Power Allocation and Signal Labelling on Physical Layer Security

Weichen Xiang

Newcastle University

Newcastle upon Tyne, UK.

A thesis submitted for the degree of

Doctor of Philosophy

March 2016

To my loving family

Sure I am that this day we are masters of our fate that the task which has been set before us is not above our strength; that its pangs and toils are not beyond my endurance. As long as we have faith in our own cause and an unconquerable will to win, victory will not be denied us.

-Winston Churchill

You do not need an invitation to make profit.

-Dhirubhai Ambani

Acknowledgements

I would like to thank Dr. Stéphane Le Goff and Dr. Martin Johnston for their continuous guidance and help on my research. Also, I would like to thank Prof. Zhiguo Ding and Dr. Kanapathippillai Cumanan for their kind support and encouragement on both my research and the Ph.D life. Finally, I would like to thank the school of Electrical and Electronic Engineering of Newcastle university for the excellent research environment.

Abstract

Secure communications between legitimate users have received considerable attention recently. Transmission cryptography, which introduces secrecy on the network layer, is heavily relied on conventionally to secure communications. However, it is theoretically possible to break the encryption if unlimited computational resource is provided. As a result, physical layer security becomes a hot topic as it provides perfect secrecy from an information theory perspective. The study of physical layer security on real communication system model is challenging and important, as the previous researches are mainly focusing on the Gaussian input model which is not practically implementable.

In this thesis, the physical layer security of wireless networks employing finite-alphabet input schemes are studied. In particular, firstly, the secrecy capacity of the single-input single-output (SISO) wiretap channel model with coded modulation (CM) and bit-interleaved coded modulation (BICM) is derived in closed-form, while a fast, sub-optimal power control policy (PCP) is presented to maximize the secrecy capacity performance. Since finite-alphabet input schemes achieve maximum secrecy capacity at medium SNR range, the maximum amount of energy that the destination can harvest from the transmission while satisfying the secrecy rate constraint is computed. Secondly, the effects of mapping techniques on secrecy capacity of BICM scheme are investigated, the secrecy capacity performances of various known mappings are compared on 8PSK, 16QAM and (1,5,10) constellations, showing that Gray mapping obtains lowest secrecy capacity value at high SNRs. We propose a new mapping algorithm, called maximum error event (MEE), to optimize the secrecy capacity over a wide range of SNRs. At low SNR, MEE mapping achieves a lower secrecy rate than other well-known mappings, but at medium-to-high SNRs MEE mapping achieves a significantly higher

secrecy rate over a wide range of SNRs. Finally, the secrecy capacity and power allocation algorithm (PA) of finite-alphabet input wiretap channels with decode-and-forward (DF) relays are proposed, the simulation results are compared with the equal power allocation algorithm.

Contents

List of Figures

List of Tables

Nomenclature

Symbols

α	The minimum value of d_e
χ	constellation
χ_i^b	sub-constellation with i-th bit value equal to b
γ	signal to noise ratio
$[\cdots]^+$	choose the maximum value
MMSE	minimum mean square error
$\mathcal{M}(\cdots)$	transformed minimum mean square error
C	channel capacity
C_S	secrecy capacity
d_e	Euclidean distance
d_H	Hamming distance
$E[\cdots]$	Expectation
$I(\cdots)$	mutual information
$N(\cdots)$	distance spectrum

Acronyms/Abbreviations

AF	Amplify and forward
$AM-GM$	Arithmetic mean-Geometric mean
APP	A Posteriori Probabilities

$AWGN$ Additive White Gaussian Noise

BER Bit Error Rate

$BICM$ Bit Interleaved Coded Modulation

$BICM-ID$ BICM with iterative decoding

$CDMA$ Code Division Multiple Access

CE Channel Estimation

CM Coded Modulation

CSI Channel State Information

DF Decode and Forward

DSP Digital Signal Processing

ECC Error Correction Coding

EH Energy harvesting

FAI Finite Alphabet Input

$FDMA$ Frequency Division Multiple Access

FSK Frequency Shift Keying

$GCSI$ Global channel statement information

$LDPC$ Low density parity check

LLR Log Likelihood Ratio

MAP Maximum a Posteriori

MEE Maximum error event

$MIMO$ Multi-antenna Input Multi-antenna Output

$MISO$ Multi-antenna Input single-antenna Output

$MMSE$ Minimum Mean Square Error

MSE Mean Square Error

$MSEW$ maximum squared Euclidean weight

$OFDM$ Orthogonal Frequency Division Multiplexing

PA Power allocation

PCP Power control policy

PDF Probability Density Function

PLS Physical layer security

QAM Quadrature Amplitude Modulation

$QPSK$ Quadrature Phase Shift Keying

RF Radio Frequency

SC secrecy capacity

$SISO$ single input single output

SNR Signal to Noise Ratio

SP Set Partitioning

TCM Trellis Coded Modulation

$TDMA$ Time Division Multiple Access

UWB Ultra wide band

$WLAN$ Wireless local area network

Chapter 1

Introduction

1.1 Introduction

In recent years, there has been a rapid growth in the research and development of wireless networks. The increase of the data rate enables users, who are under the wireless signal coverage to transfer large amount of data with fast speed. However, as people become more relying on the wireless communication, communication security issues grow more important, as the radio frequency (RF) signal can be received by unintended users due to the broadcast nature of wireless signals. The communication systems of the future require not only the fast and reliable transmission of information, but also the secure transmission of information.

The traditional method of securing the communication is by using the cryptography technique. Cryptography is applied to the network layer to secure the communication. Based on mathematical theory and computer science technology, modern cryptography generates a highly complex secrecy key and secures the communication. In theory, only secure key holders can view the encrypted message. The cryptography technique has been applied to practical use for decades and provides a considerably reliable method to secure communication. However, the cryptography technique has its own disadvantages: firstly, the channel condition in the wireless environment introduces challenges to the secret key distribution. Secondly, generating a highly secure secret key requires knowledge of complicated mathematics. Finally and most importantly, as computational power is growing rapidly with the invention of new computer techniques, the secret key is theoretically breakable by exhaustive searching providing massive computational resources are available.

On the physical layer, where the RF signals are transmitted and received, a information-theoretical method to secure the communication is introduced, namely physical layer security (PLS) [3]. The PLS explores the maximum information rate that can be transmitted whilst avoiding interception. This rate is computed based on the assumption of perfect code and decoding algorithm are applied to the wiretap channel. Thanks to the turbo code and the rediscovery of LDPC code, it is possible to transmit data at a capacity approaching rate that enables the practical secure communication to obtain close-to-theory performance. By combining PLS and cryptography techniques, the confidential message can be well secured.

The PLS is initially studied on the degraded channel model, in which the channel between the sender and the eavesdropper (wiretap channel) is a degraded version of the channel between the sender and the destination (main channel). It is shown that the confidential message can be transmitted to the intended receiver with no error, whilst being partially unnoticed by the eavesdropper. The maximum unnoticed information rate is defined as secrecy capacity with a notation of C_S. Later, the results of PLS on the degraded channel are extended to the Gaussian channels, showing that the secrecy capacity is positive if the main channel is less noisy than the wiretap channel and the value of secrecy capacity is equal to the capacity difference between the main channel and the wiretap channel.

Nowadays, wireless communication technology is widely applied in our daily life. This is demonstrated by the extensive use of mobile phones and wireless local area networks (WLAN). Due to the nature of the wireless broadcast, the transmission signals can either be received by the intended user, or be caught by any other users. In the recent past, research on PLS has extended to the fading channels, finding that a positive secrecy rate is achievable in the fading channels even if the SNR in the main channel is smaller than the SNR in the wiretap channel, on average. It is crucial to determine the secrecy capacity of the practical communication systems employing finite-size constellations.

As the decoding complexity and the computational resource costs increase dramatically with the constellation size increases, the practical communication system employs finite-alphabet input. In contrast to Gaussian input, the channel capacity of the finite-alphabet input schemes is upper bounded by $\log_2 M$, where M is the constellation size. The research on trellis coded modulation (TCM) indicate that the secrecy capacity becomes zero if the transmission power increases to infinity

and the maximum value of secrecy capacity has to found by exhaustive searching due to no closed-form solution to the mutual information so far. Similar to TCM, bit-interleaved coded modulation(BICM) is a widely applied finite-alphabet input scheme, BICM out performs TCM over Rayleigh fading channels in terms of bit error rate (BER) performance. In contrast to the TCM scheme, BICM capacity is affected by the mapping technique, therefore, the secrecy capacity performance of BICM varies if a different mapping technique is applied. Since the mutual information is used in the secrecy performance computation for finite-alphabet input schemes, the term *secrecy capacity* is not accurate to describe the secrecy performance. In the remaining of this thesis, secrecy rate R_S is used to denote the maximum equivocation rate in the finite-alphabet input wiretap channel model.

Recently, the cooperative communication technique has been introduced to the PLS in order to enhance the secrecy capacity performance and to prevent the wiretap channel from becoming less noisy than the main channel. The secrecy rate of coded modulation (CM) in the decode-and-forward (DF) relay helped wiretap channel model has been studied in [28], an iterative searching algorithm is established to optimize the transmission power and maximize the secrecy capacity. It is shown that a significant enhancement on secrecy rate performance is obtained by using multiple relays.

1.2 Motivation and challenges

The research on PLS are mainly based on the Gaussian input assumption. Under this assumption, the channel capacity of a binary message is simplified to a closed-form expression, shown as $C = \log_2(1+SNR)$, it is shown that the channel capacity is completely determined by the channel SNR. Thus, the secrecy capacity can be also presented in a function of SNR. For CM and BICM, the closed-form solution to the mutual information has not been obtained, which makes the analysis on secrecy capacity of CM and BICM very difficult. However, it has been demonstrated in relevant works [61] that the secrecy capacity performances of CM and BICM are significantly different to Gaussian input, As the secrecy capacity decreases to zero at high SNR. The power control policy developed in Gaussian input is not applicable to the CM and BICM cases. Thus, it is challenging to study the relationship between SNR and the secrecy capacity on CM and BICM wiretap channel model, moreover,

once the relationship is determined, the optimal power control policy that maximizes secrecy capacity can be obtained.

It has been demonstrated in various works [42–44] that by using the binary reflected Gray mapping, BICM obtains optimal mutual information performance over a wide range of SNR. Without considering the case of BICM with iterative decoding (BICM-ID), Gray mapping outperforms the other mappings on both mutual information and BER performance. However, to achieve maximum secrecy rate performance, one mapping is said to be optimal if it maximizes the difference of mutual information between the main channel and wiretap channel. Gray mapping does not maximize the difference, but maximizes the mutual information for both the main channel and the wiretap channel, which is not desired. Therefore, it is meaningful to study the mapping effects on secrecy rate performance and determine the optimal mapping algorithm for secrecy performance. The main challenge comes from determine the key parameter that best characterize the mapping and directly affect the secrecy rate performance.

It has been proven that positive secrecy rate is not achievable if the main channel SNR is smaller than the wiretap channel SNR for single antenna wiretap channel model. The transmission has to be paused and waiting for the main channel SNR become larger than the wiretap channel SNR. However, by using the cooperative communication technique and introducing helper relays to the wiretap channel model that establishes additional communication channels can solve this problem. Until now, on finite-alphabet input schemes, existing research has relied on exhaustive searching to find the the optimal PA algorithm, which maximizes the secrecy capacity. A PA with low computational cost while maintaining high secrecy capacity performance is demanded.

1.3 Aims

The aim of this thesis is to develop a closed-form solution to the secrecy capacity and optimal power control policy for the finite-alphabet input wiretap channel. The theoretical tools for analyzing secrecy capacity performance are derived in this thesis. With the aim of secrecy capacity maximization and transmission power minimization, the theoretical expression of the closed-form solution to the power control policy is expected. Comprehensive discussions on the mapping issues for

secrecy rate maximization are presented in this thesis in order to obtain the optimal mapping algorithm for secrecy rate performance. In addition, this study also explores the cooperative communication methods that can enhance the secrecy rate performance.

1.4 Objectives

The objectives of this thesis are outlined as follow:

- Develop a closed-form relation between secrecy capacity and MMSE over Gaussian wiretap channels with detailed proof.
- Analyse the bit-labelling effects to the secrecy rate performance and develop an optimal bit-labelling rule for secure communication.
- Develop fast power allocation policy to maximize the secrecy rate performance of SISO wiretap channels employing CM and BICM schemes over Rayleigh fading channels.
- Investigate secrecy rate performance and optimal power allocation policy for the wiretap channel with DF relay with detailed proof.

1.5 Thesis Layout

The remainder of this thesis is organized as follows: in chapter 2, the related literatures are revised. In chapter 3, we provide a brief review of the key concepts related to this thesis. In Chapter 4, the relation between channel capacity and MMSE is reviewed and the secrecy rate is formulated into a function of MMSE and SNR. By introducing a linear to logarithm domain transformation to MMSE, a fast PCP is presented and the maximum secrecy rate is formulated in a closed-form. Furthermore, by using quartic approximation to the transformed MMSE, the secrecy rate and mutual information of 8PSK and 16QAM are approximated in closed-form. Finally, with the aim of saving energy, the energy-harvesting ratio of BICM schemes under secrecy constraint is determined. Numerical simulation results are provided to validate the analysis. In Chapter 5, the effect of mapping techniques to

secrecy rate performance is investigated. In this chapter, the secrecy rate of various mappings, such as Gray mapping, set-partitioning mapping, maximum squared Euclidean weight mapping etc. are compared. By splitting the constellations into sub-constellations and investigating the effect of average Hamming distance of the mappings to the secrecy capacity performance, an optimal mapping algorithm for secrecy communication is proposed. The simulations of the proposed optimal mapping for secrecy rate performance and various other mappings are shown on 8PSK, 16QAM and (1,5,10) constellations. In Chapter 6, the secrecy rate performance of a wiretap channel model employing CM and BICM schemes helped by a relay is studied. We assume the relay acts as a helper node using the decode-and-forward technique. By employing the closed-form approximation of the secrecy rate, a computational resource saving closed-form power allocation policy is proposed. Finally, in Chapter 7, conclusions for this thesis are drawn and the future plans for continued research are listed.

1.6 List of Publications

In this research, one first author journal paper has been published and one conference paper has been published.

Journal paper:

- W. Xiang, S. Y. Le Goff, M. Johnston and K. Cumanan,"Signal mapping for bit-interleaved coded modulation schemes to achieve secure communications," *IEEE Commun. Lett.*, Vol. 4, no. 3, pp. 249-252, Jun. 2015.
  - W.xiang, S.Y. Le Goff and M. Johnston,"Closed-form solutions to the power control policy for wiretap channel employing BICM schemes," submitted to *IEEE Trans. Wireless Commun.*

Conference paper:

- W. Xiang, S, L. Goff and Z. Ding, "Achievable secrecy rate of bit-interleaved coded modulation", The First International Workshop on High Mobility Wireless Communications (HMWC), Chengdu, 2012

Chapter 2

Literature survey

2.1 Physical layer security of SISO wiretap channel model

Physical layer security is a promising technique to secure the communication from an information theory aspect. Soon after C. E. Shannon introduced the famous *shannon limit*, which defines the maximum information rate that can be perfectly recovered after transmission [2], he realized that the information can be secured on the physical layer from an information theoretical point of view [1]. Later, Wyner introduced the wiretap channel model, which models the communication among three users in a network. Within this wiretap channel model, there is a transmitter, often referred to *Alice*, one legitimate receiver named *Bob* and an eavesdropper, called *Eve*. In Wyner's wiretap channel model *Alice* is the message source and wishes to transmit a confidential message to *Bob*, *Eve* observes the communication and intercepts the confidential message. The channel between *Alice* and *Bob* is referred as main channel while the channel between *Alice* and *Eve* is referred as wiretap channel. Wyner proved that the confidential message can be perfectly secured provided the wiretap channel is a degraded version of the main channel. The maximum information rate that can be transmitted by *Alice* with total ignorance by *Eve* is defined as the *secrecy capacity*. The further study in [4] extend Wyner's conclusion, in his work, the wiretap channel is no longer a degraded version of the main channel. It shows that positive secrecy capacity is achieved provided the main channel is less noisy than the wiretap channel. In [5], both the main channel and the wiretap channel are assumed to be Gaussian channels, the study showed that the conclusion

in [4] is applicable to the Gaussian channel case. For the Gaussian wiretap channel, the secrecy capacity is equal to the channel capacity differences between the main channel and the wiretap channel. It shows that, to obtain positive secrecy capacity in the Gaussian wiretap channel, the main channel has to be less noisy than the wiretap channel.

In [10–12], the secrecy capacity is studied over ergodic fading channels. In these works, perfect wiretap channel CSI is assumed known at the transmitter, and the secrecy capacity of rate adaptive transmission is determined. However, the result holds only when the Global CSI is available at the transmitter. The secrecy capacities of slow fading channels are exploited in [6–9]. In these works, the channels in the wiretap channel model are assumed under quasi-static fading. In [6], the transmitter is assumed to know the CSI of both main channel and the wiretap channel perfectly. The optimal power allocation policy to maximize the secrecy capacity is given in a close-form expression. In [9], the transmitter is assumed to have imperfect knowledge of the wiretap channel CSI, thus, *outage probability* is evaluated to measure the probability that the eavesdropper successfully intercepts the confidential message. Moreover, the impact of channel correlation over secrecy capacity is studied in [15], in which the main channel and the wiretap channel are correlated Rayleigh fading channels, it is shown that the secrecy capacity is a logarithm function of the average channel SNR of both channels and the correlation level.

2.2 Physical layer security of MIMO wiretap channel model

The single antenna classical wiretap channel model is highly dependent on the channel condition to achieve positive secrecy capacity, when the SNR in the main channel is smaller than the SNR in the wiretap channel at one instantaneous fading realization, no positive secrecy capacity is achieved. To solve this problem, two alternative transmission scheme are introduced, namely multi-antenna communication and cooperative networking. The secrecy capacity in multi-input multi-output (MIMO) wiretap channel is studied in [13] based on the assumption of that the transmitter has perfect knowledge of the eavesdropper CSI, in which, the optimal power allocation policy is presented by using the eigenvalue maximization method. In [14],

the secrecy capacity of Gaussian MISO channels is investigated and proves that the optimal communication strategy in MISO case is beam-forming. In [16] and [17], in which A. Khisti studied the Wyner's three terminal wiretap channel modesl but with multiple antenna input, multiple antenna eavesdropper, single antenna destination (MISOME) and multiple antenna input, multiple antenna eavesdropper, multiple antenna destination (MIMOME) cases, respectively. In these works, the secrecy capacity is characterized by generalized eigenvalues, and by using beam-forming, the secrecy capacity is maximized. Also, it is shown that the perfect knowledge of the eavesdropper CSI is not strictly necessary to achieve a positive secrecy rate. Additionally, in [18], an upper bound of the secrecy capacity in MIMO case is presented at the high SNR regime provided imperfect CSI of the eavesdropper channel, it is demonstrated that the secrecy capacity performance is near optimal by introducing artificial noise. By using multi-antennas on the receivers, the SNR at the receiver side is strongly affected by the choice of combining method, such as maximum ratio combining (MRC) and selective combining (SC), thus results in different secrecy capacity performance. This combining issue is studied in [19], in which a single input, multiple output (SIMO) wiretap channel system is considered. The analysis show that MRC is more suitable for maximizing the secrecy capacity.

