $\delta \in [0, 1]$ as the required level of secrecy, and $\epsilon \to 0$ is an arbitrarily small positive number. $\delta = 1$ corresponds to perfect secrecy, where the wire-tapper is not allowed to get any information; and $\delta = 0$ corresponds to no secrecy constraint. To that end, we define two sets of secrecy constraints using the normalized equivocations for sets of users. These are:
2.2.1.1 Individual Secrecy

We define the “individual secrecy measure” for a subset of users, $S \subseteq K$, as

$$
\Delta^I_S \triangleq \frac{H(W_S|X_{Sc},Z)}{H(W_S)}, \quad \forall S \subseteq K = \{1, \ldots, K\}
$$

(2.3)

where $W_S = \{W_k\}_{k \in S}$, $\Delta^I_S$ denotes the normalized entropy of the transmitted messages of a set $S$ of users, given the received signal at the wire-tapper as well as the remaining users’ transmitted symbols. As our secrecy criterion, this guarantees that the rate of information leaked to the wire-tapper from a group of users is limited even if all the other users’ transmitted codewords are compromised. This is a stronger constraint than $H(W_S|W_{Sc},Z)$, as $H(W_S|W_{Sc},Z) \geq H(W_S|W_{Sc},X_{Sc},Z) = H(W_S|X_{Sc},Z)$. In addition, from a practical point of view, if the transmitted messages are compromised either due to byzantine users or some other side information allowing the eavesdropper to decode the transmitted messages of a group of users, there is no reason to expect that the transmitted codewords are not known to the eavesdropper. Thus, this represents a scenario where users do not have to trust each other.

We note that if the individual secrecy constraints for all users in the set $S$ are satisfied, i.e., $\Delta_k \geq \delta - \epsilon$, $\forall k \in S$, then the constraint for set $S$ is also satisfied. To see this, without loss of generality, let $S = 1, \ldots, S$ where $S \leq K$ and assume $\frac{H(W_k|X_{kc},Z)}{H(W_k)} \geq \delta - \epsilon$. We can write

$$
H(W_S|X_{Sc},Z) = \sum_{k=1}^{S} H(W_k|W_k^{k-1},X_{Sc},Z)
$$

(2.4)

$$
\geq \sum_{k=1}^{S} H(W_k|W_k^{k-1},X_{kc},Z)
$$

(2.5)

$$
= \sum_{k=1}^{S} H(W_k|X_{kc},Z)
$$

(2.6)

$$
\geq \sum_{k=1}^{S} (\delta - \epsilon)H(W_k)
$$

(2.7)

$$
= (\delta - \epsilon)H(W_S)
$$

(2.8)
where (2.5) follows using conditioning, (2.6) is due to the fact that $W_j$ is conditionally independent of all $W_k$ given $X_k, Z$. (2.7) comes from our assumption that for all $k \in S$, $\Delta^1_k \geq \delta$. Thus, for any subset of users the individual $\delta$-secrecy constraints for all users also guarantee the joint $\delta$-secrecy for the entire set.

### 2.2.1.2 Collective Secrecy

Clearly, the individual constraints defined in (2.3), are conservative, as users do not place any trust on each other. We now define a revised secrecy measure to take into account the multi-access nature of the channel where users rely on others to achieve secrecy for the whole group, that we call “collective secrecy constraints”:

\[
\Delta^C_S \triangleq \frac{H(W_S|Z)}{H(W_S)}, \quad \forall S \subseteq K
\]  

(2.9)

Using this constraint guarantees that each subset of users maintains a level of secrecy greater than $\delta$. Since this must be true for all sets of users, collectively the system has at least the same level of secrecy. However, if a group of users are somehow compromised, the remaining users may also be vulnerable. We require the secrecy constraint to be satisfied separately for each $S \subseteq K$, since otherwise it is possible to have $\Delta^C_S \geq \delta$, but $\Delta^C_J < \delta$ for some $J \subset S$. However, if $\delta = 1$, i.e., when we require perfect secrecy, we can show that $\Delta^C_K \geq 1 - \epsilon \Rightarrow \Delta^C_S \geq 1 - \epsilon'$ for all $S \subseteq K$, where $\epsilon' \to 0$ as $\epsilon \to 0$. To see this, write

\[
H(W_S|Z) + H(W_{Sc}) \geq H(W_S|Z) + H(W_{Sc}|W_S, Z)
\]  

(2.10)

\[
= H(W_K|Z)
\]  

(2.11)

\[
\geq (1 - \epsilon)H(W_K)
\]  

(2.12)

\[
= (1 - \epsilon)H(W_S) + (1 - \epsilon)H(W_{Sc})
\]  

(2.13)
where (2.11) comes from the chain rule for entropies, and (2.12) comes from the secrecy constraint. Comparing the left side of (2.10) and (2.13), we have

\[
\frac{H(W_S|Z)}{H(W_S)} \geq 1 - \epsilon - \frac{H(W_{Sc})}{H(W_S)} \epsilon
\]  

(2.14)

Thus, we have \( \Delta^C_S \geq 1 - \epsilon' \) where \( \epsilon' = \left(1 + \frac{H(W_{Sc})}{H(W_S)}\right) \epsilon \to 0 \) as \( \epsilon \to 0 \), and perfect secrecy for the ensemble of users guarantees perfect secrecy for all subsets of users.

2.2.2 The \( \delta \)-secrecy Capacity Region

**Definition 2.1 (Achievable Rates with \( \delta \)-secrecy).** Let \( \xi = I \) if using individual constraints, and \( \xi = C \) if using collective constraints. The rate \( K \)-tuple \( R = (R_1, \ldots, R_K) \) is said to be achievable with \( \delta \)-secrecy under constraint \( \xi \), if for a given \( \epsilon > 0 \) there exists a code of sufficient length \( n \) such that

\[
\frac{1}{n} \log_2 M_k \geq R_k - \epsilon \quad k = 1, \ldots, K
\]  

(2.15)

\[
P_e \leq \epsilon
\]  

(2.16)

\[
\Delta^\xi_S \geq \delta - \epsilon \quad \forall S \subseteq K
\]  

(2.17)

where user \( k \) chooses one of \( M_k \) symbols to transmit according to the uniform distribution, \( \Delta^\xi_S \) denotes the secrecy constraint, and is given by (2.3) if \( \xi = I \) and (2.9) if \( \xi = C \). We will call the set of all achievable rates with \( \delta \)-secrecy under \( \xi \) constraints, the \( \delta \)-secrecy capacity region, and denote it \( C^\xi(\delta) \).

2.2.3 Some Preliminary Definitions

Before we state our results, we also define the following quantities for any \( S \subseteq K \).

\[
P_S \triangleq \sum_{k \in S} P_k
\]  

(2.18)
\[ R_S \triangleq \sum_{k \in S} R_k \]  
(2.19)

\[ C_M^S (P) \triangleq \frac{1}{2} \log (1 + P_S) \]  
(2.20)

\[ C_W^S (P) \triangleq \frac{1}{2} \log (1 + hP_S) \]  
(2.21)

\[ \tilde{C}_W^S (P) \triangleq \frac{1}{2} \log \left( 1 + \frac{hP_S}{1 + hP_{Sc}} \right) \]  
(2.22)

In general, we will omit the argument \( P \) for (2.20)–(2.22) for clarity unless it is not clear from context. In addition, we will sometimes also use the subscript \( \text{sum} \) when \( S = \mathcal{K} \).

### 2.3 Achievable \( \delta \)-Secrecy Rate Regions

In this section, we find a set of achievable rates using Gaussian codebooks, which we denote \( \mathcal{G}(\delta) \). We first give the achievable regions satisfying the individual and collective secrecy constraints, denoted \( \mathcal{G}^I(\delta) \) and \( \mathcal{G}^C(\delta) \) respectively, using superposition coding. We then give a region obtained by TDMA, denoted \( \mathcal{G}^T(\delta) \), which satisfies both secrecy constraints. For the collective secrecy constraints, the TDMA region is seen to be smaller than the superposition coding region. For the individual secrecy constraints, the achievable region is the convex hull of the union of the superposition and TDMA regions, denoted \( \mathcal{G}^I_{\cup}(\delta) \).

#### 2.3.1 Individual Secrecy

In [10], it has been shown that codewords drawn according to a Gaussian distribution can be used to maintain secrecy for the single user Gaussian wire-tap channel. Using a similar approach, we present an achievable \( \delta \)-secrecy rate region for individual constraints. We first define the following region:

**Definition 2.2 (Superposition Region for Individual Constraints, \( \mathcal{G}^I(\delta) \)).** Consider the following region:

\[ \mathcal{R}^I(\delta) \triangleq \left\{ R : R_S \leq \min \left\{ I(X_S; Y | X_{Sc}), \right\} \right\} \]
\[ \frac{1}{\delta} \left[ I(X_S; Y|X_{Sc}) - \sum_{k \in S} I(X_k; Z|X_{kc}) \right], \quad \forall S \subseteq \mathcal{K} \]  

(2.23)

We can evaluate this region for \( X_k \sim \mathcal{N}(0, P_k) \) to write

\[ \mathcal{G}^I(\delta) \triangleq \left\{ \mathbf{R} : R_S \leq \min \left\{ \frac{1}{2} \log (1 + P_S), \frac{1}{2\delta} \left[ \log (1 + P_S) - \sum_{k \in S} \log (1 + hP_k) \right] \right\}, \quad \forall S \subseteq \mathcal{K} \right\} \]  

(2.24)

which can also be written in a more compact form using the definitions in (2.20)–(2.22) as:

\[ \mathcal{G}^I(\delta) = \left\{ \mathbf{R} : R_S \leq \min \left\{ \frac{1}{C_S^M} \frac{1}{\delta} \left( C_S^M - \sum_{k \in S} C_k^W \right) \right\}, \quad \forall S \subseteq \mathcal{K} \right\} \]  

(2.25)

**Theorem 2.1.** The region \( \mathcal{G}^I(\delta) \) given in (2.24) is achievable with \( \delta \)-secrecy for the degraded GMAC-WT under individual secrecy constraints.

**Proof.** **Coding Scheme:** Let \( \mathbf{R} = (R_1, \ldots, R_K) \) satisfy (2.24). For each user \( k \in \mathcal{K} \), consider the scheme:

1. Let \( M_k = 2^{n(R_k - \epsilon')} \) where \( 0 \leq \epsilon' < \epsilon \). Let \( M_k = M_{ks}M_{k0} \) where, for some \( \mu \) to be chosen later such that \( 1 \geq \mu_k \geq \delta \), we have \( M_{ks} = M_{k}^{\mu_k} \) and \( M_{k0} = M_{k}^{1-\mu_k} \). Then, \( R_k = R_{ks} + R_{k0} + \epsilon' \) where \( R_{ks} = \frac{1}{n} \log M_{ks} \) and \( R_{k0} = \frac{1}{n} \log M_{k0} \). We can choose \( \epsilon' \) and \( n \) to ensure that \( M_{ks}, M_{k0} \) are integers.

2. Generate 3 codebooks \( \mathcal{X}_{ks}, \mathcal{X}_{k0} \) and \( \mathcal{X}_{kx} \). \( \mathcal{X}_{ks} \) consists of \( M_{ks} \) codewords, each component of which is drawn from \( \mathcal{N}(0, \lambda_{ks}P_k - \epsilon) \). Codebook \( \mathcal{X}_{k0} \) has \( M_{k0} \) codewords with each component drawn from \( \mathcal{N}(0, \lambda_{k0}P_k - \epsilon) \) and \( \mathcal{X}_{kx} \) has \( M_{kx} \) codewords with each
component drawn from $\mathcal{N}(0, \lambda_k x P_k - \varepsilon)$. Here, $\varepsilon$ is an arbitrarily small number to ensure that the power constraints are satisfied with high probability and $\lambda_k s + \lambda_k 0 + \lambda_k x = 1$. Define $R_{kx} = \frac{1}{n} \log M_{kx}$ and $M_{kt} = M_k M_{kx}$.

3. Each message $W_k \in \{1, \ldots, M_k\}$ is mapped into a message vector $\mathbf{W}_k = (W_{ks}, W_{k0})$ where $W_{ks} \in \{1, \ldots, M_{ks}\}$ and $W_{k0} \in \{1, \ldots, M_{k0}\}$. Since user $k$ chooses $W_k$, the message to transmit, with equal probability, $W_{ks}, W_{k0}$ are also uniformly distributed.

4. To transmit message $W_k \in \{1, \ldots, M_k\}$, user $k$ finds the 2 codewords corresponding to components of $\mathbf{W}_k$ from $\mathcal{X}_{ks}$ and $\mathcal{X}_{k0}$, and also uniformly chooses a codeword from $\mathcal{X}_{kx}$. He then adds all these codewords and transmits the resulting codeword, $\mathbf{X}_k$, so that we are actually transmitting one of $M_{kt}$ codewords. Let $R_{kt} = \frac{1}{n} \log M_{kt} + \epsilon' = R_{ks} + R_{k0} + R_{kx} + \epsilon'$. In this manner, the codebook $\mathcal{X}_{ks}$ corresponds to user $k$’s secret messages, the codebook $\mathcal{X}_{k0}$ corresponds to user $k$’s open messages, and the codebook $\mathcal{X}_{kx}$ corresponds to user $k$’s added randomness to confuse the eavesdropper.

Specifically, the rates are chosen to satisfy $\forall S \subseteq K$:

$$\sum_{k \in S} R_{ks} \leq \frac{1}{2} \log (1 + P_S) - \sum_{k \in S} \frac{1}{2} \log (1 + hP_k)$$
(2.26)

$$R_{k0} + R_{kx} = \frac{1}{2} \log (1 + hP_k), \quad \forall k \in S$$
(2.27)

$$\sum_{k \in S} R_{kt} \leq \frac{1}{2} \log (1 + P_S)$$
(2.28)

or equivalently,

$$\sum_{k \in S} R_{ks} = \sum_{k \in S} \mu_k R_k \leq C^M_S - \sum_{k \in S} C^W_k$$
(2.29)

$$R_{k0} + R_{kx} = (1 - \mu_k) R_k + R_{kx} = C^W_k, \quad \forall k \in S$$
(2.30)

$$\sum_{k \in S} R_{kt} = \sum_{k \in S} [R_k + R_{kx}] \leq C^M_S$$
(2.31)
We first note that the last inequality ensures that we are operating in the capacity region of the GMAC to the intended receiver, so that the intended receiver can decode the transmitted codewords \( \{ X_k \}_{k=1}^K \) by looking for the set of codewords that are jointly typical with the received sequence \( Y \), and hence determine \( \{ W_k \}_{k=1}^K \) with vanishing probability of error [35].

Consider the sub-code \( \{ X_{ks} \}_{k=1}^K \). From this point of view, the coding scheme described is equivalent to each user \( k \in \mathcal{K} \) selecting one of \( M_{ks} \) messages, and sending a uniformly chosen codeword from among \( M_k0M_{ks} \) codewords for each. Let

\[
\hat{\Delta}^i_k = \frac{H(W_{ks}|X_{kc}, Z)}{H(W_{ks})}
\]

and write:

\[
H(W_{ks}|X_{kc}, Z) = H(W_{ks}|X_{kc}) - I(W_{ks}; Z|X_{kc})
\]  \hspace{1cm} (2.32)

\[
= H(W_{ks}) - I(W_{ks}; Z|X_{kc})
\]  \hspace{1cm} (2.33)

\[
= H(W_{ks}) - I(W_{ks}; Z|X_{kc}) + I(W_{ks}; Z|X_{kC})
\]  \hspace{1cm} (2.34)

\[
= H(W_{ks}) - h(Z|X_{kc}) + h(Z|W_{ks}, X_{kc}) + h(Z|X_{kC}) - h(Z|X_{kC}, W_{ks})
\]  \hspace{1cm} (2.35)

\[
= H(W_{ks}) - I(X_k; Z|X_{kc}) + I(X_k; Z|W_{ks}, X_{kc})
\]  \hspace{1cm} (2.36)

where (2.33) comes from the fact that the transmitted messages of user \( k \) are independent of the transmitted codewords of the other users, and (2.34) comes from the fact that \( Z \) is independent of the transmitted messages given all the transmitted codewords, \( X_{kC} \). Dividing both sides by \( H(W_{ks}) \), we arrive at

\[
\hat{\Delta}^i_k = \frac{H(W_{ks}|X_{kc}, Z)}{H(W_{ks})} = 1 - \frac{I(X_k; Z|X_{kc}) - I(X_k; Z|W_{ks}, X_{kc})}{H(W_{ks})}
\]  \hspace{1cm} (2.37)

By the converse to the coding theorem for the Gaussian Multiple Access Channel, we have \( I(X_k; Z|X_{kc}) \leq nC_k^W \). We can also write

\[
I(X_k; Z|W_{ks}, X_{kc}) = H(X_k|W_{ks}, X_{kc}) - H(X_k|W_{ks}, X_{kc}, Z)
\]  \hspace{1cm} (2.38)
For each secret message of user $k$, it sends one of $M_k x M_k$ possible codewords. By choosing $R_{k,x}, R_{k,0}$ to satisfy (2.30), our coding scheme implies that

$$H(X_k | W_{ks}, X_{kc}) = H(X_k | W_{ks}) = n C_{w}^W$$

(2.39)

Also,

$$H(X_k | W_{ks}, X_{kc}, Z) \leq n \delta_n$$

(2.40)

where $\delta_n \to 0$ due to Fano’s Inequality. This stems from the fact that given $W_{ks}$, the sub-code for user $k$ is, with high probability, a “good” code for the wiretapper. Combining these in (2.37), we can write

$$\Delta^I_k \geq 1 - \frac{n C_{w}^W - n C_{w}^W + n \delta_n}{H(W_{ks})} = 1 - \epsilon$$

(2.41)

where $\epsilon = \frac{\delta_n}{R_{ks}} \to 0$ as $n \to \infty$ since we assume $R_{ks} > 0$. If $R_{ks} = 0$, we can reclassify some open messages as secret to make $R_{ks} > 0$.

Then, we can write

$$\Delta^I_k = \frac{H(W_k | X_{kc}, Z)}{H(W_k)} \geq \frac{H(W_{ks} | X_{kc}, Z)}{H(W_k)} \geq \frac{(1 - \epsilon) H(W_{ks})}{H(W_k)} \geq \frac{(1 - \epsilon) \mu_k R_k}{R_k} \geq \delta$$

(2.42)

Since (2.42) holds for all $k = 1, \ldots, K$, from (2.8) we have $\Delta^I_S \geq \delta, \forall S \subseteq \mathcal{K}$. \hfill $\Box$

**Remark:** In this case, the maximum $\delta$-secrecy sum-rate achievable is given by

$$R_{s_{\text{sum}}}^I(\delta) = \min \left\{ C_{\mathcal{K}}^M, \frac{1}{\delta} \left[ C_{\mathcal{K}}^M - \sum_{k=1}^{K} C_{k}^W \right] \right\}$$

(2.43)

### 2.3.2 Collective Secrecy

We first define the following region:
**DEFINITION 2.3 (SUPERPOSITION REGION FOR COLLECTIVE CONSTRAINTS, $G^C(\delta)$).** Consider the following region:

$$
R^C(\delta) \triangleq \left\{ R: R_S \leq \min \left\{ I(X_S;Y|X_{Sc}), \right. \right.
\left. \frac{1}{\delta} \left[ I(X_S;Y|X_{Sc}) - I(X_S;Z) \right] \right\}, \forall S \subseteq \mathcal{K} \right\} \quad (2.44)
$$

We can evaluate this region for $X_k \sim \mathcal{N}(0,P_k)$ to write

$$
G^C(\delta) \triangleq \left\{ R: R_S \leq \min \left\{ \frac{1}{2} \log (1 + P_S), \right. \right.
\left. \frac{1}{2\delta} \left[ \log (1 + P_S) - \log \left( 1 + \frac{hP_S}{1 + hP_{Sc}} \right) \right] \right\}, \forall S \subseteq \mathcal{K} \right\} \quad (2.45)
$$

which can also be written in a more compact form using the definitions in (2.20)–(2.22) as:

$$
G^C(\delta) = \left\{ R: R_S \leq \min \left\{ C^M_S, \frac{1}{\delta} \left( C^M_S - \tilde{C}^W_S \right) \right\}, \forall S \subseteq \mathcal{K} \right\} \quad (2.46)
$$

**THEOREM 2.2.** We can transmit with $\delta$-secrecy under collective secrecy constraints at the rates in the region $G^C(\delta)$ defined in (2.45).

**PROOF.** Let $R = (R_1, \ldots, R_K)$ satisfy (2.45) and assume the coding scheme is the same as described in the individual constraints case, except that instead of (2.29)–(2.31), we will choose the rates such that for all $S \subseteq \mathcal{K},$

$$
\sum_{k \in S} R_{ks} \leq \frac{1}{2} \log (1 + P_S) - \frac{1}{2} \log \left( 1 + \frac{hP_S}{1 + hP_{Sc}} \right) \quad (2.47)
$$

$$
\sum_{k=1}^{K} [R_{k0} + R_{kx}] = \frac{1}{2} \log (1 + hP_{\mathcal{K}}) \quad (2.48)
$$

$$
\sum_{k \in S} R_{kt} \leq \frac{1}{2} \log (1 + P_S) \quad (2.49)
$$
which can also be written as,

\[
\sum_{k \in S} R_{ks} = \sum_{k \in S} \mu_k R_k \leq C^M_S - \tilde{C}_S^W
\] (2.50)

\[
\sum_{k=1}^{K} [R_{k0} + R_{kx}] = \sum_{k=1}^{K} [(1 - \mu_k) R_k + R_{kx}] = C^W_K
\] (2.51)

\[
\sum_{k \in S} R_{kt} = \sum_{k \in S} [R_k + R_{kx}] \leq C_M^S
\] (2.52)

From (2.52) and the GMAC coding theorem, with high probability the intended receiver can decode the codewords \(X_k\) with low probability of error, and hence determine \(W_k\) for all \(k\) by finding the jointly typical \(\{X_k\}_{k=1}^{K}\), \(Y\). To show \(\Delta_c^S \geq \delta, \forall S \subseteq \mathcal{K}\), we concern ourselves only with MAC sub-code \(\{X_{ks}\}_{k=1}^{K}\). From this point of view, the coding scheme described is equivalent to each user \(k \in \mathcal{K}\) selecting one of \(M_{ks}\) messages, and sending a uniformly chosen codeword from among \(M_{k0}M_{kx}\) codewords for each. Let \(W^s_S = \{W_{ks}\}_{k \in S}\) and define \(X_{\Sigma} = \sum_{k=1}^{K} X_k\). For \(\mathcal{K}\) write

\[
H(W^s_{\mathcal{K}}|Z) = H(W^s_{\mathcal{K}}) - I(W^s_{\mathcal{K}}; Z)
\] (2.53)

\[
= H(W^s_{\mathcal{K}}) - I(W^s_{\mathcal{K}}; Z) + I(W^s_{\mathcal{K}}; Z|X_{\Sigma})
\] (2.54)

\[
= H(W^s_{\mathcal{K}}) - h(Z) + h(Z|W^s_{\mathcal{K}}) + h(Z|X_{\Sigma}) - h(Z|W^s_{\mathcal{K}}, X_{\Sigma})
\] (2.55)

\[
= H(W^s_{\mathcal{K}}) - I(X_{\Sigma}; Z) + I(X_{\Sigma}; Z|W^s_{\mathcal{K}})
\] (2.56)

where (2.54) follows from the fact that \(W^s_{\mathcal{K}} \rightarrow X_{\Sigma} \rightarrow Z\). Dividing both sides by \(H(W^s_{\mathcal{K}})\), we get

\[
\Delta^c_{\mathcal{K}} = \frac{H(W^s_{\mathcal{K}}|Z)}{H(W^s_{\mathcal{K}})} = 1 - \frac{I(X_{\Sigma}; Z) - I(X_{\Sigma}; Z|W^s_{\mathcal{K}})}{H(W^s_{\mathcal{K}})}
\] (2.57)

Consider the two terms individually. First, we have the sum-rate bound of the multiple access channel to the eavesdropper:

\[
I(X_{\Sigma}; Z) \leq nC^W_{\mathcal{K}}
\] (2.58)
\[ I(X_\Sigma; Z|W_\mathcal{K}) = H(X_\Sigma|W_\mathcal{K}^s) - H(X_\Sigma|W_\mathcal{K}, Z). \]

Since user \( k \) sends one of \( M_{k0}M_{kx} \) codewords for each message, from (2.51) we have

\[ H(X_\Sigma|W_\mathcal{K}^s) = \log \left( \prod_{k=1}^{K} M_{k0}M_{kx} \right) \]
\[ = nC^W_\mathcal{K} \]  

(2.59)

(2.60)

We can also write

\[ H(X_\Sigma|W_\mathcal{K}^s, Z) \leq n\eta'_n \]  

(2.61)

where \( \eta'_n \to 0 \) as \( n \to \infty \) since, with high probability, the eavesdropper can decode \( X_\Sigma \) given \( W_\mathcal{K}^s \) due to (2.51). Using (2.50), (2.51), (2.58), (2.60) and (2.61) in (2.57), we get

\[ \tilde{\Delta}_K^c \geq 1 - \frac{C^W_\mathcal{K} - C^M_\mathcal{K} + \eta'_n}{C^M_\mathcal{K} - C^W_\mathcal{K}} \to 1 \text{ as } \eta'_n \to 0 \]  

(2.62)

The proof is completed by noting that due to (2.14), \( \tilde{\Delta}_K^c = 1 \) implies \( \tilde{\Delta}_S^c = 1, \forall S \subseteq \mathcal{K} \), and writing

\[ \Delta_S \geq \frac{H(W_S^s|Z)}{H(W_S)} = \frac{H(W_S^s)}{H(W_S)} = \frac{\sum_{k \in S} R_k}{\sum_{k \in S} R_k} \geq \delta \]  

(2.63)

We note that this way the achievable \( \delta \)-secrecy sum-rate is

\[ R_{sum}^C(\delta) = \min \left\{ C^M_\mathcal{K}, \frac{1}{\delta} \left[ C^M_\mathcal{K} - C^W_\mathcal{K} \right] \right\} \]  

(2.64)

2.3.3 Time-Division Multiple Access

We can also use TDMA to get an achievable region. In such a scheme, only one user is transmitting at a given time. Hence, both sets of constraints collapse down to a set of single-user secrecy constraints, since in this scheme \( H(W_S|X_{Sc}, Z) = H(W_S|Z) = \sum_{k \in S} H(W_k|Z) \).
The constraints can then be written as

$$\Delta_k \triangleq \frac{H(W_k|Z)}{H(W_k)} \geq \delta - \epsilon, \quad \forall k \in K$$

(2.65)

The results for a single-user wire-tap channel were given in [10]. Before we state out achievable region, we define the following:

**Definition 2.4.** Let \(\{\alpha_k\}_{k=1}^K\) be such that \(0 \leq \alpha_k \leq 1\) for all \(k \in K\), and \(\sum_{k=1}^K \alpha_k = 1\). Let \(\hat{P}_k = \bar{P}_k / \alpha_k\), \(\forall k\) and define

$$R^C(\delta, \alpha) = \left\{ R_k \leq \min \left\{ \alpha_k I(X_k; Y|X_k^c), \frac{\alpha_k}{\delta} \left[ I(X_k; Y|X_k^c) - I(X_k; Z|X_k^c) \right], \forall S \subseteq K \right\} \right\}$$

(2.66)

which, if \(X_k \sim \mathcal{N}(0, \hat{P}_k)\), becomes

$$G^T(\delta, \alpha) = \left\{ R_k \leq \min \left\{ \frac{\alpha_k}{2} \log \left( 1 + \frac{\bar{P}_k}{\alpha_k} \right), \frac{\alpha_k}{2\delta} \log \left( \frac{\alpha_k + \bar{P}_k}{\alpha_k + h\bar{P}_k} \right) \right\}, \quad k = 1, \ldots, K \right\}$$

(2.67)

and can equivalently be written as:

$$G^T(\delta, \alpha) = \left\{ R_k \leq \min \left\{ \alpha_k C^M_k(\hat{P}), \frac{\alpha_k}{\delta} \left[ C^M_k(\hat{P}) - C^W_k(\hat{P}) \right] \right\}, \quad \forall k \in K \right\}$$

(2.68)

**Theorem 2.3.** Consider this scheme: Let \(\alpha_k \in [0, 1], \, k = 1, \ldots, K\) and \(\sum_{k=1}^K \alpha_k = 1\). User \(k\) only transmits \(\alpha_k\) of the time with power \(\bar{P}_k / \alpha_k\) using the scheme described in [10]. Then, the following set of rates is achievable:

$$G^T(\delta) = \text{convex hull of } \bigcup_{\sum_{k=1}^K \alpha_k = 1} G^T(\delta, \alpha)$$

(2.69)
PROOF. Follows directly from [10, Theorem 1] with the above described TDMA scheme, and writing $\frac{1}{2} \log \left(1 + \frac{\bar{P}_k}{\alpha_k}\right) - \frac{1}{2} \log \left(1 + h\bar{P}_k\right) = \frac{1}{2} \log \left(\frac{\alpha_k + \bar{P}_k}{\alpha_k + h\bar{P}_k}\right)$.