2.3 Secure communication with cooperative communication

Cooperative communication is a promising technique to enhance the secrecy capacity performance of a wiretap channel model. Normally in cooperative communication, an additional node is introduced to the network, known as relay. The relay can either help the legitimate communication by using various forwarding techniques after receiving signals from the transmitter, or it can generate artificial interferences to confuse the eavesdropper. The jamming signal method is introduced in [20], where a relay is introduced to the wiretap channel. The relay transmits a jamming signal to interfere the eavesdropper's decoding ability and ultimately benefits the secrecy capacity of the wiretap channel. In [21–25], the secrecy capacity of cooperative jamming is computed when the legitimate receiver under the assumption of the legitimate receiver having perfect knowledge of the jamming signals while the

eavesdropper has no information about the jamming signals. The jamming signals are not necessarily transmitted from the relay, the source can also generate jamming signals to confuse the eavesdropper. This issue is studied in [27], is proven that when the wiretap link is strong, secrecy capacity performance is better when the jamming signals are generated from the relay. In [26], the secrecy capacity of cooperative jamming in the general Gaussian multiple access wiretap channel is investigated, the power allocation policy for maximizing the secrecy capacity is determined and the simulation shows that cooperative jamming among users can be of great benefit to the secrecy capacity performance. In [27–31], the secrecy capacity of various forward strategies, such as amplify-forward (AF), decode-forward (DF), etc. are studied. In [28], the secrecy capacity of DF is computed and the optimal power allocation (PA) is obtained in closed-form while the optimal PA is obtained via an iterative searching algorithm. In [32], the power allocation policy for AF relay networks under a secrecy constraint is considered, and a water-filling algorithm is used to find the optimal PA algorithm and the simulation shows the solution to be computationally efficient. For DF, the relay observes the source signal, then decodes and re-encodes the message in the same fashion as the source before transmitting them to the destination. In [33], the author considered the secrecy capacity in a wiretap channel with multiple eavesdroppers, by using DF and cooperative jamming (CJ), the optimal PA is proposed to maximize the secrecy capacity.

However, the literatures of secrecy capacity mentioned above are all based on a strong assumption: the message is infinitely long and the channel input follows Gaussian distribution, this assumption is often referred as Gaussian input assumption. However, in practical communications, the modulation size is finite and the channel input is discrete for the convenience of processing the channel output, and some information is lost in quantization [34]. Thus, the mutual information and secrecy rate performance of finite-alphabet input can be very different to the Gaussian input.

2.4 Code modulation and bit interleaved coded modulation

In practical communications, the outputs of the encoder are modulated onto a finite number of complex numbers, this communication model is often referred as finite-alphabet input. Coded modulation (CM) and bit-interleaved coded modulation (BICM) are two widely applied finite-alphabet input schemes. The trellis-coded modulation (TCM) is initially introduced by [35] for AWGN channel communications. The coding and modulation in TCM are regarded as a single entity at the transmitter, the modulated output symbols are interleaved at symbol level and transmitted. In order to optimize the bit-error rate (BER) performance of TCM, set-partitioning (SP) mapping is introduced. Despite the optimal performances in terms of channel capacity and BER over AWGN channels, the BER performance of TCM over Rayleigh fading channels is very poor. In [36–39], the optimal coding design rule of TCM over Rayleigh fading channel is investigated. However, due to the symbol level interleaving, the diversity, which is the minimum Hamming distance of the code, is an important parameter for fading channel BER performance can hardly be increased, thus, the BER performance of TCM over Rayleigh fading channels is not optimal. Aware that the BER performance over Rayleigh fading channel is heavily dependent on the minimum Hamming distance (code diversity) of the code rather than the minimum Euclidean distance of the code, Zehavi introduced bit-interleaved coded modulation (BICM) in [41], where the coding and modulation are no longer combined as a single entity, a bit-wise interleaver is introduced between the encoder and the modulator. The output of the encoder is interleaved at bit level and forwarded to the modulator. In the BICM scheme, the coding and modulation are optimized independently. Later, in [42], the BICM is studied in detail and BICM mutual information is computed by using Monte-Carlo method. It is shown that the BICM mutual information is smaller than the CM mutual information for the same constellation size but has better BER performance over fading channels. Gray mapping obtains the best mutual information performance of the BICM scheme over a medium to high SNR range [43]. In [46], the optimal mapping for ultra wideband (UWB) is studied and strictly regular set partitioning mapping outperforms Gray mapping at a very low SNR range in terms of mutual information. The iterative decoding is initially introduced for Turbo code [51, 52] decoding, as the maximum

likelihood (ML) decoding is over complex to implement. The BER performance of iterative decoding is very close to the ML algorithm if enough iteration is performed. Later, the iterative decoding method is applied onto BICM schemes, the new communication structure is named as bit-iterative coded modulation with iterative decoding (BICM-ID). However, in BICM-ID, the BER performance of Gray mapping shows very little improvement to the increment of iteration, while the BER performances of other mapping schemes, such as set-partitioning, shows great improvement as the number of decoding iteration increases. Considerable amount of research have done in searching for the optimal mapping scheme, which obtains the lowest bit error rate (BER) performance. In [45, 47, 49, 50], various mapping techniques are introduced for BICM-ID, although these mappings show poor performances on mutual information, the BER performances are better than Gray mapping with iterative decoding algorithm. The shape of constellation also affects the BER performances of BICM and a complete study of the constellation shaping is given in [53]. The physical layer security of code modulation systems is studied in [61,62], it is shown that the secrecy rate performance of finite-alphabet input is significantly different to the Gaussian input case, where the secrecy rate at high SNR regime is zero if no PA is applied. Due to the lack of closed-form solution to the AMI of CM schemes, both papers optimize the pre-coding matrix of the transmitter by using the exhaustive searching method. The secrecy rate of a relay wiretap channel with DF transmission strategy is considered in [63], using an adaptive searching method, the optimal power control algorithm is provided.

2.5 Wiener meets Shannon

The major difficulty of secrecy rate research employing finite-alphabet input comes from the lack of closed-form solution to the mutual information. For CM and BICM, the mutual information are evaluated by using the Monte-Carlo method. The closed-form approximation of the mutual information for CM and BICM are obtained over a limited range of SNR. It seems that obtaining a closed-form solution to the secrecy rate is over difficult by only using information theory [65] [64]. In [64], a general formula of AMI in the wideband regime is proposed, and it is shown that the AMI can be approximated by a quadratic function of SNR. The channel capacity of the BICM scheme is further studied in [66], it is proved that CM performs better than

BICM in terms of AMI in the UWB regime. In [65], the AMI of finite-alphabet input is studied at the high SNR range, the author presents an upper-bound and a lower bound in closed-form for the AMI of the BICM scheme.

The research on the fundamental connection between information theory and estimation theory can be traced back to the 1970s. In [54–60], the log-likelihood ratio (LLR) associated with signal detection in Gaussian noise has been investigated, it is shown in [58, 59] that there exists a simple relation between conditional mean estimation and the gradient and Laplacian of the LLR. The mutual information is expressed as the expectation of the LLR of conditional and unconditional measures. It is well known that LLR is a fundamental notion in signal detection and estimation, we can see that information theory and estimation theory is bridged by LLR. Recently, a fundamental relation between the mutual information (MI) and the minimum mean square error (MMSE), which is a fundamental quantity in estimation theory, is presented in [68]. Regardless of the input distribution, MMSE measured at the output is equal to the slope of the MI as long as the channel is exhibiting additive Gaussian noise. The MMSE of the finite-alphabet input schemes are studied in [69, 70], the power control policy for fading channels is presented, furthermore, the MMSE of some commonly used constellations, such as BPSK, 4PAM, 8PSK and 16QAM are obtained and simplified. By using the relation of MMSE and MI, the pre-coding techniques for MIMOME CM schemes over fading channels are presented in [61, 62], in which, the secrecy capacity performance is enhanced by minimizing the information rate at the eavesdropper.

In summery, most of the research on PLS are based on the Gaussian input assumption. However, few researches have been done on the secrecy rate and optimal power control policy of finite-alphabet input schemes. Moreover, the closed-form solutions to the secrecy rate for finite-alphabet input schemes are not obtained. In the next chapter, the mathematical expressions of some key contributions of existing research are presented.

Chapter 3

The background theory

3.1 The channel capacity

The channel capacity defines the maximum throughput of error free data transmission over a communication channel for a given bandwidth in the presence of noise. The Gaussian input channel capacity is a common assumption for research and we start by introducing the Gaussian input channel capacity followed by the finite-alphabet input channel capacity.

Assume X is the channel input, N is the additive white Gaussian noise with zero mean and a variance value of σ^2, the channel output Y is given by

$$Y = X + N. \tag{3.1}$$

We assume that there is a constraint on the input power P, for the input codeword $(x_1, x_2, \ldots, x_n)$, the average power constraint is given by

$$\frac{1}{n}\sum_{i=1}^{n} x_i^2 \leq P. \tag{3.2}$$

The mutual information of the AWGN channel is given by

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y|X) \\ &= H(Y) - H(X+N|X) \\ &= H(Y) - H(N|X) \\ &\leq \frac{1}{2}\log_2 2\pi e(P+\sigma^2) - \frac{1}{2}\log_2 2\pi e\sigma^2 \\ &= \frac{1}{2}\log_2(1+\frac{P}{\sigma^2}). \end{aligned} \tag{3.3}$$

Where e is the base of the natural logarithm.By definition, the channel capacity is the maximum of the mutual information and (3.3) is maximized when X follows Gaussian distribution, so that $E[Y^2] = P + \sigma^2$. The channel capacity in (3.3) can be further written as a function of the signal to noise ratio, which is given by

$$C = \frac{1}{2}\log_2(1+SNR). \tag{3.4}$$

This equation shows that the channel capacity is only determined by the channel SNR. The channel capacity C increases to infinity if the SNR continuous to increase.

However, in practical terms, the Gaussian input model is not implementable as it requires an infinite number of input and the codeword can be infinitely long, thus the decoding complexity is too high for practical implementation. The modulation schemes in real world communication are of finite size, specifically, the modulation size in most cases is set to $M = 2^m$, where m is a positive real number.

The most significant difference between Gaussian input and finite alphabet input is that the information rate of finite-alphabet input schemes do not increase to infinity as SNR rises, the maximum information rate is determined by the size of the modulation M rather than the channel SNR,

$$R_{max} = \log_2 M. \tag{3.5}$$

In the following sections, the system model and the mutual information of two widely used modulation schemes, namely coded modulation (CM) and bit-interleaved coded modulation (BICM) are introduced in detail.

3.1.1 Coded modulation

With the aim of maximizing the minimum Euclidean distance for bandwidth and power-efficient transmission over the AWGN channel, Ungerboeck introduced trellis-coded modulation [35] in 1982. Since then, it is generally accepted that the coding and the modulation blocks have to be combined in a single entity and jointly optimized.

In the CM, the source message is encoded to the codeword $\mathcal{C}$, an ideal interleaver π interleaves $\mathcal{C}$ at the symbol level. The modulator is m-dimensional memoryless and maps the interleaved codeword sequences over a signal set χ following one-to-one labelling rule, where $|\chi| = M$. The m-bit codeword sub-sequence of $\mathcal{C}$ uniquely correspond to a symbol on the constellation. In the TCM, Ungerboeck propose the set-partitioning mapping which is obtained by an m-level partitioning of χ. The transmitted signal is denoted as $X = \{x_1, x_2, \cdots, x_k, \cdots\}$. Let

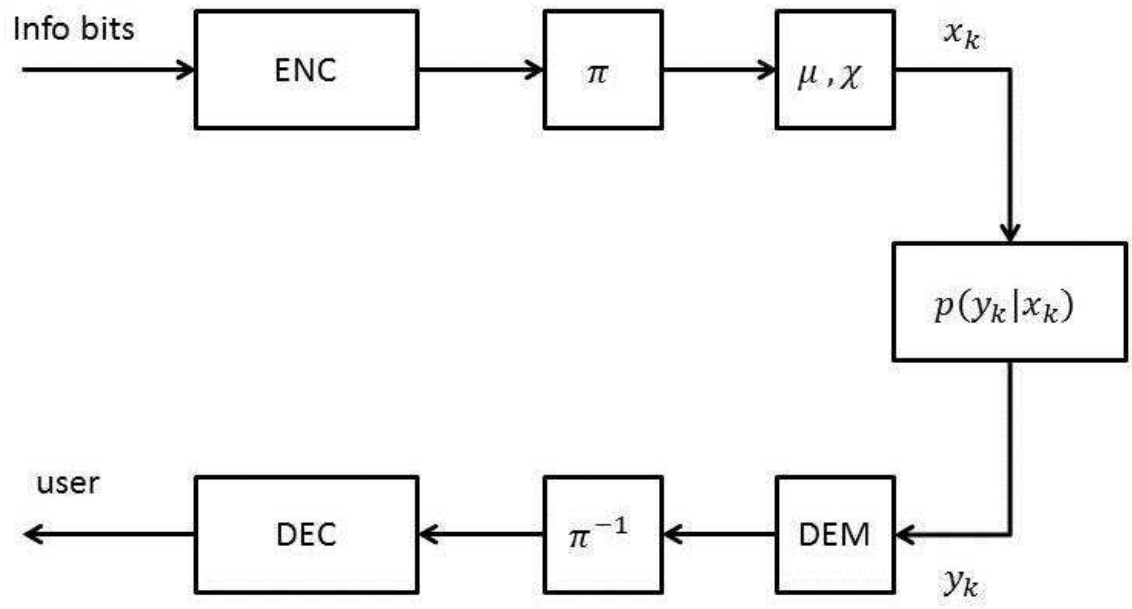

Figure 3.1: Block diagram of the CM or BICM transmission. In the case of CM, π interleaves at the symbol level. In the case of BICM, π interleaves at the bit level.

$Y = \{y_1, y_2, \cdots, y_k, \cdots\}$ denotes the received signal sequence of the corresponding transmitted X, while $H = \{h_1, h_2, \cdots, h_k, \cdots\}$ designate the channel state information (CSI). Assume the noise follows Gaussian distribution, with zero mean and unit variance, the conditional output probability density function is given by

$$p_{Y|X,H}(y_k|x_k, h_k) = \frac{1}{2\pi} \exp(-|y_k - h_k x_k|^2). \tag{3.6}$$

In the remainder of this thesis, the $p_{Y|X,H}(y_k|x_k, h_k)$ is denoted as $P(y|hx)$ for simplicity. Assuming perfect CSI at the receiver, the size of the signal set is M, the mutual information under uniform inputs constraint is given by the conditional average mutual information (AMI)

$$C = I(X;Y) = m - E_{X,Y}\left[\log_2 \frac{\sum_{s\in\chi} p(y|hs)}{p(y|hx)}\right]. \tag{3.7}$$

In this equation, s denotes the constellation points and $m = \log_2 M$. In the remainder of this thesis, we refer this MI by *CM MI*.

3.1.2 Bit-interleaved coded modulation

The BICM is an alternative scheme to CM for bandwidth efficient communications over fading channels, the concept of BICM was first introduced by Zehavi [41] and applied to 8-PSK constellations. There are two main differences between BICM and CM schemes: firstly, the BICM treats coding and modulation as separate components, thus, the BICM receiver is much simpler to design compare to the CM receiver. Secondly, the interleaver used in the BICM scheme perform bit-wise interleaving rather than symbol level interleaving. The codeword sequence $\mathcal{C}$ is interleaved by π, the interleaved sequence $\pi(\mathcal{C})$ is then mapped onto χ. In BICM, the one-to-one correspondence is at the bit level, let $\mathcal{C}_{k,i}$ be the k-th bit of the i-th sub-sequence of $\mathcal{C}$, after interleaving, the m-bit sequence is $\hat{\mathcal{C}}$ and $\mathcal{C}_{k,i}$ is interleaved to $\hat{\mathcal{C}}_{,|}k$, while $\hat{k}$ and j denote the bit position and the number of the m-bit sequence of $\hat{\mathcal{C}}$, respectively.

The mutual information of BICM is much more complex to evaluate than the CM case, due to the bit-wise interleaver "breaks" the relationship between the encoder output bit sequence and the constellation symbol. In [42], the interleaving process is modelled by a random switch followed by m parallel independent and memoryless channels, which is named "parallel channel model". By definition, the AMI of BICM is equal to summing up all AMI in the m branches. For a 2^m-ary signal constellation with additive Gaussian noise N exhibiting a fading coefficient h, the mutual information is given by [42], [53]

$$I(x,y) = m - \sum_{i=1}^{m} E_{b,y}\left\{\log_2 \frac{\sum_{s\in\chi} p(y|hs)}{\sum_{s\in\chi_i^b} p(y|hs)}\right\}. \tag{3.8}$$

Where the operator $E_{b,y}[\,\cdot\,]$ designates the expected value over all possible values in the binary vectors $\mathcal{C}$ and channel output samples y. In this equation, χ_i^b is the sub-set of all signals belonging to χ whose labels are equal to $b \in \{0, 1\}$ at position $i = 0, \ldots, m$ in the mapping. In the remainder of this thesis, we refer this MI by *BICM MI*.

3.2 The wiretap channel model

In [3], Wyner considered the communication model in the presence of an eavesdropper. In this model, the transmitter *Alice* sends a confidential message to the intended receiver *Bob*. The channel between *Alice* and *Bob* is named as the main channel. *Eve* is the eavesdropper, by tapping a wire to the main channel, *Eve* tries to intercept the confidential message. The communication channel between *Alice* and *Eve* is called the wiretap channel or eavesdropper channel. In many secrecy communication researches, including Wyner's work, the channel knowledge of the wiretap channel is assumed known to the transmitter. This assumption is realistic when *Eve* is one active user in the communication network, however, *Eve* is not permitted to all communications. Thus, the active user *Eve* becomes a potential eavesdropper, while *Alice* gains perfect CSI of *Eve*.

Wyner's work has been extended by Csiszár and Körner in [4], in which the secrecy capacity of non-degraded channel version is studied. The Gaussian wiretap channel model is studied in [5], where both the main channel and the wiretap channel are Gaussian channels. The Gaussian wiretap channel model can be extend to the fading channel case easily, as each fading realization can be modelled as the Gaussian channel with complex AWGN.

Fig. 3.2 shows the general Gaussian wiretap channel model, where h_D and h_E denote the channel coefficients of the main channel and wiretap channel, respectively. The noises n_D and n_E are zero mean and unit variance Gaussian noise.

One assumption is made throughout the whole thesis, that is: the channel state information of both main channel and wiretap channel are known at the transmitter. This assumption is practical when both *Bob* and *Eve* are legitimate users in the communication network, however, the message from *Alice* are only for *Bob* in a certain time period. In this model, both *Bob* and *Eve* are active users, they perfectly estimate the CSI of the respective channel and feed back this information to *Alice*.

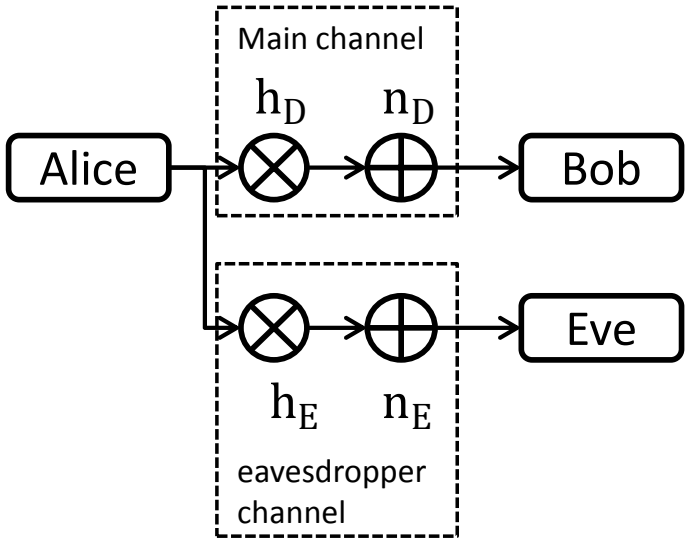

Figure 3.2: The wiretap channel model with one eavesdropper

3.3 The secrecy capacity and the secrecy rate

In 1948, C. E. Shannon considered communications under the secrecy constraint in [1]. In his work, information-theoretical security of the confidential message is guaranteed, this strong secrecy is not affected by the computational resource of the eavesdropper's receiver. In 1978, Wyner built up a wiretap model and studied the secrecy communication in this model [3]. Wyner proved that the confidential message between *Alice* and *Bob* can be transmitted at an information rate R_S with the eavesdropper *Eve* being totally unaware, the maximum value of R_S is defined as the secrecy capacity C_S. Later, the secrecy capacity for the Gaussian channel and Rayleigh fading channel are investigated [5, 6]. In [5], the mutual information for the Gaussian wiretap channel is given by

$$\begin{aligned} C_S &= C_D - C_E \\ &= I(\gamma_D) - I(\gamma_E), \end{aligned} \tag{3.9}$$

where γ_D and γ_E denotes the SNRs of the main channel and the wiretap channel, respectively. It is shown that the secrecy capacity is a bi-variable function of the main channel SNR and the wiretap channel SNR.

We introduce the secrecy capacity of a wireless communication system by considering two cases: perfect wiretap channel CSI is known at *Alice* and imperfect wiretap CSI is known at *Alice*.

We assume that *Bob* and *Eve* have perfect CSI of the main channel and the wiretap CSI, respectively. These assumptions are practical in a slow fading environment, where the channel coefficients remain constant long enough for *Bob* and *Eve* to obtain perfect CSI. We also assume that *Alice* has perfect global CSI. This corresponds with, for instance *Eve* being another active user in the wireless network, for example: in the time-division multiple-access (TDMA) environment. We assume that the both channels are block Rayleigh fading channels, in which the channel coefficients remain constant for every transmission block and vary block to block following Rayleigh distribution. For every transmission block, the wiretap channel can be equivalent to a complex Gaussian channel, the instantaneous secrecy capacity is given by

$$C_S(\gamma_D, \gamma_E) = \left[I(\gamma_D) - I(\gamma_E)\right]^+, \tag{3.10}$$

The operation $[\cdots]^+$ keeps the positive value but scales negative value to 0. This is because *Alice* is able to pause the transmission whenever the wiretap channel is less noisy than the main channel.

By using an adaptive coding technique, the transmission rate can be adapted to every fading realization. Therefore, by taking expectation over all instantaneous secrecy capacity values, the average secrecy capacity is obtained, which is given by

$$\bar{C}_S = E_{h_D,h_E}\left[C_S(\gamma_D, \gamma_E)\right]. \tag{3.11}$$

Therefore, $\bar{C}_S$ is the maximum information rate that *Alice* and *Bob* can hide from the eavesdropper.

Throughout this thesis, the term secrecy capacity refers to the secrecy performance obtained by Gaussian input scheme, while we use *secrecy rate* to describe the secrecy performance of the finite-alphabet input schemes.

3.4 The outage probability

To obtain the secrecy capacity of a wiretap channel model, the CSI of both the main channel and wiretap channel are essential at the transmitter. However, in some cases, it is difficult or even impossible to precisely measure the CSI of the wiretap channel. When *Alice* only knows imperfect CSI of the wiretap channel is known by *Alice*, there is no method to precisely determine the secrecy capacity

and the only solution for *Alice* is to set the secrecy rate to R_S. By doing so, the transmitter is assuming that the mutual information of the wiretap channel is equal to

$$\hat{C}_E = C_D - R_S. \tag{3.12}$$

Where $\hat{C}_E$ denotes the estimation of the wiretap mutual information under imperfect CSI. If $C_E < \hat{C}_E$, perfect CSI can be obtained and R_S is achieved. Otherwise, if $C_E > \hat{C}_E$, the secrecy capacity C_S is smaller than R_S and information theoretic security is compromised [9]. However, if strict secrecy is not required, a lower level of secrecy can be obtained by using the imperfect CSI of the wiretap channel. To measure the security level of the system, outage probability is introduced.

The outage probability $\mathcal{P}_{out}(R_S)$ is the probability of the event $C_S < R_S$, which is given by

$$\begin{aligned}
\mathcal{P}_{out}(R_S) &= P[C_S \leq R_S] \\
&= 1 - P[C_S \geq R_S] \\
&= 1 - P[\log_2(\frac{1+\gamma_D}{1+\gamma_E}) > R_S] \\
&= 1 - \frac{\bar{\gamma}_D}{\bar{\gamma}_D + 2^{R_S}\bar{\gamma}_E} \exp\left(-\frac{2^{R_S}-1}{\bar{\gamma}_D}\right).
\end{aligned} \tag{3.13}$$

where $\bar{\gamma}_D$ and $\bar{\gamma}_E$ denote the average SNR of the main channel and wiretap channel, respectively.

3.5 The secrecy capacity at low SNR regime

If the communication system is power limited but has large bandwidth, the transmission power is averaged over the entire bandwidth and, the SNR is very low. This model is also called the ultra wide band (UWB) model. The problem of maximum mutual information for a power-limited system was initially considered by Claude Shannon, let P denote the received power, N_0 is the one-sided noise power spectral level. The mutual information of an ideal band-limited AWGN channel approaches

$$C = \lim_{B\to\infty} B\log_2(1 + \frac{P}{BN_0}) = \frac{P}{N_0}\log_2 e. \tag{3.14}$$

Since P is limited, the SNR decreases when B increases.

The mutual information at a low SNR regime is initially studied by using Taylor expansion on $\log(1+SNR)$ at $SNR=0$. The obtained function indicates that the mutual information is approximately linear when the SNR is very low.

$$C^{low} \approx \dot{C}(0)\gamma + \ddot{C}(0)\gamma^2 + o(\gamma^2), \tag{3.15}$$

where $\dot{C}(0), \ddot{C}(0)$ denote the first and second order of derivative of C at $SNR=0$, respectively. By definition, the secrecy capacity over an AWGN channel at the low SNR regime is approximated by

$$C_S^{low} \approx \dot{C}(0)(\gamma_D - \gamma_E) + \ddot{C}(0)(\gamma_D^2 - \gamma_E^2). \tag{3.16}$$

It is shown that the secrecy capacity over an AWGN channel at low SNR can be approximated to a linear function of the SNR difference. If the channel follows Rayleigh fading, C_S^{low} is given by

$$C_S^{low} \approx \dot{C}(0)(E[\gamma_D] - E[\gamma_E]) + \ddot{C}(0)(E[\gamma_D^2] - E[\gamma_E^2]), \tag{3.17}$$

where the expectation is taking on all fading realizations. For the Gaussian input case, it is easy to obtain that $\dot{C}(0)=1$ and $\ddot{C}(0)=-\frac{1}{2}$ by applying a derivative to the mutual information. However, compared to Gaussian input, the $\dot{C}(0)$ and $\ddot{C}(0)$ of the finite-alphabet input schemes are more complex to evaluate. In [72], V. Prelov and S. Verdú studied the first two Taylor expansions of mutual information for proper complex constellations χ that are introduced by Neeser and Massey [73], the $\dot{C}(0)$ and $\ddot{C}(0)$ are given by

$$\dot{C}(0) = E[|s|^2] - |E[s]|^2 \tag{3.18}$$

$$\ddot{C}(0) = -\frac{1}{2}[(E[|s|^2] - |E[s]|^2)^2 + |E[s^2] - E^2[s]|^2], \tag{3.19}$$

where s are the constellation points on χ. However, (3.19) is only valid for CM schemes. The $\dot{C}(0)$ and $\ddot{C}(0)$ of the BICM scheme can be obtained by applying the relationship between CM capacity and the BICM capacity [66], which is given by

$$C_\chi^{BICM} = \frac{1}{2}\sum_{i=1}^{m}\sum_{b=0,1}(C_\chi^{CM} - C_{\chi_b^i}^{CM}). \tag{3.20}$$

Thus, the $\dot{C}(0)$ and $\ddot{C}(0)$ of the BICM scheme is computed by

$$\dot{C}(0) = \frac{1}{2}\sum_{i=1}^{m}\sum_{b=0,1}|E[s_b^i]|^2 \tag{3.21}$$

$$\begin{aligned}\ddot{C}(0) =& \frac{1}{4}\sum_{i=1}^{m}\sum_{b=0,1}((E[|s_b^i|^2] - |E^2[s_b^i]|)^2 - (1 + |E[s^2]|^2) \\ &+ |E[(s_b^i)^2] - E^2[s_b^i]^2|),\end{aligned} \tag{3.22}$$

It is worth noting that (3.22) are for the zero mean and unit variance constellation χ with 2^m constellation points, each point corresponds to one m-bit sequence.

3.6 The secrecy capacity at high SNR regime

Considering a Wyner channel model, all channels are AWGN, *Alice* transmits the signals at power level P_S, σ_D^2 and σ_E^2 are the noise variances of the main channel and the wiretap channel, respectively. The average signal power $E[|X|^2] = 1$. The secrecy capacity C_S is by definition given by

$$C_S = \log_2(1 + \frac{P_S}{\sigma_D^2}) - \log_2(1 + \frac{P_S}{\sigma_E^2}). \tag{3.23}$$

Assume that the value of P_S is very large compared to the noise power, (3.23) is approximated to

$$C_S = \log_2(\frac{\sigma_D^2}{\sigma_E^2}). \tag{3.24}$$

Equation (3.24) indicates that secrecy capacity at high SNR is not affected by the transmission power, but is completely defined by the noise power level differences between the two channels.

It is well known that the mutual information of any input scheme with finite-size constellation achieves $\log_2 M$ if SNR is high enough. Thus, without a proper power control policy, the secrecy capacity decreases to 0 when SNR are very high and we have following relationships

$$\lim_{SNR\to 0} C_S = 0, \lim_{SNR\to\infty} C_S = 0, C_S \geq 0, \tag{3.25}$$

it is indicated that for CM and BICM, to obtain the maximum value of C_S, the transmission power has to be controlled at a moderate value rather than increased to infinity. In later chapters, we investigate the optimal power allocation for finite-alphabet input schemes under secrecy constraints.

3.7 The minimum mean square error

In communication, control and signal processing, making precise estimates, predictions or decisions of some quantities based on information observed from other quantities are the core motivations of research. Because the noise exists in the communication process, the estimation of the original information based on the noisy observation may not be perfect, it is possible to make biased estimation when the SNR is very smaller. One method to describe the level of errors is to measure the mean value of the squared errors. This process is referred as mean square error (MSE).

To begin with, assume the transmitter sends message X through an AWGN channel to the destination. The noise in the channel is denoted as N, the noisy signals observed at the receiver are denoted as Y. The estimation of X based on the observation of Y and the channel SNR is referred as the conditional mean estimator, denoted as $\hat{X}(Y; SNR)$, which is given by

$$\hat{X}(Y; SNR) = E[X|Y; SNR]. \tag{3.26}$$

The MSE measures the error between X and $\hat{X}(Y; SNR)$ in the mean squared sense

$$E[(X - \hat{X}(Y; SNR))^2]. \tag{3.27}$$

The MMSE is the minimum value of MSE, this value is affected by the estimation algorithm and the choose of the estimator.

Chapter 4

The closed-form solution for secrecy rate and power control policy for CM and BICM schemes

4.1 Introduction

Until now, the Gaussian input has been the basis for most research on secrecy capacity. It is well known that the channel capacity of Gaussian input has a simple closed-form relation to the channel SNR. Therefore, by definition, on an AWGN channel, the secrecy capacity is given by $\log_2(\frac{1+SNR_D}{1+SNR_E})$, where SNR_D and SNR_E denote the SNRs of the main channel and the wiretap channel, respectively. Most research on secrecy capacity maximization problems and optimal power control policy (PCP) are based on this model.

However, the PCP derived from Gaussian input model is not applicable to the finite alphabet input model. Significant differences have been found between the secrecy rate of finite alphabet input schemes and the Gaussian input assumption especially at high SNR range, where zero secrecy rate is obtained with a finite-alphabet input scheme if it lacks any PCP. By assuming the channels are slow fading and massive computational resources are available, an exhaustive search method is introduced to obtain optimal PCP and maximise secrecy rate in [63]. Although by using exhaustive searching, the secrecy rate is maximized and the PCP is optimal, but this method is inefficient and not applicable to the fast fading channels.

It was shown in [68] that the derivative of the mutual information $I(SNR)$ of a

channel with respect to the SNR is equal to the minimum mean square error (MMSE) measured at the receiver side. By using this relationship, the optimization of the secrecy rate for CM is found in [61] with an adaptive searching algorithm. In this work, a transformation for this relationship is introduced, focusing on the optimal power control policy of finite-alphabet input schemes and the secrecy rate at a high SNR range. It is worth mentioning that we assume the receiver performs perfect channel estimation (CE) and the global CSI is known at the transmitter, which is proved realistic when both *Bob* and *Eve* are active users in the communication network.

In the remainder of this chapter, the following problems are solved:

- What is the relationship of the secrecy rate C_S and the SNR difference between the main channel and the wiretap channel?
- What is the optimal power control policy?
- Is it possible to estimate the maximum secrecy rate when Global CSI is available at the transmitter?

4.2 Mutual information vs. minimum mean square error

Mutual information is a fundamental concept in information theory, measuring the information rate that a channel can transmit at with no errors given a certain input signalling. Until now, the closed-form solution of the mutual information for a finite-alphabet input remains an open problem. Therefore, the secrecy rate of finite-alphabet input is difficult to analyse mathematically. Previous research on optimizing the transmission power P_S under a secrecy constraint relies on exhaustive searching. In consideration of efficiency, a fast power control policy is necessary.

The mean square error (MSE) is a basic quantity in estimation theory, where MMSE is the minimum value of the MSE. MMSE measures how accurately the channel input can be recovered by observing of the channel output. Consider the AWGN channel where the channel input-output function is given by

$$Y = \sqrt{\gamma}X + N, \tag{4.1}$$

where N is the zero mean, unit variance Gaussian noise and X and Y are the channel input symbol vector and channel output signal vector, respectively. The γ denotes the instantaneous channel SNR. The probability density function (pdf) of the output is

$$p_{Y|X}(y|x) = \frac{1}{\pi} e^{-|y-\sqrt{\gamma}x|^2}. \tag{4.2}$$

Let $\hat{X}$ denote the estimate of the channel input X based on the observation of the channel output Y and the error of the estimation is measured using the mean square. The conditional mean estimator gives the best estimation of X [68], denoted as $\hat{X}$,

$$\hat{X} = E[X|\sqrt{\gamma}X + N]. \tag{4.3}$$

The mean square error is the expectation value of the difference between X and $\hat{X}$, which is given by

$$E[|X - \hat{X}|^2], \tag{4.4}$$

while the MMSE is the minimum value of (4.4). Let $\mathbf{MMSE}(\gamma)$ denote the MMSE as a function of SNR and $\hat{X}$ as the soft estimation of the channel input X, then we have

$$\mathbf{MMSE}(\gamma) = \min E[|X - \hat{X}|^2]. \tag{4.5}$$

Let $I(\gamma)$ denote the mutual information of the channel. A relationship between $I(\gamma)$ and $\mathbf{MMSE}(\gamma)$ is given by

$$\mathbf{MMSE}(\gamma) = \frac{dI(\gamma)}{d\gamma}. \tag{4.6}$$

If the channel is AWGN and the input follows a Gaussian distribution, the MMSE is then given by

$$\mathbf{MMSE}(\gamma) = \frac{1}{1+\gamma} \log_2 e, \tag{4.7}$$

where e is the base of natural logarithm. For the CM, in the presence of zero mean, unit variance Gaussian noise, the soft estimation of the transmitted symbol s is denoted as $\hat{s}$, which is given by

$$\hat{S}(y,h) = \frac{\sum_{s\in\chi} s \exp(-|y-hs|^2)}{\sum_{s\in\chi} \exp(-|y-hs|^2)}, \tag{4.8}$$

where χ denotes the constellation. The MMSE by definition is given by

$$\mathbf{MMSE}_{\chi}(\gamma) = E[|X|^2] - E\left[\left|\frac{\sum_{s\in\chi} s\exp(-|y-hs|^2)}{\sum_{s\in\chi}\exp(-|y-hs|^2)}\right|^2\right]. \tag{4.9}$$

It is important to note that (4.9) is only valid for a CM scheme and not applicable to BICM, due to the channel input of BICM schemes being bit-wise interleaved. We obtain the relationship between MMSE and mutual information for BICM using an alternative method by applying the relationship between CM and BICM [66],

$$I^{BI}(\gamma) = \sum_{i=1}^{m}\frac{1}{2}\sum_{b=0,1}(I^{CM}(\gamma) - I^{CM}_{\chi_i^b}(\gamma)). \tag{4.10}$$

The mutual information for BICM is given by:

$$\mathbf{MMSE}^{BI}(\gamma) = \sum_{i=1}^{m}\frac{1}{2}\sum_{b=0,1}(\mathbf{MMSE}_{\chi}(\gamma) - \mathbf{MMSE}_{\chi_i^b}(\gamma)), \tag{4.11}$$

where $\mathbf{MMSE}_{\chi_i^b}$ denotes the MMSE of the sub-constellation χ_i^b.

By using this relationship, the MMSE of BICM is obtained and the mutual information of the finite-alphabet input can be obtained by integrating the MMSE. In the next section, some transformations are introduced in order to obtain the secrecy performance and power allocation policy for finite-alphabet input schemes.

4.3 secrecy rate and logarithm transformed MMSE

In this section, we denote the parameters for the source-to-destination channel (main channel) and the source-to-eavesdropper channel (wiretap channel) by adding the subscript D and E, respectively. By definition, the secrecy rate C_S is given by the difference of the mutual information of the main channel and the eavesdropper channel,

$$C_S = C_D - C_E. \tag{4.12}$$

If the input alphabet is infinite and Gaussian distributed, the secrecy capacity is given by

$$C_S = \log_2\left(\frac{1+\gamma_D}{1+\gamma_E}\right). \tag{4.13}$$

By using 4.13, it is very easy to determine the value of secrecy capacity and optimal power control policy for Gaussian input systems. However, the MMSE of a finite-alphabet input relies on Monte-Carlo evaluation and the channel SNR difference changes when the transmission power varies. For these two reasons, the value of secrecy rate of a finite-alphabet input is hard to determine. Previous research on the secrecy rate of a finite-alphabet input does not give a closed-form solution to the above problems, so, adaptive search algorithms are widely applied in [28] [63] [75] [61].

Instead of considering the secrecy performance in $C_D - C_E$ form, we consider it in integration form, which is given by

$$C_S = \int_{\gamma_E}^{\gamma_D} \frac{dC}{d\gamma} d\gamma. \tag{4.14}$$

By combining (4.2) and (4.14), C_S is an integral equation of $\mathbf{MMSE}(\gamma)$, which is shown below

$$\begin{aligned} C_S &= \int_{\gamma_E}^{\gamma_D} \mathbf{MMSE}(\gamma)\gamma, \\ &= \mathbf{M\bar{M}SE}(\gamma)(\gamma_D - \gamma_E), \end{aligned} \tag{4.15}$$

where $\mathbf{M\bar{M}SE}$ is the average MMSE value within $[\gamma_E, \gamma_D]$. However, this integrated form of the channel secrecy rate does not simplify the computation of C_S because the range of $[\gamma_E, \gamma_D]$ varies with the transmission power P_S. The MMSE values of some popular input schemes are shown in the figures below.

It is indicated in Fig.4.1 that MMSE decreases when SNR increases, while $[\gamma_E, \gamma_D]$ increases. Thus, the maximum C_S can only be found by changing P_S in steps and exhaustive searching.

To save computational resources, we present a transformed C_S formula, which is not constraint by the input distribution as long as the signals are affected by Gaussian noise.