Note that with this scheme, the achievable $\delta$-secrecy sum-rate is given by

$$R_{\text{sum}}^T(\delta, \alpha) = \sum_{k=1}^{K} \min \left\{ \frac{\alpha_k}{2} \log \left(1 + \frac{\bar{P}_k}{\alpha_k}\right), \frac{\alpha_k}{2\delta} \log \left(\frac{\alpha_k + \bar{P}_k}{\alpha_k + \delta\bar{P}_k}\right) \right\}$$

(2.70)

THEOREM 2.4. The above described TDMA scheme achieves a maximum sum-rate of

$$R_{\text{sum}}^T(\delta) = \min \left\{ \frac{C^M}{K}, \frac{1}{\delta} \left[ \frac{C^M}{K} - C^W \right] \right\}$$

(2.71)

using the optimum time-sharing parameters

$$\alpha^*_k = \frac{\bar{P}_k}{\sum_{j=1}^{K} \bar{P}_j} = \frac{\bar{P}_k}{\bar{P}_K}$$

(2.72)

PROOF. The problem can be written as

$$\max_{\alpha} \sum_{k=1}^{K} \min \left\{ \frac{\alpha_k}{2} \log \left(1 + \frac{\bar{P}_k}{\alpha_k}\right), \frac{\alpha_k}{2\delta} \log \left(\frac{\alpha_k + \bar{P}_k}{\alpha_k + \delta\bar{P}_k}\right) \right\}$$

(2.73)

which is of the form

$$\max_{\alpha} \sum_{k} \min \left\{ f_k(\alpha_k), g_k(\alpha_k) \right\}$$

(2.74)

for some sequence of functions $f_k, g_k$. Let

$$\alpha^* = \arg \max \min \left\{ \sum_k f_k(\alpha_k), \sum_k g_k(\alpha_k) \right\}$$

(2.75)
We note that
\[
\min \left\{ \sum_k f_k(\alpha^*), \sum_k g_k(\alpha^*) \right\} = \max_{\alpha} \min \left\{ \sum_k f_k(\alpha), \sum_k g_k(\alpha) \right\} \geq \max_{\alpha} \sum_k \min \{ f_k(\alpha), g_k(\alpha) \}
\] (2.76)

which is satisfied with equality if \( f_k(\alpha^*) \geq g_k(\alpha^*) \) or \( g_k(\alpha^*) \geq f_k(\alpha^*) \) for all \( k \). Thus, if the \( \alpha^* \) that maximizes the max-min-sum problem satisfies this constraint, then the max-sum-min equation achieves, as its maximum, the same value with the same optimum \( \alpha^* \). Thus, we first find
\[
\max_{\alpha} \min \left\{ \sum_{k=1}^K \frac{\alpha_k}{2} \log \left( 1 + \frac{\bar{P}_k}{\alpha_k} \right), \sum_{k=1}^K \frac{\alpha_k}{2} \log \left( \frac{\alpha_k + \bar{P}_k}{\alpha_k + h\bar{P}_k} \right) \right\}
\] (2.77)

We first look at
\[
\max_{\alpha} \sum_{k=1}^K \frac{\alpha_k}{2} \log \left( 1 + \frac{\bar{P}_k}{\alpha_k} \right)
\] (2.78)

This is the standard GMAC TDMA sum-rate optimization problem. By taking the derivative and equating it to zero, we get
\[
0 = \frac{1}{2} \log \left( 1 + \frac{\bar{P}_k}{\alpha_k} \right) - \frac{\bar{P}_k}{2(\alpha_k + \bar{P}_k)} + \lambda
\] (2.80)

for all \( k \). Hence, we must have
\[
\log \left( 1 + \frac{\bar{P}_k}{\alpha_k} \right) - \frac{\bar{P}_k}{\alpha_k + \bar{P}_k} = \log \left( 1 + \frac{\bar{P}_j}{\alpha_j} \right) - \frac{\bar{P}_j}{\alpha_j + P_j}
\] (2.81)

for all \( j, k \in K \). We can easily verify that \( \alpha_k^* = \frac{\bar{P}_k}{\bar{P}_K} \) satisfies this equation and the constraints on \( \alpha_k \). Now consider
\[
\max_{\alpha} \sum_{k=1}^K \frac{\alpha_k}{2} \log \left( \frac{\alpha_k + \bar{P}_k}{\alpha_k + h\bar{P}_k} \right)
\] (2.82)
with the constraint $\sum_{k=1}^{K} \alpha_k = 1$. This is also a straightforward convex optimization problem. Writing the Lagrangian and taking the derivative with respect to $\alpha_k$, we get

$$0 = \frac{1}{2\delta} \log \left( \frac{\alpha_k + \bar{P}_k}{\alpha_k + h\bar{P}_k} \right) - \frac{\alpha_k(1-h)\bar{P}_k}{2\delta(\alpha_k + P_k)(\alpha_k + hP_k)} + \lambda$$

(2.83)

which implies that for any two users $j, k$, we must have

$$\log \left( \frac{\alpha_k + \bar{P}_k}{\alpha_k + h\bar{P}_k} \right) = \log \left( \frac{\alpha_j + \bar{P}_j}{\alpha_j + h\bar{P}_j} \right)$$

(2.84)

It is easy to verify that $\alpha_k^* = \frac{\bar{P}_k}{P_K}$ again makes both the logarithmic and the other terms equal each other, and hence is the optimum $\alpha_k$. Since this choice maximizes both terms in the minimum in (2.78) simultaneously, it is the solution to the max-min problem. Now, noting that

$$\log \left( 1 + \frac{\bar{P}_k}{\alpha_k^*} \right) = \log \left( 1 + \frac{\bar{P}_K}{\alpha_K^*} \right)$$

(2.85)

and

$$\frac{1}{\delta} \log \left( \frac{\alpha_k^* + \bar{P}_k}{\alpha_k^* + h\bar{P}_k} \right) = \frac{1}{\delta} \log \left( \frac{1 + \bar{P}_K}{1 + h\bar{P}_K} \right)$$

(2.86)

do not depend on $k$, from (2.77) we see that $\alpha_k^*$ is the solution to (2.73). □

Since in this scheme only one user is transmitting at any given time, both individual and collective constraints are satisfied. We see that for collective secrecy constraints, this region is a subset of $G^C(\delta)$. For individual secrecy constraints, this does not hold, as seen in Figure 2.2. We can then, using time-sharing arguments, find a new achievable region for individual constraints that is the convex-closure of the union of the two regions:

**THEOREM 2.5.** The following region is achievable for individual secrecy constraints:

$$G^I(\delta) = \text{convex closure of } \left( G^I(\delta) \cup G^T(\delta) \right)$$

(2.87)
2.4 \( \delta \)-Secrecy Sum Capacity

In this section, we present an upper bound on the \( \delta \)-secrecy sum-rate, denoted \( C_{sum}(\delta) \), for both individual and collective constraints, and show that this bound corresponds to the \( \delta \)-secrecy sum-rate achievable under both constraints, giving us the secrecy sum-capacity of GMAC-WT for individual and collective constraints. We note that a sum-rate constraint on both individual and collective constraints can be obtained using the constraints for the set \( K \). In this case, both sets of constraints collapse down to

\[
\Delta_K \triangleq \frac{H(W_K | Z)}{H(W_K)} \geq \delta
\]  

(2.88)

**Theorem 2.6.** For the GMAC-WT, the \( \delta \)-secrecy sum-capacity for both individual and collective secrecy constraints is given by

\[
C_{sum}(\delta) = \min \left\{ C_{K}^M - \frac{1}{\delta} \left[ C_{K}^M - C_{K}^W \right] \right\}
\]  

(2.89)

**Proof.** We first show that the right-hand side of (2.89) is an upper bound on the \( \delta \)-secrecy sum-rate for both constraints. Observe that (2.89) is equal to the secrecy sum-rate achievable in (2.64) for collective constraints using superposition coding, and by TDMA in (2.71), which satisfies both collective and individual constraints. Hence, we get the \( \delta \)-secrecy sum-capacity of the GMAC-WT for both individual and collective constraints.

The first term in the minimum of (2.89) is due to the converse for the GMAC, since the intended receiver needs to be able to decode the transmitted messages. If \( \delta = 0 \), we have no secrecy constraint and only the first term applies. To see the second term, assume \( \delta > 0 \). We first note that from Fano’s inequality, we have

\[
H(W_K | Y, Z) \leq H(W_K | Y) \leq n \eta_n
\]  

(2.90)
where $\eta_n \to 0$ as $n \to \infty$. We then use the constraint in (2.88):

$$R_K = \frac{1}{n} H(W_K)$$

(2.91)

$$\leq \frac{1}{n \delta} H(W_K|Z)$$

(2.92)

$$\leq \frac{1}{n \delta} [H(W_K|Z) + n \eta_n - H(W_K|Y, Z)]$$

(2.93)

$$= \frac{1}{n \delta} I(W_K; Y|Z) + \eta'_n$$

(2.94)

$$\leq \frac{1}{n \delta} I(X_K; Y|Z) + \eta'_n$$

(2.95)

where we used (2.90) to write (2.93), and $W_K \rightarrow X_K \rightarrow Y \rightarrow Z$ in the last step. We now adopt Lemma 10 in [10] to upper bound the differences between the received signal entropies at the receiver and wire-tapper:

**Lemma 2.1 (Lemma 10 in [10]).** Let $\xi = \frac{1}{n} h(Y)$ where $Y, Z$ are as given in (2.2). Then,

$$h(Y) - h(Z) \leq n \xi - n \phi(\xi) = \frac{n}{2} \log \left[ 2\pi e \left( 1 - h + \frac{h^2 \xi^2}{2\pi e} \right) \right]$$

(2.96)

where

$$\phi(\xi) \triangleq \xi - \frac{1}{2} \log \left[ 2\pi e \left( 1 - h + \frac{h^2 \xi^2}{2\pi e} \right) \right]$$

(2.97)

**Proof.** The proof follows using the entropy power inequality [35]. Recall that we can write $h(Z) = h(\sqrt{n} Y + N_{MW})$. Then, by the entropy power inequality, we have

$$\frac{2}{2^n} h(Z) = \frac{2}{2^n} h(\sqrt{n} Y + N_{MW}) \geq \frac{2}{2^n} [h(Y) + n \log \sqrt{n}] + \frac{2}{2^n} h(N_{MW})$$

(2.98)

Now $h(Y) = n \xi$ and $h(N_{MW}) = \frac{n}{2} \log [2\pi e (1 - h)]$. Hence,

$$\frac{2}{2^n} h(Z) \geq h^2 \xi + 2\pi e (1 - h)$$

(2.99)
which, after taking the log, gives

\[ h(Z) \geq \frac{n}{2} \log \left[ h^{2\xi} + 2\pi e(1 - h) \right] \] (2.100)

\[ = \frac{n}{2} \log \left[ 2\pi e \left( 1 - h + \frac{h^{2\xi}}{2\pi e} \right) \right] \] (2.101)

subtracting from \( h(Y) = n\xi \) completes the proof of the lemma.

\[ \Box \]

**Corollary 2.1.**

\[ h(Y) - h(Z) \leq n \left[ C^M_K - C^W_K \right] \] (2.102)

**Proof.** From the converse to the GMAC coding theorem, [35], we can show that

\[ h(Y) \leq \frac{n}{2} \log (2\pi e(1 + P_K)) \] (2.103)

Let \( h(Y) = n\xi \). Then, \( \xi \leq \frac{1}{2} \log (2\pi e(1 + P_K)) \), and since

\[ \frac{\partial \phi}{\partial \xi} = \frac{2\pi e(1 - h)}{2\pi e(1 - h) + h^{2\xi}} \geq 0 \] (2.104)

making \( \phi(\xi) \) is a non-increasing function of \( \xi \), we get \( \phi(\xi) \geq \phi \left( \frac{1}{2} \log (2\pi e(1 + P_K)) \right) \). Thus,

\[ h(Y) - h(Z) \leq \frac{n}{2} \log (2\pi e(1 + P_K)) - \frac{n}{2} \log \left[ 2\pi e \left( 1 - h + h(1 + P_K) \right) \right] \] (2.105)

\[ = n \left[ C^M_K - C^W_K \right] \] (2.106)

\[ \Box \]

Now, we can use (2.95) to write

\[ I(X_K; Y|Z) = I(X_K; Y, Z) - I(X_K; Z) \] (2.107)

\[ = I(X_K; Y) + I(X_K; Z|Y) - I(X_K; Z) \] (2.108)
\[ I(\mathbf{X}_K; \mathbf{Y}) - I(\mathbf{X}_K; \mathbf{Z}) = h(\mathbf{Y}) - h(\mathbf{Y}|\mathbf{X}_K) - h(\mathbf{Z}) + h(\mathbf{Z}|\mathbf{X}_K) \tag{2.109} \]

\[ = \sum_{i=1}^{n} \left[ h(Z_i|\mathbf{X}_{K,i}) - h(Y_i|\mathbf{X}_{K,i}) \right] + [h(\mathbf{Y}) - h(\mathbf{Z})] \tag{2.111} \]

\[ = \left[ \frac{n}{2} \log(2\pi e) - \frac{n}{2} \log(2\pi e) \right] + [h(\mathbf{Y}) - h(\mathbf{Z})] \tag{2.112} \]

\[ = h(\mathbf{Y}) - h(\mathbf{Z}) \tag{2.113} \]

\[ \leq n \left[ C^M_K - C^W_K \right] \tag{2.114} \]

where we used the fact that \( \mathbf{X}_K \rightarrow \mathbf{Y} \rightarrow \mathbf{Z} \Rightarrow I(\mathbf{X}_K; \mathbf{Z}|\mathbf{Y}) = 0 \) to get (2.109), and applied Corollary 2.1 to get the last step. Using (2.114) in (2.95) completes the proof. \( \square \)

To see when we the secrecy constraint is more constraining on the sum-rate than the decodability constraint, we can write (2.89) also as

\[ C_{sum}(\delta) = \begin{cases} 
\frac{1}{2} \log \left(1 + P_K\right), & \text{if } \delta \leq 1 - \frac{\log(1+hP_K)}{\log(1+P_K)} \\
\frac{1}{2}\delta \log \left(\frac{1+P_K}{1+hP_K}\right), & \text{if } \delta \geq 1 - \frac{\log(1+hP_K)}{\log(1+P_K)} \end{cases} \tag{2.115} \]

### 2.5 Numerical Results and Observations

It can be seen that if the wire-tapper’s channel is much worse than that of the legitimate receiver, i.e., \( h \rightarrow 0 \), then \( C_{sum}(\delta) \rightarrow C(P_K) \), we incur no loss in \( \delta \)-secrecy sum-capacity and can still communicate with secrecy. On the other hand, if the wire-tapper’s channel is almost as good, i.e., \( h \rightarrow 1 \), then \( C_{sum}(\delta) \rightarrow 0 \), and it is no longer possible to communicate with secrecy.

An interesting point to note is that \( C_{sum}(\delta) \leq \frac{1}{2}\delta \log \left(\frac{1+P_K}{1+hP_K}\right) \) is an increasing function of \( P_K \) for \( h < 1 \), but as \( P_K \rightarrow \infty \), \( C_{sum}(\delta) \) is upper bounded by \(-\frac{1}{2}\delta \log h \). We see that regardless of how much power we have available, the \( \delta \)-secrecy sum-capacity with a non-zero level of secrecy is limited by the channel’s degradedness, \( h \), and the level of secrecy required,
Also, it is inversely proportional to the level of secrecy desired, \( \delta \), but inversely proportional to the logarithm of \( h \), the degradedness of the channel. Since in the range \([0, 1]\), \( \log(x) \) goes to 0 faster than \(-x^{-1}\), an increase in \( h \) affects \( \delta \)-secrecy sum-capacity more than a similar increase in \( \delta \). This can be seen in Figures 2.2–2.4 which show the region \( \mathcal{G} \) for \( \delta = 0.01, 0.5, 1 \) and \( h = 0.1, 0.5, 0.9 \) for two users. When \( \delta \to 0 \), we are not concerned with secrecy, and the resulting region corresponds to the standard GMAC region, \([35]\). The region for \( \delta = 1 \) corresponds to the perfect secrecy region, that is, transmitting at rates within this region, it is possible to limit the rate of information leakage to the wire-tapper to arbitrarily small values. It is seen that relaxing the secrecy constraint may provide a larger region, the limit of which is the GMAC region. In addition, it is possible to send at capacity of the GMAC and still provide a non-zero level of secrecy, the minimum value of which depends on the level of degradedness, \( h \).

Especially when the degradedness is high, i.e., \( h \to 0 \), then we note that the achievable secrecy regions for \( \delta = 0.01 \) and \( \delta = 0.5 \) coincide with the GMAC region without secrecy constraint. Also shown in the figures are the regions achievable by the TDMA scheme described in the previous section. Although TDMA achieves the secrecy sum capacity with optimum time-sharing parameters, this region is in general contained within \( \mathcal{G}^C(\delta) \). Depending on \( h \) and \( \delta \), the TDMA region is sometimes a superset of \( \mathcal{G}^I(\delta) \), as observed in Figures 2.2, 2.3, sometimes a subset of \( \mathcal{G}^I(\delta) \), as seen in Figure 2.4 when \( \delta = 0.01 \) or \( \delta = 0.5 \), and sometimes the two regions can be used with time-sharing to enlarge the achievable region with individual constraints, see Figure 2.4 with \( \delta = 1 \). Close examination of these figures show that when the eavesdropper has a much worse channel, i.e., low \( h \), and the secrecy constraint \( \delta \) is small, then \( \mathcal{G}^I(\delta) \) gives a larger region. However, as we increase the secrecy constraint and the eavesdropper has a less noisy version of the intended receiver’s signal, the TDMA region becomes more dominant.

Another interesting note is that even when a user does not have any information to send, it can still generate and send random codewords to confuse the eavesdropper and help other users when considering the collective secrecy constraints. This can be seen in Figures 2.2–2.4 as the TDMA region does not end at the “legs” of \( \mathcal{G}^C(\delta) \) when \( \mathcal{G}^C(\delta) \) is not equal to the GMAC capacity region. In addition, as noted in \([9]\), the intended receiver decodes the codeword
Fig. 2.2: Regions for $P_1 = 10$, $P_2 = 5$, $\delta = \{0.01, 0.5, 1\}$ and $h = 0.1$
Fig. 2.3: Regions for $P_1 = 10$, $P_2 = 5$, $\delta = \{0.01, 0.5, 1\}$ and $h = 0.5$
Fig. 2.4: Regions for $P_1 = 10$, $P_2 = 5$, $\delta = \{0.01, 0.5, 1\}$ and $h = 0.9$
transmitted completely, and as such $\lfloor \frac{1}{3} \rfloor$ low-rate messages can be transmitted each in perfect secrecy by the users.

### 2.6 Conclusions and Future Work

This chapter examined secure communications in a multiple access environment in the presence of a wire-tapper. Defining the appropriate secrecy measures for this environment, we have found achievable secrecy rate regions, and established the secrecy sum-capacity of the degraded GMAC-WT.

A main contribution of this work is showing that the multiple-access nature of the channel can be utilized to improve the secrecy of the system. Allowing confidence in the secrecy of all users, the secrecy rate of a user may be increased since the undecoded messages of any set of users acts as additional noise at the wire-tapper and precludes him from decoding the remaining set of users. Our secrecy capacity results are based on the wire-tapper having access to a degraded version of the intended receiver’s signal.

These ideas are explored in detail in the follow-up work, [43], which is presented in the next chapter.
Chapter 3

The General Gaussian Multi-Access Wire-Tap Channel

3.1 Introduction

A rigorous analysis of information theoretic secrecy was first given by Shannon in [2]. In this work, Shannon showed that to achieve perfect secrecy in communications, which is equivalent to providing no information to an enemy cryptanalyst, the conditional probability of the message given a cryptogram must be independent of the actual transmitted message. In other words, the a posteriori probability of a message must be equivalent to its a priori probability.

In [8], Wyner applied this concept to the discrete memoryless channel. He defined the wire-tap channel, where there is a wire-tapper who has access to a degraded version of the intended receiver’s signal. Using the normalized conditional entropy $\Delta$, of the transmitted message given the received signal at the wire-tapper as the secrecy measure, he found the region of all possible $(R, \Delta)$ pairs, and the existence of a secrecy capacity, $C_s$, the rate up to which it is possible to limit the rate of information transmitted to the wire-tapper to arbitrarily small values.

In [9], it was shown that for Wyner’s wire-tap channel, it is possible to send several low-rate messages, each completely protected from the wire-tapper individually, and use the channel at close to the main channel capacity. However, if any of the messages are available to the wire-tapper, the secrecy of the rest may also be compromised. Reference [10] extended Wyner’s results in [8] and Carleial and Hellman’s results in [9] to Gaussian channels. The seminal work by Csiszár and Körner, [11], improved Wyner’s results to weaker, “less noisy” and “more capable” channels. Furthermore, it examined sending common information to both the receiver and the wire-tapper, while maintaining the secrecy of some private information that is communicated to the intended receiver only. Reference [16] suggested that the secrecy constraint developed by Wyner needed to be strengthened, since it constrains the rate of information leaked
to the wire-tapper, rather than the total information, and the information of interest might be
in this small amount. It was then shown that the results of [8, 11] can be extended to “strong”
secrecy constraints for discrete channels, where the limit is on the total leaked information rather
than just the rate, with no loss in achievable rates [16].

In the past two decades, common randomness has emerged as a valuable resource for
secret key generation, [12] and [13]. In [12], it was shown that the existence of a “public”
feedback channel can enable the two parties to be able to generate a secret key even when the
wire-tap capacity is zero. References [14] and [15] examined the secret key capacity and com-
mon randomness capacity, for several channels. These results also benefit from [16] to provide
“strong” secret key capacities. Maurer also examined the case of active adversaries, where the
wire-tapper has read/write access to the channel in [17]–[19]. The secret key generation prob-
lem was investigated from a multi-party point of view in [20] and [21]. Notably, Csiszár and
Narayan considered the case of multiple terminals where a number of terminals try to distill a
secret key and a subset of these terminals can act as helper terminals to the rest in [22], [23].

Recently, several new models have emerged, examining secrecy for parallel channels,
[24, 25], relay channels, [26], and fading channels, [27, 28]. Fading and parallel channels were
examined together in [29, 30]. Broadcast and interference channels with confidential messages
were considered in [31]. References [32, 33] examined a different multiple access channel with
confidential messages, where two transmitters try to keep their messages secret from each other
while communicating with a common receiver. In [32], an achievable region was found in gen-
eral, and the capacity region was found for some special cases. MIMO channels were considered
in [49, 50].

The capacity of the conventional multi-access channel was determined in [51, 52]. In
[39, 40, 38], we investigated multiple access channels, where transmitters communicate with
an intended receiver in the presence of an external wire-tapper from whom the messages must
be kept confidential. In these works, we considered the case where the wire-tapper gets a de-
graded version of a GMAC signal, and defined two separate secrecy measures extending Wyner’s
measure to multi-user channels to reflect the level of trust the network may have in each node.
Achievable rate regions were found for different secrecy constraints, and it was shown that the secrecy sum-capacity can be achieved using Gaussian codebooks and stochastic encoders. In addition, TDMA was shown to also achieve the secrecy sum-capacity.

In this chapter, we consider the General Gaussian Multiple Access Wire-Tap Channel (GGMAC-WT) and the Gaussian Two-Way Wire-Tap Channel (GTW-WT), both of which are of interest in wireless communications as they correspond to the case where a single physical channel is utilized by multiple transmitters, such as in an ad-hoc network. We consider an external eavesdropper\(^1\) that receives the transmitters’ signals through a general Gaussian multiple access channel (GGMAC) in both system models. We utilize a suitable secrecy constraint which is the normalized conditional entropy of the transmitted secret messages given the eavesdropper’s signal, corresponding to the “collective secrecy” constraints used in [38]. We show that satisfying this constraint implies the secrecy of the messages for all users. In both scenarios, transmitters are assumed to have one secret and one open message to transmit. This is different from [38] in that the secrecy rates are not constrained to be at least a fixed portion of the overall rates. We find an achievable secrecy rate region, where users can communicate with arbitrarily small probability of error with the intended receiver under perfect secrecy from the eavesdropper. We note that when we say perfect secrecy, we are referring to “weak” secrecy, where the rate of information leaked to the adversary is limited. We also find an upper bound on the secrecy sum-capacity, which is shown to coincide with the achievable secrecy sum-rate, giving the secrecy sum-capacity, for the special case of the degraded GGMAC-WT. We also find the sum-rate maximizing power allocations for the general case, which is more interesting from a practical point of view. It is seen that as long as the users are not single-user decodable at the eavesdropper, a secrecy-rate trade off is possible between the users. Next, we show that a non-transmitting user can help increase the secrecy capacity for a transmitting user by effectively “jamming” the eavesdropper, and even enable secret communications that would not be possible in a single-user scenario. We term this new scheme cooperative jamming.

\(^1\)Even though we faithfully follow Wyner’s terminology in naming the channels, admittedly in wireless system models, eavesdropper is a more appropriate term for the adversary.
The rest of this chapter is organized as follows: Section 3.2 describes the system model for the GGMAC-WT and the problem statement. Section 3.3 describes the general achievable rates for the GGMAC-WT. Sections 3.4 and 3.5 give the sum-secrecy rate maximizing power allocations, and the achievable rates with cooperative jamming. We present an upper bound to the GGMAC-WT secrecy sum-rate in Section 3.6. Section 3.7 gives our numerical results followed by our conclusions and future work in Section 3.8.

3.2 System Model and Problem Statement

We consider $K$ users communicating with an intended receiver in the presence of an eavesdropper who has the same capabilities. Each transmitter $k \in K \triangleq \{1, \ldots, K\}$ has two messages, $W_s^k$ which is secret and $W_o^k$ which is open, from two sets of equally likely messages $W_s^k = \{1, \ldots, M_{s}^k\}$, $W_o^k = \{1, \ldots, M_{o}^k\}$. Let $W_k = (W_s^k, W_o^k)$, $W_k = W_s^k \times W_o^k$, $M_k = M_{s}^k M_{o}^k$, $W_s^S = \{W_s^k\}_{k \in S}$, and $W_o^S = \{W_o^k\}_{k \in S}$. The messages are encoded using $(2^{nR_k}, n)$ codes into $\{\tilde{X}_k^{n_k}(W_k)\}$, where $R_k = \frac{1}{n} \log_2 M_k = \frac{1}{n} \log_2 M_{s}^k + \frac{1}{n} \log_2 M_{o}^k = R_s^k + R_o^k$. The encoded messages $\{\tilde{X}_k\} = \{\tilde{X}_k^{n_k}\}$ are then transmitted. We assume the channel parameters are universally known, including at the eavesdropper, and that the eavesdropper also has knowledge of the codebooks and the coding scheme. In other words, there is no shared secret. Both the main and the eavesdropper channels are modeled as Gaussian multiple-access channels as shown in Figure 3.1. The intended receiver and the wire-tapper get $\tilde{Y} = \tilde{Y}^n$ and $\tilde{Z} = \tilde{Z}^n$, respectively. The receiver decodes $\tilde{Y}$ to get an estimate of the transmitted messages, $\hat{W}_k^s$, $\hat{W}_k^o$. We would like to communicate with the receiver with arbitrarily low probability of error, while maintaining perfect secrecy of the secret messages, $\hat{W}_k^s$, at the eavesdropper. The signals at the intended receiver and the wiretapper are given by

$$\tilde{Y} = \sum_{k=1}^{K} \sqrt{\frac{1}{h_{k}^M}} \tilde{X}_k + \tilde{N}_M$$  \hspace{1cm} (3.1a)

\footnote{We would like to stress that open is not the same as public, i.e., we do not impose a decodability constraint for the open messages at the eavesdropper.}
\[ \tilde{Z} = \sum_{k=1}^{K} \sqrt{h_k^W} \tilde{X}_k + \tilde{N}_W \] (3.1b)

where \( \tilde{N}_M, \tilde{N}_W \) are the AWGN, \( \tilde{X}_k \) is the transmitted codeword of user \( k \), and \( h_k^M, h_k^W \) are the channel gains of user \( k \) to the intended receiver (main channel), and the eavesdropper (wire-tap channel), respectively. Each component of \( \tilde{N}_M \sim \mathcal{N} \left( 0, \sigma^2_M \right) \) and \( \tilde{N}_W \sim \mathcal{N} \left( 0, \sigma^2_W \right) \). We also assume the following transmit power constraints:

\[ \frac{1}{n} \sum_{i=1}^{n} \tilde{X}_{ki}^2 \leq \tilde{P}_k, \quad k = 1, \ldots, K \] (3.2)

Fig. 3.1: The standardized GMAC-WT system model.
Similar to the scaling transformation to obtain the standard form of the interference channel, [48], we can represent any GMAC-WT by an equivalent standard form, [38]:

\[ Y = \sum_{k=1}^{K} X_k + N_M \]  
\[ Z = \sum_{k=1}^{K} \sqrt{h_k} X_k + N_W \]

where, for each \( k \),

- the original codewords are scaled to get \( X_k = \sqrt{\frac{h_k}{\sigma^2_M}} \tilde{X}_k \);
- The new maximum power constraints are \( \tilde{P}_k = \frac{h_M}{\sigma^2_M} \tilde{P}_k \);
- The wiretapper’s new channel gains are \( h_k = \frac{h_k W^2}{h^2 W^2_M} \);
- The noises are normalized by \( N_M = \frac{\tilde{N}_M}{\sigma^2_M} \) and \( N_W = \frac{\tilde{N}_W}{\sigma^2_W} \).

We can show that the eavesdropper gets a stochastically degraded version of the receiver’s signal if \( h_1 = \ldots = h_K \equiv h < 1 \). We considered this special case in [40, 38].

### 3.2.1 Preliminary Definitions

In this section, we present some useful preliminary definitions including the secrecy constraint we will use. In particular, the secrecy constraint we used is the “collective constraint” we defined in [39, 38], and is suitable for the multi-access nature of the systems of interest since it aims to provide secrecy for the terminals collectively.

**Definition 3.1 (Secrecy Constraint).** We use the normalized joint conditional entropy of the transmitted messages given the eavesdropper’s received signal as our secrecy constraint, i.e.,

\[ \Delta S \triangleq \frac{H(W_s^S|Z)}{H(W_s^S)} \]  

(3.4)
for any set $S \subseteq K$ of users. For perfect secrecy of all transmitted secret messages, we would like

$$\Delta_K = \frac{H(W_K^S|Z)}{H(W_K^S)} \to 1.$$  \hfill (3.5)

Assume $\Delta_K \geq 1 - \epsilon$ for some arbitrarily small $\epsilon$ as required. Then,

$$H(W_K^S|Z) \geq H(W_K^S) - \epsilon H(W_K^S)$$  \hfill (3.6)

$$H(W_S^S|Z) \geq H(W_S^S) + H(W_{Sc}^S|W_S^S) - \epsilon H(W_K^S) - H(W_{Sc}^S|W_S^S, Z)$$  \hfill (3.7)

$$\geq H(W_S^S) - \epsilon H(W_K^S)$$  \hfill (3.8)

$$\Delta_S \geq 1 - \epsilon'$$  \hfill (3.9)

where $\epsilon' \triangleq \frac{H(W_K^S)}{H(W_S^S)} \epsilon \to 0$ as $\epsilon \to 0$. If $H(W_S^S) = 0$, then we define $\Delta_S = 1$. Thus, the perfect secrecy of the system implies the perfect secrecy of any group of users, guaranteeing that when the system is secure, so is each individual user.

**Definition 3.2 (Achievable Rates).** Let $R_k = (R_k^s, R_k^o)$. We say that the rate vector $R = (R_1, \ldots, R_K)$ is said to be achievable if for any $\epsilon > 0$ there exists a code of sufficient length $n$ such that

$$\frac{1}{n} \log M_k^s \geq R_k^s - \epsilon, \quad k = 1, \ldots, K$$  \hfill (3.10a)

$$\frac{1}{n} \log M_k^o \geq R_k^o - \epsilon, \quad k = 1, \ldots, K$$  \hfill (3.10b)

and

$$P_e = \frac{1}{\prod_{k=1}^{K} M_k} \sum_{W \in \times_{k=1}^{K} W_k} \mathbb{P}\{\hat{W} \neq W|W \text{ sent}\} \leq \epsilon$$  \hfill (3.10c)
is the average probability of error. In addition, we need
\[ \Delta_K \geq 1 - \epsilon \]  
(3.10d)

where \( \Delta_K \) denotes our secrecy constraint and is defined in (3.5). We will call the set of all achievable rates, the secrecy-capacity region, and denote it \( C^{MA} \) for the GGMAC-WT, and \( C^{TW} \) for the GTW-WT, respectively.

Before we state our results, we define the following notation which will be used extensively in the rest of this chapter:

\[ [\xi]^+ \triangleq \max [\xi, 0] \]  
(3.11)

\[ C^M_S(P) \triangleq \frac{1}{2} \log \left( 1 + \sum_{k \in S} P_k \right), \quad S \subseteq K \]  
(3.12)

\[ C^W_S(P) \triangleq \frac{1}{2} \log \left( 1 + \sum_{k \in S} h_k P_k \right), \quad S \subseteq K \]  
(3.13)

\[ \tilde{C}^W_S(P) \triangleq \frac{1}{2} \log \left( 1 + \frac{\sum_{k \in S} h_k P_k}{1 + \sum_{k \in S} c h_k P_k} \right), \quad S \subseteq K \]  
(3.14)

\[ \mathcal{P} \triangleq \{ P : 0 \leq P_k \leq \bar{P}_k, \forall k \} \]  
(3.15)

\[ \bar{P} \triangleq \{ \bar{P}_1, \ldots, \bar{P}_K \} \]  
(3.16)

Lastly, we informally call a user \( k \) strong if \( h_k \leq 1 \), and weak if \( h_k > 1 \). This is a way of indicating whether the intended receiver or the wiretapper is at a more of an advantage concerning that user, and is equivalent to stating whether the single-user secrecy capacity of that user is positive or zero. We later extend this concept to refer to users who can achieve positive secrecy rates and those who cannot. In addition, we will say that a user is single-user decodable by the eavesdropper if its rate is such that its transmitted message can be decoded by the eavesdropper by treating the other users as noise. A user group \( S \) is single-user decodable by the eavesdropper if \( C^M_S(P) \leq \tilde{C}^W_S(P) \). Our achievable scheme cannot guarantee secrecy for such a group of users.
3.3 Achievable Secrecy Rate Regions

In this section, we present our main results for the GGMAC-WT. We first define two separate regions and then give an achievable region:

**Definition 3.3 (GGMAC-WT Superposition Region, \(G_{\text{MA-S}}\)).** First define the following rate region

\[
G_{\text{MA-S}}(P) \triangleq \left\{ \begin{array}{l}
R : \\
\sum_{k \in S} \left( R^s_k + R^o_k \right) \leq I(X_S; Y | X_{Sc}), \quad \forall S \subseteq \mathcal{K} \\
\sum_{k \in S} R^s_k \leq \left[ I(X_S; Y | X_{Sc}) - I(X_S; Z) \right]^+, \quad \forall S \subseteq \mathcal{K}
\end{array} \right\}
\] (3.17)

Let \( X_k \sim \mathcal{N}(0, P_k) \) for all \( k \). Then, the superposition region, \( G_{\text{MA-S}} \), is given by evaluating the above expression to get

\[
G_{\text{MA-S}}(P) = \left\{ \begin{array}{l}
R : \\
\sum_{k \in S} \left( R^s_k + R^o_k \right) \leq \frac{1}{2} \log \left( 1 + \sum_{k \in S} P_k \right), \quad \forall S \subseteq \mathcal{K} \\
\sum_{k \in S} R^s_k \leq \frac{1}{2} \left[ \log \left( 1 + \sum_{k \in S} P_k \right) - \log \left( 1 + \sum_{k \in S} h_k P_k \right) \right] + , \quad \forall S \subseteq \mathcal{K}
\end{array} \right\}
\] (3.18)

or in short, using (3.12)–(3.14).

\[
G_{\text{MA-S}}(P) = \left\{ \begin{array}{l}
R : \\
\sum_{k \in S} \left( R^s_k + R^o_k \right) \leq C^M_S(P), \quad \forall S \subseteq \mathcal{K} \\
\sum_{k \in S} R^s_k \leq \left[ C^M_S(P) - \tilde{C}^W_S(P) \right]^+, \quad \forall S \subseteq \mathcal{K}
\end{array} \right\}
\] (3.19)

**Definition 3.4 (GGMAC-WT TDMA Region, \(G_{\text{MA-T}}\)).** Let \( \{\alpha_k\} \) be such that \( 0 \leq \alpha_k \leq 1 \) for all \( k \) and \( \sum_{k=1}^{K} \alpha_k = 1 \). Then, the TDMA region, \( G_{\text{MA-T}} \), is given by

\[
G_{\text{MA-T}}(P, \alpha) \triangleq \left\{ \begin{array}{l}
R : \\
P_k^s + R_k^o \leq \alpha_k I(X_k; Y | X_{kc}), \quad \forall k \in \mathcal{K} \\
R_k^s \leq \alpha_k \left[ I(X_k; Y | X_{kc}) - I(X_k; Z | X_{kc}) \right]^+, \quad \forall k \in \mathcal{K}
\end{array} \right\}
\] (3.20)
which, when $X_k \sim \mathcal{N}(0, P_k/\alpha_k)$ for all $k$, becomes

$$G_{\text{MA-T}}(P, \alpha) \triangleq \left\{ \begin{array}{l} \mathbb{R}: \quad R^s_k + R^o_k \leq \frac{\alpha_k}{2} \log \left( 1 + \frac{P_k}{\alpha_k} \right), \quad \forall k \in \mathcal{K} \\ R^s_k \leq \frac{\alpha_k}{2} \left[ \log \left( 1 + \frac{P_k}{\alpha_k} \right) - \log \left( 1 + \frac{h_k P_k}{\alpha_k} \right) \right]^+, \quad \forall k \in \mathcal{K} \end{array} \right\} \quad (3.21)$$

or, in accordance with the definitions in (3.12)–(3.14),

$$G_{\text{MA-T}}(P, \alpha) = \left\{ \begin{array}{l} \mathbb{R}: \quad R^s_k + R^o_k \leq \alpha_k \frac{C^M_k \left( \frac{P_k}{\alpha_k} \right)}{C^W_k \left( \frac{P_k}{\alpha_k} \right)}), \quad \forall k \in \mathcal{K} \\ R^s_k \leq \alpha_k \left[ C^M_k \left( \frac{P_k}{\alpha_k} \right) - C^W_k \left( \frac{P_k}{\alpha_k} \right) \right]^+, \quad \forall k \in \mathcal{K} \end{array} \right\} \quad (3.22)$$

**Theorem 3.1.** The rate region given below is achievable for the GGMAC-WT:

$$G^\text{MA} = \text{convex closure of} \left( \bigcup_{P \in \mathcal{P}} G^\text{MA-S}(P) \right) \bigcup \left( \bigcup_{0 \leq \alpha \leq 1} \bigcup_{\sum_k \alpha_k = 1} G^\text{MA-T}(\bar{P}, \alpha) \right) \quad (3.23)$$

**Proof.** We first show that the superposition encoding rate region given in (3.18) for a fixed power allocation is achievable. Consider the following coding scheme for rates $R \in G^\text{MA-S}(P)$ for some $P \in \mathcal{P}$:

**Superposition Encoding Scheme:** For each user $k$, consider the following scheme:

1. Generate 3 codebooks $\mathcal{X}^s_k$, $\mathcal{X}^o_k$ and $\mathcal{X}^x_k$. $\mathcal{X}^s_k$ consists of $M^s_k$ codewords, each component of which is drawn from $\mathcal{N} \left( 0, \lambda^s_k P_k - \varepsilon \right)$. Codebook $\mathcal{X}^o_k$ has $M^o_k$ codewords with each component randomly drawn from $\mathcal{N} \left( 0, \lambda^o_k P_k - \varepsilon \right)$ and $\mathcal{X}^x_k$ has $M^x_k$ codewords with each component randomly drawn from $\mathcal{N} \left( 0, \lambda^x_k P_k - \varepsilon \right)$ where $\varepsilon$ is an arbitrarily small number to ensure that the power constraints on the codewords are satisfied with high probability and $\lambda^s_k + \lambda^o_k + \lambda^x_k = 1$. Define $R^s_k = \frac{1}{n} \log M^s_k$ and $M^s_k = M^s_k M^o_k M^x_k$.

2. To transmit message $W_k = (W^s_k, W^o_k) \in \mathcal{W}^s_k \times \mathcal{W}^o_k$, user $k$ finds the 2 codewords corresponding to components of $W_k$ and also uniformly chooses a codeword $W^x_k$ from
User $k$ then adds all these codewords and transmits the resulting codeword, $X_k$, so that it actually transmits one of $M_k^t$ codewords. Let $R_k^t = \frac{1}{n} \log M_k^t = R_k^o + R_k^s + R_k^x$. Note that since all codewords are chosen uniformly, user $k$ essentially transmits one of $M_k^o M_k^x$ codewords at random for each message $W_k^s$, and its overall rate of transmission is $R_k^t$.

Specifically, we choose the rates to satisfy

$$
\sum_{k \in S} \left( R_k^s + R_k^o + R_k^x \right) \leq \frac{1}{2} \log \left( 1 + \sum_{k \in S} P_k \right), \quad \forall S \subseteq \mathcal{K}
$$

(3.24)

$$
\sum_{k \in S} \left( R_k^o + R_k^x \right) \leq \frac{1}{2} \log \left( 1 + \sum_{k \in S} h_k P_k \right), \quad \forall S \subseteq \mathcal{K}, \text{ with equality if } S = \mathcal{K}
$$

(3.25)

$$
\sum_{k \in S} R_k^s \leq \frac{1}{2} \left[ \log \left( 1 + \sum_{k \in S} P_k \right) - \log \left( 1 + \frac{\sum_{k \in S} h_k P_k}{1 + \sum_{k \in S^c} h_k P_k} \right) \right]^+, \quad \forall S \subseteq \mathcal{K}
$$

(3.26)

which we can also write as:

$$
\sum_{k \in S} \left( R_k^s + R_k^o + R_k^x \right) \leq C^M_S, \quad \forall S \subseteq \mathcal{K}
$$

(3.27)

$$
\sum_{k \in S} \left( R_k^o + R_k^x \right) \leq C^W_S, \quad \forall S \subseteq \mathcal{K}, \text{ with equality if } S = \mathcal{K}
$$

(3.28)

$$
\sum_{k \in S} R_k^s \leq \left[ C^M_S - \tilde{C}^W_S \right]^+, \quad \forall S \subseteq \mathcal{K}.
$$

(3.29)

Note that if (3.29) is zero for a group of users, we cannot achieve secrecy for those users.

When $S = \mathcal{K}$, if the sum-capacity of the main channel is less than that of the eavesdropper channel, i.e., $C^M_\mathcal{K} \leq C^W_\mathcal{K}$, secrecy is not possible for the system. Assume this quantity is positive.

To ensure that we can mutually satisfy both (3.29), (3.28), we can reclassify some open messages as secret. Clearly, if we can guarantee secrecy for a larger set of messages, secrecy is achieved for the original messages.

From the first set of conditions in (3.23) and the GMAC coding theorem, [35], with high probability the receiver can decode the codewords with low probability of error by looking for the jointly typical $\{X_k\}_{k=1}^K, Y$. To show the secrecy condition in (3.10), first note
that the coding scheme described is equivalent to each user $k$ selecting one of $M^s_k$ messages, and sending a uniformly chosen codeword from among $M^0_k M^x_k$ codewords for each. Define $X_\Sigma = \sum_{k=1}^K \sqrt{h_k} X_k$, and we have

\begin{align}
H(W^s_{K_c}|Z) &= H(W^s_{K_c}) - I(W^s_{K_c}; Z) \\
&= H(W^s_{K_c}) - I(W^s_{K_c}; Z) + I(W^s_{K_c}; Z|X_\Sigma) \\
&= H(W^s_{K_c}) - h(Z) + h(Z|W^s_{K_c}) + h(Z|X_\Sigma) - h(Z|W^s_{K_c}, X_\Sigma) \\
&= H(W^s_{K_c}) - I(X_\Sigma; Z) + I(X_\Sigma; Z|W^s_{K_c})
\end{align}

(3.30)

where we used $W^s_{K_c} \rightarrow X_\Sigma \rightarrow Z$, and thus we have $h(Z|W^s_{K_c}, X_\Sigma) = h(Z|X_\Sigma)$ to get (3.33). We will consider the two terms individually. First, we have the trivial bound due to channel capacity:

$$I(X_\Sigma; Z) \leq n C^W_{K_c} (P)$$

(3.34)

Now write

$$I(X_\Sigma; Z|W^s_{K_c}) = H(X_\Sigma|W^s_{K_c}) - H(X_\Sigma|W^s_{K_c}, Z)$$

(3.35)

Since user $k$ independently sends one of $M^0_k M^x_k$ codewords equally likely for each secret message,

\begin{align}
H(X_\Sigma|W^s_{K_c}) &= \log \left( \prod_{k=1}^K (M^0_k M^x_k) \right) \\
&= n \left( \sum_{k=1}^K (R^0_k + R^x_k) \right) \\
&= n C^W_{K_c} (P).
\end{align}

(3.36)

(3.37)

(3.38)

We can also write

$$H(X_\Sigma|W^s_{K_c}, Z) \leq n \delta_n$$

(3.39)
where $\delta_n \to 0$ as $n \to \infty$ since, with high probability, the eavesdropper can decode $X_\Sigma$ given $W^s_K$, due to (3.28) and code generation. Using (3.34), (3.35), (3.38) and (3.39) in (3.33), we get

$$H(W^s_K|Z) \geq H(W^s_K) - nC^W_K(P) + nC^W_K(P) - n\delta_n$$

$$= H(W^s_K) - n\delta_n.$$  \hfill (3.41)

Now, let us consider the TDMA region given in (3.21). This region is obtained when users who can achieve single-user secrecy use a single-user wire-tap code as in [10] in a TDMA schedule, where the time-share of each user $k$ is given by $0 \leq \alpha_k \leq 1$ and $\sum_{k=1}^{K} \alpha_k = 1$. A transmitter $k$ who can achieve secrecy, i.e., having $h_k < 1$, transmits for $\alpha_k$ portion of the time when all other users are silent, using $\frac{P_k}{\alpha_k}$ power, satisfying its average power constraint over the TDMA time-frame. This approach was used in [38] to achieve secrecy sum-capacity for individual constraints. When the channel is degraded, i.e., $h_k = h$ for all $k \in K$, then for collective constraints the TDMA region is seen to be a subset of the superposition region. However, this is not necessarily true for the general case, and by time-sharing between the two schemes we can generally achieve a larger achievable region, given in (3.23).

We remark that it is possible to further divide the “open” messages to get more sets of “private” messages which are also perfectly secret, i.e., if we let $\mathcal{V}^o_k = \mathcal{V}^s_k \times \mathcal{V}^o_k$, then as long as we impose the same restrictions on $\mathcal{R}^s_k$ as $\mathcal{R}^o_k$, we can achieve perfect secrecy of $\mathcal{W}^s_k$, as in [10]. However, this does not mean that we have perfect secrecy at channel capacity, as the secrecy sub-codes carry information about each other.

Observe that even for $K = 2$ users, a rate point in this region is four dimensional, and hence cannot be accurately drawn. We can instead focus on the secrecy rate region, the region of all achievable $\mathcal{R}^s$. The sub-regions $G^{MA-S}$, $G^{MA-T}$ are shown for different channel gains in Figure 3.2 for fixed transmit powers, and $K = 2$ users. Figure 3.3 represents how these regions change with different transmit powers when the channel gains are fixed. For the case shown, we need the convex hull operation, as the achievable region is a combination of different superposition and TDMA regions. Note also that the main extra condition for the superposition
region is on the total extra randomness added. As a result, it is possible for “stronger” users to help “weak” users by contributing more to the necessary extra number of codewords, which is the sum-capacity of the eavesdropper. Such a weak user only has to make sure that it is not single-user decodable, provided the stronger users are willing to sacrifice some of their own rate and generate more superfluous codewords. In other words, we see that users in a set $\mathcal{S}$ are further protected from the eavesdropper by the fact that users in set $\mathcal{S}^c$ are also undecodable, compared to the single-user case. The TDMA region, on the other hand, does not allow users to help each other this way. As such, only users whose channel gains allow them to achieve secrecy on their own are allowed to transmit.

For the special degraded case of $h_1 = \ldots = h_K \triangleq h \leq 1$, the perfect secrecy rate region for $R_k^s$ becomes the region given by [38, Theorem 1] for $\delta = 1$. We also observe that even though there is a limit on the secrecy sum-rate achieved by our scheme, it is possible to send open messages to the intended receiver at rates such that the sum of the secrecy rate and open rate for all users is in the capacity region of the MAC channel to the intended receiver. Even though we cannot send at capacity with secrecy, the codewords used to confuse the eavesdropper may be used to communicate meaningful information to the intended receiver.

### 3.4 Maximization of Sum Rate

The achievable region given in Theorem 3.1 depends on the transmit powers. We are, thus, naturally interested in the power allocation $\mathbf{P}^*$ that would maximize the total secrecy sum-rate. Recall that the standardized channel gain for user $k$ is $h_k = \frac{h_k W \sigma^2 M}{h_k W \sigma^2}$, and that the higher $h_k$ is, the better the corresponding eavesdropper channel. Without loss of generality, assume that users are ordered in terms of increasing standardized eavesdropper channel gains, i.e., $h_1 \leq \ldots \leq h_K$. Note that, we only need to concern ourselves with the case $h_1 < \ldots < h_K$, since we can combine users with the same channel gains into one super-user. We can then split the resulting optimum power allocation for a super-user among the actual constituting users in any way we choose, since they would all result in the same sum-rate. In addition, from a
physical point of view, assuming that the channel parameters are drawn according to a continuous
distribution and then fixed, the probability that two users would have the same exact standardized
channel gain is zero.

We first examine the superposition region given in (3.18). The secrecy sum-rate achievable with superposition coding for the GGMAC-WT was given in Theorem 3.1 as

$$R_{\text{sum}}^{\text{MA-S}} = \frac{1}{2} \left[ \log \left(1 + \sum_{k=1}^{K} P_k\right) - \log \left(1 + \sum_{k=1}^{K} h_k P_k\right) \right]^+$$

(3.42)

and we would like to find the power allocation that maximizes this quantity. Stated formally, we
are interested in the transmit powers that solve the following optimization problem:

$$\max_{P \in \mathcal{P}} \frac{1}{2} \log \left(1 + \sum_{k=1}^{K} P_k\right) - \frac{1}{2} \log \left(1 + \sum_{k=1}^{K} h_k P_k\right) = \min_{P \in \mathcal{P}} \frac{1}{2} \log \phi_{\mathcal{K}}(P)$$

(3.43)

$$\equiv \min_{P \in \mathcal{P}} \phi_{\mathcal{K}}(P)$$

(3.44)

where

$$\phi_{\mathcal{S}}(P) \triangleq \frac{1 + \sum_{k \in \mathcal{S}} h_k P_k}{1 + \sum_{k \in \mathcal{S}} P_k}, \quad \mathcal{S} \subseteq \mathcal{K}$$

(3.45)

and $\mathcal{S} = \mathcal{K}$ yields (3.44). In obtaining (3.44), we simply used the monotonicity of the $\log$
function. The solution to this problem is given below:

**Theorem 3.2.** The secrecy sum-rate maximizing power allocation for $G^{\text{MA-S}}$ satisfies $P_k^* = \bar{P}_k$ if $k \leq T$ and $P_k^* = 0$ if $k > T$ where $T \in \{1, \ldots, K\}$ is some limiting user satisfying

$$h_T < \frac{1 + \sum_{k=1}^{T} h_k \bar{P}_k}{1 + \sum_{k=1}^{T} \bar{P}_k} \leq h_{T+1}$$

(3.46)

and if this cannot be satisfied $T = 1$, we cannot achieve secrecy. Note that this allocation shows
that only a *subset of the strong users* must be transmitting.
PROOF. The problem is formally stated as:

\[
\min_{\mathbf{P}} \phi_{\mathcal{K}}(\mathbf{P}) \quad \text{s. t.} \quad 0 \leq P_k \leq \bar{P}_k, \forall k
\]  

(3.47)

We start with writing the Lagrangian to be minimized:

\[
\mathcal{L}(\mathbf{P}, \boldsymbol{\mu}) = \phi_{\mathcal{K}}(\mathbf{P}) - \sum_{k=1}^{K} \mu_1 k P_k + \sum_{k=1}^{K} \mu_2 k (P_k - \bar{P}_k)
\]  

(3.48)

Equating the derivative of the Lagrangian to zero, we get

\[
\frac{\partial \mathcal{L}(\mathbf{P}^*, \boldsymbol{\mu})}{\partial P_j^*} = \phi_{\mathcal{K}}'(\mathbf{P}^*) - \mu_1 j + \mu_2 j = 0
\]  

(3.49)

where we define

\[
\phi_{\mathcal{S}}'(\mathbf{P}) \triangleq \frac{\partial \phi_{\mathcal{S}}(\mathbf{P})}{\partial P_j} = \frac{h_j - \phi_{\mathcal{S}}(\mathbf{P})}{1 + \sum_{k\in\mathcal{S}} P_k}
\]  

(3.50)

for any set \( \mathcal{S} \subseteq \mathcal{K} \).