The main problem of (4.15) is that the SNR difference and MMSE both change

values if P_S varies. However, the SNR difference in dB ($\Delta\gamma_{dB}$) is constant,

$$\begin{aligned}\Delta\gamma^{dB} &= 10\log_{10}(P_S|h_D|^2) - 10\log_{10}(P_S|h_E|^2) \\ &= 10\log_{10}\left(\frac{|h_D|^2}{|h_E|^2}\right).\end{aligned} \tag{4.16}$$

It is simpler to start by focusing on the AWGN channel case, since the block fading channels are equivalent to AWGN channels within every single fading block. Later, the power allocation policy for fading channels can be easily derived from the AWGN chanel case.

We define $I_{dB}(\gamma_{dB})$ as the mutual information when the SNR is in dB and $I_{dB}(\gamma_{dB}) = I(\gamma)$. Equation (4.15) is transformed as:

$$\begin{aligned}C_S &= I_{dB}(\gamma_{D,dB}) - I_{dB}(\gamma_{E,dB})) \\ &= \max_{P_S}\int_{\gamma_{E,dB}}^{\gamma_{D,dB}} \frac{dI_{dB}(\gamma_{dB})}{d\gamma_{dB}} d\gamma_{dB}, \\ &= \max_{P_S}\int_{\gamma_{E,dB}}^{\gamma_{D,dB}} \frac{dI(\gamma)}{d\gamma}\frac{d\gamma}{d\gamma_{dB}} d\gamma_{dB}, \\ &= \max_{P_S}\int_{\gamma_{E,dB}}^{\gamma_{D,dB}} 0.1\log_2(10)10^{0.1\gamma_{dB}}\frac{dI(\gamma)}{d\gamma} d\gamma_{dB}.\end{aligned} \tag{4.17}$$

Here, we denote $0.1\log_2(10)10^{0.1\gamma_{dB}}\frac{dI(\gamma)}{d\gamma}$ by $\mathcal{M}(\gamma_{dB})$ and the secrecy rate is given by

$$C_S = \max_{P_S}\int_{\gamma_{E,dB}}^{\gamma_{D,dB}} \mathcal{M}(\gamma_{dB}) d\gamma_{dB}. \tag{4.18}$$

Firstly, we consider the Gaussian input case, the channel capacity is given by $\log_2(1+\gamma)$. Then $\mathbf{MMSE}(\gamma) = \frac{1}{(+\gamma)}\log_2 e$ and the secrecy capacity is given by:

$$C_s^G = 0.1\log(10)\int_{\gamma_{E,dB}}^{\gamma_{D,dB}} 10^{0.1\gamma_{dB}}\frac{\log_2 e}{1+10^{0.1\gamma_{dB}}} d\gamma^{dB}. \tag{4.19}$$

When the transmission power is large, $P_S \to \infty$, the secrecy capacity is:

$$C_s^G \approx 0.33(\gamma_{D,dB} - \gamma_{E,dB}) \tag{4.20}$$

The transformed gradient of the mutual information for the Gaussian coded input is a positive constant value at high SNR, which indicates that infinite transmission power is optimal for secrecy transmission. However, the transformed gradient of the

Table 4.1: OPTIMAL P_S SEARCHING STEPS

Compare γ_{opt} and $\gamma_{M,dB} = 10\log_{10}(\lvert h_M\rvert^2 P_T)$.
If $\gamma_{D,dB} \leq \gamma_{opt}$, transmits with full power $P_S = P_T$. Searching stops.
If $\gamma_{D,dB} \geq \gamma_{opt}$, first, adjust P_S so that $\gamma_{D,dB} = \gamma_{opt}$.
Increment P_S and compute the average value of $\bar{\mathcal{M}}(\gamma_{dB})$ between the SNR interval $[\gamma_{E,dB}, \gamma_{D,dB}]$, until $\bar{\mathcal{M}}(\gamma_{dB})$ is maximum.

mutual information for the finite-alphabet input case is very different at high SNR, which will result in a completely different power control policy at the transmitter for secrecy transmission. Since the value of $\mathcal{M}(\gamma_{dB})$ is finite and non-negative and

$$\lim_{\gamma\to 0} \mathcal{M}(\gamma_{dB}) = 0; \lim_{\gamma\to\infty} \mathcal{M}(\gamma_{dB}) = 0; \tag{4.21}$$

then, according to the property of a continuous function, the secrecy rate of a finite-alphabet input has a global maximum value at a finite SNR. In the next section, we propose an optimal power control policy solution using exhaustive searching and an alternative convenient sub-optimal solution for power control.

4.4 secrecy rate maximization under transmission power constraint

The transformed secrecy rate formula was introduced in the last section and it is possible to perform power allocation according to (4.15). The variation of transmission power P_S does not affect the value of $\Delta\gamma^{dB} = \gamma_{D,dB} - \gamma_{E,dB}$, but shifts the interval $[\gamma_{E,dB}, \gamma_{D,dB}]$ on the SNR axis as is shown in Fig.4.2. To achieve the maximum secrecy rate, the transmitter has to adapt the transmission power P_S and shift $[\gamma_{E,dB}, \gamma_{D,dB}]$, where $\bar{\mathcal{M}}$ within the interval is maximum.

We define the SNR where the transformed MMSE achieves its maximum value as γ_{opt} and the transmission power constraint $P_S \leq P_T$. The optimal PCP is given in table 4.1. It is clear that the searching range for the optimal P_S is limited around γ_{opt}, thus, the complexity of PCP is greatly reduced compared with the exhaustive searching method presented in [63].

If the strict maximal of secrecy rate is not required, the PCP can be significantly simplified with ignorable scarifies of secrecy rate performance, this PCP is referred to fast PCP in the remainder of this thesis. It is clear that $\mathcal{M}(\gamma_{dB})$ is a concave

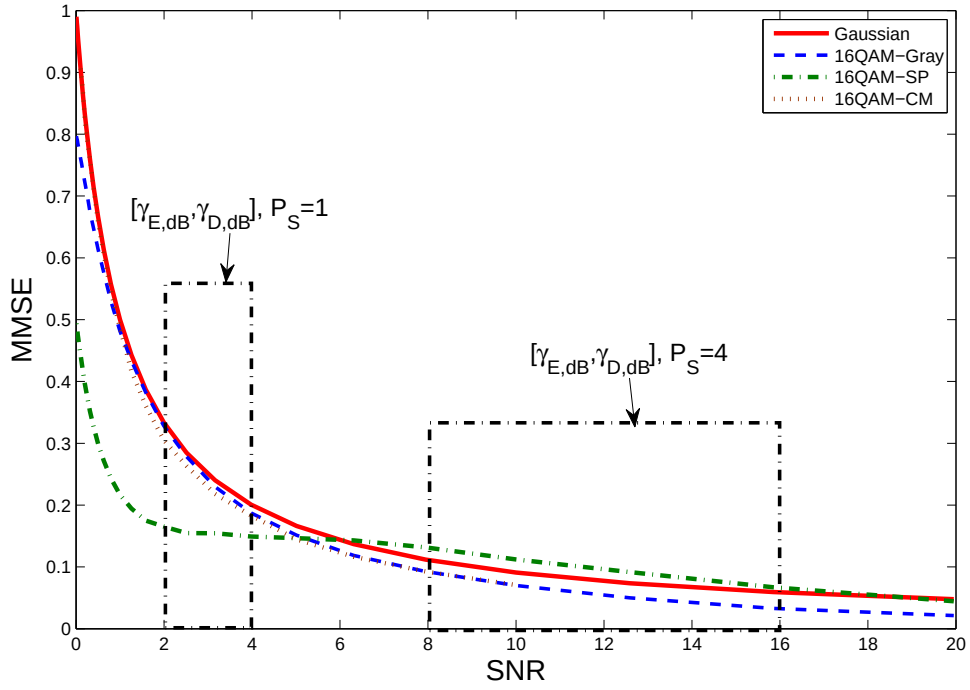

Figure 4.1: MMSE of 16QAM, dashed line is CM, full lines are different mappings for the BICM schemes. .

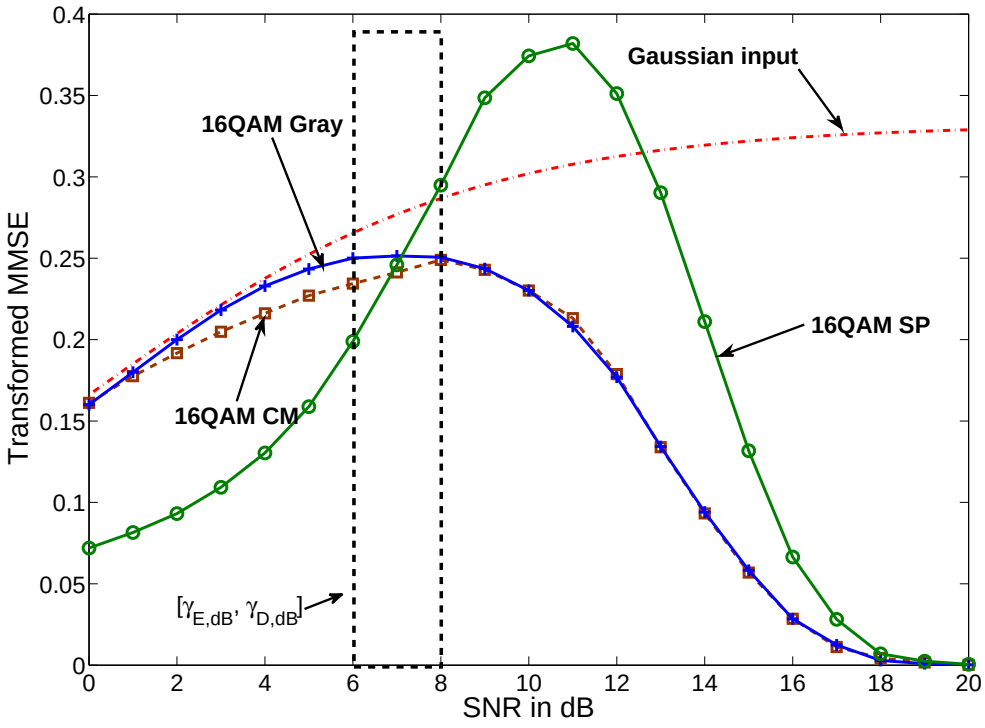

Figure 4.2: Transformed MMSE of 16QAM, dashed line is CM, full lines are different mappings for the BICM scheme. .

Table 4.2: The maximum value of $\mathcal{M}(\gamma_{dB})$ and the corresponding γ_{opt}

Input schemes	$\mathcal{M}_{max}$	γ_{opt}
16QAM-CM	0.244	8 dB
16QAM-Gray	0.252	7 dB
16QAM-SP	0.382	10.7 dB
64QAM-CM	0.288	14.7 dB
64QAM-Gray	0.308	13 dB
64QAM-SP	0.398	16 dB

function, so rather than optimizing $\bar{\mathcal{M}}$, a simpler solution is to set γ_{opt} in the center of $[\gamma_{E,dB}, \gamma_{D,dB}]$, which is shown as:

$$\gamma_{opt} = \frac{\gamma_{E,dB} + \gamma_{D,dB}}{2}. \tag{4.22}$$

By substituting the value of $\gamma_{E,dB}$ and $\gamma_{D,dB}$ into (4.22), the suboptimal PCP is given by:

$$\hat{P_S} = \begin{cases} \frac{10^{0.1\gamma_{opt}}}{|h_D||h_E|}, & \text{if} \frac{10^{0.1\gamma_{opt}^{dB}}}{|h_D||h_E|} \leq P_T \\ P_T, & \text{if} \frac{10^{0.1\gamma_{opt}}}{|h_D||h_E|} \geq P_T \end{cases} \tag{4.23}$$

The γ_{opt} of some input schemes are listed in table 4.2. The γ_{opt} of Gray mapping is smaller than other mapping schemes if the constellation is unchanged, which indicates lower P_S is required to achieve the maximum secrecy rate than other mappings. However, Gray mapping achieves lower $\mathcal{M}(\gamma_{opt})$ values than all other mapping schemes, in other words, the maximum possible secrecy rate of Gray mapping is the lowest. According to (4.15), by assuming $\bar{\mathcal{M}} = \mathcal{M}_{max}$, the maximum value of the secrecy rate within the whole SNR range is given by

$$C_S^{max} \leq \mathcal{M}_{max}(\gamma)(\gamma_{D,dB} - \gamma_{E,dB}). \tag{4.24}$$

In the remainder of this section, simulation results of the secrecy performances with suboptimal PCP over Rayleigh fading channels and the maximum values of the secrecy rate over AWGN channels are presented.

In Fig.4.3, the secrecy rate of finite-alphabet input schemes at high SNR and suboptimal PCP does not decrease to 0 as SNR increases to infinity. In Fig.4.4 there are two general trends, on one hand, the bounds of CM and BICM with Gray mappings are very tight compared to other mapping schemes. On the other hand,

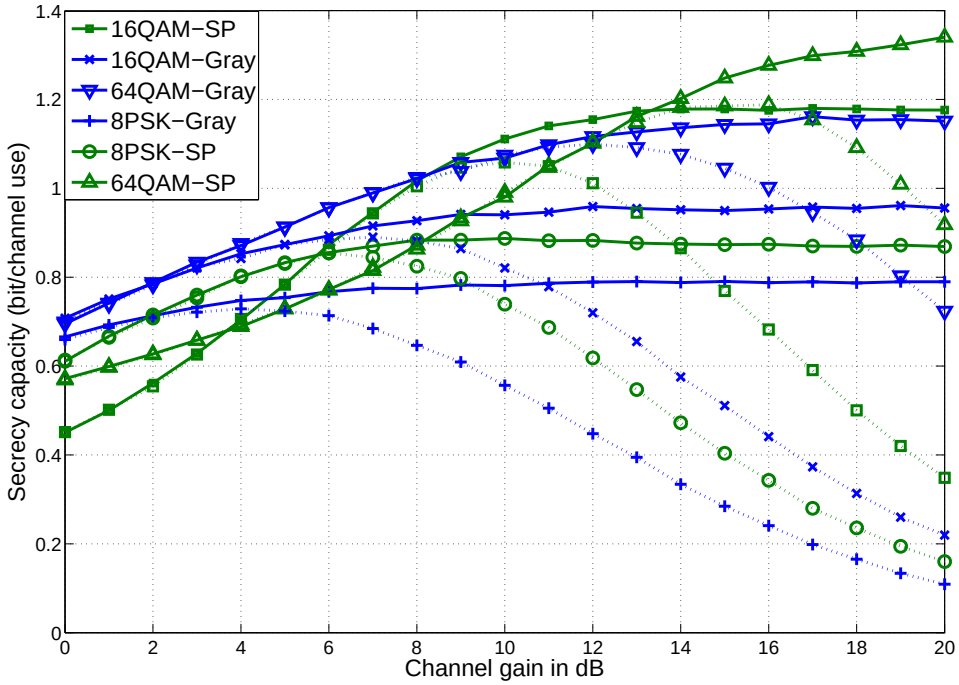

Figure 4.3: secrecy rate over Rayleigh fading channels with sub-optimal power control policy. The channel gain is $|h|^2$, $\bar{\gamma_D} = \bar{\gamma_E}$, $P_T = 1$. The dotted lines are the secrecy rate with flat power transmission.

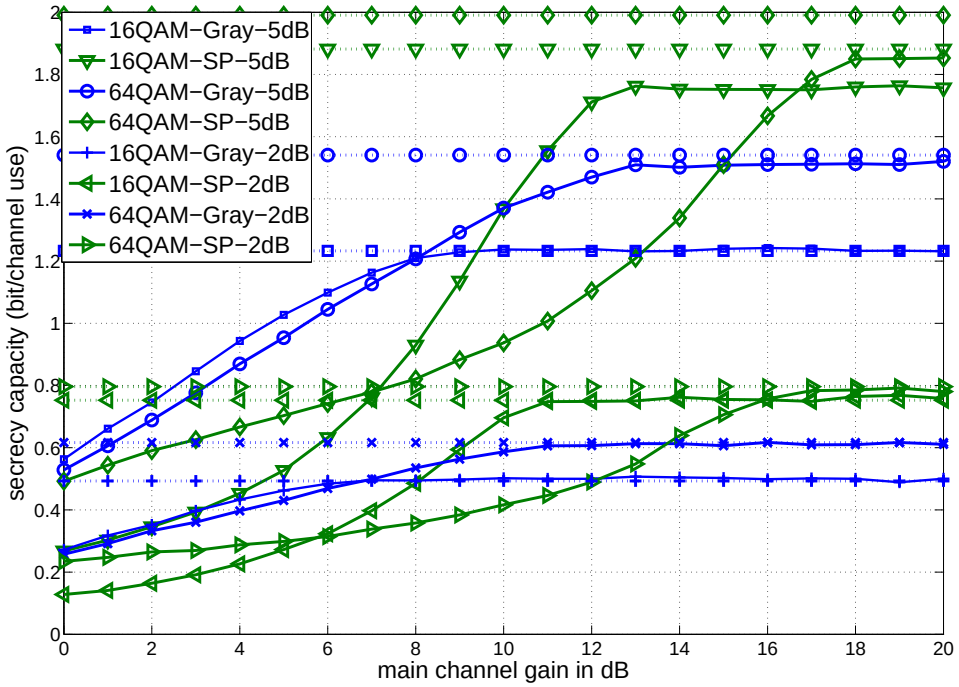

Figure 4.4: secrecy rate over AWGN channels. The channel gain is $|h|^2$, the SNR gap is 2dB and 5dB, the $P_T = 1$. The dotted lines are the upper bounds of secrecy rate.

the bound is tighter when the SNR gap between two channels is smaller. This is mainly because of the smaller difference between $\mathcal{M}_{max}$ and $\bar{\mathcal{M}}$ of CM and Gray mapping and other input schemes within $[\gamma_{E,dB}, \gamma_{D,dB}]$.

4.5 Transmission power minimization with a target secrecy rate

The variable rate communication requires the coding scheme to adapt the coding rate to the instantaneous channel condition. Although maximum secrecy rate is achieved by using this technique, the design complexity is high. Instead, transmitting the confidential message at a constant rate can greatly reduce the design complexity for the transmitter.

It has been demonstrated that $\mathcal{M}(\gamma_{dB})$ is a concave function. Thus, there exist a range of P_S values to achieve the target rate R_T. Although the maximum secrecy rate can be obtained, in some cases, a steady transmission at a fixed information rate is required, for example, the transmitter is not able to adapt the channel coding rate to the CSI. Under this assumption, the optimal algorithm is to transmit the confidential message at the target rate R_T whenever R_T satisfies

$$R_T < \max(\bar{\mathcal{M}})(\gamma_{D,dB} - \gamma_{E,dB}), \tag{4.25}$$

where $\max(\bar{\mathcal{M}})$ denotes the maximum value of $\bar{\mathcal{M}}$ obtained by shifting $[\gamma_{E,dB}, \gamma_{D,dB}]$. This indicates that R_T is achieved when $\frac{\gamma_{E,dB}+\gamma_{D,dB}}{2} < \gamma_{opt}$. The target function is given by

$$\begin{aligned} &\min \ P_S \\ &\text{s.t.} \\ &C_S \geq R_T. \end{aligned} \tag{4.26}$$

To obtain the minimum P_S, we introduce the approximation functions of the secrecy rate.

4.5.1 Closed-form approximation of secrecy rate

The closed-form solution of mutual information or secrecy rate of a BICM scheme is an attractive target in information theory. It was introduced in the previous sections that secrecy rate of finite-alphabet input schemes are concave functions with one global maximum value at γ_{opt}. Hence, an approximation of the C_S curves in a limited SNR range is possible. However, the approximation may not perfectly

match $\mathcal{M}(\gamma_{dB})$ at entire SNR range, as it is analysed, we are mostly interested with the $\mathcal{M}(\gamma_{dB})$ in $(-\infty, \gamma_{opt}]$. To start with, we obtain a closed-form approximation of the $\mathcal{M}(\gamma)$ curves from low SNR to γ_{opt}.