It is easy to see that if \( h_j > \phi_{\mathcal{K}}(\mathbf{P}^*) \), then \( \mu_1 j > 0 \), and we have \( P_j^* = \bar{P}_j \). If \( h_j < \phi_{\mathcal{K}}(\mathbf{P}^*) \), then we similarly find that \( P_j^* = 0 \). Finally, if \( h_j = \phi_{\mathcal{K}}(\mathbf{P}^*) \), then we also have

\[
h_j = \frac{1 + \sum_{k\in\mathcal{K}\setminus j} h_k P_k^*}{1 + \sum_{k\in\mathcal{K}\setminus j} h_k P_k^*}
\]  

(3.51)

and \( \phi_{\mathcal{K}}(\mathbf{P}^*) = \phi_{\mathcal{K}\setminus j}(\mathbf{P}^*) \) does not depend on \( P_j \), so we can set \( P_j^* = 0 \) with no effect on the secrecy sum-rate. Thus, we have \( P_j^* = \bar{P}_j \) if \( h_j < \phi_{\mathcal{K}}(\mathbf{P}^*) \), and \( P_j^* = 0 \) if \( h_j \geq \phi_{\mathcal{K}}(\mathbf{P}^*) \). Then, the optimal set of transmitters is of the form \( \mathcal{T} = \{1, \ldots, T\} \) since if a user \( T \) is transmitting, all users such that \( h_k < h_T \) must also be transmitting. We also note that \( \phi_{\mathcal{K}}(\mathbf{P}^*) = \phi_{\mathcal{T}}(\mathbf{P}) \). Let \( T \) be the last user satisfying this property, i.e. \( h_T < \phi_{\mathcal{T}}(\mathbf{P}) \) and
\[ h_{T+1} \geq \phi_{T \cup \{T+1\}}(\bar{P}). \] Note that

\[ h_T < \frac{1 + \sum_{k=1}^{T} h_k \bar{P}_k}{1 + \sum_{k=1}^{T} \bar{P}_k} = \frac{1 + \sum_{k=1}^{T-1} h_k \bar{P}_k + h_T \bar{P}_T}{1 + \sum_{k=1}^{T-1} \bar{P}_k + \bar{P}_T}. \] (3.52)

\[ h_{T-1} < h_T < \frac{1 + \sum_{k=1}^{T-1} h_k \bar{P}_k}{1 + \sum_{k=1}^{T-1} \bar{P}_k} = \phi_{T \setminus \{T\}}(P). \] (3.53)

In other words, all sets \( S = \{1, \ldots, S\} \) for \( S \leq T \) also satisfy this property, and are viable candidates for the optimal set of transmitting users. Therefore, we can claim that \( T \) is the optimum set of transmitting users, since from above we can iteratively see that \( \phi_T(\bar{P}) < \phi_S(\bar{P}) \) for all \( S < T \).

Note that, for the special case of \( K = 2 \) users, the optimum power allocation is

\[
(P_1^*, P_2^*) = \begin{cases} 
(\bar{P}_1, \bar{P}_2), & \text{if } h_1 < 1, \ h_2 < \frac{1 + h_1 \bar{P}_1}{1 + \bar{P}_1} \\
(\bar{P}_1, 0), & \text{if } h_1 < 1, \ h_2 \geq \frac{1 + h_1 \bar{P}_1}{1 + \bar{P}_1} \\
(0, 0), & \text{otherwise}
\end{cases}
\] (3.54)

We also need to consider the TDMA region. In this case, the maximum achievable secrecy sum-rate is:

\[
0 \leq \alpha \leq 1: \max_{\alpha_k} \sum_{k=1}^{K} \alpha_k \neq 1 \left\{ \log \left(1 + \frac{\bar{P}_k}{\alpha_k} \right) - \log \left(1 + \frac{h_k \bar{P}_k}{\alpha_k} \right) \right\} \] (3.55)

This is a simple complex optimization problem that can easily be solved numerically. For the degraded case, we can obtain a closed form solution: \( \alpha_k = \frac{\bar{P}_k}{\sum_k \bar{P}_k} \) as in [38]. In general, we cannot obtain such a solution. However, it is trivial to note that users with \( h_k \geq 1 \) should not be transmitting in this scheme. The secrecy sum-rate is then the maximum of the solutions given by the superposition and TDMA regions.
3.5 Secrecy Through Cooperative Jamming

In the previous section, we found the secrecy sum-rate maximizing power allocations. We saw that if the eavesdropper is not “disadvantaged enough” for some users, then these users’ transmit powers are set to zero. We posit that such a user may be able to “help” a transmitting user, since it can cause more harm to the eavesdropper than to the intended receiver. We only consider the superposition region, since in the TDMA region a user has a dedicated time-slot, and hence does not affect the others. We will next show that this type of cooperative behavior is indeed useful, notably exploiting the fact that the established achievable secrecy sum-rate is a difference of the sum-capacity expressions for the intended channel(s) and the eavesdropper’s channel. As a result, reducing the latter more than the former actually results in an increase in the achievable secrecy sum-rate.

Formally, the scheme we are considering implies partitioning the set of users, \( \mathcal{K} \) into a set of transmitting users, \( T \) and a set of jamming users \( T^c = \mathcal{K} - T \). If a user \( k \) is jamming, then it transmits \( X_k \sim \mathcal{N}(P_k^x I, 0) \) instead of codewords. In this case, we can show that we can achieve higher secrecy rates when the “weaker” users are jamming. Once again, without loss of generality, we consider \( h_1 < \ldots < h_K \). In addition, we will assume that a user can either take the action of transmitting its information or jamming the eavesdropper, but not both. It is readily shown below that we do not lose any generality by doing so, and that splitting the power of a user between the two actions is suboptimal from the secrecy sum-rate maximization point of view.

The problem is then formally presented below:

\[
\max_{T \subseteq \mathcal{K}, P \in \mathcal{P}} \frac{1}{2} \log \left( 1 + \frac{\sum_{k \in T} P_k}{1 + \sum_{k \in T^c} P_k} \right) - \frac{1}{2} \log \left( 1 + \frac{\sum_{k \in T} h_k P_k}{1 + \sum_{k \in T^c} h_k P_k} \right) \quad (3.56)
\]

\[
\equiv \min_{T \subseteq \mathcal{K}, P \in \mathcal{P}} \frac{\phi_T(P)}{\phi_{T^c}(P)} \quad (3.57)
\]

\[
\phi_T(P) = \frac{1}{2} \log \left( 1 + \frac{\sum_{k \in T} P_k}{1 + \sum_{k \in T^c} P_k} \right)
\]

\[
\phi_{T^c}(P) = \frac{1}{2} \log \left( 1 + \frac{\sum_{k \in T^c} h_k P_k}{1 + \sum_{k \in T^c} h_k P_k} \right)
\]
where we recall that $\phi_{S}(P)$ is given by (3.45), such that

$$
\phi_{K}(P) = \frac{1 + \sum_{k \in K} h_k P_k}{1 + \sum_{k \in K} P_k},
$$

(3.58)

$$
\phi_{T_c}(P) = 1 + \frac{\sum_{k \in T_c} h_k P_k}{1 + \sum_{k \in T_c} P_k},
$$

(3.59)

To see that we are not losing generality by letting a user split its power among jamming and transmitting, it is sufficient to note that regardless of how a user splits its power, $\phi_{K}(P)$ will be the same, and the user only affects $\phi_{T_c}(P)$. Assume the optimum solution is such that user $j$ splits its power, so $j \in T$ and $j \in T_c$. Then, it is easy to see that if $h_j < \phi_{T_c}(P^*)$, the sum-rate is increased when that user uses its jamming power to transmit, and when $h_j > \phi_{T_c}(P^*)$, the sum-rate is increased when the user uses its transmit power to jam. When $h_j = \phi_{T_c}(P^*)$, then regardless of how its power is split, the sum-rate is the same, and we can assume user $j$ either transmits or jams.

Note that we must have $\phi_{K}(P) \leq \phi_{T_c}(P)$ to have a non-zero secrecy sum-rate, and $\phi_{T_c}(P) > 1$, as otherwise it would be better to stop jamming. This scheme can be shown to achieve the following secrecy sum-rate:

**Theorem 3.3.** The secrecy sum-rate using cooperative jamming is

$$
R_{S-CJ}^{\text{sum}} = \frac{1}{2} \log \left( 1 + \frac{\sum_{k \in T} P_k^*}{1 + \sum_{k \in T_c} P_k^*} \right) - \frac{1}{2} \log \left( 1 + \frac{\sum_{k \in T} h_k P_k^*}{1 + \sum_{k \in T_c} h_k P_k^*} \right),
$$

(3.60)

where $T$ is the set of transmitters and the optimum power allocation is of the form

$$
\begin{align*}
\{1, \ldots, T, T + 1, \ldots, J - 1, J, J + 1, \ldots, K\} \\
\begin{array}{c}
\{P_k^* = P_k\} \\
\{P_k^* = 0\} \\
\{P_j^* = P_k\} \\
\end{array}
\end{align*}
$$

transmitting, i.e., $\in T$

jamming, i.e., $\in T_c$

with

$$
P_j^* = \min \left\{ P_j, \frac{-c_2 + \sqrt{c_2^2 - 4c_1 c_3}}{2c_1} \right\}^+
$$

(3.61)
and

\[ c_1 = h_J \left( h_J \sum_{k \in T} P_k^* - \sum_{k \in T} h_k P_k^* \right) \] (3.62)

\[ c_2 = h_J \left( 2 + \sum_{k \in K \setminus J} h_k P_k^* + \sum_{k \in T \setminus J} h_k P_k^* \right) \sum_{k \in T} P_k^* \]

\[ - h_J \left( 2 + \sum_{k \in K \setminus J} P_k^* + \sum_{k \in T \setminus J} P_k^* \right) \sum_{k \in T} h_k P_k^* \] (3.63)

\[ c_3 = \left( 1 + \sum_{k \in K \setminus J} h_k P_k^* \right) \left( 1 + \sum_{k \in T \setminus J} h_k P_k^* \right) \sum_{k \in T} P_k^* \]

\[ - h_J \left( 1 + \sum_{k \in K \setminus J} P_k^* \right) \left( 1 + \sum_{k \in T \setminus J} P_k^* \right) \sum_{k \in T} h_k P_k^* \] (3.64)

whenever the positive real root exists, and 0 otherwise.

**Proof.** We first solve the subproblem of finding the optimal power allocation for a set of given transmitters, \( T \). The solution to this will also give us insight into the structure of the optimal set of transmitters, \( T^* \). Without loss of generality, we also assume that for all \( k \in T^c \), i.e., all jamming users, we have \( P_k^* > 0 \), since we can always move a user who is jamming with zero power to the transmitter set and achieve the same secrecy sum-rate. Formally put, the problem is:

\[
\min_{P} \frac{\phi_K(P)}{\phi_{T^c}(P)} \quad \text{s. t.} \quad 0 \leq P_k \leq \bar{P}_k, \ \forall k
\] (3.65)

We start with writing the Lagrangian:

\[
\mathcal{L}(P, \mu) = \frac{\phi_K(P)}{\phi_{T^c}(P)} - \sum_{k=1}^{K} \mu_{1k} P_k + \sum_{k=1}^{K} \mu_{2k} (P_k - \bar{P}_k)
\] (3.66)
The derivative of the Lagrangian depends on the user:

$$\frac{\partial \mathcal{L}(P^*, \mu)}{\partial P^*_j} = 0 = \begin{cases} \frac{\dot{\phi}_K(P^*) - \mu_1 j + \mu_2 j}{\phi_T(P^*)} & \text{if } j \in T \\
\frac{\dot{\phi}_K(P^*)}{\phi_T(P^*)} & \text{if } j \in T^c \end{cases}$$ (3.67)

since a user $j \in T^c$ satisfies $P^*_j > 0$, it must have $\mu_1 j = 0$.

Consider a user $j \in T$. The same argument as in the sum-rate maximization proof leads to $P^*_j = \bar{P}_j$ if $h_j < \phi_K(P^*)$ and $P^*_j = 0$ if $h_j \geq \phi_K(P^*)$.

Now examine a user $j \in T^c$. We can write (3.67) as

$$\frac{\partial \mathcal{L}(P^*, \mu)}{\partial P^*_j} = \frac{\rho_j(P^*)}{(1 + \sum_{k \in K} P_k)^2} + \mu_2 j = 0$$ (3.68)

where

$$\rho_j(P) \triangleq -h_j \left( 1 + \sum_{k \in K} P_k \right) \left( 1 + \sum_{k \in T^c} P_k \right) \sum_{k \in T} h_k P_k + \left( 1 + \sum_{k \in K} h_k P_k \right) \left( 1 + \sum_{k \in T^c} h_k P_k \right) \sum_{k \in T} P_k.$$ (3.69)

Let

$$\Phi_T(P) \triangleq \phi_K(P) \phi_{T^c}(P) \frac{\sum_{k \in T} P_k}{\sum_{k \in T} h_k P_k}.$$ (3.70)

Then, we have $\rho_j(P) \leq 0$ iff $h_j \geq \Phi_T(P)$, and $\rho_j(P) > 0$ iff $h_j < \Phi_T(P)$. Since $\mu_2 j \geq 0$, we cannot have $\rho_j(P) > 0$, and we find that we must have $h_j \geq \Phi_T(P^*)$ for all $j \in T^c$. Also, if $h_j > \Phi_T(P^*)$, then $P^*_j = \bar{P}_j$. Only if $h_j = \Phi_T(P^*)$, can we have $0 < P^*_j < \bar{P}_j$.

Now, using $\phi_{T^c}(P^*) \geq \phi_K(P^*)$, we can easily show that $\phi_K(P^*) \geq \frac{\sum_{k \in T} h_k P_k^*}{\sum_{k \in T} h_k P_k^*}$.

Combining these two, we get $\phi_{T^c}(P^*) \frac{\sum_{k \in T} P^*_k}{\sum_{k \in T} h_k P_k^*} \geq 1$, and hence we can write $\Phi_T(P^*) \geq$
\( \phi_{Te}(P^*) \geq \phi_K(P^*) \). Then, we know that for a given set of transmitters, \( T \), the solution is such that all users \( j \in T \) transmit with power \( \bar{P}_j \) if \( h_j \leq \phi_K(P^*) \). In the set of jammers \( T^c \), all users have \( h_j \geq \Phi_{\mathcal{T}}(P^*) \), and when this inequality is not satisfied with equality, the jammers jam with maximum power. If the equality is satisfied for some users \( j \), their jamming powers can be found from solving \( h_j = \Phi_{\mathcal{T}}(P^*) \). By rearranging terms in (3.69), we note that the optimum power allocation for this user, call it user \( J \), is found by solving the quadratic

\[
\rho_J(P^*) = c_1 P_J^*^2 + c_2 P_J^* + c_3 = 0
\]

where \( c_1, c_2, c_3 \) are as given in (3.62)–(3.64).

Note that (3.71) defines an (upright) parabola. If the positive root of (3.71) exists and is positive, it is given by

\[
P_J^* = \frac{-c_2 \pm \sqrt{c_2^2 - 4c_1c_3}}{2c_1}, \text{ and } P_J^* = \min \left\{ \bar{P}_j, P_J^* \right\}.
\]

This comes from the fact that if \( P_J^* > \bar{P}_j \), then \( \rho_J(P) < 0 \) for all \( 0 < P_J < \bar{P}_j \), and we must have \( \mu_{2J} > 0 \). If, on the other hand, (3.71) gives a complex or negative solution, then the parabola does not intersect the \( P_J \) axis, and is always positive. Hence, \( h_J < \Phi_{\mathcal{T}}(P^*) \), and \( J \) does not belong to \( T^c \), i.e. \( P_J^* = 0 \).

The form of this solution is intuitively pleasing, since it makes more sense for “weaker” users to jam as they harm the eavesdropper more than they do the intended receiver. What we see is that all transmitting users \( j \), such that \( P_J^* > 0 \), transmit with maximum power as long as their standardized channel gain \( h_j \) is less than some limit \( \phi_K(P^*) \), and all jamming users must have \( h_j > \phi_K(P^*) \).

We claim that all users in \( T^* \) must have \( h_j < \Phi_{\mathcal{T}}(P^*) \) and all users in \( T^*^c \) have \( h_j \geq \Phi_{\mathcal{T}}(P^*) \). To make this argument, we need to show that a \( T \) such that there exists some \( m \in T \) with \( P_m^* = 0 \) and \( n \in T^c \) such that \( h_m > h_n \) cannot be the optimum set. To see this, let \( P^* \) be the optimum power allocation for a set \( T \). Consider a new power allocation and set such that \( \mathcal{U} = T \setminus \{m\} \), i.e., user \( m \) is now jamming, and let

\[
Q_k = P_k^*, \forall k \neq m, n, Q_m = \pi
\]
and \( Q_n = P_n^* - \pi \), for some small \( \pi \). We then have

\[
\frac{\phi_K(Q)}{\phi_U^c(Q)} = \frac{1 + \sum_{k \in K} h_k Q_k}{1 + \sum_{k \in U^c} h_k Q_k} = \frac{1 + \sum_{k \in K} h_k P_k^* + (h_m - h_n) \pi}{1 + \sum_{k \in T^c} h_k P_k^*}
\] (3.72)

which is a lower value for the objective function, proving that \( (T, P^*) \) is not optimum. This shows that all users \( j \in T^{*c} \) must have \( h_j > h_k \) for all users \( k \in T^* \). Since the last user in \( T^{*c} \) has \( h_J = \Phi_T(P^*) \), necessarily \( h_j \geq \Phi_T(P^*) \) for all \( j \in T^{*c} \), and \( h_j < \Phi_T(P^*) \) for all \( j \in T^* \).

Summarizing, the optimum power allocation is such that there is a set of transmitting users \( \{1, \ldots, T\} \) with \( P_k^* = \bar{P}_k \) for \( k = 1, \ldots, l \), there is a set of silent users \( \{T + 1, \ldots, J - 1\} \), and a set of jamming users \( \{J, \ldots, K\} \) with \( P_k^* = \bar{P}_k \) for \( k = J + 1, \ldots, K \) and \( P_J^* \) is found from \( h_J = \Phi_T(P^*) \). This is what is presented in the statement in Theorem 3.3.

Now, to find \( T, J \), we can simply do an exhaustive search as we have narrowed the number of possible optimal sets to \( K(K - 1) \) instead of \( 2^K - 1 \) and found the optimal power allocations for each.
3.6 Upper Bound on the Secrecy Sum-Rate for GGMAC-WT

In this section, we present an upper bound to the achievable secrecy sum-rate, \( \sum_{k=1}^{K} R_s^k \) for the general \( K \)-user GMAC-WT. We start with a strong secrecy constraint in the sense of \([16]\), which is clearly also an upper bound on the “weak” secrecy sum-rate. Let \( W_s^S = \{ W_s^k \}_{k \in S} \) be the set of secret messages in the subset \( S \subseteq K \) of users. We constrain that for any \( \epsilon > 0 \)

\[
H(W_s^K|Z) \geq H(W_s^K) - \epsilon. \tag{3.76}
\]

Clearly, any rates that satisfy this constraint, satisfy our original constraints. We then have the following theorem:

**Theorem 3.4.** The secrecy sum-rates for the GMAC-WT must satisfy

\[
\sum_{k \in K} R_s^k \leq \frac{1}{2} \log \left( 1 + \sum_{k} \sqrt{h_k} \bar{P}_k \right) - \frac{1}{2} \log \left( 1 + \sum_{k} h_k \bar{P}_k \right) \tag{3.77}
\]

where \( \nu^* \) is the solution to \( \nu^2 - \zeta \nu + 1 = 0 \) satisfying \( |\nu^*| \leq 1 \) and

\[
\zeta \triangleq \frac{\sum_k \bar{P}_k + \sum_k h_k \bar{P}_k + \sum_k \bar{P}_k \sum_k h_k \bar{P}_k - \sum_k \sqrt{h_k} \bar{P}_k}{\sum_k \sqrt{h_k} \bar{P}_k}. \tag{3.78}
\]

**Proof.** We start by writing

\[
n \sum_{k \in K} R_s^k = H(W_s^K) \tag{3.79}
\]

\[
\leq H(W_s^K|Z) + \epsilon \tag{3.80}
\]

\[
\overset{(a)}{\leq} H(W_s^K|Z) + \epsilon + n \epsilon_n - H(W_s^K|Y, Z) \tag{3.81}
\]

\[
= I(W_s^K; Y|Z) + n \epsilon_n \tag{3.82}
\]

\[
\overset{(b)}{=} \sum_{i=1}^{n} I(W_s^K; Y_i|Y^{i-1}, Z) + n \epsilon_n \tag{3.83}
\]
\[
= \sum_{i=1}^{n} h(Y_i | Y^{i-1}, Z) - \sum_{i=1}^{n} h(Y_i | W_K^i, Y^{i-1}, Z) + n\epsilon_n \tag{3.84}
\]
\[
\leq \sum_{i=1}^{n} h(Y_i | Z_i) - \sum_{i=1}^{n} h(Y_i | W_K^i, X_{K,i}, Y^{i-1}, Z) + n\epsilon_n \tag{3.85}
\]
\[
= \sum_{i=1}^{n} h(Y_i | Z_i) - \sum_{i=1}^{n} h(Y_i | X_{K,i}^i) + n\epsilon_n \tag{3.86}
\]
\[
\leq \sum_{i=1}^{n} h(Y_i | Z_i) - \sum_{i=1}^{n} h(Y_i | X_{K,i}^i, Z_i) + n\epsilon_n \tag{3.87}
\]
\[
= \sum_{i=1}^{n} I(X_{K,i}; Y_i | Z_i) + n\epsilon_n \tag{3.88}
\]
\[
= \frac{1}{n} \sum_{i=1}^{n} I(X_{K,Q}; Y_Q | Z_Q, Q = i) + n\epsilon_n \tag{3.89}
\]
\[
= n I(X_{K,Q}; Y_Q | Z_Q, Q) + n\epsilon_n \tag{3.90}
\]
\[
= n \left( h(Y_Q | Z_Q, Q) - h(Y_Q | X_{K,Q}, Z_Q, Q) + \epsilon_n \right) \tag{3.91}
\]
\[
\leq n \left( h(Y_Q | Z_Q) - h(Y_Q | X_{K,Q}, Z_Q) + \epsilon_n \right) \tag{3.92}
\]
\[
= n \left( I(X_{K,Q}; Y_Q | Z_Q) + \epsilon_n \right) \tag{3.93}
\]

where we get

(a) from Fano’s Inequality with \( H(W_K | Y, Z) < H(W_K | Y) < n\epsilon'_n \).

(b) using the chain rule,

(c) by removing conditioning, we have \( h(Y_i | Y^{i-1}, Z) \leq h(Y_i | Z_i) \). Since conditioning reduces entropy, we have \( h(Y_i | W_K^i, Y^{i-1}, Z) \geq h(Y_i | W_K^i, X_{K,i}, Y^{i-1}, Z) \),

(d) as \( h(Y_i | W_K^i, X_{K,i}^i, Y^{i-1}, Z) = h(Y_i | X_{K,i}^i) \) since \( Y_i \) is independent of all else given \( X_{K,i}^i \),

(e) because conditioning reduces entropy,
by introducing a new time-sharing variable $Q$ uniformly distributed on $\{1, \ldots, n\}$,

by definition of conditional mutual information,

since conditioning reduces entropy, and $Y_Q$ is independent of all else given $X_K, Q$.

Thus, there exists random variables $X_K$ with some joint distribution satisfying

$$\sum_{k \in K} R_k^s \leq I(X_K; Y | Z) + \epsilon_n. \quad (3.94)$$

We write the upper bound on the achievable secrecy sum-rate starting from (3.94),

$$\sum_{k \in K} R_k^s \overset{(i)}{\leq} \min_{p(N_1, N_2)} \max_{\prod_{k=1}^K p(X_k)} I(X_K; Y | Z) \quad (3.95)$$

$$= \min_{p(N_1, N_2)} \max_{\prod_{k=1}^K p(X_k)} h(Y | Z) - h(Y | X_K, Z) \quad (3.96)$$

$$\overset{(j)}{=} \min_{p(N_1, N_2)} \max_{\prod_{k=1}^K p(X_k)} h(Y | Z) - h(N_1 | N_2) \quad (3.97)$$

$$\overset{(k)}{=} \min_{p(N_1, N_2)} \max_{\prod_{k=1}^K p(X_k)} h(Y - \xi Z | Z) - h(N_1 | N_2) \quad (3.98)$$

$$\overset{(l)}{\leq} \min_{p(N_1, N_2)} \max_{\prod_{k=1}^K p(X_k)} h(Y - \xi Z) - h(N_1 | N_2) \quad (3.99)$$

where we tighten the outer bound by considering all noise correlations. Since the capacity of this channel only depends on the marginal probabilities, its capacity should be equal to that of the least favorable noise,

since $h(Y | X_K, Z) = h(N_1 | X_K, Z) = h(N_1 | X_K, Z, N_2) = h(N_1 | N_2)$.

since translation does not change entropy. In particular, we will let $\xi$ be the MMSE estimate of $Y$ from $Z$. Then, $Y - \xi Z$ is the minimum mean squared error of this estimate,
(d) by removing conditioning. This is satisfied with equality iff $Y, Z$ are jointly Gaussian, making the error a Gaussian independent of $Z$. Since the marginals would then be Gaussian, and each of $Y, Z$ are sums of random variables, all $X_k$ must then also be Gaussian.

We proceed in a way similar to [53]. Taking $Y, Z$ to be jointly Gaussian (with a specified covariance matrix), we can then write

$$Y = \xi Z + \eta$$

(3.100)

where $\eta \sim \mathcal{N}(0, \sigma^2_\eta)$ and

$$\xi = \frac{\sigma_{YZ}}{\sigma^2_Z}$$

(3.101)

$$\sigma^2_\eta = \sigma^2_Y - \xi^2 \sigma^2_Z = \frac{\sigma^2_Y \sigma^2_Z - \sigma^2_{YZ}}{\sigma^2_Z}.$$  

(3.102)

Let

$$K_{N_1 N_2} = \begin{bmatrix} 1 & \nu \\ \nu & 1 \end{bmatrix}$$

(3.103)

$$K_{YZ} = \begin{bmatrix} 1 + \sum_k P_k & \nu + \sum_k \sqrt{h_k} P_k \\ \nu + \sum_k \sqrt{h_k} P_k & 1 + \sum_k h_k P_k \end{bmatrix}.$$  

(3.104)

We then have,

$$\sigma^2_\eta = \frac{(1 + \sum_k P_k)(1 + \sum_k h_k P_k) - (\nu + \sum_k \sqrt{h_k} P_k)^2}{1 + \sum_k h_k P_k}$$

(3.105)

and we can thus write

$$\sum_{k \in K} R_k^s \leq \min_{\nu: \nu \leq 1, P_k \leq P_k, \forall k} \left[ \frac{1}{2} \log \{2\pi e \sigma^2_\eta\} - \frac{1}{2} \log \{2\pi e (1 - \nu^2)\} \right]$$

(3.106)
\[
\min_{\nu: |\nu|\leq 1} \max_{P_k \leq \bar{P}_k, \forall k} \frac{1}{2} \log f(P, \nu) \tag{3.107}
\]

where

\[
f(P, \nu) \triangleq \frac{\sigma^2}{1 - \nu^2}. \tag{3.108}
\]

Since the logarithm is a monotonically increasing function, equivalently we can find the powers that

\[
\min_{\nu: |\nu|\leq 1} \max_{P_k \leq \bar{P}_k, \forall k} f(P, \nu). \tag{3.109}
\]

We first maximize over the transmit powers:

\[
\frac{\partial f(P, \nu)}{\partial P_j} = \left[ \frac{(1 + \sum_k h_k P_k) - \sqrt{h_j} (\nu + \sum_k \sqrt{h_k} P_k)}{(1 - \nu^2) (1 + \sum_k h_k P_k)^2} \right]^2 \tag{3.110}
\]

and we see that for all \( \nu, P \), we have \( \frac{\partial f(P, \nu)}{\partial P_j} \geq 0 \). Thus, maximum powers always maximize \( f(P, \nu) \), regardless of \( \nu \).