It is shown in Fig. 4.2 that the $\mathcal{M}(\gamma_{dB})$ curves of various mappings around γ_{opt} are similar to the curves of a quadratic function. To estimate the $\mathcal{M}$ value, we define a quadratic function $A(\gamma_{dB})$ to approximate the $\mathcal{M}(\gamma_{dB})$ curves. The quadratic function $A(\gamma_{dB})$ is given by

$$A(\gamma_{dB}) = \beta_1 \gamma_{dB}^2 + \beta_2 \gamma_{dB} + \beta_3. \tag{4.27}$$

The coefficients $\beta_1, \beta_2, \beta_3$ are obtained by substituting $(\gamma_{dB}, \mathcal{M}(\gamma))$ values on the curves into $A(\gamma_{dB})$. The optimal $\beta_1, \beta_2, \beta_3$ are obtained by minimizing the estimation error between $A(\gamma_{dB})$ and $\mathcal{M}(\gamma_{dB})$. The error between the approximation $A(\gamma_{dB})$ and $\mathcal{M}(\gamma_{dB})$ is measured by computing the MMSE, denoted as $\mathcal{E}(\gamma_{dB})$ between $A(\gamma_{dB})$ and $\mathcal{M}(\gamma_{dB})$ at the SNR range we interested in,

$$\mathcal{E}(\gamma_{dB}) = \sum_{\gamma_{l,dB}}^{\gamma_{h,dB}} |A(\gamma_{opt}) - \mathcal{M}(\gamma_{opt})|^2. \tag{4.28}$$

Where $\gamma_{l,dB}$ and $\gamma_{h,dB}$ are the lower and upper bounds of the SNR range of interest in dB form. In this chapter, we are mostly interested in the medium SNR range.

Some quadratic approximations of $\mathcal{M}(\gamma)$ on 16QAM and 8PSK constellations around γ_{opt} are listed below.

For 16QAM, Gray mapping: $\beta_1 = -0.0019, \beta_2 = 0.027, \beta_3 = 0.155$, we obtain the approximation function as

$$A_{16QAM}(\gamma_{dB}) = -0.0019\gamma_{dB}^2 + 0.027\gamma_{dB} + 0.155, \tag{4.29}$$

For 8PSK, Gray mapping: $\beta_1 = -0.0019, \beta_2 = 0.0168, \beta_3 = 0.158$ and the quadratic function is shown as

$$A_{8PSK}(\gamma_{dB}) = -0.0019\gamma_{dB}^2 + 0.0168\gamma_{dB} + 0.1580, \tag{4.30}$$

It is shown that around γ_{opt} and lower SNRs, the $A_\chi(\gamma)$ curves approximate the $\mathcal{M}_\chi$ curves very well, while at high SNRs, the approximation is higher than the

actual value. According to (4.27), the secrecy rate can be approximated by

$$\tilde{C_S} \approx \frac{\beta_1}{3}(\gamma_{D,dB}^3 - \gamma_{E,dB}^3) + \frac{\beta_2}{2}(\gamma_{D,dB}^2 - \gamma_{E,dB}^2) + \beta_3(\gamma_{D,dB} - \gamma_{E,dB}). \tag{4.31}$$

The curves compared in Fig. 4.6 show that the approximation of secrecy rate matches the simulation results very well at medium SNR range, while at high SNR, the approximation tends to be optimistic on the R_S values. It is also shown in Fig. 4.6 that the approximation for 4QAM is very accurate from low SNR to γ_{opt}, while the accuracy of the approximation decreases as the constellation size increases. However, the dotted curves still match the full lines very well for 16QAM Gray mapping from 1dB to 9dB.

4.5.2 Closed-form approximation on channel capacity

With the help of the second order approximation on $\mathcal{M}$, it is possible to obtain a close-form approximation of the channel capacity for finite-alphabet input schemes. It is shown that the channel capacity of finite-alphabet input schemes at medium SNRs can be approximated to a single variable, cubic function. Assume the channel capacity at $SNR = t$ is denoted as $C(t)$. Then denote $t_{dB} = 10\log_{10}(t)$ and let $\hat{C}(t_{dB}) = C(t)$ so that

$$C(t) = \int_0^t \mathbf{MMSE}(\gamma)d\gamma. \tag{4.32}$$

This can be rewritten as

$$\begin{aligned} C(t) &= \hat{C}(t_{tB}) && (4.33)\\ &= \int_{-\infty}^{t_{dB}} M(\gamma_{dB})d\gamma_{dB}, && (4.34)\\ &= \int_{u_{dB}}^{t_{dB}} M(\gamma_{dB})d\gamma_{dB} + \hat{C}(u_{dB}), && (4.35)\\ &= \frac{\beta_1}{3}(t_{dB}^3 - u_{dB}^3) + \frac{\beta_2}{2}(t_{dB}^2 - u_{dB}^2) \\ &\quad +\beta_3(t_{dB} - u_{dB}) + \hat{C}(u_{dB}) + v, && (4.36) \end{aligned}$$

where u_{dB} is the SNR in decibel form where $A_\chi(\gamma_{dB})$ begins to match well with $M(\gamma_{dB})$ and v is a constant produced by the integration process. Taking 16QAM

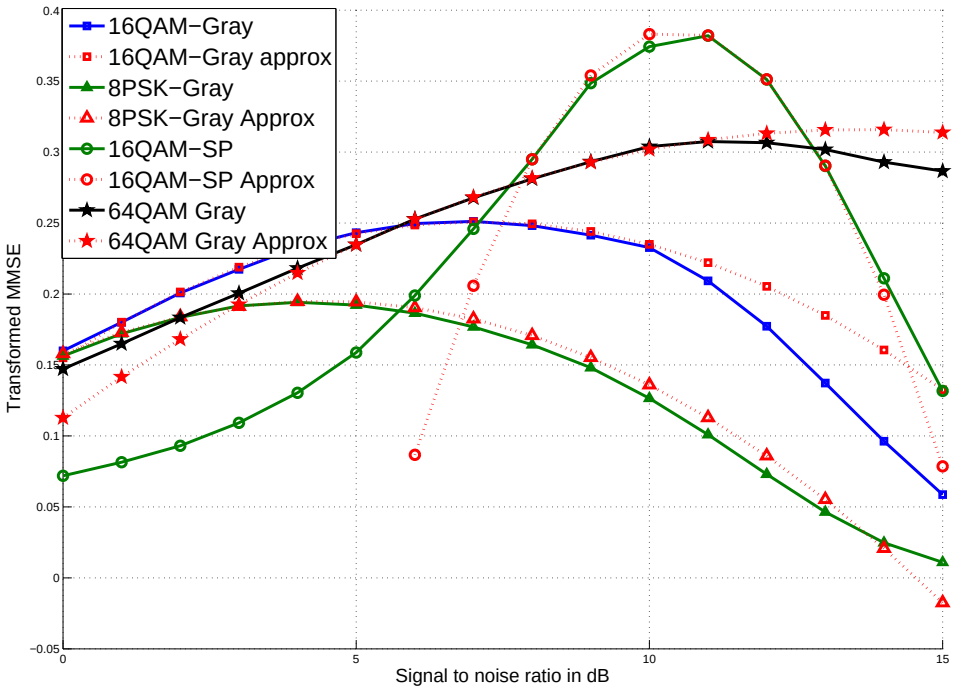

Figure 4.5: The MMSE and the approximation curves of Gray mapping on 16QAM and 8PSK

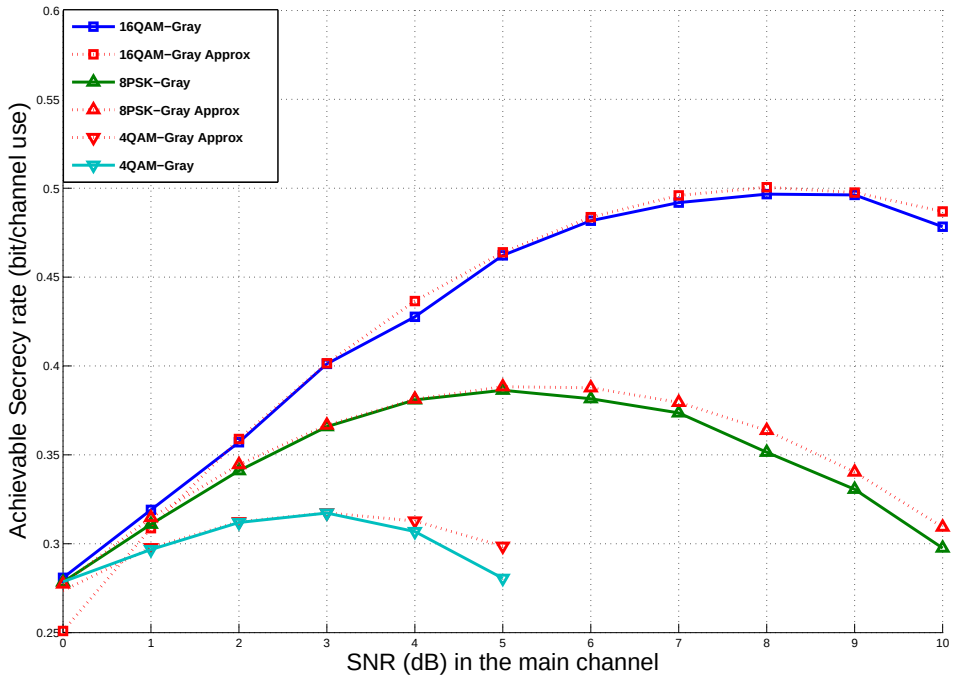

Figure 4.6: The secrecy rate and the approximation curves of Gray mapping on 16QAM and 8PSK

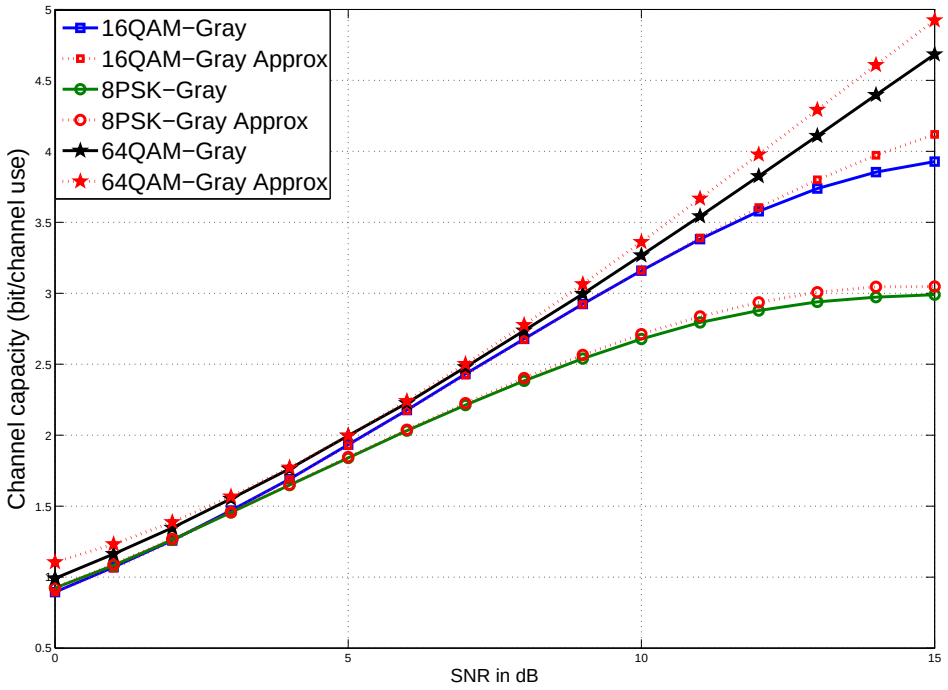

Figure 4.7: The channel capacity and the approximation curves of Gray mapping on 8PSK, 16QAM and 64QAM.

with Gray mapping as an example, $u_{dB} = 0$, $v = 0$ and $\hat{C}(0) = 0.8942$. The channel capacity approximation is then given as

$$C(\gamma_{dB}) \approx \frac{\beta_1}{3}\gamma_{opt}^3 + \frac{\beta_2}{2}\gamma_{opt}^2 + \beta_3 + 0.8942. \tag{4.37}$$

4.5.3 Transmission power minimization

To determine the minimum P_S for R_T, we further simplify (4.31) into a function of P_S

$$\begin{aligned} R_T &\leq C_S \\ &= (\gamma_{D,dB} - \gamma_{E,dB})(\beta_1(\gamma_{D,dB}^2 + \gamma_{E,dB}^2 + \gamma_{D,dB}\gamma_{E,dB}) + \beta_2(\gamma_{D,dB} + \gamma_{E,dB}) + \beta_3) \\ &= \frac{3\beta_1}{4}\Delta\gamma_{dB}T^2 + \beta_2\Delta\gamma_{dB}T + \frac{\beta_1}{4}\Delta\gamma_{dB}^3 + \beta_3\Delta\gamma_{dB}, \end{aligned} \tag{4.38}$$

Where $T = \gamma_{D,dB} + \gamma_{E,dB}$. For the SISO wiretap channel, the SNR gap is constant and irrelevant to P_S, while T can be expressed by

$$T = 10\log_{10}|h_D|^2 + 10\log_{10}|h_E|^2 + 20\log_{10}P_S. \tag{4.39}$$

It is shown that T is a incremental function of P_S, the minimum P_S is obtained when T is minimized. The minimum T is obtained by solving

$$\frac{3\beta_1}{4}\Delta\gamma_{dB}T^2 + \beta_2\Delta\gamma_{dB}T + \frac{\beta_1}{4}\Delta\gamma_{dB}^3 + \beta_3\Delta\gamma_{dB} - R_T = 0. \tag{4.40}$$

Because $\beta_1 < 0$, the minimum T value is given by

$$T = \frac{-\beta_2\Delta\gamma_{dB} + \sqrt{\beta_2^2\Delta\gamma_{dB}^2 - 3\beta_1\Delta\gamma_{dB}(\beta_3\Delta\gamma_{dB} + \frac{\beta_1}{4}\Delta\gamma_{dB}^3 - R_T)}}{\frac{3}{2}\beta_1\Delta\gamma_{dB}}. \tag{4.41}$$

Note that there exist two values of T satisfy (4.40), the larger one denotes the maximum value of P_S for the wiretap channel to achieve R_T. Thus, the minimum transmission power is given by

$$P_S = \frac{10^{\frac{T}{20}}}{\sqrt{|h_D|^2|h_E|^2}}. \tag{4.42}$$

It is shown in Fig. 4.8 and Fig. 4.9 that the minimum transmission power decreases exponentially as h_E increases. For $h_E = 1$, the P_S for $R_T = 0.2$bit/channel use is smaller than the P_S values for $R_T = 0.4$bit/channel use and $R_T = 0.6$bit/channel use. However, as the target rate R_T increases to 0.8bit/channel use, $P_S = 0$. This is because the target rate R_T is larger than the secrecy rate achievable for the SNR gap provided.

In Fig. 4.9, the SNR gap is increased to 4dB, the simulation shows that except $R_T = 0.8$bit/channel use, the required P_S values are smaller for the R_T shown in Fig. 4.8. It is shown that with $\Delta\gamma = 4$dB, $R_T = 0.8$bit/channel use is achievable and the minimum P_S value required is the maximum.

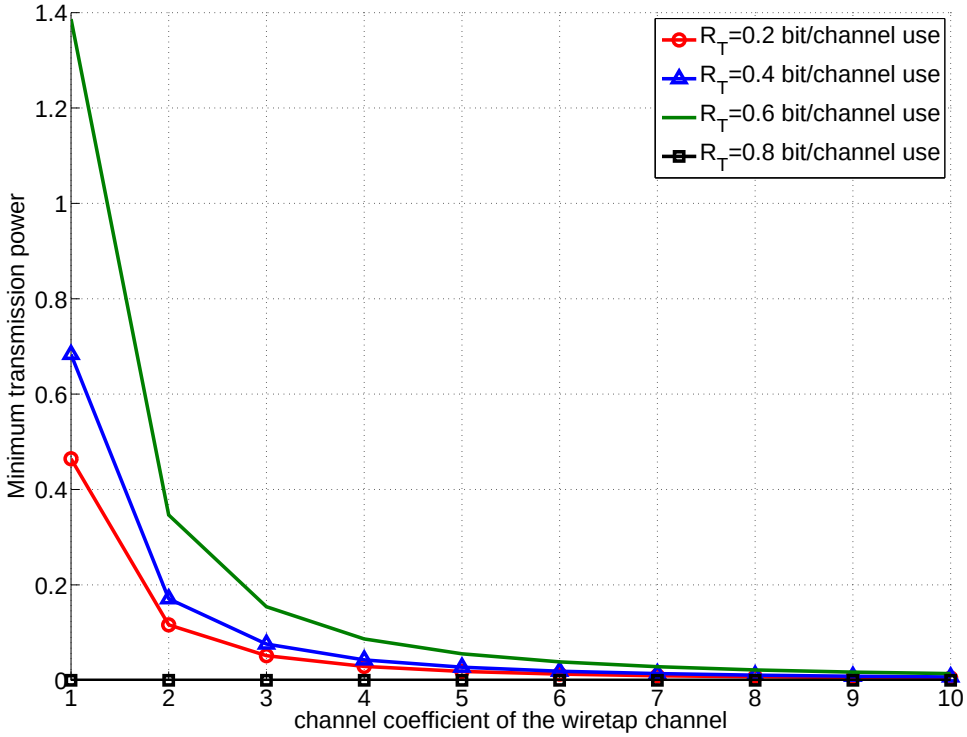

Figure 4.8: The minimum P_S for target R_T. The $\Delta\gamma = 2$dB.

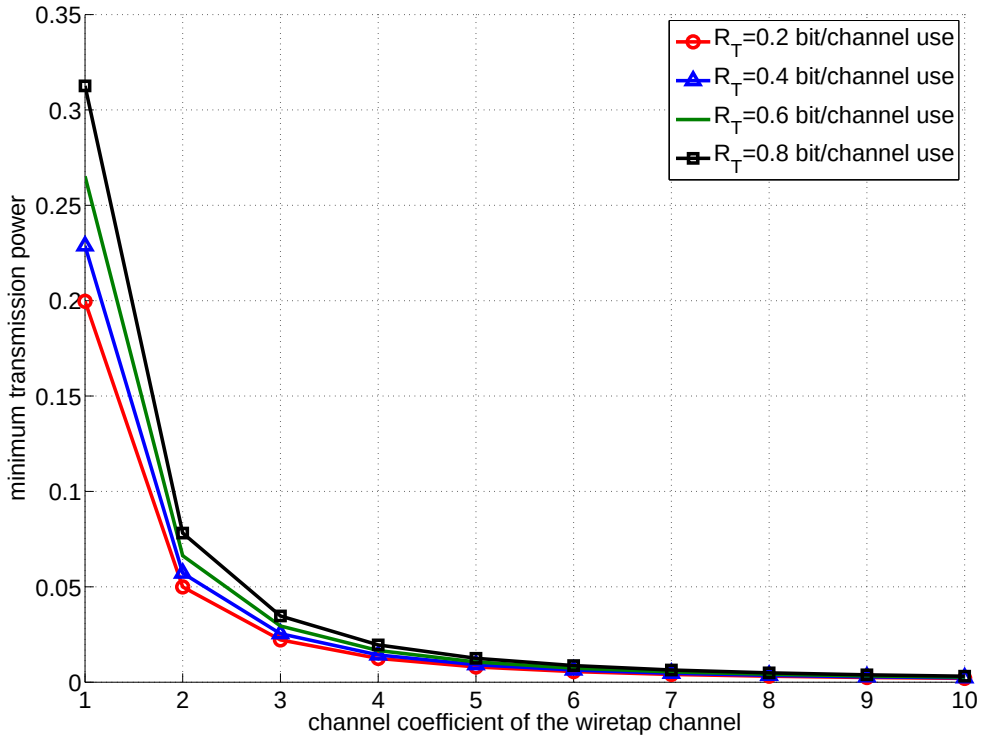

Figure 4.9: The minimum P_S for target R_T. The $\Delta\gamma = 4$dB.