Next, we minimize this quantity over \( \nu \). We have

\[
\frac{\partial f(P, \nu)}{\partial \nu} = -\frac{2 \left( \sum_k \sqrt{h_k} P_k \right) (\nu^2 - \zeta \nu + 1)}{(1 - \nu^2)^2 (1 + \sum_k h_k P_k)} \tag{3.111}
\]

where \( \zeta \) is defined in (3.78). We can find the possible optima as:

\[
\nu_{1,2} = \frac{\zeta \pm \sqrt{\zeta^2 - 4}}{2}. \tag{3.112}
\]

We now use the following lemma, the proof of which is given at the end of this section:

\textbf{Lemma 3.1.} With \( \zeta \) defined as in (3.78), we always have \( \zeta \geq 2 \), and furthermore \( f(\bar{P}, \nu) \) is convex in \( \nu \) for \( |\nu| \leq 1 \).
We will always have $\nu_1 \nu_2 = 1$, so only one of these roots will satisfy the constraint $|\nu| \leq 1$. Using the above lemma, this root is then the optimum noise correlation, $\nu^\ast$. Using (3.112) in (3.107), we arrive at

$$\sum_{k \in K} R^s_k \leq \frac{1}{2} \log \left( 1 + \frac{(\zeta - 2\nu^\ast) (\sum_k \sqrt{h_k P_k})}{1 - \nu^\ast} \right) - \frac{1}{2} \log \left( 1 + \sum_k h_k P_k \right).$$

(3.113)

Using the fact that $1 + \nu^\ast = \zeta \nu^\ast$, we have

$$\frac{\zeta - 2\nu^\ast}{1 - \nu^\ast} = \frac{\zeta \nu^\ast - 2\nu^\ast}{\nu^\ast(1 - \nu^\ast)} = \frac{\nu^\ast + 1 - 2\nu^\ast}{\nu^\ast(1 - \nu^\ast)} = \frac{\nu^\ast}{\nu^\ast}$$

(3.114)

which, with (3.113), gives us (3.77).

For the degraded case, the standardized gains are $h_1 = \ldots = h_K = h$, and we can easily verify that $\zeta = \sqrt{h} + \frac{1}{\sqrt{h}}$, and hence $\nu_1 = \frac{1}{\sqrt{h}}$ and $\nu_2 = \sqrt{h}$, giving:

$$\sum_{k \in K} R^s_k \leq \begin{cases} \frac{1}{2} \log \left( 1 + \frac{\sum_k P_k}{1 + h \sum_k P_k} \right), & \text{if } h < 1 \Rightarrow \nu^\ast = \sqrt{h} \\ 0, & \text{if } h \geq 1 \Rightarrow \nu^\ast = \frac{1}{\sqrt{h}} \end{cases}$$

(3.115)

in accordance with [38]. Note that in general we have a gap of $\Gamma = I(X; Y | Z) - [I(X; Y) - I(X; Z)] = I(X; Z | Y)$ between the achievable secrecy sum-rate using the superposition region, and upper bound. This gap disappears as shown in [38] for the degraded case since $X_K \rightarrow Y \rightarrow Z$ implies $I(X_K; Z | Y) = 0$.

**Proof of Lemma 3.1.** We first show that $\zeta \geq 2$. To see this, write

$$\zeta = \frac{\sum_k \bar{P}_k + \sum_k h_k \bar{P}_k + \sum_k \bar{P}_k \sum_k h_k \bar{P}_k - (\sum_k \sqrt{h_k P_k})^2}{\sum_k \sqrt{h_k P_k}}$$

(3.116)

$$= \frac{(1 + \sum_k \bar{P}_k) (1 + \sum_k h_k \bar{P}_k) - 1 - (\sum_k \sqrt{h_k P_k})^2}{\sum_k \sqrt{h_k P_k}}$$

(3.117)
where we have

\[
\left(1 + \sum_k \bar{P}_k\right) \left(1 + \sum_k h_k \bar{P}_k\right) \geq \left(1 + \sum_k \sqrt{h_k \bar{P}_k}\right)^2
\]  

(3.120)

from the Cauchy-Schwarz Inequality, with equality iff \(h_k = 1\) for all \(k\). Now, to see that \(f\) is convex in \(\nu\), we take the second derivative to write

\[
\frac{\partial^2 f(\mathbf{P}, \nu)}{\partial \nu^2} = \frac{2 \left( \sum_k \sqrt{h_k \bar{P}_k}\right) \zeta \nu^2 - 4\nu + \zeta}{1 + \sum_k h_k \bar{P}_k} \left(1 - \nu^2\right)^3 \geq \frac{4 \left( \sum_k \sqrt{h_k \bar{P}_k}\right) \left(\nu - 1\right)^2}{1 + \sum_k h_k \bar{P}_k} \left(1 - \nu^2\right)^3 \geq 0
\]

(3.121)

(3.122)

(3.123)

and hence \(f\) is convex in \(\nu\) for \(|\nu| \leq 1\).

\[\square\]

### 3.7 Numerical Results and Observations

In this section, we present numerical results to illustrate the achievable rates obtained, as well as the cooperative jamming scheme and its effect on achievable secrecy sum-rates. Examples of achievable secrecy rate regions are given in Figure 3.3.

For the GGMAC-WT with \(K = 2\), the achievable maximum secrecy sum-rate, \(R_1^s + R_2^s\) is limited by the channel parameters. It was shown in [40] that for the degraded case, \(h \leq 1\), the secrecy sum-capacity, \(C_{KM}^M(\mathbf{P}) - C_{KW}^W(\mathbf{P})\), is an increasing function of the total sum power, \(\bar{P}_\Sigma = \bar{P}_1 + \bar{P}_2\). However, it is limited since \(C_{KM}^M(\mathbf{P}) - C_{KW}^W(\mathbf{P}) \to -\frac{1}{2} \log h\) as \(\bar{P}_\Sigma \to \infty\). For the general case, where \(\bar{P}_1, \bar{P}_2 \to \infty\), Theorem 3.2 implies that assuming \(h_2 > h_1\), the sum-rate is maximized when only user 1 transmits, and is bounded similarly by \(-\frac{1}{2} \log h_1\).
Next, we examine the secrecy sum-rate maximizing power allocations and optimum powers for the cooperative jamming scheme. Figures 3.4, 3.5 show the achievable secrecy rate improvement for the cooperative jamming scheme for various channel parameters with $K = 2$. The achievable secrecy sum-rate when a user is jamming is the single-user secrecy capacity for the transmitting user. When $h_1 \geq 1$, the secrecy capacity is seen to be zero, unless user 2 has enough power to make user 1’s re-standardized channel gain less than 1.

Since the coding schemes considered here assume knowledge of eavesdropper’s channel gains, applications are limited. One practical application could be securing of a physically protected area such as inside a building, when the eavesdropper is known to be outside. In such a case we can design for the worst case scenario. An example is given in Figure 3.6 for the GGMAC-WT, where we assume a simple path-loss model and fixed locations for two mobile stations (MS) and one base station (BS) at the center. We examine the transmit/jam powers for this area when the eavesdropper is known to be at $(x, y)$ using a fixed path-loss model for the channel gains, and plot the transmit/jam powers and the achieved secrecy sum-rates as a function of the eavesdropper location. It is readily seen that when the eavesdropper is close to the BS, the secrecy sum-rate falls to zero. Also, when the eavesdropper is in the vicinity of a transmitter, that transmitter cannot transmit in secrecy. However, in this case, the transmitter can jam the eavesdropper very effectively with low power, and allow the other transmitter to transmit and/or increase its secrecy rate with little jamming power.

### 3.8 Conclusions and Future Work

We have considered the general Gaussian multiple access channels in the presence of an intelligent external eavesdropper who receives the transmitted signals through another multiple-access channel, and provided achievable rates with perfect secrecy. We have shown that the multiple-access nature of the channels considered can be utilized to improve the secrecy of the system. In particular, we have shown that the total extra randomness is what matters mainly concerning the eavesdropper, rather than the individual randomness in the codes. As such, it
Fig. 3.2: GGMAC-WT achievable regions for different channel parameters, $G^\text{MA}(P_1 = 4, P_2 = 2)$. 
Fig. 3.3: GGMAC-WT achievable secrecy region when $\bar{P}_1 = 4, \bar{P}_2 = 4, h_1 = .1, h_2 = .3$. 
Fig. 3.4: GGMAC-WT cooperative jamming secrecy sum-rate as a function of $P_2$ with different $h_1$ for $P_1 = P_2 = 2$, $h_2 = 1.4$. The circles indicate optimum jamming power.
Fig. 3.5: GGMAC-WT cooperative jamming secrecy sum-rate as a function of $P_2$ with different $h_1$ for $P_1 = P_2 = 100$, $h_2 = 1.4$. The circles indicate optimum jamming power.
Fig. 3.6: GGMAC-WT cooperative jamming example - darker shades correspond to higher values.
may possible for users whose single-user wire-tap capacity are zero, to communicate in perfect secrecy as long as it is possible to put the eavesdropper at an overall disadvantage.

We found achievable perfect secrecy rate regions for the General Gaussian Multiple-Access Wire-Tap Channel (GGMAC-WT). We also showed that for the GGMAC-WT the secrecy sum-rate is maximized when only users with ‘strong” channels to the intended receiver as opposed to the eavesdropper transmit, and they do so using all their available power.

We also proposed a scheme termed *cooperative jamming*, where a disadvantaged user may help improve the secrecy rate by jamming the eavesdropper. We found the optimum power allocations for the transmitting and jamming users, and showed that significant rate gains may be achieved, especially when the eavesdropper has much higher SNR than the receivers and normal secret communications is not possible. This cooperative behavior is useful when the maximum secrecy sum-rate is of interest.

Finally, we note that the results provided are of mainly theoretical interest, since as of yet there are no currently known practical codes for multi-access wire-tap channels unlike the single-user case where, in some cases, practical codes have been shown to be useful for the wire-tap channel, [54, 55]. Furthermore, accurate estimates of the eavesdropper channel parameters are required for code design for wire-tap channels where the channel model is quasi-static, as in the model considered in this chapter.
Chapter 4

The Gaussian and Binary Additive Two-Way Wire-Tap Channels

4.1 Introduction

Information theoretic secrecy was first developed by Shannon in [2]. In this work, Shannon showed that to achieve perfect secrecy in communications, which is equivalent to providing no information to an enemy cryptanalyst, the a posteriori probability of a message must be equivalent to its a priori probability.

In [8], Wyner applied this concept to the discrete memoryless channel by defining the wire-tap channel, where there is a wire-tapper who has access to a degraded version of the intended receiver’s signal. Using the normalized conditional entropy of the transmitted message given the received signal at the wire-tapper as the secrecy measure, he found the region of all possible rate/equivocation pairs, and the existence of a secrecy capacity, $C_s$, the rate up to which it is possible to transmit zero information to the wire-tapper.

Reference [10] extended Wyner’s results to Gaussian channels. Csiszár and Körner, [11], improved Wyner’s results to weaker, “less noisy” and “more capable” channels. Furthermore, they examined sending common information to both the receiver and the wire-tapper, while maintaining the secrecy of private information that is communicated to the receiver only.

In [12], it is shown that the existence of a “public” feedback channel can enable the two parties to be able to generate a secret key even when the wire-tap capacity is zero. More recently, the notion of the wire-tap channel has been extended to parallel channels, [24], relay channels, [26], and fading channels, [27]. Broadcast and interference channels with confidential messages are considered in [31]. References [32, 33] examine the multiple access channel with confidential messages where two transmitters try to keep their messages secret from each other while communicating with a common receiver. Gaussian multiple-access wire-tap (GMAC-WT)
channels are considered in [39, 40, 38, 41], where transmitters communicate with an intended receiver in the presence of an external wire-tapper. In [40, 38], we considered the case where the wire-tapper gets a degraded version of the signal at the legitimate receiver, and found the secrecy-sum capacity for the collective set of constraints using Gaussian codebooks and stochastic encoders. In [41], the general (non-degraded) GMAC-WT was considered, and an achievable rate region for perfect secrecy with collective secrecy measures was found.

We consider the two-way channel where two nodes communicate with each other over a common channel, first introduced in [37]. We introduce the two-way wire-tap (TW-WT) channel where an external eavesdropper receives the transmitters’ signals through a general MAC. In particular, we consider the Gaussian Two-Way Wire-Tap Channel (GTW-WT), and the Binary Additive Two-Way Wire-Tap Channel (BATW-WT). The capacity region for the conventional Gaussian two-way channel was found in [56], and that capacity region for the conventional two-way binary channel was found in [37]. In both channels, it was seen that to achieve the channel capacity, the users can just subtract their self-interference from their respective received signals to achieve rates equal to their single-user capacities for these channels. We utilize as our secrecy constraint, the normalized conditional entropy of the transmitted secret messages given the eavesdropper’s signal, as termed “collective secrecy constraints” in [38]. We show that satisfying this constraint implies the secrecy of the messages for both users. In both scenarios, transmitters are assumed to have one secret and one open message to transmit. We find an achievable secrecy rate region, for both cases, where users can communicate with arbitrarily small probability of error with the intended receiver under perfect secrecy from the eavesdropper.

We also show that in cases where a user is not able to achieve secrecy, that user may help the other user increase its secrecy rate or achieve secrecy if it was not possible before, by jamming the eavesdropper. Thus, similar to the Gaussian multiple-access wire-tap channel, [41], cooperative jamming helps increase the secrecy rate.
4.2 GTW-WT System Model

We consider two users communicating in the presence of an intelligent and informed eavesdropper. Each transmitter \( k \in \mathcal{K} \triangleq \{1, 2\} \) has a secret message, \( W_k \), from a set of equally likely messages \( W_k = \{1, \ldots, M_k\} \). The messages are encoded using \((2^n R_k, n)\) codes into \( \{\tilde{X}_k^n(W_k)\} \), where \( R_k = \frac{1}{n} \log_2 M_k \). The encoded messages \( \{\tilde{X}_k\} = \{\tilde{X}_k^n\} \) are then transmitted.

Each receiver \( k = 1, 2 \) gets \( Y_k = Y_k^n \) and the eavesdropper \( Z = Z^n \). Receiver \( k \) decodes \( Y_k \) to get an estimate of the transmitted message of the other user. The users would like to communicate with arbitrarily low probability of error, while maintaining perfect secrecy of the messages, \( W \). We assume the channel parameters are universally known, including at the eavesdropper, and that the eavesdropper also knows the codebooks and coding scheme.

For the GTW-WT, we can write the signals at the intended receiver and the eavesdropper as

\[
Y_1 = \tilde{X}_1 + \sqrt{h_2^M} \tilde{X}_2 + \tilde{N}_1 \quad (4.1a)
\]
\[
Y_2 = \sqrt{h_1^M} \tilde{X}_1 + \tilde{X}_2 + \tilde{N}_2 \quad (4.1b)
\]
\[
Z = \sqrt{h_1^W} \tilde{X}_1 + \sqrt{h_2^W} \tilde{X}_2 + \tilde{N}_W \quad (4.1c)
\]

such that \( \frac{1}{n} \sum_{i=1}^{n} \tilde{X}_{ki}^2 \leq \tilde{P}_k \), for \( k = 1, 2 \) and \( \tilde{N}_k \sim \mathcal{N} \left(0, \sigma_k^2\right) \) and \( \tilde{N}_W \sim \mathcal{N} \left(0, \sigma_W^2\right) \).

For simplicity, without loss of generality, we consider an equivalent standard form as in [38] as illustrated in Figure 4.1.

\[
Y_1 = \sqrt{\alpha_1} X_1 + X_2 + N_1 \quad (4.2a)
\]
\[
Y_2 = X_1 + \sqrt{\alpha_2} X_2 + N_2 \quad (4.2b)
\]
\[
Z = \sqrt{h_1} X_1 + \sqrt{h_2} X_2 + N_W \quad (4.2c)
\]
where, for $k = 1, 2$,

- the codewords $\{\tilde{X}\}$ are scaled to get $X_1 = \sqrt{\frac{h^M_1}{\sigma^2}} \tilde{X}_1$ and $X_2 = \sqrt{\frac{h^M_2}{\sigma^2}} \tilde{X}_2$;

- the maximum powers are scaled to get $\bar{P}_1 = \frac{h^M_1}{\sigma^2} \tilde{P}_1$ and $\bar{P}_2 = \frac{h^M_2}{\sigma^2} \tilde{P}_2$;

- the transmitters’ new channel gains are given by $\alpha_1 = \frac{\sigma^2_1}{h^M_1 \sigma^2}$ and $\alpha_2 = \frac{\sigma^2_2}{h^M_2 \sigma^2}$;

- the wiretapper’s new channel gains are given by $h_1 = \frac{h^W_1}{h^M_1 \sigma^2}$ and $h_2 = \frac{h^W_2}{h^M_2 \sigma^2}$;

- the noises are normalized by $N_k = \frac{\tilde{N}_k}{\sigma^2_k}$ and $N_W = \frac{\tilde{N}_W}{\sigma^2_W}$.

We now define the achievable secrecy rates for the general two-way wire-tap channels (TW-WT).
DEFINITION 4.1 (ACHIEVABLE SECRECY RATES). The rate pair \((R_1, R_2)\) is said to be achievable for the TW-WT, if for \(\epsilon > 0\) there exists a code of sufficient length \(n\) such that

\[
\frac{1}{n} \log_2 M_k \geq R_k - \epsilon \quad k = 1, 2
\]

(4.3a)

\[
P_e \leq \epsilon
\]

(4.3b)

\[
\frac{H(W^s | Z)}{H(W^s)} \geq 1 - \epsilon
\]

(4.3c)

where

\[
P_e = \frac{1}{M_1 M_2} \sum_{W \in W_1 \times W_2} P\{\hat{W} \neq W | W \text{ was sent}\}.
\]

(4.4)

is the average probability of error for a given code.

4.3 GTW-WT Achievable Rates

In this section, we present an achievable region for the GTW-WT using a superposition coding similar to that used to achieve the region \(G^{\text{MA-S}}\) for the GGMAC-WT, [43]. We first define

DEFINITION 4.2 (GTW-WT SUPERPOSITION REGION, \(G^{\text{TW}}(P)\)). Define

\[
R^{\text{GTW}}(P) = \left\{ \begin{array}{l}
R^s_j + R^o_j \leq I(X_k; Y | X_{k,c}), \quad k = 1, 2 \\
\sum_{k \in S} R^s_k \leq \left[ \sum_{k \in S} I(X_k; Y | X_{k,c}) - I(X_K; Z) \right]^+, \quad \forall S \subseteq K 
\end{array} \right\}
\]

(4.5)

Then, the GTW-WT superposition region, \(G^{\text{TW}}(P)\), is given by evaluating \(R^{\text{GTW}}(P)\) when

\[
X_k \sim \mathcal{N}(0, P_k):
\]

\[
G^{\text{TW}}(P) = \left\{ \begin{array}{l}
R^s_k + R^o_k \leq \frac{1}{2} \log (1 + P_k), \quad k = 1, 2 \\
\sum_{k \in S} R^s_k \leq \frac{1}{2} \left[ \sum_{k \in S} \log (1 + P_k) - \log \left( 1 + \frac{\sum_{k \in S} P_k}{1 + \sum_{k \in S^c} P_k} \right) \right]^+, \quad \forall S \subseteq K 
\end{array} \right\}
\]

(4.6)
or more compactly as

\[
\mathcal{G}_{TW}^T(P) = \left\{ \mathbf{R} : \begin{array}{l}
R_s^k + R_o^k \leq C_s^M(P), \quad k = 1, 2 \\
\sum_{k \in S} R_s^k \leq \left[ \sum_{k \in S} C_s^M(P) - \tilde{C}^W_S(P) \right]^+, \quad \forall S \subseteq \mathcal{K}
\end{array} \right\} \quad (4.7)
\]

**Theorem 4.1.** The rate region given below is achievable for the GTW-WT:

\[
\text{convex closure of} \bigcup_{P \in \mathcal{P}} \mathcal{G}_{TW}^T(P) \quad (4.8)
\]

**Proof.** We use the same coding scheme as was used for the GMAC-WT in [43]. We present it here:

**Superposition Encoding Scheme:** For each user \(k = 1, 2\), consider the following scheme:

1. Generate 3 codebooks \(\mathcal{X}_s^k, \mathcal{X}_o^k, \mathcal{X}_x^k\). \(\mathcal{X}_s^k\) consists of \(M_s^k\) codewords, each component of which is drawn from \(\mathcal{N}(0, \lambda_s^k P_k - \varepsilon)\). Codebook \(\mathcal{X}_o^k\) has \(M_o^k\) codewords with each component randomly drawn from \(\mathcal{N}(0, \lambda_o^k P_k - \varepsilon)\) and \(\mathcal{X}_x^k\) has \(M_x^k\) codewords with each component randomly drawn from \(\mathcal{N}(0, \lambda_x^k P_k - \varepsilon)\) where \(\varepsilon\) is an arbitrarily small number to ensure that the power constraints on the codewords are satisfied with high probability and \(\lambda_s^k + \lambda_o^k + \lambda_x^k = 1\). Define \(R_x^k = \frac{1}{n} \log M_x^k\) and \(M_t^k = M_s^k M_o^k M_x^k\). \(\mathcal{X}_s^k\) corresponds to the codebook corresponding to the secret messages, \(\mathcal{X}_o^k\) corresponds to the open messages, and \(\mathcal{X}_x^k\) corresponds to the extra randomness added.

2. To transmit message \(W_k = (W_s^k, W_o^k) \in \mathcal{W}_s^k \times \mathcal{W}_o^k\), user \(k\) finds the 2 codewords corresponding to components of \(W_k\) and also uniformly chooses a codeword \(W_x^k\) from \(\mathcal{X}_x^k\). User \(k\) then adds all these codewords and transmits the resulting codeword, \(\mathcal{X}_k\), so that it actually transmits one of \(M_t^k\) codewords. Let \(R_t^k = \frac{1}{n} \log M_t^k = R_o^k + R_s^k + R_x^k\). Note that since all codewords are chosen uniformly, user \(k\) essentially transmits one of \(M_t^k\) codewords at random for each message \(W_s^k\), and its overall rate of transmission is \(R_t^k\).
We choose $R^s_k, R^o_k, R^x_k$ to satisfy

$$R^s_k + R^o_k + R^x_k \leq \frac{1}{2} \log (1 + P_k), \quad k = 1, 2$$  \hspace{1cm} (4.9)$$

$$\sum_{k \in S} \left( R^o_k + R^x_k \right) \leq \frac{1}{2} \log (1 + \sum_{k \in S} h_k P_k), \quad \forall S \subseteq \mathcal{K} \text{ with equality if } S = \mathcal{K}$$  \hspace{1cm} (4.10)$$

$$\sum_{k \in S} R^s_k \leq \sum_{k \in S} \frac{1}{2} \left[ \sum_{k \in S} \log (1 + P_k) - \log \left( 1 + \frac{\sum_{k \in S} P_k}{1 + \sum_{k \in S \cap \mathcal{C}} P_k} \right) \right]^+, \quad \forall S \subseteq \mathcal{K}$$  \hspace{1cm} (4.11)$$

or equivalently

$$R^s_k + R^o_k + R^x_k \leq C^M_k, \quad k = 1, 2$$  \hspace{1cm} (4.12)$$

$$\sum_{k \in S} \left( R^o_k + R^x_k \right) \leq C^W_S, \quad \forall S \subseteq \mathcal{K} \text{ with equality if } S = \mathcal{K}$$  \hspace{1cm} (4.13)$$

$$\sum_{k \in S} R^s_k \leq \left[ \sum_{k \in S} C^M_k - C^W_S \right]^+, \quad \forall S \subseteq \mathcal{K}$$  \hspace{1cm} (4.14)$$

assuming (4.14) is positive. The decodability of $W^s_K$ from $Y_1, Y_2$ comes from (4.12) and the capacity region of the Gaussian Two-Way Channel [56]. This gives the first set of terms in the achievable region. The key here is that since each transmitter knows its own codeword, it can subtract its self-interference from the received signal and get a clear channel. Therefore, the Gaussian two-way channel decomposes into two parallel channels.

The second group of terms in (4.6), resulting from the secrecy constraint, can be shown the same way as the proof of [43, Theorem 1], since $Z$ has the same form for both the 2-user GMAC-WT and the GTW-WT. In other words, as far as the eavesdropper is concerned, the channel is still a GMAC with $K = 2$ users. As such, we need to send $C^W_K$ extra codewords in total, which need to be shared by the two-terminals. However, if any of the users is single-user decodable by the eavesdropper, it cannot achieve secrecy. The details are as follows:

If (4.14) is zero for any user or both, we cannot achieve secrecy for those users. When $S = \mathcal{K}$, if the sum-capacity of the main channel is less than that of the eavesdropper channel, i.e., $C^M_{\mathcal{K}} \leq C^W_{\mathcal{K}}$, secrecy is not possible for the system. Assume this quantity is positive. To ensure
that we can mutually satisfy both (4.14), (4.13), we can reclassify some open messages as secret.

From the first set of conditions in (4.8) and the capacity of the two-way Gaussian Channel, [56], with high probability the receiver can decode the codewords with low probability of error. To show the secrecy condition, we first note that, the coding scheme described is equivalent to each user \( k \) selecting one of \( M_o^k \) messages, and sending a uniformly chosen codeword from among \( M_o^k M_x^k \) codewords for each. Define \( X_\Sigma = \sum_{k=1}^{2} \sqrt{h_k} X_k \), and we have

\[
H(W_s^K | Z) = H(W_s^K) - I(W_s^K; Z) \tag{4.15}
\]

\[
= H(W_s^K) - I(W_s^K; Z) + I(W_s^K; Z | X_\Sigma) \tag{4.16}
\]

\[
= H(W_s^K) - h(Z) + h(Z | W_s^K) + h(Z | X_\Sigma) - h(Z | W_s^K, X_\Sigma) \tag{4.17}
\]

\[
= H(W_s^K) - I(X_\Sigma; Z) + I(X_\Sigma; Z | W_s^K) \tag{4.18}
\]

where we used \( W_s^K \rightarrow X_\Sigma \rightarrow Z \), and thus we have \( h(Z | W_s^K, X_\Sigma) = h(Z | X_\Sigma) \) to get (4.18).