4.6 Energy harvesting under secrecy constraint

Reducing the energy cost and extending the battery life of mobile devices is crucial for wireless networks. In the case of sensor networks, replacing the batteries of sensors, such as implant devices in medical use, can be very difficult or even impossible. Such devices are often equipped with a fixed battery and the device will run out of power if it is not recharged. Therefore, energy harvesting is a technique that receives considerable attention as it allows the device to collect energy from the surrounding environment to overcome the issue of battery limit.

Conventional energy harvesting techniques rely on external energy sources, such as those based on solar power or wind energy and are not a part of the communication network. A promising energy harvesting approach to gather energy from the radio frequency signals has been introduced in [77, 78], which has proved that power and information can be carried by RF signals simultaneously.

The design of a sustainable receiver on wiretap channels is investigated, where the users (intended receiver and eavesdropper) are equipped with an energy-harvesting component in their receivers. The transmitter is both an information source and energy source that broadcasts RF signals to all terminals. The intended receiver and eavesdropper receiver harvest energy from the observation of RF signals and store them in the corresponding batteries. The extra power will be discarded if the battery is fully charged. We consider a wiretap channel where the transmitter maintains a constant rate of transmission of the confidential message and the information rate is equal to the target secrecy rate R_S. The transmitter is assumed to have full knowledge of the global CSI, it performs fast PCP and evaluates the secrecy rate. If $C_S > R_S$, the transmitter knows that the channel is good enough and the transmission starts, otherwise, the transmission pauses. It is possible that at some fading realizations C_S is much larger than the required target secrecy rate R_S. In this case, part of the transmission power is actually wasted, which can be collected by using energy harvesting techniques. In the wiretap channel model, the intended receiver does not set the energy harvesting level itself, but is instructed by the transmitter because the transmitter is the only user who has perfect knowledge of the global CSI.

Of the various energy-harvesting techniques, we focus on power splitting. Assume an infinitely long confidential message is transmitted on a wiretap channel

model with a target secrecy rate R_S. The power splitting coefficient $0 < \rho < 1$ of the intended receiver and the eavesdropper receiver are denoted as ρ_D and ρ_E, respectively. If $\rho = 0$, the receiver harvests no energy from the RF signals and uses all power for information decoding, while $\rho = 1$ implies that the receiver collects all energy from the RF signal. The transmitter broadcasts the confidential message to the intended receiver at a power level P_S while the eavesdropper observes the communication and tries to intercept the confidential message. The main channel (transmitter to destination) and the wiretap channel (transmitter to eavesdropper) are independent and identical flat fading channels. In the energy harvesting systems, there exist two types of noise: noise introduced by the channel and the noise introduced by the analogue-to-digital conversion(ADC) process. As we are interested in the medium SNR range secrecy rate performance, the channel noise is very small and ignorable compared to the signal power, the ADC noise takes dominant effects in the decoding process. Thus, in the remaining of this section, we only consider the ADC noise and assume the channel noise is equal to 0. The receiver observations of the channel output are given by

$$y_D = \sqrt{P_S} h_D x + n_D, \tag{4.43}$$

$$y_E = \sqrt{P_S} h_E x + n_E. \tag{4.44}$$

where n_D and n_E are Gaussian noises with zero mean and unit variance. After power splitting, the received signals are given by

$$y'_D = \sqrt{(1-\rho_D)P_S} h_D x + \sqrt{(1-\rho_D)} n_D, \tag{4.45}$$

$$y'_E = \sqrt{(1-\rho_E)P_S} h_E x + \sqrt{(1-\rho_D)} n_E. \tag{4.46}$$

It is assumed that the transmitter knows the global CSI and the splitting ratio of the intended receiver, but the transmitter does not know the splitting ratio of the eavesdropper. Let γ and $\hat{\gamma}$ denote the SNR measured by the receiver before power

splitting and after power splitting, respectively.

$$\gamma_D = |h_D|^2 P_S, \tag{4.47}$$

$$\gamma_E = |h_E|^2 P_S, \tag{4.48}$$

$$\hat{\gamma}_D = (1-\rho_D)|h_D|^2 P_S, \tag{4.49}$$

$$\hat{\gamma}_E = (1-\rho_E)|h_E|^2 P_S. \tag{4.50}$$

In terms of secrecy rate, the worst case is that the eavesdropper uses all power for decoding the confidential message and harvests no energy from the RF signals, i.e., $\rho_E = 0$. We use γ_{dB} to denote the SNR in decibels, thus, $\gamma_{D,dB}$ and $\hat{\gamma}_{D,dB}$ satisfy the following relations

$$\begin{aligned} \hat{\gamma}_{D,dB} &= 10\log_{10}|h_D|^2 P_S + 10\log_{10}(1-\rho_D) \\ &= \gamma_{d,dB} + \mu, \end{aligned} \tag{4.51}$$

$$\hat{\gamma}_{E,dB} = \gamma_{E,dB}. \tag{4.52}$$

To achieve the target secrecy information rate R_T, the energy harvesting ratio of the destination receiver has to be chosen properly and satisfy the following conditions,

$$R_T < C_S, \tag{4.53}$$

subject to

$$\rho_D > 0, P_S > 0. \tag{4.54}$$

If ρ_D is set too small, too much energy is wasted and the battery of the receiver is charged slowly. If ρ_D is too large, then the secrecy rate of the wiretap channel is smaller than the predefined target secrecy rate and as a result, the confidential message cannot be transmitted to the destination with perfect secrecy. The secrecy rate of 4QAM, 8PSK and 16QAM were approximated at moderate SNR values with high accuracy in the previous sections, the condition in (4.53) can be reformulated

to

$$\begin{aligned} R_T &\leq C_S \\ &\leq \frac{\beta_1}{3}(\hat{\gamma}_{D,dB}^3 - \gamma_{E,dB}^3) + \frac{\beta_2}{2}(\hat{\gamma}_{D,dB}^2 - \gamma_{E,dB}^2) + \beta_3(\hat{\gamma}_{D,dB} - \gamma_{E,dB}). \end{aligned} \quad (4.55)$$

The minimum $\hat{\gamma}_{D,dB}$ is obtained when $R_T = C_S$, define $J(\hat{\gamma}_{D,dB})$ as a function of $\hat{\gamma}_{D,dB}$,

$$J(\hat{\gamma}_{D,dB}) = \frac{\beta_1}{3}\hat{\gamma}_{D,dB}^3 + \frac{\beta_2}{2}\hat{\gamma}_{D,dB}^2 + \beta_3\hat{\gamma}_{D,dB} - \omega \quad (4.56)$$

where

$$\omega = -(\frac{\beta_1}{3}\gamma_{E,dB}^3 + \frac{\beta_2}{2}\gamma_{E,dB}^2 + \beta_3\gamma_{E,dB}) - R_T. \quad (4.57)$$

Let $J(\hat{\gamma}_{D,dB}) = 0$, and the three roots of $J(\hat{\gamma}_{D,dB})$ are denoted as $\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3$. We assume the three roots follows

$$\mathcal{R}_1 \leq \mathcal{R}_2 \leq \mathcal{R}_3. \quad (4.58)$$

Only $\mathcal{R}_2$ is in the range $(\gamma_{E,dB}, \gamma_{D,dB})$, as $\mathcal{R}_1$ and $\mathcal{R}_3$ are generated by the negative values of the secrecy rate approximation formula. The range of the energy splitting

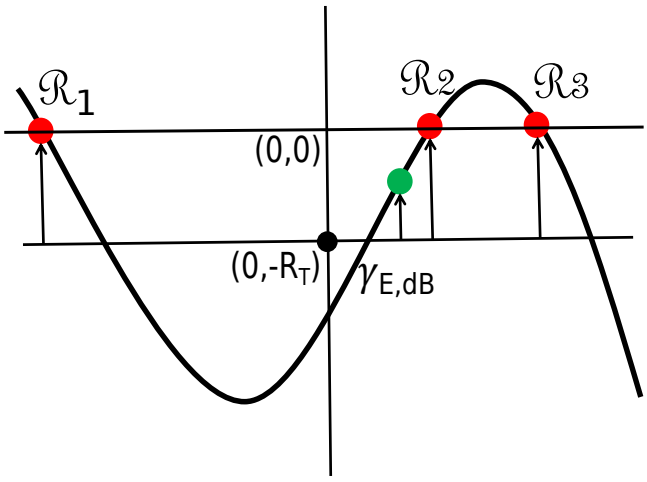

Figure 4.10: The three roots for $J(\hat{\gamma}_{D,dB})$, The green point denotes $\gamma_{E,dB}$. The whole curve is shifted downward by R_T and the original (0,0) pint becomes (0,$-R_T$).

ratio ρ_D is given by

$$0 < \rho_D < 1 - 10^{0.1(\mathcal{R}_2 - \gamma_{D,dB})}. \quad (4.59)$$

If $\mathcal{R}_2$ has no real value solution, it indicates that there is no solution to obtain the

target secrecy rate even if using the full received signal power. Fig.4.11 and Fig.

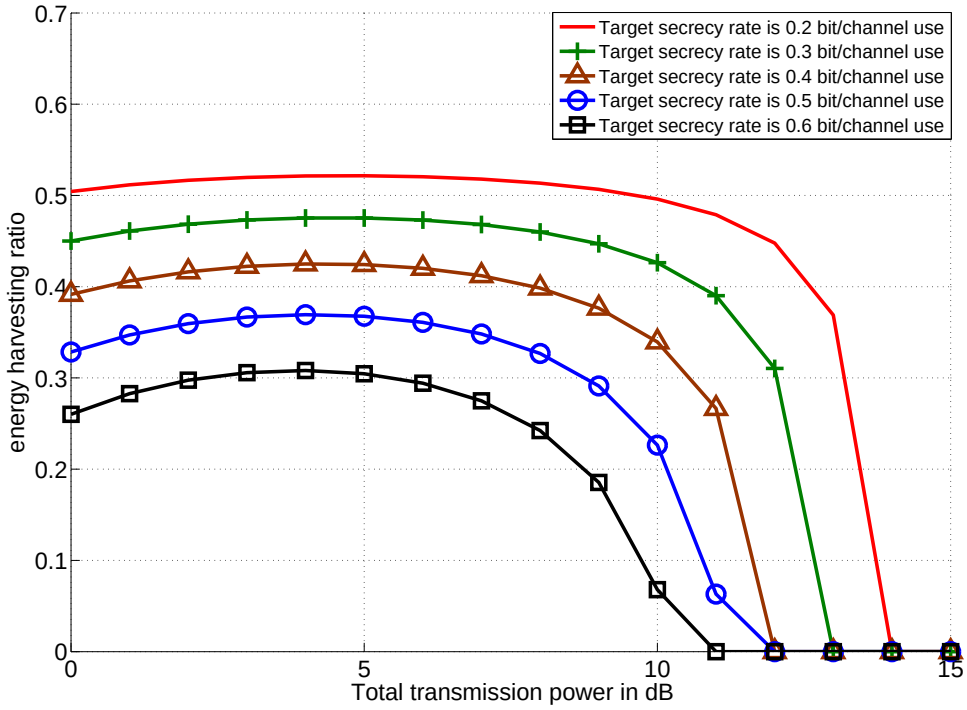

Figure 4.11: The maximum energy harvesting ratio at the destination receiver, the main channel gain is 6dB and the wiretap channel gain is 2dB.

4.12 demonstrate the maximum energy harvesting ratio at the destination receiver providing the target secrecy rate R_T. It is shown that, as the target secrecy rate increases, the amount of harvested energy is reduced, the energy harvesting ratio is a concave function of the input transmission power. At high P_S values, the ρ_D decreases to 0, this is because the information rate in the wiretap channel is increased and the secrecy rate $C_S < R_T$, thus, no energy from the RF signal can be harvested.

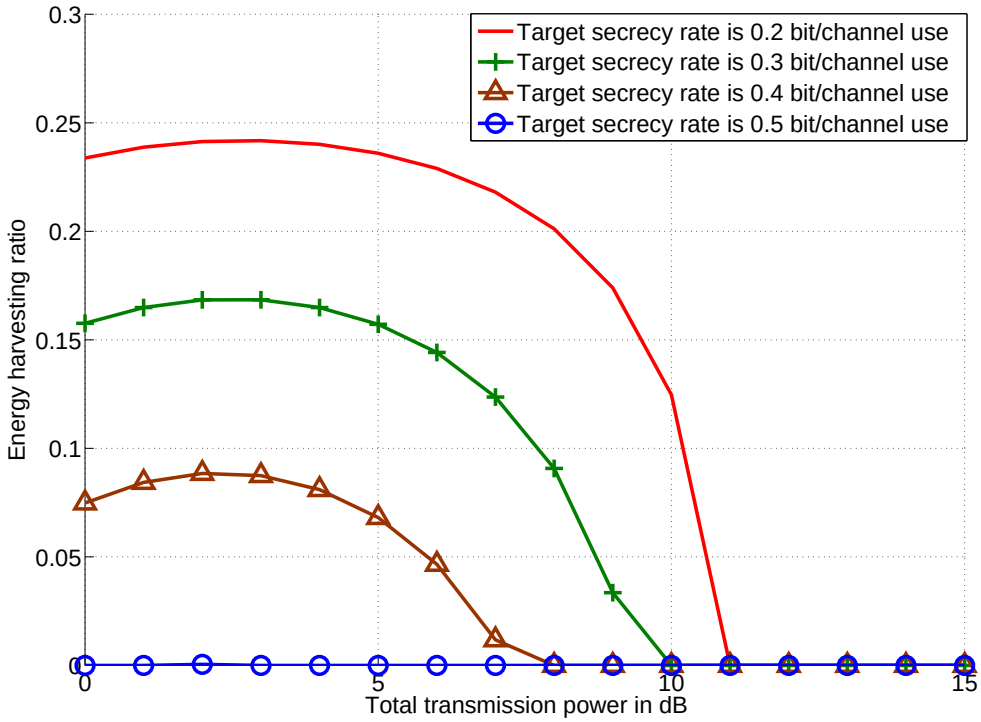

Figure 4.12: The maximum energy harvesting ratio at the destination receiver, the main channel gain is 6dB and the wiretap channel gain is 4dB.

4.7 Conclusion

In this chapter, the secrecy rate of finite-alphabet input schemes was investigated. First the relationship between secrecy rate and MMSE over AWGN channels was introduced and defined secrecy rate in a integration form of MMSE. By applying the logarithm domain transformation, it was found that the secrecy rate has a definite relationship with the SNR differences between two channels in decibel. Then, a fast PCP to optimize the transmission power P_S was presented in order to prevent the secrecy rate C_S reducing at high SNRs, although this PCP is not strictly optimal in terms of maximizing the secrecy rate. However, massive computational resources are saved compared to the exhaustive searching of the optimal PCP introduced in [63]. Furthermore, when the global CSI is available at the transmitter, the maximum value of secrecy rate that an input scheme could achieve can be determined. Finally, by using a quadratic approximation of the transformed MMSE curves, the secrecy rate and mutual information of 4QAM, 8PSK, 16QAM with Gray mapping are approximated in closed-form. This shows that in the medium range of SNR, the secrecy rate and mutual information behave in a similar manner to a bi-variate cubic function and uni-variate cubic function, respectively. By using the closed-form approximation of the secrecy rate, the maximum energy harvesting ratio for a predefined target secrecy rate is determined. The devices with energy harvesting receivers can communicates under perfect secrecy while harvesting energy from the RF signals simultaneously.

The simulation in this chapter considered Gray mapping and SP mapping on BICM schemes, the results have demonstrated that the mappings on BICM schemes affect the secrecy rate severely. In fact, Gray mapping performs the worst in terms of achievable secrecy rate at high SNR. SP mapping outperforms Gray mapping in terms of maximum secrecy rate at all SNRs. In the next chapter, the effect of signal mappings on secrecy performance is studied.

Chapter 5

Signal mapping for bit-interleaved coded modulation schemes to achieve secure communications

5.1 Introduction

Before BICM was introduced, the trellis coded modulation (TCM), which was introduced by Ungerboeck with optimal performance over AWGN channels, was generally accepted as the default communication structure. However, the BER performance of TCM is severally degraded when TCM is applied over Rayleigh fading channels. It is indicated that the *code diversity*, which is described by the Euclidean distances between the codewords has higher impact than the Hamming distance at the bit error rate (BER) performance over Rayleigh fading channels. However, it is difficult to obtain high *code diversity* in TCM since it combines coding and modulation as one entity. Thus, despite TCM schemes having large Hamming distance of the codes, the BER performance over Rayleigh fading channels is poor.

To improve the communication quality of wireless communications, an inspiring design in [79] showed that improved performance is obtained by separating the decoder and the demodulator. Inspired by this contribution, Zehavi introduced BICM as an alternative of CM in [41]. There are some advantages of BICM over TCM, firstly, because coding and modulation are treated as separate entities, the Euclidean distance between the codeword are greatly increased compared to the TCM scheme, the BER performance of BICM is better than TCM over Rayleigh fading channels.

Secondly, it is very complex to jointly optimize the coding/modulation entity and the decoding/demodulation entity in a TCM scheme, while in a BICM scheme, coding/modulation and decoding/demodulation are optimized separately, the design complexity is greatly reduced. Because of the low design complexity and good BER performance in the wireless communication environment, the BICM scheme is the *de facto* standard of wireless communications nowadays.

In BICM, the encoder outputs are forwarded into an ideal interleaver π and broken into m-bit subsequences, the interleaved subsequences are then mapped to the 2^m-ary symbols on constellation χ according to the mapping schemes. The receiver estimates the log-likelihood ratio (LLR) of each bit rather than the transmitted symbol after receiving the signals via the communication channel, this process is also called demapping. After demapping, the LLRs of each bit are de-interleaved in the same fashion π^{-1} with the transmitter interleaver and forwarded to the decoder. Among all the mapping schemes, binary reflected Gray mapping is known by the optimal performance of mutual information at a wide range of SNRs [43]. However, it is indicated in chapter 4 that Gray mapping achieves a lower secrecy rate than SP mapping at high SNR under optimal power allocation policy. It is indicated that the mapping technique can affect the secrecy rate performance in BICM schemes. In the previous section, only SP mapping is illustrated as the comparison of secrecy rate performance to Gray mapping, while a large number of mapping techniques have not been compared. In this chapter, the effects of mapping technique to the secrecy rate performance is studied by investigating various mapping schemes. The optimal labelling rule to secure the communication is presented and the performance of the optimal mapping is compared with various well-known mappings.

5.2 The impact of constellation and mappings on mutual information

The major keying methods in the modern communication are: amplitude shift keying (ASK), frequency shift keying (FSK) and phase shift keying (PSK). Among all the keying methods, 8PSK and 16QAM are very widely applied in modern communications. In this section, we analyse the effect of mapping and constellation (8PSK and 16QAM) over block fading channels with Wyner's classical wiretap channel

model. The channel coefficients follow Rayleigh distribution but remain constant within one transmission block period. Before process any further, the system model has to be clarified: we assume that *Bob* and *Eve* are the legitimate users in the communication network, *Alice* is the base station. Both *Bob* and *Eve* measures the channel condition of their respective channels and feed back the CSI to *Alice*, however, in some time period, *Alice* wishes to communicate with *Bob* in confidential, in this case, *Eve* becomes a eavesdropper. Thus, it is reasonable to assume that the transmitter knows the global CSI and each receiver has their own channel CSI. It is also reasonable to assume that *Eve* is able to possess full knowledge of the signal constellation and labelling technique employed by *Alice* and *Bob*.