We will consider the two terms individually. First, we have the trivial bound due to channel capacity:

\[
I(X_\Sigma; Z) \leq n C_W^W(P) \tag{4.19}
\]

Now write

\[
I(X_\Sigma; Z | W_s^K) = H(X_\Sigma | W_s^K) - H(X_\Sigma | W_s^K, Z) \tag{4.20}
\]

Also, any one of \( M_o^k M_x^k \) codewords are equally likely for each secret message,

\[
H(X_\Sigma | W_s^K) = \log \left( \prod_{k=1}^{K} (M_o^k M_x^k) \right) \tag{4.21}
\]

\[
= n \left( \sum_{k=1}^{K} (R_o^k + R_x^k) \right) \tag{4.22}
\]

\[
= n C_W^W(P). \tag{4.23}
\]
We can also write
\[ H(X_{\Sigma}|W_s^{K}, Z) \leq n\delta_n \] (4.24)
where \( \delta_n \to 0 \) as \( n \to \infty \) since, with high probability, the eavesdropper can decode \( X_{\Sigma} \) given \( W_s^{K} \) due to (4.13) and code generation. Using (4.19), (4.20), (4.23) and (4.24) in (4.18), we get

\[ H(W_s^{K}|Z) \geq H(W_s^{K}) - nC^W_K(P) + nC^W_K(P) - n\delta_n \] (4.25)

\[ = H(W_s^{K}) - n\delta_n. \] (4.26)

For different channel gains, the region of all \( R_s \) satisfying (4.6) is shown in Figure 4.2. Since we require four dimensions for an accurate depiction of the complete rate region, we only focus on our main interest, i.e., the secrecy rate region. Figure 4.3 shows the achievable secrecy rate region as a function of transmit powers. We note that higher powers always result in a larger region. We indicate the constraint on the overall rates, corresponding to the capacity region of the Gaussian Two-Way Channel, by the dotted line.

Note that the secrecy region has a structure similar to the GGMAC-WT with \( K = 2 \). As far as the eavesdropper is concerned, there is no difference between the two channels. However, since the main channel between users decomposes into two parallel channels, higher rates can be achieved between the legitimate terminals (users). Thus, in effect, each user’s transmitted codewords act as a secret key for the other user’s transmitted codewords, requiring fewer extraneous codewords overall to confuse the eavesdropper, and a larger secrecy region. We note that a user may achieve secrecy as long as it is not single-user decodable by the eavesdropper. As a result, TDMA does not enlarge the region, since each user can at least achieve their single-user secrecy rates. To see this, note that the constraint on the secrecy sum-rate can be written as:

\[
\log(1 + P_1) + \log(1 + P_2) - \log(1 + h_1 P_1 + h_2 P_2)
= \log(1 + P_1) - \log(1 + h_1 P_1) + \log(1 + P_2) - \log \left( 1 + \frac{h_2 P_2}{1 + h_1 P_1} \right)
\] (4.27)
Fig. 4.2: GTW-WT achievable regions for different channel parameters, $G^{TW}(P_1 = 4, P_2 = 2)$. 
Fig. 4.3: GTW-WT achievable secrecy region when $\bar{P}_1 = 4$, $\bar{P}_2 = 2$, $h_1 = .3$, $h_2 = .7$. 
\[ \geq \log(1 + P_1) - \log(1 + h_1 P_1) + \log(1 + P_2) - \log(1 + h_2 P_2) \]  \hspace{1cm} (4.28)

so that transmitting in the two-way channel always provides an advantage over the single-user channels.

### 4.4 Sum-Rate Maximization for GTW-WT

The secrecy sum-rate achievable in Theorem 4.1 depend on the transmit powers. As such, we are interested in the power allocation \( P^* \) that would maximize the total secrecy sum-rate. We recall that the standardized channel gain for user \( k \) is \( h_k = \frac{h_k W_{\text{eave}}^2}{h_k W_{\text{M}}^2} \). Without loss of generality, assume that users are ordered in terms of increasing standardized eavesdropper channel gains, i.e., \( h_1 \leq h_2 \). From a physical point of view, assuming that the channel parameters are drawn according to a continuous distribution and then fixed, the probability that two users would have the same exact standardized channel gain is zero, so we would only need to consider \( h_1 < h_2 \). We write the question as maximizing

\[ R_{\text{sum}}^{\text{TW}} = \frac{1}{2} \left[ \log (1 + P_1) + \log (1 + P_2) - \log (1 + h_1 P_1 + h_2 P_2) \right] \]  \hspace{1cm} (4.29)

This problem is formally stated below:

\[ \max_{P \in P} \frac{1}{2} \log (1 + P_1) + \frac{1}{2} \log (1 + P_2) - \frac{1}{2} \log (1 + h_1 P_1 + h_2 P_2) \equiv \min_{P \in P} \psi \left( P \right) \]  \hspace{1cm} (4.30)

where

\[ \psi_S (P) \equiv \frac{1 + \sum_{k \in S} h_k P_k}{\prod_{k \in S} (1 + P_k)} \]  \hspace{1cm} (4.31)

and \( S = K \) yields (4.30). The optimum power allocation is stated below:
THEOREM 4.2. The secrecy sum-rate maximizing power allocation for the GTW-WT is given by

\[
(P_1^*, P_2^*) = \begin{cases} 
(\bar{P}_1, \bar{P}_2), & \text{if } h_1 \leq 1 + h_2\bar{P}_2, \ h_2 < 1 + h_1\bar{P}_1 \\
(\bar{P}_1, 0), & \text{if } h_1 < 1, \ h_2 \geq 1 + h_1\bar{P}_1 \\
(0, 0), & \text{otherwise}
\end{cases}
\]  

(4.32)

PROOF. We would like to

\[
\min_{\mathbf{P}} \psi_{\mathcal{K}}(\mathbf{P}) \quad \text{s.t.} \quad 0 \leq P_k \leq \bar{P}_k 
\]  

(4.33)

The Lagrangian is,

\[
\mathcal{L}(\mathbf{P}, \mathbf{\mu}) = \psi_{\mathcal{K}}(\mathbf{P}) - \sum_{k=1}^{2} \mu_{1k}P_k + \sum_{k=1}^{2} \mu_{2k}(P_k - \bar{P}_k). 
\]  

(4.34)

Equating the derivative of the Lagrangian to zero for user \( j \), we get

\[
\frac{\partial \mathcal{L}(\mathbf{P}^*, \mathbf{\mu})}{\partial P_j^*} = \psi^{(j)}_{\mathcal{K}}(\mathbf{P}^*) - \mu_{1j} + \mu_{2j} = 0 
\]  

(4.35)

where

\[
\psi^{(j)}_{\mathcal{K}}(\mathbf{P}) \triangleq \frac{\partial \psi_{\mathcal{K}}(\mathbf{P})}{\partial P_j} = \frac{h_j - \frac{1 + \sum_{k \in \mathcal{K}} h_k P_k^*}{1 + P_j^*}}{\prod_{k \in \mathcal{K}} (1 + P_k)}. 
\]  

(4.36)

We see that for user \( j \), if \( h_j > \frac{1 + \sum_{k \in \mathcal{K}} h_k P_k^*}{1 + P_j^*} \), or equivalently if \( h_j > 1 + h_{j^c}P_{j^c}^* \), where \( j^c \) is the other user, then \( P_j^* = 0 \). When equality is satisfied, i.e., \( h_j = 1 + h_{j^c}P_{j^c}^* \), then \( \psi^{(j)}_{\mathcal{K}}(\mathbf{P}) = 0 \) regardless of \( P_j \), and as such \( \psi_{\mathcal{K}}(\mathbf{P}^*) \) does not depend on \( P_j \). To conserve power, we again set \( P_j = 0 \) in this case. On the other hand, if \( h_j < 1 + h_{j^c}P_{j^c}^* \), then \( P_j^* = \bar{P}_j \), since we must have \( \mu_{2j} > 0 \).
Consider user 1. If $P_1^* = 0$, and $P_2^* > 0$, this implies that $h_2 < 1$. Since $h_1 \leq h_2 < 1$, we automatically satisfy $h_1 < 1 + h_2 P_2$ and cannot have $P_1^* = 0$. As a consequence of this contradiction, we see that $P_2^* = 0$ whenever $P_1^* = 0$.

Assume the other possibility, i.e., $P_1^* = \bar{P}_1$. Consider the two alternatives for $P_2^*$. We will have $P_2^* = \bar{P}_2$ if $h_2 < 1 + h_2 \bar{P}_1$, and $P_2^* = 0$ if $h_2 \geq 1 + h_1 \bar{P}_1$. These cases correspond to $h_1 < 1$, and $h_1 < 1 + h_2 \bar{P}_2$, respectively. Thus, we have (4.32) as the secrecy sum-rate maximizing power allocation.

Remark: Observe that the sum-rate maximizing power allocation given in Theorem 4.2 has a structure similar to that of the GGMAC-WT in [43, Theorem 3]. In summary, it is seen that as long as a user is not single-user decodable, it should be transmitting with maximum power. Hence, when both users can be made to be non-single-user decodable, then the maximum powers will provide the largest secrecy sum-rate. If this is not the case, then the user who is single-user decodable cannot transmit with non-zero secrecy and will just make the secrecy sum-rate constraint tighter for the remaining user by transmitting open messages.

4.5 Secrecy Through Cooperative Jamming

In the previous section, we found the secrecy sum-rate maximizing power allocations. We noted that for the GTW-WT, if the eavesdropper is not “disadvantaged enough” for a user, i.e., it is single-user decodable, it is prevented from transmission since it cannot achieve secrecy.

We posit that such a user may be able to “help” a transmitting user, since it can cause more harm to the eavesdropper than to the intended receiver. In this case, we can show that we can achieve higher secrecy rates when the “weaker” users are jamming. We note that the GTW-WT, has a big advantage compared to the GGMAC-WT, [43], in that the receiver already knows the jamming sequence and can subtract it from its received sequence. As such, this scheme only harms the eavesdropper and not the intended receivers, achieving an even higher secrecy sum-rate. Once again, without loss of generality, we consider $h_1 \leq h_2$. 
Once again, we propose to maximize the secrecy sum-rate using cooperative jamming when useful. This problem is formally stated as follows:

$$\max_{\mathcal{T} \subseteq \mathcal{K}, \mathbf{P} \in \mathcal{P}} \sum_{k \in \mathcal{T}} \frac{1}{2} \log (P_k) - \frac{1}{2} \log \left( 1 + \frac{\sum_{k \in \mathcal{T}} h_k P_k}{1 + \sum_{k \in \mathcal{T}^c} h_k P_k} \right)$$

(4.37)

$$\equiv \min_{\mathcal{T} \subseteq \mathcal{K}} \min_{\mathbf{P} \in \mathcal{P}} \frac{\psi_{\mathcal{K}}(\mathbf{P})}{\psi_{\mathcal{T}^c}(\mathbf{P})}$$

(4.38)

where we recall that $\psi_{\mathcal{S}}(\mathbf{P})$ is given by (4.31) and

$$\psi_{\mathcal{K}}(\mathbf{P}) = \frac{1 + \sum_{k \in \mathcal{K}} h_k P_k}{\prod_{k \in \mathcal{K}} (1 + P_k)}$$

(4.39)

$$\psi_{\mathcal{T}^c}(\mathbf{P}) = \frac{1 + \sum_{k \in \mathcal{T}^c} h_k P_k}{\prod_{k \in \mathcal{T}^c} (1 + P_k)}.$$ 

(4.40)

Note that $\mathcal{K} = \{1, 2\}$ since there are only two terminals. A similar argument to the GGMAC-WT case can easily be used to establish that we can assume a user to be either transmitting or jamming, but not both. Since the jamming user is also the receiver that the other user is communicating with and knows the transmitted signal, this scheme entails no loss of capacity as far as the transmitting user is concerned. The optimum power allocations are given as follows.

**Theorem 4.3.** The achievable secrecy sum-rate for the the collaborative scheme described is

$$R_{sum}^{TW-CJ} = \sum_{k \in \mathcal{T}} \frac{1}{2} \log (P_k) - \frac{1}{2} \log \left( 1 + \frac{\sum_{k \in \mathcal{T}} h_k P_k^*}{1 + \sum_{k \in \mathcal{T}^c} h_k P_k^*} \right)$$

(4.41)
where $T$ is the set of transmitting users and the optimum power allocations are given by

$$
(P_1^*, P_2^*) = \begin{cases} 
(\bar{P}_1, \bar{P}_2), & \text{both transmit if } h_1 < h_2 \leq 1 \\
(\bar{P}_1, \bar{P}_2), & \text{1 transmits, 2 jams if } h_1 \leq 1 < h_2 \\
(\bar{P}_1, \bar{P}_2), & \text{1 transmits, 2 jams if } 1 < h_1 < 1 + h_2 \bar{P}_2 \text{ and } \psi_2(\bar{P}) > \psi_1(\bar{P}) \\
(\bar{P}_1, \bar{P}_2), & \text{2 transmits, 1 jams if } 1 < h_1 < h_2 < 1 + h_1 \bar{P}_1 \text{ and } \psi_1(\bar{P}) > \psi_2(\bar{P}) \\
(0, 0), & \text{otherwise}
\end{cases}
$$

(4.42)

**Proof.** Similar to the GGMAC-WT, we start with the sub-problem of finding the optimal power allocation given a jamming set, i.e.,

$$
\min_{\mathbf{P}} \frac{\psi_K(\mathbf{P})}{\psi_{T^c}(\mathbf{P})} \quad \text{s. t. } 0 \leq P_k \leq \bar{P}_k 
$$

(4.43)

The Lagrangian is given by

$$
\mathcal{L}(\mathbf{P}, \mu) = \frac{\psi_K(\mathbf{P})}{\psi_{T^c}(\mathbf{P})} - \sum_{k=1}^{2} \mu_{1k} P_k + \sum_{k=1}^{2} \mu_{2k} (P_k - \bar{P}_k).
$$

(4.44)

Taking the derivative we have

$$
\frac{\partial \mathcal{L}(\mathbf{P}^*, \mu)}{\partial P_j^*} = 0 = \begin{cases} 
\frac{\psi_K(\mathbf{P}^*) - \mu_{1j} + \mu_{2j}}{\psi_{T^c}(\mathbf{P}^*)} & \text{if } j \in T \\
\frac{\psi_K(\mathbf{P}^*) - \psi_{T^c}(\mathbf{P}^*)}{\psi_{T^c}(\mathbf{P}^*)} & \text{if } j \in T^c
\end{cases}
$$

(4.45)

since a user $j \in T^c$ satisfies $P_j^* > 0$, it must have $\mu_{1j} = 0$.

Consider user $j \in T$. We again argue that if $h_j > \frac{1 + \sum_{k \in K} h_k P_k}{1 + P_j^*}$, then $P_j^* = 0$ and if $h_j < \frac{1 + \sum_{k \in K} h_k P_k}{1 + P_j^*}$, then $P_j^* = \bar{P}_j$. 

Now examine user \( j \in T^c \). It is easy to see that since such a user only harms the jammer, the optimal jamming strategy should have \( P_j^* = \bar{P}_j \), i.e., the maximum power. This can also be seen by noting that (4.45) for this case simplifies to

\[
\frac{\partial L(P^*, \mu)}{\partial P_j^*} = \frac{-h_j \sum_{k \in T} h_k P_k^*}{\left(1 + \sum_{k \in T} h_k P_k^* \right)^2 \left( \prod_{k \in K} (1 + P_k^*) \right)^2} + \mu_{2j} = 0
\]

(4.46)

and hence we must have \( \mu_{2j} > 0 \) \( \Rightarrow P_j^* = \bar{P}_j \) for all \( j \in T^c \), as long as there is a user who is transmitting with non-zero power.

The jamming set will be one of \( \emptyset, \{1\}, \{2\} \), since there is no point in jamming when there is no transmission. Also, if any of the two users is jamming, by the argument above, \( P_j^* = \bar{P}_j \), \( j = 1, 2 \).

We can easily see that jamming by a user \( j \) only offers an advantage if \( h_j > 1 \), i.e., \( \psi_{T^c}(P) > 1 \) iff \( h_j > 1 \) for \( j \in T^c \). Thus, when \( h_1 < h_2 \leq 1 \), both users should be transmitting instead of jamming. However, when any user has \( h_j > 1 \), jamming always does better than the case when both users are transmitting. In this case, \( \psi_j(P) \geq \psi_{j^c}(P) \) for some user \( j \), and the objective function in (4.38) is minimized when this user is jamming, and the other one is transmitting. If, however, \( h_{j^c} > 1 + h_j \bar{P}_j \), then it will not transmit, and we should not be jamming. Consolidating all of these results, we come up with the power allocation in in Theorem 4.3.

Remark: A sufficient, but not necessary condition for the weaker user to be the jamming user is if \( h_2 \bar{P}_2 > h_1 \bar{P}_1 \); this case corresponds to having higher SNR at the eavesdropper for the original, non-standardized model. This can be interpreted as “jam with maximum power if it is possible to change user 1’s effective channel gain such that it is no longer single-user decodable”. For the simple case of equal power constraints, \( \bar{P}_1 = \bar{P}_2 = \bar{P} \), it is easily seen that user 1 should
never be jamming. The optimal power allocation in that case reduces to

\[(P_1^*, P_2^*) = \begin{cases} 
(\bar{P}, \bar{P}), & \text{both transmit, if } h_1 < h_2 \leq 1 \\
(\bar{P}, \bar{P}), & 1 \text{ transmits, 2 jams, if } h_1 < 1 + h_2 \bar{P} \\
(0,0), & \text{otherwise}
\end{cases} \] (4.47)

4.6 The BATW-WT System Model

The Binary Additive Two-Way Wire-Tap Channel model, shown in Figure 4.4, corresponds to a more classical wire-tapped channel, where the binary signals of two transmitters are superimposed on a common wire, as in [37], and random bit errors are produced as in a binary symmetric channel.

![Fig. 4.4: BATW-WT system model.](image-url)
For the BATW-WT, the received signals are given by

\[ Y_1 = X_1 \oplus X_2 \oplus E_1 \]  
\[ Y_2 = X_1 \oplus X_2 \oplus E_2 \]  
\[ Z_1 = X_1 \oplus X_2 \oplus E_W \]  

where \( E_1, E_2, E_W \) are \( n \)-vectors of binary random variables representing errors, such that if \( \varepsilon_k \) is the error probability at receiver \( k = 1, 2 \), and \( \varepsilon_W \) is the error probability at the wiretapper, we write \( P\{E_k = 1\} = \varepsilon_k < \frac{1}{2} \) and \( P\{E_W = 1\} = \varepsilon_W < \frac{1}{2} \).

We also define the following quantity before we proceed:

\[ h_b(p) \triangleq -p \log p - (1-p) \log(1-p). \]  

4.7 BATW-WT Achievable Rates

**Theorem 4.4.** For the BATW-WT, we can achieve the following set of rates:

\[
\mathcal{R}^{BATW} = \left\{ (R_1, R_2) : \begin{array}{c}
R^s_k + R^o_k \leq 1 - h_b(\varepsilon_k) \quad k = 1, 2 \\
R^s_1 + R^s_2 \leq \left[ 1 + h_b(\varepsilon_W) - h_b(\varepsilon_1) - h_b(\varepsilon_2) \right]^+ \end{array} \right\} 
\]  

**Proof.** The proof follows along the same lines as the proof of GTW-WT achievability in Theorem 4.1. We use the same superposition coding scheme, but for the BATW-WT, codewords in \( X_1 \) and \( X^x_1 \) are drawn uniformly according to a binary distribution with \( p = \frac{1}{2} \), and the rates are chosen to satisfy

\[ R^s_k + R^o_k + R^x_k \leq 1 - h_b(\varepsilon_k), \quad k = 1, 2 \]  

\[ \sum_{k=1}^{2} R^o_k + R^x_k = 1 - h_b(\varepsilon_W) \]  

\[ R^s_1 + R^s_2 \leq 1 + h_b(\varepsilon_W) - h_b(\varepsilon_1) - h_b(\varepsilon_2) \]
instead of (4.12)–(4.14). Then, letting $X = X_1 \oplus X_2$, we can write

\[
H(W_s^k | Z) = H(W_s^k) - I(W_s^k; Z)
\] (4.54)

\[
= H(W_s^k) - I(W_s^k; Z) + I(W_s^k; Z | X_S)
\] (4.55)

\[
= H(W_s^k) - H(Z) + H(Z | W_s^k) + H(Z | X_S) - H(Z | W_s^k, X_S)
\] (4.56)

\[
= H(W_s^k) - I(X_S; Z) + I(X_S; Z | W_s^k)
\] (4.57)

Writing the two terms separately, we first have the channel capacity bound:

\[
I(X_S; Z) \leq n(1 - h_b(\epsilon_W))
\] (4.58)

Now write

\[
I(X_S; Z | W_s^k) = H(X_S | W_s^k) - H(X_S | W_s^k, Z)
\] (4.59)

and since user $k$ independently sends one of $M_k^o M_k^x$ codewords equally likely for each secret message,

\[
H(X_S | W_s^k) = \log \left( \prod_{k=1}^{K} (M_k^o M_k^x) \right)
\] (4.60)

\[
= n \left( \sum_{k=1}^{K} (R_k^o + R_k^x) \right)
\] (4.61)

\[
= n(1 - h_b(\epsilon_W)).
\] (4.62)

We can also write

\[
H(X_S | W_s^k, Z) \leq n \delta_n
\] (4.63)
where \( \delta_n \to 0 \) as \( n \to \infty \) since, with high probability, the eavesdropper can decode \( X_\Sigma \) given \( W^s_K \) due to (4.52) and code generation. Using these in (4.57), we get

\[
H(W^s_K|Z) \geq H(W^s_K) - n(1 - h_b(\varepsilon_W)) + n(1 - h_b(\varepsilon_W)) - n\delta_n \quad (4.64)
\]

\[
= H(W^s_K) - n\delta_n. \quad (4.65)
\]

4.8 Numerical Results and Observations

In this section, we present numerical results to illustrate the achievable rates obtained, as well as the cooperative jamming scheme and its effect on achievable secrecy sum-rates.

Examples of the achievable secrecy rate region is given in Figure 4.3 for the GTW-WT. As seen in 4.3, we see that the GTW-WT achieves a larger secrecy rate region then the GGMAC-WT, and offers more protection to “weak” users, [43]. In addition, TDMA does not enlarge the achievable region for GTW-WT since superposition coding always allows users to achieve their single-user secrecy rates for any transmit power.

We also note that for the GTW-WT, unlike the GGMAC-WT, it is possible to increase the secrecy capacity by increasing the transmit powers. This mainly stems from the fact that the users now have the extra advantage over the eavesdropper that they know their own transmitted codewords. In effect, each user helps encrypt the other user’s transmission. To see this more clearly, consider the symmetric case where \( \alpha_1 = \alpha_2 = h_1 = h_2 = 1 \) and \( \bar{P}_1 = \bar{P}_2 = \bar{P} \), which makes all users receive a similarly noisy version of the same sum-message. The only disadvantage the eavesdropper has, is that he does not know any of the codewords whereas user \( k \) knows \( X_k \). In this case, \( R^s_1 + R^s_2 \leq \frac{1}{2} \log \left( 1 + \bar{P}^2/(1 + 2\bar{P}) \right) \) is achievable, and this rate approaches \( \frac{1}{2} \log(\frac{1}{2}\bar{P}) \) as \( \bar{P} \gg 1 \). Thus, it is possible to achieve a secrecy-rate increase at the same rate as the increase in channel capacity.

Next, we examine the secrecy sum-rate maximizing power allocations and optimum powers for the cooperative jamming scheme. For the GTW-WT, it is always optimal for user 2 to jam
as long as it enables user 1 to transmit, as seen in Figure 4.5. The results show, as expected, that secrecy is achievable for both users so long as we can keep the eavesdropper from single-user decoding the transmitted codewords by treating the remaining user as noise.

Since the coding schemes considered here assume knowledge of eavesdropper’s channel gains, applications are limited. One practical application could be securing of a physically protected area such as inside a building, when the eavesdropper is known to be outside. In such a case we can design for the worst case scenario. An example is given in Figure 4.6 for the GTW-WT, where we assume a simple path-loss model and fixed locations for two transmitters (T). We examine the transmit/jam powers for this area when the eavesdropper is known to be at \((x, y)\) using a fixed path-loss model for the channel gains, and plot the transmit/jam powers and the achieved secrecy sum-rates as a function of the eavesdropper location. In this case, we see that it is possible to provide secrecy for large area, as the jamming signal does not hurt the intended receiver.

4.9 Conclusions and Future Work

In this chapter, we have considered the Gaussian and Binary Additive Two-Way channels in the presence of an external eavesdropper who receives the transmitted signals through a multiple-access channel, and provided achievable secrecy rates. We have shown that the multiple-access nature of the channels considered can be utilized to improve the secrecy of the system. In particular, we have shown that the total extra randomness is what matters mainly concerning the eavesdropper, and even though the eavesdropper’s channel gain may be better than a terminal’s, the extra knowledge of its own codeword by that terminal enables communication in perfect secrecy as long as the eavesdropper’s received signal is not strong enough to allow single-user decoding. As such, it is possible for users whose single-user wire-tap capacity are zero, to communicate with non-zero secrecy rate, as long as it is possible to put the eavesdropper at an overall disadvantage.
Fig. 4.5: GTW-WT cooperative jamming secrecy sum-rate as a function of $P_2$ with different $h_1$ for $\bar{P}_1 = \bar{P}_2 = 2$, $h_2 = 4.2$. The circles indicate optimum jamming power.
Fig. 4.6: GTW-WT cooperative jamming example.
We found achievable secrecy rate regions for the GTW-WT. In this case, the sum-rate is maximized when both terminals transmit with maximum power as long as the eavesdropper’s channel is not good enough to decode a terminal by treating the other user as noise.

Finally, we utilized cooperative jamming, where a disadvantaged user may help improve the secrecy rate by jamming the eavesdropper, to improve our secrecy sum-rates. We found the optimum power allocations for the transmitting and jamming users, and showed that significant rate gains may be achieved, especially when the eavesdropper has much higher SNR than the receivers and normal secret communications is not possible. The gains can be significant for GTW-WT. This cooperative behavior is useful when the maximum secrecy sum-rate is of interest. We have also contrasted the secrecy sum-rate of the GTW-WT to that of the GMAC-WT, noting the benefit of the two-way channels where the fact that each receiver has perfect knowledge of its transmitted signal brings an advantage with each user effectively encrypting the communications of the other user. We note that we only present achievable secrecy rates for the GTW-WT and BATW-WT. The secrecy capacity region for these channels are still open problems.
Chapter 5

The Fading Gaussian Multi-Access Wire-Tap Channel

5.1 Introduction

Wyner, in [8], defined the wire-tap channel, where there is a wire-tapper who has access to a degraded version of the intended receiver’s signal. He found the region of all possible rate/equivocation pairs, and the existence of a secrecy capacity, $C_s$, the rate up to which it is possible to transmit zero information to the wire-tapper. Reference [10] extended this result to Gaussian channels. Later, Csiszár and Körner, [11], generalized Wyner’s results to channels satisfying some weaker conditions than degradedness.

Gaussian multiple-access wire-tap (GMAC-WT) channels are considered in [39, 40, 38, 41, 43], where transmitters communicate with an intended receiver in the presence of an external wire-tapper. In [40, 38], we considered the case where the wire-tapper gets a degraded version of the signal at the legitimate receiver, and found the secrecy-sum capacity for the collective set of constraints using Gaussian codebooks and stochastic encoders. In [41], the general (non-degraded) GMAC-WT was considered, and an achievable rate region for perfect secrecy with collective secrecy measures was found.

In [57], a Gaussian channel was presented where both the receiver and transmitter know the instantaneous channel gains. Given a long-term power constraint and a stationary ergodic distribution on the channel gains, it was shown that a water-filling power allocation over the fading states, where transmission stopped during deep-fades was capacity-optimal. Knopp and Humblet examined the multiple-access case and showed that it was optimal for a single-user to be transmitting with a water-filling power allocation at any given time, [58]. Single-user wire-tap channels were examined from this perspective in [29, 46]. It was shown that in this case, the optimal power allocation is not water-filling, but takes a more complicated form.
This chapter examines achievable sum-rates for the block-fading Gaussian multiple-access wire-tap channel (GMAC-WT). For the GMAC-WT, the capacity region is not yet known, but an achievable rate was given in [40, 38] for the case where the eavesdropper is a degraded version of the intended receiver, and generalized in [41]. It was also shown in [40, 38], that this scheme achieved the sum-capacity for the degraded GMAC-WT. In this chapter, we find the sum-rate maximizing power allocation for the GMAC-WT and compare it with the sum-rate maximizing instantaneous power control solution found in [41, 43]. We then examine the case where we utilize cooperative jamming, which was proposed in [41]. For this case, we give partial solutions to the optimal power allocation for some cases, and show how to find a numerical solution for the remaining cases. We see that utilizing cooperative jamming allows us to achieve a secrecy-sum rate close to the outer bound.

5.2 System Model and Problem Statement

We consider \( K = 2 \) users communicating with a receiver in the presence of an eavesdropper. Transmitter \( k = 1, 2 \) chooses a message \( W_k \) from a set of equally likely messages \( \mathcal{W}_k = \{1, \ldots, M_k\} \). The messages are encoded using \((2^n R_k, n)\) codes into \( \{X_k^n(W_k)\} \), where \( R_k = \frac{1}{n} \log_2 M_k \). The encoded messages \( \{X_k\} = \{X_k^n\} \) are then transmitted, and the intended receiver and the eavesdropper each get a copy \( Y = Y^n \) and \( Z = Z^n \). The receiver decodes \( Y \) to get an estimate of the transmitted messages, \( \hat{W} \). We would like to communicate with the receiver with arbitrarily low probability of error, while maintaining perfect secrecy of the transmitted messages. The signals at the intended receiver and the eavesdropper are given by

\[
Y = \sum_{k=1}^{K} \sqrt{h_k^M} X_k + N_M \tag{5.1}
\]

\[
Z = \sum_{k=1}^{K} \sqrt{h_k^W} X_k + N_W \tag{5.2}
\]
where $N_M, N_W$ are the AWGN, and without loss of generality, we assume $N_M, N_W \sim \mathcal{N}(0, 1)$ and the following transmit power constraints:

$$\frac{1}{n} \sum_{i=1}^{n} X_{ki}^2 \leq P_k, \; k = 1, 2$$  \hspace{1cm} (5.3)

---

**Fig. 5.1:** Two-user general Gaussian Multiple-Access Wire-Tap Channel (GGMAC-WT) system model.

We use the collective secrecy constraints defined in [39] to take into account the multi-access nature of the channel.

$$\Delta_S \triangleq \frac{H(W_S|Z)}{H(W_S)} \quad \forall \mathcal{S} \subseteq \mathcal{K} \triangleq \{1, \ldots, K\}$$  \hspace{1cm} (5.4)

It was shown in [40] that guaranteeing the secrecy of all users is sufficient to guarantee the secrecy of all groups of users, i.e., $\frac{H(W_S|Z)}{H(W_S)} \geq 1 - \epsilon \Rightarrow \frac{H(W_S|Z)}{H(W_S)} \geq 1 - \epsilon$ for any $\mathcal{S} \subseteq \mathcal{K}$ of users.
**Definition 5.1 (Achievable Rates).** The rate vector $\mathbf{R} = (R_1, R_2)$ is said to be *achievable with perfect secrecy* if for any given $\epsilon > 0$ there exists a code of sufficient length $n$ such that

$$\frac{1}{n} \log_2 M_k \geq R_k - \epsilon \quad k = 1, 2$$

(5.5)

$$P_e \leq \epsilon$$

(5.6)

$$\Delta S \geq 1 - \epsilon \quad \forall S \subseteq K = \{1, 2\}$$

(5.7)

where user $k$ chooses one of $M_k$ symbols to transmit according to the uniform distribution and $P_e$ is the average probability of error.

### 5.3 Sum-Rates with Ergodic Fading

**Theorem 5.1.** Let $\mathbf{h} = (h_1^M, h_2^M, h_1^W, h_2^W)$ and $\text{d} \mathbf{h} = dh_1^M dh_2^M dh_1^W dh_2^W$. Given a power control policy $\{P_k(\mathbf{h})\}_{k=1}^2$ satisfying

$$\int_0^\infty \int_0^\infty \int_0^\infty \int_0^\infty P_k(\mathbf{h})p(\mathbf{h})d\mathbf{h} \leq \bar{P}_k$$

(5.8)

we can achieve the secrecy rates

$$R_1 \leq \frac{1}{2} \int_0^\infty \cdots \int_0^\infty \left[ \log \left( \frac{(1 + h_1^M P_1(\mathbf{h}))(1 + h_2^W P_2(\mathbf{h}))}{1 + h_1^W P_1(\mathbf{h}) + h_2^W P_2(\mathbf{h})} \right) \right]^+ p(\mathbf{h})d\mathbf{h}$$

(5.9a)

$$R_2 \leq \frac{1}{2} \int_0^\infty \cdots \int_0^\infty \left[ \log \left( \frac{(1 + h_1^W P_1(\mathbf{h}))(1 + h_2^M P_2(\mathbf{h}))}{1 + h_1^M P_1(\mathbf{h}) + h_2^W P_2(\mathbf{h})} \right) \right]^+ p(\mathbf{h})d\mathbf{h}$$

(5.9b)

$$R_1 + R_2 \leq \frac{1}{2} \int_0^\infty \cdots \int_0^\infty \left[ \log \left( \frac{1 + h_1^M P_1(\mathbf{h}) + h_2^M P_2(\mathbf{h})}{1 + h_1^W P_1(\mathbf{h}) + h_2^W P_2(\mathbf{h})} \right) \right]^+ p(\mathbf{h})d\mathbf{h}$$

(5.9c)

where $[x]^+ \triangleq \max\{x, 0\}$. 
PROOF. The proof is similar to the proofs of the Coding Theorem in [57] and Theorem 1 in [46], with the main difference being that there are now 4 integrals to consider for the two-user scenario.

Let \( P(h) \in \mathcal{P} \) be a feasible power control policy and \( q > 0 \) be small. Define

\[
a_{k,i} = \frac{i}{q} \quad k = 1, 2; \quad i = 0, 1, \ldots, qA_k
\]

(5.10)

\[
b_{k,i} = \frac{i}{q} \quad k = 1, 2; \quad i = 0, 1, \ldots, qB_k
\]

(5.11)

and also \( a_{1,qA_1+1} = a_{2,qA_2+1} = b_{1,qB_1+1} = a_{2,qB_2+1} = \infty \).

Let

\[
\mathcal{H}(i_1, i_2, j_1, j_2) = \{ h : a_{1,i_1} \leq h_1 \leq a_{1,i_1+1}, \quad a_{2,i_2} \leq h_2 \leq a_{2,i_2+1},
\]

\[
b_{1,j_1} \leq h_1 \leq b_{1,j_1+1}, \quad b_{2,j_2} \leq h_2 \leq b_{2,j_2+1}\}.
\]

(5.12)

We say that the channel is in fading state \( h_{i_1,i_2,j_1,j_2} \) if \( h \in \mathcal{H}(i_1, i_2, j_1, j_2) \).

In addition, we define a new quantized power control policy by

\[
P_k(h) = \inf_{h \in \mathcal{H}} P_k(h), \quad k = 1, 2
\]

(5.13)

and we can easily verify that if \( P_k(h) \) satisfies the power constraint \( \int P(h)dh \leq \bar{P}_k \), then so does \( P_k(h) \).

We showed in [41] that we can find a code for fading state \( h_{i_1,i_2,j_1,j_2} \) that achieves the following rates:

\[
R_1 \leq r_1(i_1, i_2, j_1, j_2, P)
\]

(5.14)

\[
R_2 \leq r_2(i_1, i_2, j_1, j_2, P)
\]

(5.15)

\[
R_1 + R_2 \leq r_s(i_1, i_2, j_1, j_2, P)
\]

(5.16)
where

\[
    r_1(i_1, i_2, j_1, j_2, P) \triangleq \frac{1}{2} \log \left\{ \frac{1 + a_{1,i_1} P_1(h)}{1 + b_{2,j_2+1} P_2(h)} \right\} \quad (5.17)
\]

\[
    r_2(i_1, i_2, j_1, j_2, P) \triangleq \frac{1}{2} \log \left\{ \frac{1 + a_{2,i_2} P_2(h)}{1 + b_{1,j_1+1} P_1(h)} \right\} \quad (5.18)
\]

\[
    r_s(i_1, i_2, j_1, j_2, P) \triangleq \frac{1}{2} \log \left\{ 1 + a_{1,i_1} P_1(h) + a_{2,i_2} P_2(h) \right\} \\
    - \log \left\{ 1 + b_{1,j_1+1} P_1(h) + b_{2,j_2+1} P_2(h) \right\} \quad (5.19)
\]

and we consider the worst case scenario for the eavesdropper gains.

If \( n \) is the total number of channel uses, as \( n \to \infty \), from the ergodicity of the channel, we have that \( n_{i_1,i_2,j_1,j_2} \), the number of times the channel is in state \( h_{i_1,i_2,j_1,j_2} \), is given by

\[
    n_{i_1,i_2,j_1,j_2} = n \Pr \{ h_{i_1,i_2,j_1,j_2} \} \quad (5.20)
\]

\[
    = n \Pr \{ h \in \mathcal{H}(i_1, i_2, j_1, j_2) \} \quad (5.21)
\]

Let \( R_s = R_1 + R_2 \). Thus, as \( n \to \infty \), we can achieve an overall rate of transmission of

\[
    \lim_{n \to \infty} R_s = \sum_{i_1=0}^{qA_1} \sum_{i_2=0}^{qA_2} \sum_{j_1=0}^{qB_1} \sum_{j_2=0}^{qB_2} r_s(i_1, i_2, j_1, j_2) \frac{n_{i_1,i_2,j_1,j_2}}{n} \quad (5.22)
\]

\[
    = \sum_{i_1=0}^{qA_1} \sum_{i_2=0}^{qA_2} \sum_{j_1=0}^{qB_1} \sum_{j_2=0}^{qB_2} r_s(i_1, i_2, j_1, j_2) \Pr \{ h_{i_1,i_2,j_1,j_2} \} \quad (5.23)
\]

Thus, for a given \( \epsilon > 0 \), there exists some \( n \) sufficiently large such that

\[
    R_s \geq \sum_{i_1=0}^{qA_1} \sum_{i_2=0}^{qA_2} \sum_{j_1=0}^{qB_1} \sum_{j_2=0}^{qB_2} r_s(i_1, i_2, j_1, j_2) \Pr \{ h_{i_1,i_2,j_1,j_2} \} - \epsilon \quad (5.24)
\]
Similarly, we can show that the average error probability also goes to zero:

$$\lim_{n \to \infty} P_e \leq \sum_{i_1=0}^{qA_1} \sum_{i_2=0}^{qA_2} \sum_{j_1=0}^{qB_1} \sum_{j_2=0}^{qB_2} P_e(i_1, i_2, j_1, j_2) \mathbb{P}_{h_{i_1,i_2,j_1,j_2}} = 0$$  \hspace{1cm} (5.25)

We now need to show that the power control policy achieves the rate given in Theorem 5.1. In other words, we need to show that for a given $\epsilon > 0$, there exist $q, A_1, A_2, B_1, B_2$ such that

$$\sum_{i_1=0}^{qA_1} \sum_{i_2=0}^{qA_2} \sum_{j_1=0}^{qB_1} \sum_{j_2=0}^{qB_2} r_s(i_1, i_2, j_1, j_2) \mathbb{P}_{h_{i_1,i_2,j_1,j_2}} \geq C - \epsilon$$  \hspace{1cm} (5.26)

where

$$C \triangleq \int_0^\infty \cdots \int_0^\infty \int_0^\infty \frac{1}{2} \log \left( \frac{1 + h_1^M P_1(h) + h_2^M P_2(h)}{1 + h_1^W P_1(h) + h_2^W P_2(h)} \right) p(h) dh$$  \hspace{1cm} (5.27)

We first show that $C$ is finite. Write

$$\int \cdots \int_0^\infty \log \left( \frac{1 + h_1^M P_1(h) + h_2^M P_2(h)}{1 + h_1^W P_1(h) + h_2^W P_2(h)} \right) p(h) dh$$

$$\leq \int \cdots \int_0^\infty \frac{1}{1 + h_1^M P_1(h) + h_2^M P_2(h)} \log \frac{h_1^M P_1(h)}{h_1^W P_1(h)} + \log \frac{h_2^M P_2(h)}{h_2^W P_2(h)} p(h) dh$$  \hspace{1cm} (5.28)

$$\leq \int \cdots \int_0^\infty \log \frac{h_1^M}{h_1^W} p(h) dh + \int \cdots \int_0^\infty \log \frac{h_2^M}{h_2^W} p(h) dh$$  \hspace{1cm} (5.29)

where we used the log-sum inequality in the first step. We can write the first term as

$$\int \cdots \int_0^\infty \log \frac{h_1^M}{h_1^W} dh_1 = \int_0^\infty \log \frac{h_1^M}{h_1^W} dh_1^M - \int_0^\infty \log h_1^W p(h_1^W) dh_1^W$$  \hspace{1cm} (5.30)

where each term can again be considered separately to get

$$\int_0^\infty \log h_1^M p(h_1^M) dh_1^M \leq \int_0^\infty \frac{1}{\ln 2} h_1^M p(h_1^M) dh_1^M$$  \hspace{1cm} (5.31)
and since each term is finite, we conclude that the integral is finite. Thus, for a given $\epsilon > 0$, there exist $M_1(\epsilon), M_2(\epsilon), M'_1(\epsilon), M'_2(\epsilon)$ such that

$$
\int_0^{M_1(\epsilon)} \int_0^{M_2(\epsilon)} \int_0^{M'_1(\epsilon)} \int_0^{M'_2(\epsilon)} \frac{1}{2} \log \left( \frac{1 + h_1^M P_1(h) + h_2^M P_2(h)}{1 + h_1^{W} P_1(h) + h_2^{W} P_2(h)} \right) p(h) \, dh \geq C - \epsilon
$$

(5.33)

Then, by the monotone convergence theorem, we can write

$$
\lim_{q \to \infty} \sum_{i_1=0}^{qA_1} \sum_{i_2=0}^{qA_2} \sum_{j_1=0}^{qB_1} \sum_{j_2=0}^{qB_2} r_s(i_1, i_2, j_1, j_2) \mathcal{P}(h_{i_1, i_2, j_1, j_2})
$$

(5.34)

$$
= \sum_{i_1=0}^{a_1} \sum_{i_2=0}^{a_2} \sum_{j_1=0}^{b_2} \sum_{j_2=0}^{b_2} \int_{a_1,i_1}^{a_1,i_1+1} \int_{a_2,i_2}^{a_2,i_2+1} \int_{b_1,j_1}^{b_1,j_1+1} \int_{b_2,j_2}^{b_2,j_2+1} r_s(i_1, i_2, j_1, j_2) p(h) \, dh
$$

(5.35)

$$
\geq \int_0^{M_1(\epsilon)} \int_0^{M_2(\epsilon)} \int_0^{M'_1(\epsilon)} \int_0^{M'_2(\epsilon)} \frac{1}{2} \log \left( \frac{1 + h_1^M P_1(h) + h_2^M P_2(h)}{1 + h_1^{W} P_1(h) + h_2^{W} P_2(h)} \right) p(h) \, dh
$$

(5.36)

$$
\geq C - \epsilon
$$

(5.37)

where we chose $A_k = \lceil M_k(\epsilon)/q \rceil$ and $B_k = \lceil M'_k(\epsilon)/q \rceil$. Thus, we have shown (5.9c). Equations (5.9a) and (5.9b) can also be shown by proceeding similarly to complete the proof.

We also provide an upper bound to the secrecy sum-rate that is a similar extension to the upper bound given in [45]. This is stated below:

**Theorem 5.2.** The sum-rate obtainable is limited by

$$
\max_{P_1(h), P_2(h)} \int_0^\infty \cdots \int_0^\infty \frac{1}{2} \log \left( \frac{\Phi^M(\nu^*)}{\Phi^W} \right)
$$

(5.38)
where $\Phi^M(\nu) = 1 + \frac{\sqrt{h_1} P_1(h)}{\nu} + \frac{\sqrt{h_2} P_2(h)}{\nu} - P_2(h)$, $P_1(h), P_2(h)$ are power control policies as described in Theorem 5.1, and $\nu^*(h, P(h))$ for a given $P$ is the solution to $\nu^2 - \zeta \nu + 1 = 0$ satisfying $|\nu| \leq 1$, and $\zeta$ is given by

$$\zeta = \frac{\sum_k P_k h_k P_k + \sum_k P_k \sum_k h_k P_k - \sum_k \sqrt{h_k} P_k}{\sum_k \sqrt{h_k} P_k}.$$  \hspace{1cm} (5.39)

PROOF. The proof of this theorem is the same as the proof of Theorem 3.4 for a given feasible power control policy, given in Chapter 3 of this dissertation. By then maximizing this quantity over all feasible power control policies, we arrive at (5.38). \hfill \square

### 5.4 Sum Rate Maximization

We are interested in finding the power allocation that will maximize the achievable sum-rate as described in Theorem 5.1. We can write the optimization problem as

$$\max_{P_1(h), P_2(h)} \int_0^{\infty} \cdots \int_0 \log \left( \frac{\Phi^M}{\Phi^W} \right) p(h) dh$$ \hspace{1cm} (5.40)

subject to

$$\int_0^{\infty} \cdots \int_0 P_k(h) p(h) dh \leq \bar{P}_k, \quad k = 1, 2 \hspace{1cm} (5.41)$$

$$P_k(h) \geq 0, \quad k = 1, 2 \hspace{1cm} (5.42)$$

where

$$\Phi^M = 1 + h_1^M P_1(h) + h_2^M P_2(h)$$ \hspace{1cm} (5.43)$$

$$\Phi^W = 1 + h_1^W P_1(h) + h_2^W P_2(h)$$ \hspace{1cm} (5.44)$$
We can then write the Lagrangian to be maximized as

\[
\mathcal{L} = \int_0^\infty \ldots \int_0^\infty \log \left( \frac{\Phi^M}{\Phi^W} \right) p(h) \, dh - 2 \sum_{k=1}^2 \lambda_k \left( \int_0^\infty P_k(h) p(h) \, dh - \bar{P}_k \right) + 2 \sum_{k=1}^2 \mu_k P_k
\]

(5.45)

and its derivative as

\[
\frac{\partial \mathcal{L}}{\partial P_k} = \frac{h_k^M}{\Phi^M} - \frac{h_k^W}{\Phi^W} - \lambda_k + \mu_k = 0, \quad k = 1, 2
\]

(5.46)

Note that we always have \( \Phi^M \geq \Phi^W \) to have non-negative achievable rate. We can also see that the optimum powers will not violate this since we can just shut the users down for \( h_k \) values that do not satisfy this condition, and achieve higher sum secrecy rate while obeying the power constraint. In addition, if any user is transmitting, we will have \( \Phi^M > \Phi^W \) since the sum-rate would be zero, and we should just conserve power. As a result, we can easily see that we have

\[
\lambda_k - \mu_k = \frac{1}{\Phi^M} \left( h_k^M - \frac{\Phi^M}{\Phi^W} h_k^W \right), \quad k = 1, 2
\]

(5.47)

\[
\leq \frac{1}{\Phi^M} \left( h_k^M - h_k^W \right)
\]

(5.48)

\[
\leq h_k^M - h_k^W
\]

(5.49)

with equality only when no users are transmitting. Hence,

\[
P_k = 0 \quad \text{if} \quad h_k^M - h_k^W \leq \lambda_k
\]

(5.50)

We are looking for the case when \( P_k > 0 \), i.e. assume \( \mu_k = 0 \). Consider user 1. We can write from (5.46),

\[
\lambda_1 h_1^M h_1^W P_1^2 + \lambda_1 \bar{\theta}_1 P_1 + (\lambda_1 \psi_1 - \theta_1) = 0
\]

(5.51)
where we define

\[ \theta_1 \triangleq h_1^M (1 + h_2^W P_2) - h_1^W (1 + h_2^M P_2) \] (5.52)

\[ \bar{\theta}_1 \triangleq h_1^M (1 + h_2^W P_2) + h_1^W (1 + h_2^M P_2) \] (5.53)

\[ \psi_1 \triangleq (1 + h_2^M P_2)(1 + h_2^W P_2) \] (5.54)

Since we are only interested in the non-negative solution, we can write

\[ P_1 = \frac{-\lambda_1 \bar{\theta}_1 + \sqrt{\lambda_1^2 \theta_1^2 - 4\lambda_1^2 h_1^M h_1^W \psi_1 + 4\lambda_1 h_1^M h_1^W \theta_1}}{2\lambda_1 h_1^M h_1^W} \] (5.55)

and proceeding similarly for user 2, we arrive at

\[ P_k = \frac{-\lambda_k \bar{\theta}_k + \sqrt{\lambda_k^2 \theta_k^2 + 4\lambda_k h_k^M h_k^W \theta_k}}{2\lambda_k h_k^M h_k^W}, \quad k = 1, 2 \] (5.57)

where

\[ \theta_2 \triangleq h_2^M (1 + h_1^W P_1) - h_2^W (1 + h_1^M P_1) \] (5.58)

\[ \bar{\theta}_2 \triangleq h_2^M (1 + h_1^W P_1) + h_2^W (1 + h_1^M P_1) \] (5.59)

\[ \psi_2 \triangleq (1 + h_2^M P_1)(1 + h_1^W P_1) \] (5.60)

We note that if the optimum power for user \( k \) is positive,

\[ \lambda_k^2 \left( 2h_k^M h_k^W P_k + \bar{\theta}_k \right)^2 = \lambda_k^2 \theta_k^2 + 4\lambda_k h_k^M h_k^W \theta_k \] (5.61)

\[ \lambda_k(2h_k^M \Phi^W h_k^M) = 4h_k^M h_k^W \theta_k \] (5.62)

\[ \Psi \triangleq \Phi^M \Phi^W = \frac{\theta_k}{\lambda_k} \] (5.63)
so that when both users have non-zero optimum power,

\[
\frac{\theta_1}{\lambda_1} = \frac{\theta_2}{\lambda_2} = \Psi
\]  

(5.64)

Note that if \(h_1^W = h_2^W = 0\), i.e. the no eavesdropper case, we would have \(\theta_k = h_k^M\) and this would simplify to

\[
\frac{h_1^M}{\lambda_1} = \frac{h_2^M}{\lambda_2}
\]  

(5.65)

and since we have \(h_k^M\) drawn according to a continuous distribution, the probability of this event would be zero, implying that only one user should be transmitting, which is the solution found in [58]. However, in our case it is possible that the powers will satisfy this equality. We also easily verify from (5.63) that to have \(P_k > 0\), we must have

\[
\frac{\theta_k}{\psi_k} > \frac{\theta_k}{\Psi} = \lambda_k
\]  

(5.66)

Since \(\Psi \geq \psi_k \geq 1\), \(k = 1, 2\), if \(\theta_k \leq 0\), we cannot have \(P_k > 0\). We can also write the above result as:

\[
P_1 > 0 \text{ iff } \frac{h_1^M}{1 + h_2^W P_2} - \frac{h_1^W}{1 + h_2^W P_2} > \lambda_1
\]  

(5.67)

\[
P_2 > 0 \text{ iff } \frac{h_2^M}{1 + h_1^W P_1} - \frac{h_2^W}{1 + h_1^W P_1} > \lambda_2
\]  

(5.68)

WLOG, let \(\frac{h_2^M}{h_2^W} < \frac{h_1^M}{h_1^W}\) and consider the four possibilities:

5.4.1 \(\frac{h_1^M}{h_1^W} \leq \lambda_1\), \(\frac{h_2^M}{h_2^W} \leq \lambda_2\)

We showed earlier that \(P_1 = P_2 = 0\).
5.4.2 \( h_1^M - h_1^W > \lambda_1, h_2^M - h_2^W \leq \lambda_2 \)

We showed earlier that in this case \( P_2 = 0 \). Hence, we have \( P_1 > 0 \), and we can find \( P_1 \) from (5.57) which simplifies to:

\[
P_1 = \frac{1}{2} \left[ \left( \frac{\theta_1}{h_1^M h_1^W} \right)^2 + \frac{4}{\lambda_1} \frac{\theta_1}{h_1^M h_1^W} - \frac{\bar{\theta}_1}{h_1^M h_1^W} \right] \tag{5.69}
\]

\[
P_1 = \frac{1}{2} \left[ \left( \frac{1}{h_1^W} - \frac{1}{h_1^M} \right)^2 + \frac{4}{\lambda_1} \left( \frac{1}{h_1^W} - \frac{1}{h_1^M} \right) - \frac{1}{2} \left( \frac{1}{h_1^W} + \frac{1}{h_1^M} \right) \right] \tag{5.70}
\]

(5.70) is the solution given in [29,46] for the single user case, also found by setting \( h_2^W = h_2^M = 0 \). This solution, as noted in [29], is not the standard water-filling solution. However, in the high SNR regime, in the sense that \( \frac{1}{\lambda_1} \ll \frac{1}{h_1^W} - \frac{1}{h_1^M} \), we have

\[
P_1 = \frac{1}{2} \left[ \left( \frac{\theta_1}{h_1^M h_1^W} \right)^2 + \frac{4}{\lambda_1} \frac{\theta_1}{h_1^M h_1^W} - \frac{\bar{\theta}_1}{h_1^M h_1^W} \right] \tag{5.71}
\]

\[
\approx \frac{1}{2} \left[ \left( \frac{\theta_1}{h_1^M h_1^W} \right)^2 + \frac{4}{\lambda_1} \frac{\theta_1}{h_1^M h_1^W} + \frac{4}{\lambda_2} - \frac{\bar{\theta}_1}{h_1^M h_1^W} \right] \tag{5.72}
\]

\[
= \frac{1}{2} \left[ \frac{\theta_1}{h_1^M h_1^W} + \frac{2}{\lambda_1} - \frac{\bar{\theta}_1}{h_1^M h_1^W} \right] \tag{5.73}
\]

\[
= \frac{1}{\lambda_1} - \frac{1}{h_1^M} \tag{5.74}
\]

which is the well-known water-filling solution, [57]. Note that if \( h_1^W \to 0 \), this is always true.

5.4.3 \( h_1^M - h_1^W \leq \lambda_1, h_2^M - h_2^W > \lambda_2 \)

This can be treated the same way as the previous case. We have \( P_1 = 0 \), and

\[
P_2 = \frac{1}{2} \left[ \left( \frac{\theta_2}{h_2^M h_2^W} \right)^2 + \frac{4}{\lambda_2} \frac{\theta_2}{h_2^M h_2^W} - \frac{\bar{\theta}_2}{h_2^M h_2^W} \right] \tag{5.75}
\]
\[
\frac{1}{2} \lambda \left[ \frac{1}{h^W_2} - \frac{1}{h^M_2} \right]^2 + \frac{4}{\lambda_2} \left[ \frac{1}{h^W_2} - \frac{1}{h^M_2} \right] - \frac{1}{2} \left( \frac{1}{h^W_2} + \frac{1}{h^M_2} \right)
\] (5.76)

5.4.4 \(h^M_1 - h^W_1 > \lambda_1, h^M_2 - h^W_2 > \lambda_2\)

In this case, it is easy to see that at least one user must be transmitting. Without loss of
generality, assume \( \frac{h^M_1}{h^W_1} \geq \frac{h^M_2}{h^W_2} \). We will examine two sub-cases:

5.4.4.1 \(\frac{h^M_1 - h^W_1}{\lambda_1} \geq \frac{h^M_2 - h^W_2}{\lambda_2}\)

We first examine the conditions and power allocations when both users should be trans-
mittting. We can write (5.64) as

\[
\lambda_2 \left[ h^M_1 (1 + h^W_2 P_2) - h^W_1 (1 + h^M_2 P_2) \right] = \lambda_1 \left[ h^M_2 (1 + h^W_1 P_1) - h^W_2 (1 + h^M_1 P_1) \right]
\] (5.77)

which gives us

\[
P_2 = \frac{\lambda_1 (h^M_2 - h^W_2) - (h^M_1 - h^W_1)}{h^M_2 h^W_1 - h^M_1 h^W_2} - \frac{\lambda_1 P_1}{\lambda_2}
\] (5.78)

\[
P_1 = \frac{(h^M_2 - h^W_2) - \lambda_2 \lambda_1 (h^M_1 - h^W_1)}{h^M_2 h^W_1 - h^M_1 h^W_2} - \frac{\lambda_2 P_2}{\lambda_1}
\] (5.79)

which can also be written as

\[
\lambda_2 P_2 + \lambda_1 P_1 = \frac{\lambda_1 (h^M_2 - h^W_2) - \lambda_2 (h^M_1 - h^W_1)}{h^M_2 h^W_1 - h^M_1 h^W_2} \equiv \Lambda
\] (5.80)

Note that we cannot have positive \(P_1, P_2\) if \(\frac{h^M_1 - h^W_1}{\lambda_1} \geq \frac{h^M_2 - h^W_2}{\lambda_2}\), which means that our
assumption that both users transmit is wrong, and only one user should actually be transmitting.