An independent uniformly distributed binary source generates a sequence of information bits and forwards the bits to the channel encoder. The information bits are encoded at the predefined code rate R_c, the encoder output sequence is interleaved by a random/pseudo-random interleaver and then divided into m-bit ($m = 4$ for 16QAM and $m = 6$ for 64QAM) vectors $\mathcal{C} = \{c_1, c_2, \ldots, c_i, \ldots, c_m\}$. The transmitter *Alice* maps each m-bit vector onto a complex symbol x, which is drawn from a 16QAM or 64QAM signal constellation. The sequence of complex symbols is then sent through the main channel to *Bob*, whereas *Eve* observes the communication between *Alice* and *Bob* through the wiretap channel. The channel coefficients of the main channel and the wiretap channel are denoted as h_D and h_E, respectively. The channel outputs are given by

$$y_D = \sqrt{P_S} h_D x + n_D, \tag{5.1}$$

$$y_E = \sqrt{P_S} h_E x + n_E, \tag{5.2}$$

where P_S is the transmission power at the transmitter, the $n_D \sim \mathcal{CN}(0, 1)$ and $n_E \sim \mathcal{CN}(0, 1)$ are white Gaussian noises. The mutual information of BICM scheme is given by

$$I(x, y) = m - \sum_{i=1}^{m} E_{b,y} \left\{ \log_2 \frac{\sum_{s \in \chi} p(y|hs)}{\sum_{s \in \chi_i^b} p(y|hs)} \right\}, \tag{5.3}$$

where s is the constellation symbols, χ_i^b denotes the constellation symbols whose i-th bit value is equal to $b = \{0, 1\}$. The expectation $E_{b,y}[\cdot]$ is taken over each received

signal y and all bit values. By definition, the secrecy rate C_S is given by

$$C_S = \max \left[I(x, y_D) - I(x, y_E) \right]^+ . \tag{5.4}$$

Combining (5.3) and (5.4), the secrecy rate of a BICM scheme is obtain by solving following equation

$$C_S = \left[\sum_{i=1}^{m} E_{b,y} \left\{ \log_2 \frac{\sum_{s \in \chi} p(y_E | \sqrt{P_S} h_E s) \sum_{s \in \chi_i^b} p(y_D | \sqrt{P_S} h_D s)}{\sum_{s \in \chi} p(y_D | \sqrt{P_S} h_D s) \sum_{s \in \chi_i^b} p(y_E | h_E s)} \right\} \right]^+ . \tag{5.5}$$

The value of (5.5) can be obtained by using the Monte-Carlo method. However, the effects of mapping technique over secrecy rate can be analyzed without an exact closed-form solution to (5.5).

We start the analysis from two aspects, specifically: the effects of neighbouring constellation points of the current transmission symbol and the effect of sub-constellation shape. To obtain the design rules of high secrecy rate mapping scheme, it is convenient to rewrite (5.5) into following form

$$C_S = \sum_{i=1}^{m} E_{b,y} [F(\gamma) + G(\chi_i^b)]^+, \tag{5.6}$$

where

$$F(\gamma) = \log_2 \frac{\sum_{s \in \chi} p(y_E | h_E s)}{\sum_{s \in \chi} p(y_D | h_D s)}. \tag{5.7}$$

It is shown that the value of $F(\gamma)$ is only affected by the channel SNR, while $G(\chi_i^b)$ value is affected by both SNR and the mapping schemes.

First, we study the effects of the neighbour constellation points on the secrecy rate. At high SNRs, the value of $\sum_{s \in \chi_i^b} p(y|hs)$ is mostly determined by the current transmitted symbol x and the nearest neighbour symbols. Let s_n denote the constellation symbols with smallest Euclidean distance to the transmitted symbol x

while satisfying $s_n \in \chi_i^b$. It is reasonable to approximate $G(\chi_i^b)$ to

$$\begin{aligned} G(\chi_i^b) &= \sum_{i=1}^{m} E_{b,y}\left\{\log_2 \frac{\sum_{s\in\chi_i^b} p(y_M|\sqrt{P_S}h_D s)}{\sum_{s\in\chi_i^b} p(y_W|\sqrt{P_S}h_E s)}\right\} \\ &\approx \sum_{i=1}^{m} E_{b,y}\left\{\log_2 \frac{p(y_D|h_D x)+\sum_{k=1}^{l} p(y_D|h_D s_n^k)}{p(y_E|h_E x)+\sum_{k=1}^{l} p(y_E|h_E s_n^k)}\right\} \\ &\leq \sum_{i=1}^{m} E_{b,y}\left\{\log_2\left(\frac{p(y_D|h_D x)}{p(y_E|h_E x)} + \max_{k=1}^{l} \frac{p(y_D|h_D s_n^k)}{p(y_E|h_E s_n^k)}\right)\right\}, \end{aligned} \tag{5.8}$$

where s_n^k is the k-th ($k = 1, \ldots, l$) symbol in s_n. This equation shows that the secrecy rate is reduced if more numbers of s_n^k exist for every constellation symbol. Thus, to achieve a high secrecy rate, the number of signal points in sub-constellation χ_i^b need to be designed as small as possible.

Then, we investigate how to design the shape of the sub-constellations χ_i^b for secure communications. Let λ ($= \lambda_D$ or λ_E, depending on the channel considered) denote the log-likelihood bit metric [47, 48] for the main channel or the wiretap channel, respectively. The log-likelihood bit metric for $c_i = b$ is denoted as $\lambda(c_i^b)$ and the value of $\lambda(c_i^b)$ is computed by

$$\lambda(c_i^b) = \ln p(y|c_i = b) \tag{5.9}$$

$$= \ln \sum_{s\in\chi_i^b} p(y|\sqrt{P_S}hs) \tag{5.10}$$

$$\approx -\min_{s\in\chi_i^b} |y - \sqrt{P_S}hs|^2. \tag{5.11}$$

Using this notation, the C_S can then be rewritten as

$$C_S = E_{b,y}\left[\log_2 \prod_{i=1}^{m}\left[\frac{1+\exp(\lambda_E(C_i^{\bar{b}}) - \lambda_E(C_i^b))}{1+\exp(\lambda_D(C_i^{\bar{b}}) - \lambda_D(C_i^b))}\right]\right]^+. \tag{5.12}$$

It is important to note that the value of $\lambda_E(C_i^{\bar{b}})$ depends on the Euclidean distance between y and all signal points on the sub-constellation $\chi_i^{\bar{b}}$, which is the complement of the sub-constellation χ_i^b. Let $K_i = \frac{1+\exp(\lambda_E(C_i^{\bar{b}}) - \lambda_E(C_i^b))}{1+\exp(\lambda_D(C_i^{\bar{b}}) - \lambda_D(C_i^b))}$, the secrecy rate is given by

$$C_S \leq \max_{\bar{\gamma}\geq 0} E_{b,y}\left[\log_2\left(\sum_{i=1}^{m}\frac{K_i}{m}\right)^m\right]^+, K_i > 0. \tag{5.13}$$

The inequality in (5.13) is obtained by the arithmetic mean – geometric mean (AM-GM) inequality, it can be written as equality if and only if $K_1 = K_2 = \ldots K_i \ldots$.

This equality condition in AM-GM inequality indicates that the shape of sub-constellations χ_i^b and $\chi_i^{\bar{b}}$ have to be as similar as possible.

5.3 Well known mappings on 8-ary and 16-ary constellations

Before introducing the optimal mapping for secrecy communication, the well known mappings on 8-ary and 16-ary constellations are revised. Gray mapping is known as the optimal mapping technique by its optimal mutual information performance, this conjecture was supported by a number of simulation results, further studies on signal mapping in [44] [53] indicate that the BICM mutual information of Gray mapping only has optimal performance for moderate to high SNR values. SP mapping is introduced by G. Ungerboeck to jointly optimises the encoding and modulation entity of CM schemes, while one special class of SP mapping, namely *strictly regular set partitioning mapping* shows optimal BICM capacity performance at low SNR range [46]. After iterative decoding is introduced, a lot of error-floor removing mappings, such as maximum square Euclidean weight (MSEW) mapping [45], M16^a and M16^r mappings [49] are introduced due to excellent bit error rate (BER) performances in bit interleaved coded modulation with iterative decoding (BICM-ID) over AWGN and Reyleigh fading channels, respectively. We study the secrecy rate performances of Gray, SP, MSEW and M16^r mapping on 16-QAM constellation, and Gray, SP, MSEW on 8-PSK constellation. In the remainder of this chapter, we call the constellation point at the minimum Euclidean distance to the target point the neighbour point.

5.3.1 Various mappings on 8PSK constellation

On 8PSK, Gray, SP and MSEW mappings are revised and the sub-constellations of these mappings are presented.

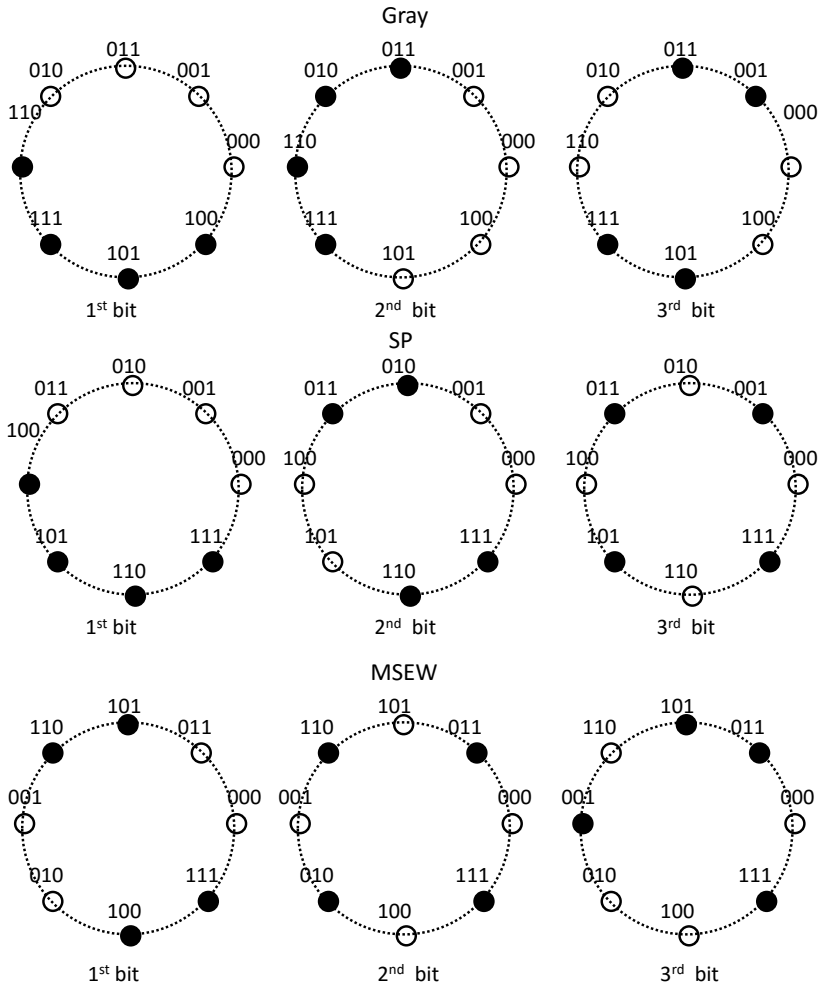

Figure 5.1: The sub-constellations of different mappings on 8-PSK constellation.

In Fig.5.1, the filled and unfilled points denote that the bit value at the corresponding bit position is equal to 1 and 0, respectively. The radius of the circle (dash line) is set to 1 in order to provide unit average energy constellation symbols.

For Gray mapping, for the first bit and second bit sub-constellations, the two filled and unfilled points have two neighbours at the minimum Euclidean distance on their respective sub-constellations, while the remaining four constellation points on each sub-constellation have one neighbour point. For the third bit, every constellation point has only one neighbour point on the sub-constellations. The first and second bit sub-constellations of SP mapping are similar to the second and third bit of Gray mapping, while on the third bit sub-constellation of SP mapping, every constellation point has no neighbour point on the sub-constellation. For MSEW mapping, the first and second bit sub-constellations are the same as the second and third bit sub-constellations, while for the third bit sub-constellation, only two constellation points have one neighbour point.

5.3.2 Various mappings on 16QAM and (1,5,10) constellations

For 16-ary constellations, Gray, SP, MSEW and M16^r mappings are illustrated both on 16QAM and (1,5,10) constellations. The Gray and SP mappings show optimal BER performance over BICM and TCM, while MSEW and M16^r mappings perform low error floor over BICM-ID. Fig. 5.2 shows the sub-constellations of the mappings on 16QAM constellation. The filled points represent the bit value at corresponding bit position equal to 1, while the unfilled points designate the bit value equal to 0. The minimum Euclidean distance between two constellation symbols is equal to $\frac{1}{2\sqrt{10}}$, thus, the average constellation symbol energy is equal to 1.

We compare the neighbour points on the sub-constellations for Gray mapping and SP mapping to demonstrate that the sub-constellation points on Gray mapping are more "crowded" than the other mapping schemes.

For Gray mapping, on the first and third bit sub-constellations, there are four filled points with two neighbours at the minimum Euclidean distance, while the remaining four filled points only have one neighbour point. For the unfilled points, four points have three neighbours and the other four points have two neighbours. On the second and fourth bit constellations, four filled points have three neighbours

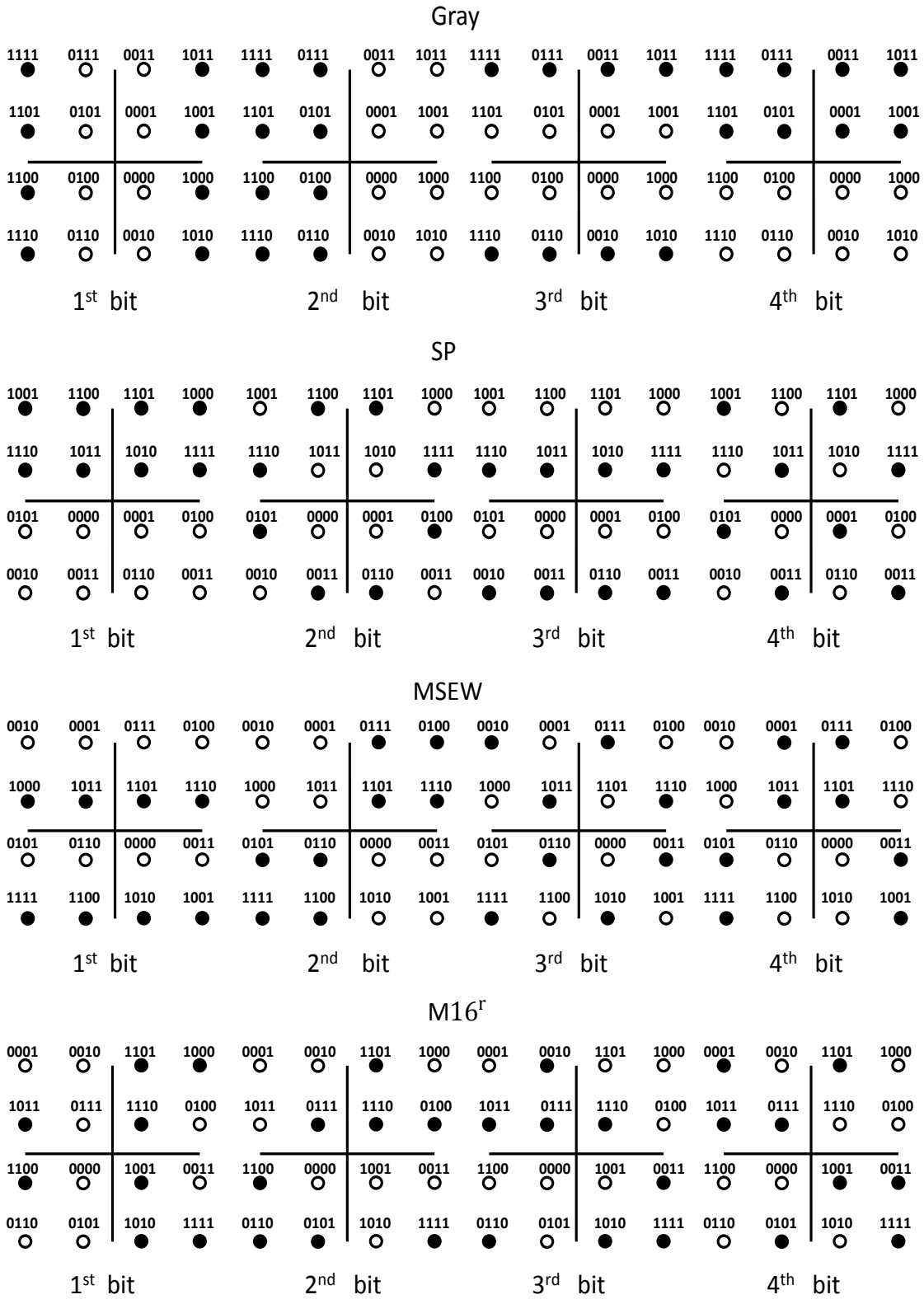

Figure 5.2: The sub-constellations of Gray,SP, MSEW and M16^r mapping on 16QAM constellation.

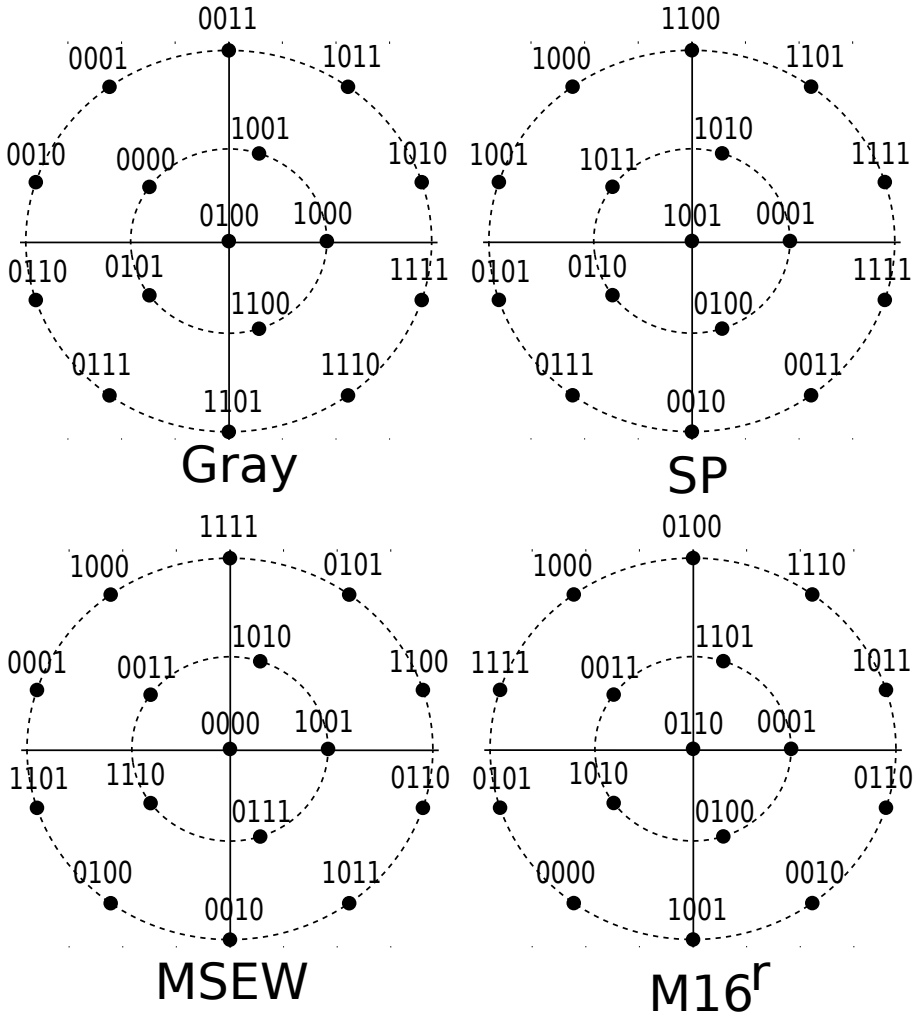

Figure 5.3: The quasi-Gray, quasi-SP, quasi-MSEW and quasi-M16^r mappings on the (1, 5, 10) constellation.

and the other four have two neighbours, four unfilled points have three neighbours and the other four have two neighbours.

For SP mapping, the first bit sub-constellation is similar to the fourth bit sub-constellation of Gray mapping. For the second bit sub-constellations, all filled points have only one neighbour while four of the unfilled points have two neighbours and the other four unfilled points have no neighbour point. For the third bit sub-constellations, four filled and unfilled points have two neighbours and the other four filled and unfilled points have one neighbour. For the fourth bit sub-constellations, there is no neighbour point for every filled and unfilled point.

The (1, 5, 10) constellation is basically a APSK modulation, this kind of modulation is not widely applied in daily life use, however, the APSK is commonly used in satellite and deep space communication, as one major purpose of the satellite communication is for the military use, it is meaningful to study the secrecy performance of mappings on (1, 5, 10) constellation. The (1, 5, 10) constellation is generated by placing one symbol at $(0, 0)$ and rest of the symbols on two concentrically circles, the radius of the inner circle and the radius of the outer circle are denoted as r_{inner} and r_{outer}, respectively. To maximize the mutual information, it is indicated in [53] that the optimal radius values are $r_{inner} = 1.8294$ and $r_{outer} = 3.7851$. The constellation symbols are scaled by $\frac{1}{4\sqrt{10}}$ after modulation in order to satisfy the symbol energy condition $E[|E_S|^2] = 1$.

The strict Gray, SP and MSEW mappings are not applicable to the (1, 5, 10) constellation, alternatively, quasi-Gray, quasi-SP and quasi-MSEW mappings are generated on this constellation.

5.4 The optimal mapping for optimal secrecy rate performance

In this section, the design rule of signal mapping to achieve a high secrecy rate is studied. The secrecy rate curves of BICM schemes are concave and one global maximum value is achieved at medium SNR range. The "optimal" mapping that is interested obtains larger global maximum value than other mappings. However, the secrecy rate performance at low SNRs are not interested. Hereby, we recall the relationship between MMSE and secrecy rate

$$\begin{aligned} C_S &= 0.1\log_2 10 \int_{\gamma_{E,dB}}^{\gamma_{M,dB}} \gamma \mathbf{MMSE}(\gamma) d\gamma_{dB} \\ &= \int_{\gamma_{E,dB}}^{\gamma_{M,dB}} \mathcal{M}(\gamma_{dB}) d\gamma_{dB}. \end{aligned} \tag{5.14}$$

Since $\gamma_{D,dB} - \gamma_{E,dB}$ is constant in one transmission block, to maximise C_S is equivalent to maximize $\mathcal{M}(\gamma_{dB})$. Despite Gaussian input schemes obtain maximum $\mathcal{M}(\gamma_{dB})$ at $\gamma \to +\infty$, the global maximum values of various mappings in fig.4.2 is at medium to high SNR range, it indicates that to maximise the secrecy rate, the error events at the receiver has to be maximized at medium to high SNR. For BICM schemes, the error events indicates the estimation error between the input bit sequences and the estimation of the bits based on the observation of the received signals. Note that the enhance of the secrecy rate performance is based on the cost of the detection accuracy at the receiver, which implied lower throughput and system performance for normal communications.

5.4.1 The distance spectrum

In the previous sections, the analysis show that the optimal mapping for secure communication have following characteristics:

- The number of neighbour symbols with the minimum Euclidean distance to x on χ_i^b has to be minimized.
- The points on the sub-constellations χ_i^b and $\chi_i^{\bar{b}}$ has to be spread.
- The mapping maximizes the MMSE at medium to high SNR range.

The first and second condition can be satisfied with no contradicting to each other by maximizing the average Hamming distance of the mapping. For the third condition, It has been proved that Gray mapping obtains the lowest MMSE among all mappings, in other words, Gray mapping produces less error events than the other mappings. The error events for a mapping scheme can be well described by the distance spectrum.

Hereby, we introduce the distance spectrum $N(d_e)$, which is defined as the expected number of error events $Er(d_e, s)$ that are made at a Euclidean distance d_e, averaged over entire sub-constellation points $s \in \chi_i^b$ and all bit positions $i = 1, \ldots, m$

$$N(d_e) = \frac{1}{m2^m} \sum_{i=0}^{m} \sum_{b=0}^{1} \sum_{s \in \chi_i^b} Er(d_e, s). \tag{5.15}$$

The error event $Er(d_e, s)$ is equal to the Hamming distance between s and the other constellation symbols, at Euclidean distance d_e. Specifically, for 16QAM, the d_e can take value from the set $(\alpha, 2\alpha, 4\alpha, 5\alpha, 8\alpha, 9\alpha, 10\alpha, 13\alpha, 18\alpha)$, where α represents the minimum squared Euclidean distance between two constellation points, while for 8PSK, the d_e values are chosen from $(\alpha, 5.828\alpha, 6.828\alpha)$. As (5.8) shows that the the constellation symbols with smaller Euclidean distance to s have higher affects to the secrecy rate performance than the distant symbols, thus, we concentrate on the distance spectrum values with the minimum and the second minimum Euclidean distances.

5.4.2 The optimal mapping for secrecy communication

In this section, we develop a new signal-mapping algorithm called maximum error event (MEE) mapping. The algorithm is presented in Algorithm I. According to

Table 5.1: ALGORITHM I: MEE MAPPING

1	Set $d_e = \alpha$.
2	Begin with an initial random mapping M. Compute the $N(d_e)$.
3	Generate a new mapping $\mathfrak{M}$, compare $N_{\mathsf{M}}(d_e)$ and $N_{\mathfrak{M}}(d_e)$
4	Let $\mathsf{M} = \max_{N(d_e)}(\mathsf{M}, \mathfrak{M})$.
5	Repeat step 3 and 4, until no new $\mathfrak{M}$.
6	Increase d_e, repeat 2 to 5.

MEE algorithm, the MEE mapping on 8PSK, 16QAM and (1,5,10) constellations

are presented and the sub-constellations are shown. The distance spectrum of the MEE mappings on 8PSK, 16QAM (1,5,10) are listed in the following tables.

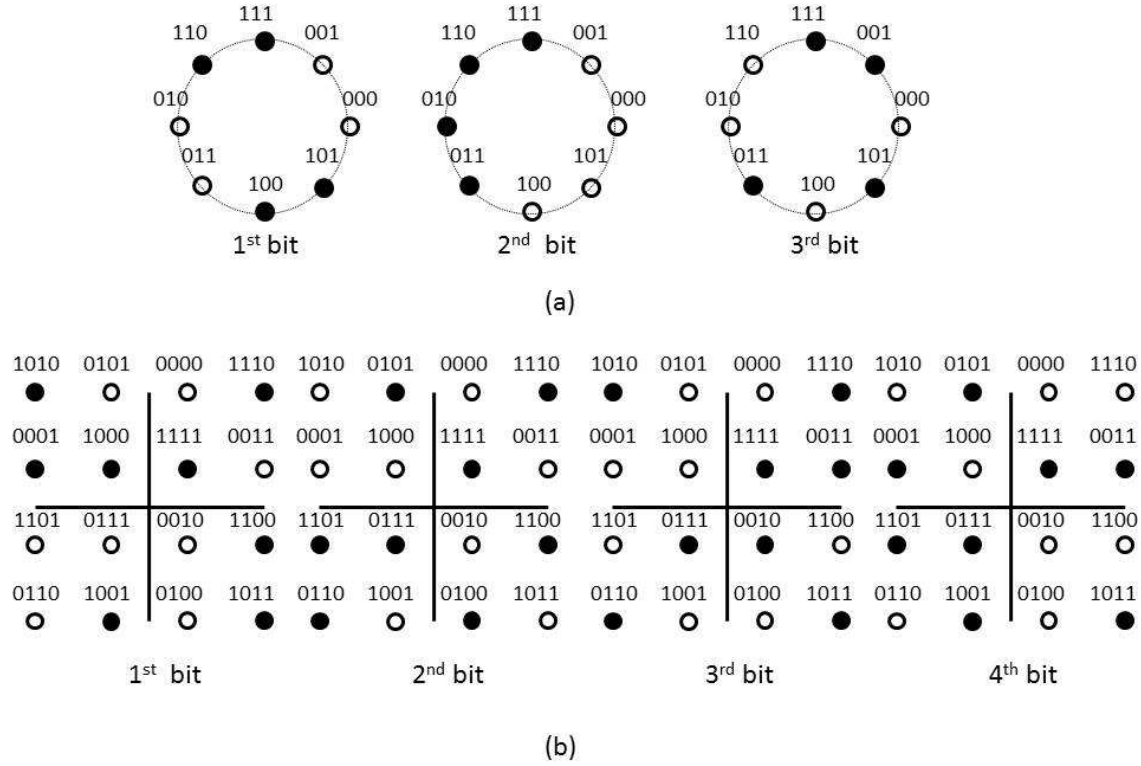

Figure 5.4: The sub-constellations of MEE mappings, (a) are the sub-constellations on 8-PSK constellation, (b) are the sub-constellations on 16QAM constellation.

Table 5.2: Values of $N(d_e(n))$ of mappings on the 8PSK.

8PSK	Gray	SP	MSEW	MEE
$N(\alpha)$	0.67	1.17	1.50	1.67
$N(5.828\alpha)$	1.33	1	1	0.667

It is shown in Table 5.2 that Gray mapping has a minimum value of $N(\alpha) = 0.67$ and a maximum value of $N(5.828\alpha) = 1.33$, it is expected to achieve the minimum value of secrecy rate. For SP and MSEW mappings, the $N(5.828\alpha)$ values are the same but SP mapping has smaller $N(\alpha)$ value, thus, MSEW mapping can achieve higher secrecy rate performance than SP mapping, finally, for MEE mapping ,the $N(\alpha)$ value is much larger than the other mappings, although the $N(5.828\alpha)$ value is the minimum among all mappings, MEE mapping is expected to achieve maximum secrecy rate.

In Table 5.3, the Gray mapping results in the minimum value of both $N(\alpha)$ and $N(2\alpha)$, thus, Gray mapping should achieve the minimum value of secrecy rate

Table 5.3: Values of $N(d_e(n))$ of mappings on the 16QAM.

16QAM	Gray	SP	MSEW	M16^r	MEE
$N(\alpha)$	0.75	1.75	1.63	1.75	2.92
$N(2\alpha)$	1.88	2.75	2.94	3.06	3.94

Table 5.4: Values of $N(d_e(n))$ of mappings on the (1, 5, 10) constellation.

(1,5,10)	q-Gray	q-SP	q-MSEW	q-M16^r	MEE
$N(\alpha)$	0.47	0.64	0.75	0.75	0.97

among all mappings compared. The distance spectrum values of SP, MSEW and M16^r are very similar, their secrecy rate performances are expected to be similar at a medium SNR range, MEE mapping achieves maximum $N(\alpha)$ and $N(2\alpha)$ values, it is expected to achieve the maximum secrecy rate performance.

Table 5.5: MEE mapping on (1,5,10) constellation, $r_1 = 1.8294$, $r_2 = 3.7851$. The constellation points are denoted as by radius and phase

constellation	0000	0001	0010	0011	0100	0101	0110	0111
(1,5,10,)	$r_1, 0\pi$	$r_1, \frac{8\pi}{5}$	$r_2, \frac{13\pi}{10}$	$r_1, \frac{2\pi}{5}$	$r_2, \frac{5\pi}{10}$	$r_1, \frac{6\pi}{5}$	$r_2, \frac{9\pi}{10}$	$r_2, \frac{15\pi}{10}$
	1000	1001	1010	1011	1100	1101	1110	1111
(1,5,10,)	$r_2, \frac{11\pi}{10}$	$r_1, \frac{4\pi}{5}$	$r_2, \frac{7\pi}{10}$	$r_2, \frac{19\pi}{10}$	$r_2, \frac{17\pi}{10}$	$r_2, \frac{3\pi}{10}$	$0, 0$	$r_2, \frac{1\pi}{10}$

It is shown in Table 5.4 that MEE mapping achieves higher $N(\alpha)$ value than the other mappings and Gray mapping obtains the lowest $N(\alpha)$ value. For MSEW and M16^r mappings, the $N(\alpha)$ value is the same, so their secrecy rate performance will be very close. The SP mapping obtains a larger $N(\alpha)$ value than Gray mapping, thus it will achieve a higher secrecy rate than Gray mapping.

5.5 Numerical results

In this section, the secrecy rate of various mappings discussed in this chapter are simulated and compared. We begin the comparison of secrecy rate from the mappings on 16QAM and followed by the mappings on 8PSK, both constellations are illustrated with SNR gap values equal to 0dB, 5dB and -5dB, respectively.

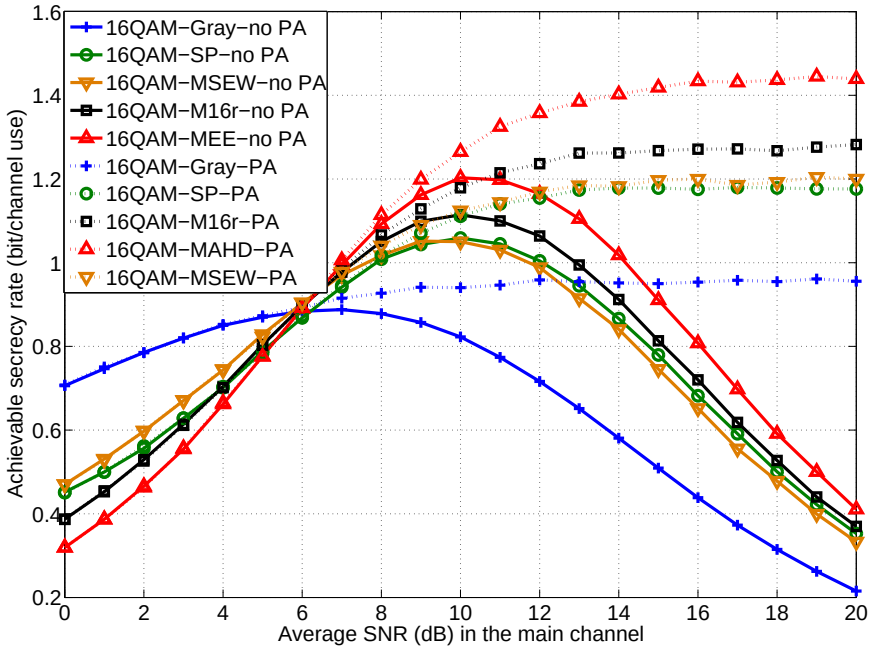

Figure 5.5: The secrecy rate performances of various mappings on 16QAM constellation, the full lines are with flat power allocation, while the dotted lines are with the fast power allocation. The SNR gap $\Delta\gamma = 0dB$

.

5.5.1 Example: secrecy rate performances on 16QAM

It is shown in Fig.5.5 that MEE mapping outperforms the other mappings at moderate to high SNR values in terms of secrecy rate. When $\Delta\gamma = 0$, Gray mapping obtains higher secrecy rate than the rest of the mappings if the average SNR of the main channel is smaller than 6dB, meanwhile, MEE mapping achieves the lowest secrecy rate value in this SNR range. It is shown in Fig.5.5 that almost all mapping schemes achieves the same secrecy rate value at $\bar{\gamma}_M = 6$dB and the secrecy rate of MEE mapping surpasses other mapping schemes when the SNR grows larger than 6dB. The secrecy rate of SP mapping and MSEW mapping have very close performance from 0dB to 20dB, comparing with their $N(d_e)$ values, we can see that SP mapping has a larger $N(\alpha)$ value than MSEW mapping (1.75 vs. 1.63), but MSEW mapping obtains a larger $N(2\alpha)$ value than SP mapping (2.94 vs. 2.75). The $N(\alpha)$ value of SP mapping and M16^r mapping are equal, but the $N(2\alpha)$ value of M16^r mapping is 3.06, which is larger than the $N(2\alpha) = 2.75$ of SP mapping, thus, the secrecy rate performance of M16^r mapping is higher than SP mapping. The dotted curves show the secrecy rate of various mappings under fast PCP as proposed in Chapter 4, the MEE mapping obtains the highest secrecy rate at high SNR while

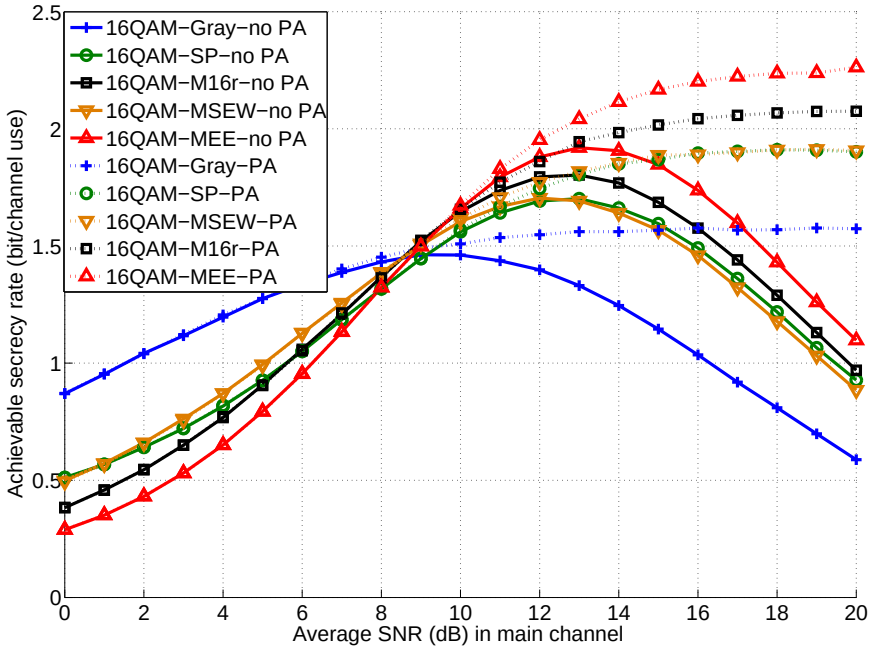

Figure 5.6: The secrecy rate performances of various mappings on 16QAM constellation, the full lines are with flat power allocation, while the dotted lines are with the fast power allocation. The SNR gap $\Delta\gamma = 5dB$

.

Gray mapping achieves lowest value of secrecy rate.

Fig.5.6 and Fig.5.7 show the secrecy capacities of various mappings with SNR gap equal to 5dB and -5dB, respectively. The secrecy rate of MEE remains highest at high SNR range, while Gray mapping's optimal performance is at low SNR range. When $\Delta\gamma = 5$dB, the secrecy rate of Gray mapping is surpassed by other mappings around 9dB, while the secrecy rate of Gray mapping is surpassed by other mapping schemes at 2dB when $\Delta\bar{\gamma} = -5$dB. This is when $\bar{\gamma}_{D,dB} - \bar{\gamma}_{dB} = 5$dB, the interval of