Assume this is the case, and user 2 is the transmitting user and user 1 is silent, i.e. \(\frac{h^M_1}{1 + h^M_2 P_2} - \frac{h^W_1}{1 + h^M_2 P_2} \equiv \Lambda\)
Then, we can write

\[
\frac{h_1^W}{1 + h_2^W P_2} \leq \lambda_1 \quad \text{and} \quad h_2^M - h_2^W > \lambda_2. \]

Then, we can write

\[
h_1^M (1 + h_2^W P_2) - h_1^W (1 + h_2^M P_2) \leq \lambda_1 (1 + h_2^M P_2)(1 + h_2^W P_2) \tag{5.81}
\]

\[
\frac{\theta_2}{\lambda_2} = \Psi \Rightarrow \frac{h_2^M - h_2^W}{\lambda_2} = (1 + h_2^M P_2)(1 + h_2^W P_2) \tag{5.82}
\]

Combining the two, we get

\[
\frac{h_2^M - h_2^W}{\lambda_2} \geq \frac{h_1^M (1 + h_2^W P_2) - h_1^W (1 + h_2^M P_2)}{\lambda_1} \geq \frac{h_1^M - h_1^W}{\lambda_1} \tag{5.83}
\]

which violates the assumption that \(\frac{h_1^M - h_1^W}{\lambda_1} \geq \frac{h_2^M - h_2^W}{\lambda_2}\). Thus, we see that only user 1 should be transmitting in this case.

**5.4.4.2 \( \frac{h_1^M - h_1^W}{\lambda_1} < \frac{h_2^M - h_2^W}{\lambda_2} \)**

We first note that, if our solution is such that \(\frac{h_2^M - h_2^W}{\lambda_2} < \Psi\), then we have \(\frac{\theta_2}{\Psi} < \lambda_2\) and \(P_2 = 0\). However, this implies that \(\frac{h_1^M - h_1^W}{\lambda_1} < \Psi\) as well, and no user would be transmitting. Thus, we must have \(\frac{h_2^M - h_2^W}{\lambda_2} \geq \Psi\).

Assume the solution is such that \(\frac{h_2^M - h_2^W}{\lambda_2} \geq \Psi \geq \frac{h_1^M - h_1^W}{\lambda_1}\). First consider the conditions when both users transmit. Following from above, substituting (5.79) into (5.63), after some algebra we can write

\[
(\lambda_1 h_2^M - \lambda_2 h_1^M) \left[ (h_1^M - h_1^W) + (h_1^M h_2^W - h_2^M h_1^W) P_2 \right]
\]

\[
\times (\lambda_1 h_2^M - \lambda_2 h_1^M) \left[ (h_1^M - h_1^W) + (h_1^M h_2^W - h_2^M h_1^W) P_2 \right]
\]

\[
= \lambda_1 (h_1^M h_2^W - h_2^M h_1^W)^2 \left[ (h_1^M - h_1^W) + (h_1^M h_2^W - h_2^M h_1^W) P_2 \right] \tag{5.84}
\]
and since \((h_1^M - h_1^W) + (h_1^M h_2^W - h_2^M h_1^W)P_2 > 0\), we get

\[
\left[(h_1^M - h_1^W) + (h_1^M h_2^W - h_2^M h_1^W)P_2\right] = \frac{\lambda_1(h_1^M h_2^W - h_2^M h_1^W)}{\left(h_2^M - \lambda_2 h_1^W\right)(\lambda_1 h_2^W - \lambda_2 h_1^W)}
\]

which gives

\[
P_2 = \frac{\lambda_1(h_1^M h_2^W - h_2^M h_1^W)}{\left(h_2^M - \lambda_2 h_1^W\right)(\lambda_1 h_2^W - \lambda_2 h_1^W)} - \frac{h_1^M - h_1^W}{h_2^W - h_2^M h_1^W}
\]

as we cannot have

\[
P_2 = \frac{h_1^W - h_1^M}{h_1^W h_2^W - h_2^M h_1^W} < 0
\]

Similarly, substituting (5.78) into (5.63), we can write

\[
(\lambda_2 h_1^M - \lambda_1 h_2^W) \left[(h_2^M - h_2^W) - (h_1^M h_2^W - h_2^M h_1^W)P_1\right] \times (\lambda_2 h_1^W - \lambda_1 h_2^M) \left[(h_2^M - h_2^W) - (h_1^M h_2^W - h_2^M h_1^W)P_1\right]
\]

\[
= \lambda_2(h_1^M h_2^W - h_2^M h_1^W) \left[(h_2^M - h_2^W) - (h_1^M h_2^W - h_2^M h_1^W)P_1\right]
\]

(5.88)

which gives us either

\[
P_1 = \frac{h_1^M - h_2^W}{h_1^W h_2^W - h_2^M h_1^W}
\]

(5.89)

or

\[
P_1 = \frac{-\lambda_2(h_1^M h_2^W - h_2^M h_1^W)}{(\lambda_1 h_2^W - \lambda_2 h_1^M)(\lambda_1 h_2^W - \lambda_2 h_1^W)} + \frac{h_1^M - h_2^W}{h_1^W h_2^W - h_2^M h_1^W}
\]

(5.90)

where it is easily verified that (5.89) corresponds to (5.87) and does not satisfy (5.80). Thus, \(P_1\) is given by (5.90).
We note that it will be optimal for both users to transmit iff

\[
\frac{h_2^M - h_2^W}{\lambda_2} \geq \frac{(h_1^M h_2^W - h_1^W h_2^M)^2}{(\lambda_1 h_2^M - \lambda_2 h_1^M)(\lambda_1 h_2^W - \lambda_2 h_1^W)} \geq \frac{h_1^M - h_1^W}{\lambda_1}
\]  

(5.91)

We can verify that the above quantities are all positive, since from our assumption earlier, \(\lambda_1 (h_2^M - h_2^W) > \lambda_2 (h_1^M - h_1^W)\), we have \(\lambda_1 h_2^M - \lambda_2 h_1^M > \lambda_1 h_2^W - \lambda_2 h_1^W\), and furthermore

\[
\lambda_1 (h_2^M - h_2^W) > \lambda_2 (h_1^M - h_1^W)
\]  

(5.92)

\[
\geq \lambda_2 \left( h_1^M - \frac{h_1^M h_2^M}{h_2^M} \right)
\]  

(5.93)

\[
= \lambda_2 \frac{h_1^M}{h_2^M} (h_2^M - h_2^W)
\]  

(5.94)

which allows us to write

\[
\frac{\lambda_1}{\lambda_2} > \frac{h_1^M}{h_2^M} \geq \frac{h_1^W}{h_2^W}
\]  

(5.95)

It is straightforward to verify that

\[
\frac{(h_1^M h_2^W - h_1^W h_2^M)^2}{(\lambda_1 h_2^M - \lambda_2 h_1^M)(\lambda_1 h_2^W - \lambda_2 h_1^W)} = \Psi = \Phi^M \Phi^W
\]  

(5.96)

for the power allocations given in (5.90) and (5.86).

We now consider the remaining case, which is when the solution satisfies \(h_2^M - h_2^W > \frac{h_1^M - h_1^W}{\lambda_1} > \Psi\). In this situation, we see that

\[
\frac{\theta_1}{\lambda_1} \geq \frac{h_1^M - h_1^W}{\lambda_1} > \Psi
\]  

(5.97)
and as such, we have $P_1^* = 0$. However, if $P_1^* = 0$, we also have

$$\frac{\theta_2}{\lambda_2} = \frac{h_2^M - h_2^W}{\lambda_2} > \Psi \quad (5.98)$$

and we again have $P_2^* = 0$. Since $h_1^M - h_1^W > \lambda_1$, $h_2^M - h_2^W > \lambda_2$ implies that one user must always be transmitting, clearly this solution is not possible.

Combining our results in this section, we arrive at the following theorem:

**THEOREM 5.3.** Without loss of generality, assume $\frac{h_1^M}{h_1^W} \geq \frac{h_2^M}{h_2^W}$, and let

$$p_k \triangleq \frac{1}{2} \left( \frac{1}{h_k^W} - \frac{1}{h_k^M} \right) + 4 \left( \frac{1}{h_k^W} - \frac{1}{h_k^M} \right)^2 - \frac{1}{2} \left( \frac{1}{h_k^W} + \frac{1}{h_k^M} \right) \quad (5.99)$$

$$q_k \triangleq \frac{\lambda_k (h_1^M h_2^W - h_2^M h_1^W)}{(\lambda_1 h_2^M - \lambda_2 h_1^M)(\lambda_1 h_2^W - \lambda_2 h_1^W)} - \frac{h_k^M - h_k^W}{h_1^M h_2^W - h_2^M h_1^W} \quad (5.100)$$

The power allocation that maximizes the achievable secrecy sum-rate is as following:

$$(P_1^*, P_2^*) = \begin{cases} (0, 0), & \text{if } h_1^M - h_1^W \leq \lambda_1, \ h_2^M - h_2^W \leq \lambda_2 \\
(p_1, 0), & \text{if } h_1^M - h_1^W > \lambda_1, \ h_2^M - h_2^W \leq \lambda_2 \\
(0, p_2), & \text{if } h_1^M - h_1^W \leq \lambda_1, \ h_2^M - h_2^W > \lambda_2 \\
(p_1, 0), & \text{if } h_1^M - h_1^W > \lambda_1, \ h_2^M - h_2^W > \lambda_2 \\
(-q_1, q_2), & \text{if } h_1^M - h_1^W > \lambda_1, \ h_2^M - h_2^W > \lambda_2 \end{cases} \quad (5.101)$$
5.5 Sum Rate Maximization with Cooperative Jamming

We denote the transmission power of user $k$ as $P_k$ and jamming power of user $k$ as $Q_k$. Then, the instantaneous sum-rate achievable is given by:

\[
\frac{1}{2} \log \left( \frac{1 + h_1^M (P_1 + Q_1) + h_2^M (P_2 + Q_2)}{1 + h_1^MQ_1 + h_2^MQ_2} \right) - \frac{1}{2} \log \left( \frac{1 + h_1^W (P_1 + Q_1) + h_2^W (P_2 + Q_2)}{1 + h_1^WQ_1 + h_2^WQ_2} \right) \tag{5.102}
\]

We can write the optimization problem as

\[
\max_{P_1(h), P_2(h)} \int_0^\infty \cdots \int_0^\infty \log \left( \frac{\phi^M + \phi^M - 1}{\phi^W + \phi^W - 1} \cdot \phi^W \right) p(h) dh \tag{5.103}
\]

subject to

\[
\int_0^\infty \cdots \int_0^\infty (P_k(h) + Q_k(h)) p(h) dh \leq \bar{P}_k, \quad k = 1, 2 \tag{5.104}
\]

\[
P_k(h) \geq 0, \quad k = 1, 2 \tag{5.105}
\]

\[
Q_k(h) \geq 0, \quad k = 1, 2 \tag{5.106}
\]

where

\[
\phi^M = 1 + h_1^M Q_1 + h_2^M Q_2 \tag{5.107}
\]

\[
\phi^W = 1 + h_1^W Q_1 + h_2^W Q_2 \tag{5.108}
\]

and $\phi^M, \phi^W$ are as defined in (5.43), (5.44). We also stress that $P_1, P_2, Q_1, Q_2$ are functions of $h$ even though this is not explicitly shown.

We first show that dividing power is suboptimal, i.e., the optimum power allocation should not have $P_k, Q_k > 0$. We prove this using contradiction. Assume the optimum power
allocation is $P^*, Q^*$, and for user 1, $P_1^*, Q_1^* > 0$. Note

$$\frac{\partial \omega^W}{\partial Q_1} = \frac{h_1^W \phi^M - h_1^M \phi^W}{\phi^M^2}$$

$$= \frac{h_1^W - h_1^M - (h_1^M h_2^W - h_2^M h_1^W) Q_2}{\phi^M^2}$$

the sign of which does not depend on $Q_1$. Consider a power allocation such that $P_1 = P_1^* - \pi, Q_1 = Q_1^* + \pi$. Then, $P_1 + Q_1 = P_1^* + Q_1^*$ and $\frac{\Phi^M + \phi^M - 1}{\phi^M + \phi^W - 1}$ does not change. If (5.110) is positive, any $\pi > 0$ causes an increase in the achievable sum-rate, and jamming with the same sum power is better. If (5.110) is negative, then any $\pi < 0$ increases the sum-rate, and transmitting with the same sum power gives a higher rate. If this quantity is zero, the sum-rate does not depend on $Q_2$, and we can set it to 0. Thus, we see that the optimal allocation will have either $P_k > 0$ or $Q_k > 0$, but never both. Note that this also implies that we must have $\frac{\phi^W}{\phi^M} \geq 1$, or else a power allocation that gives the same sum power to transmission would achieve a higher rate.

We can then write the derivative of the Lagrangian with respect to the transmit power of user $k$ as

$$\frac{\partial L}{\partial P_k} = \frac{h_k^M}{\Phi^M + \phi^M - 1} - \frac{h_k^W}{\Phi^W + \phi^W - 1} - \lambda_k + \mu_k = 0$$

(5.111)

Noting that we must have

$$\frac{\Phi^M + \phi^M - 1}{\phi^M} \geq \frac{\Phi^W + \phi^W - 1}{\phi^W}$$

(5.112)

to have a non-negative secrecy rate, we can write

$$\lambda_k - \mu_k = \frac{h_k^M}{\Phi^M + \phi^M - 1} - \frac{h_k^W}{\Phi^W + \phi^W - 1}$$

(5.113)
and as a result, if \( \phi^W h^M_k - \phi^M h^W_k < \lambda_k \), we must have \( \mu_k > 0 \Rightarrow P_k = 0 \). Now consider the jamming powers:

\[
\frac{\partial L}{\partial Q_k} = \frac{h^M_k}{\Phi^M + \phi^M} - \frac{h^W_k}{\Phi^W + \phi^W} - \frac{h^M_k}{\phi^M} + \frac{h^W_k}{\phi^W} - \lambda_k + \nu_k
\]  

Using (5.111) in (5.117), we get

\[
-\frac{h^M_k}{\phi^M} + \frac{h^W_k}{\phi^W} + \nu_k = \mu_k
\]  

If a user is jamming, we must have \( \nu_k = 0, \mu_k \geq 0 \). Hence,

\[
\frac{h^W_k}{\phi^W} \geq \frac{h^M_k}{\phi^M}
\]  

Since we should not have both users jamming at the same time (in which case the achievable rate is 0 and we should stop any transmission), this implies that for the jamming user,

\[
\frac{h^W_k}{h^M_k} \geq \frac{1 + h^W_k Q_k}{1 + h^M_k Q_k} \Rightarrow h^W_k \geq h^M_k
\]  

Thus, if a user has \( h^W_k > h^M_k \), then we necessarily have \( \frac{h^W_k}{\phi^W} > \frac{h^M_k}{\phi^M} \) and as a result \( \mu_k > 0 \), indicating that user is not transmitting, as expected. If both users have \( h^W_k \geq h^M_k \), no user transmits or jams. We see that
• A user will not be transmitting if $\phi^W h_k^M - \phi^M h_k^W < \lambda_k$.

• A user will not be jamming if $\phi^W h_k^M - \phi^M h_k^W > 0$ (or equivalently $h_k^M \geq h_k^W$).

If, for both users we have $h_k^M \geq h_k^W$, neither user will be jamming, and we can find the solutions from Section 5.4.

We would like to find out when the solution takes the form if one user transmitting and the other jamming. Without loss of generality, assume $P_1 > 0, Q_2 > 0$, i.e. when user 1 is transmitting and user 2 is jamming. We can re-write (5.117) as:

$$h_2^W h_1^M P_1^\phi^M (\phi^M + \phi^M - 1) - h_2^M h_1^W P_1^\phi^M (\phi^W + \phi^W - 1)$$

$$= \lambda_2^\phi^M (\phi^M + \phi^M - 1)(\phi^W + \phi^W - 1) \quad (5.121)$$

We then need to have the following two equations simultaneously satisfied:

$$\frac{h_1^M}{\phi^M + \phi^M - 1} - \frac{h_1^W}{\phi^W + \phi^W - 1} = \lambda_1 \quad (5.122)$$

$$\frac{h_2^W h_1^W / \phi^W}{\phi^W + \phi^W - 1} - \frac{h_2^M h_1^M / \phi^M}{\phi^M + \phi^M - 1} = \frac{\lambda_2}{P_1} \quad (5.123)$$

Although we have not been able to find a simple close-form expression for this case, we see that for a given jamming power $Q_2$, user 1’s power is found from (5.57) with $Q_2$ instead of $P_2$. We note the following two observations for cooperative jamming:

1. Cooperative jamming effectively reduces the transmission threshold for the active user. Since $\phi^W \geq \phi^M$, we see that the condition to transmit is relaxed from $h_k^M - h_k^W \geq \lambda_k$ to

$$\frac{\phi^W}{\phi^M} h_k^M - h_k^W \geq \lambda_k.$$  

2. A user only jams if its main channel gain is lower than that of its eavesdropper channel gain.
5.6 Numerical Results and Observations

The secrecy sum-rate maximizing power allocation with fading is such that we use higher transmission powers when channel conditions are more favorable, i.e., high main channel gains, low eavesdropper channel gains, and cease transmission when channel conditions are unfavorable, i.e., the main channel gain is not better than the eavesdropper channel gain by a certain threshold. The power allocations in this case, however, do not have a simple water-filling interpretation as in the case without secrecy constraints. Yet, for really favorable channel conditions, the power allocation approximates the standard water-filling solution. With cooperative jamming, a user facing unfavorable channel conditions can jam the eavesdropper (with more power used for jamming when the eavesdropper channel is much stronger), and allow the other user to transmit by effectively lowering the threshold that the difference of that user’s main and wiretapper channel gains must exceed.

We also considered independent Rayleigh fading for all channels where the power gains $h^M_1, h^M_2, h^W_1, h^W_2$ obey exponential distributions. Letting the mean gain for the main channels to be 1, we plot the achievable ergodic secrecy sum-rate and upper bound in Figure 5.2 as a function of the mean eavesdropper channel gain. The dashed lines represent instantaneous power control, where we impose the same maximum power constraint on each fading block. The solid lines represent ergodic fading case, where we maintain a long-term average power constraint. The lines denoted by $\nabla$ show achievable rates, the lines denoted by $*$ represent achievable rates with cooperative jamming, and the lines denoted by $\triangle$ show the outer bounds. We see that the outer bounds and achievable rates for both instantaneous and ergodic power control are close when the eavesdropper channel is weak, but drift apart as the eavesdropper channel gets stronger. Cooperative jamming improves the achievable secrecy sum-rate most when the eavesdropper channel is strong, as it is possible to more effectively jam the eavesdropper. We note the increase in the achievable secrecy sum-rate when the transmitters have, on average, a high eavesdropper channel. In this case, when one of the transmitters has a good, and the other had a bad channel, cooperative jamming allows very high instantaneous rates.
5.7 Conclusions

In this chapter, we examined the block-fading Gaussian Multiple-Access Wire-Tap Channels (GMAC-WT). We provided achievable regions and the secrecy sum-rate upper bound to the block-fading GMAC-WT. We gave the sum-rate optimizing power allocations for the GMAC-WT. We showed that the optimum power allocation does not have a simple water-filling interpretation as opposed to the standard GMAC. In addition, there are certain cases where unlike GMAC, it is optimal for both users to transmit. We then gave a solution when we incorporate cooperative jamming, and note that cooperative jamming is useful when one of the transmitters has a better eavesdropper channel than its main channel, and furthermore the other transmitter has a main channel that is better than its eavesdropper channel by a certain margin that is lower than the non-jamming case. We gave numerical results showing the achievable secrecy sum-rates and upper bound in a Rayleigh fading setting, and showed that cooperative jamming provides a clear improvement in the achievable rates.
Fig. 5.2: Achievable secrecy sum-rate and upper bound as a function of mean eavesdropper channel gain $h_W$. 
Chapter 6

Conclusion

6.1 Thesis Summary

In this thesis, we investigated physical layer secrecy strategies for some multiple access channels. Specifically, we considered information theoretical, provable, measures of secrecy for Gaussian multiple-access, Gaussian two-way and binary additive two-way channels under quasi-static channel models. Lastly, we also considered the Gaussian multiple-access wire-tap channel under an ergodic fading, full channel state information assumption.

First, we looked at the degraded Gaussian multiple-access wire-tap channel (GMAC-WT). We defined two secrecy measures, which we termed collective and individual secrecy constraint, to reflect two different scenarios corresponding to the cases where users trust each other or not. Under these constraints, we developed achievable secrecy rate regions, and also found an upper bound on the secrecy sum-rates. We showed that the trust that users place on each other allows a larger rate region to be achievable under collective constraints. However, both sets of constraint can achieve the same secrecy sum-rate, which is seen to correspond to the upper bound, giving the same secrecy sum-capacities for both constraints.

Next, we considered the general Gaussian multiple-access wire-tap channel under the more interesting collective secrecy constraints. We found an achievable secrecy rate region, and an upper bound on the achievable secrecy sum-rate. We showed that the achievable rates and the upper bound only coincide for the degraded case, and in general there is some gap. We also noted that, under collective constraints, users are essentially allowed to provide secrecy for each other, allowing a user to sacrifice some of its rate to generate secrecy for another user who would otherwise not be able to achieve secrecy on its own. This is shown to be suboptimal from a secrecy sum-rate maximization point of view, resulting in a fairness/sum-rate trade-off.
Motivated by this, we also proposed a new scheme, called \textit{cooperative jamming}, where users who cannot transmit in secrecy jam the eavesdropper instead, allowing the remaining users to achieve a higher secrecy sum-rate. This scheme was numerically shown to achieve a secrecy sum-rate much closer to the upper bound.

Later, we considered the Gaussian and binary-additive two-way channels, which we called GTW-WT and BATW-WT, respectively, under the collective constraints. We found achievable secrecy rates for these two channels, and observed that the nature of these channels provide what is essentially side-information to each transmitter. By subtracting their self-interference, each user obtains a clear channel to the other user, whereas the eavesdropper is confused by the multiple-access channel. This extra information results in higher achievable rates compared to the Gaussian multiple-access channel with the same channel parameters. For the BATW-WT, the same applies, as each user’s transmitted codewords acts almost like a one-time pad for the other user’s codewords. We noted that as long a user is not decodable by treating the other user as noise, it can transmit with maximum power, and as such there is no fairness/sum-rate tradeoff. We also investigated cooperative jamming for these channels, and saw that if a user is not able to achieve secrecy, it can jam the eavesdropper with maximum power without hurting the other user, since it knows the jamming sequence. We showed that for the BATW-WT, this allows the transmitting user to achieve its single-user channel capacity with perfect secrecy.

Finally, we considered the block-fading Gaussian multiple-access wire-tap channel under an ergodic fading process assumption and perfect channel state information at all points. We noted that by not transmitting during unfavorable channel states, and transmitting during very favorable states, while maintaining a long-term average power constraint, it is possible to achieve higher secrecy rates. We then considered cooperative jamming for this scenario. We showed that even if the fading process favors the eavesdropper in general, the achievable secrecy sum-rates may actually increase, since there are more fading states where a user has a favorable channel to transmit, and the other user has a very unfavorable channel, which allows it to jam the eavesdropper effectively.
In summary, we note that multiple-access channels provide additional avenues for providing system secrecy and are, in general, more robust than single-user channels when considering secrecy at the physical layer. “Good” users may help “weak” users in providing secrecy if the design goal is fairness, and “weak” users may help “good” users by jamming the eavesdropper if the design goal is total throughput. Most of the results presented in this thesis were presented at academic conferences, [39,40,41,42,44,45], and also submitted as journal publications, [38,43].

6.2 Future Work

Throughout the thesis, we mostly considered achievable secrecy rate regions and quasi-static and known channel parameters. We mostly concerned ourselves with the achievable secrecy sum-rates, and developed upper bounds for these rates. More general outer bounds on the achievable secrecy rates have thus far proved elusive. In addition, the sum-rate upper bound we gave for the GMAC-WT can only analytically be shown to be tight for the degraded eavesdropper case, although we showed numerically that cooperative jamming can give rather tight results in some cases. Thus, finding tighter outer bounds in general would be a valuable addition to the state of research in this area, as the capacity regions for these channels are still unknown.

Another limitation of this work is that code design and rate-selection requires knowledge of eavesdropper channel parameters, which are not easily available in practice. While, in this theoretical framework, knowledge of these statistics is essential for the quasi-static channel models, effects of estimation errors is an important and interesting question. In addition, while there is some progress on finding practical codes for the single-user wire-tap channels [54], finding similar codes for these multiple-access channels brings other challenges, and will need to be addressed before a practical implementation.

Finally, for the ergodic fading scenario, investigation of achievable rates with only knowledge of eavesdropper channel statistics and not their actual values would be of interest for more practical applications of the wire-tap channel concept.
References


[12] U. M. Maurer, “Secret key agreement by public discussion from common information,”


[17] ——, “Secret-key agreement over unauthenticated public channels - part I: Definitions and a completeness result,”

[18] ——, “Secret-key agreement over unauthenticated public channels - part II: The simulatability condition,”

[19] ——, “Secret-key agreement over unauthenticated public channels - part III: Privacy amplification,”


[21] ——, “The common randomness capacity of a network of discrete memoryless channels,”

[22] I. Csiszár and P. Narayan, “Common randomness and secret key generation with a helper,”


Ender Tekin was born in Ankara, Turkey in 1978. He received his Bachelor of Science degree in Electrical and Electronics Engineering from Bogazici University, Istanbul, Turkey in 2000, and his Master of Science degree from the Pennsylvania State University, University Park, PA in 2001. He has been with the Wireless Communications and Networking Laboratory, working under the supervision of Prof. Aylin Yener as his advisor since 2002. He also worked as a teaching assistant between 2002-2006. In 2006, he was awarded the Cingular Wireless Graduate Fellowship. His main research interests are information theory and multi-user digital communications systems. During his Ph.D. studies, he focused on provably secure communications systems for multiuser networks. He is a member of IEEE since 2001, and has served as reviewer for several IEEE journals and conferences. A comprehensive list of his publications can be found as references [39,40,41,42,44,45,38,43].

Selected Publications:
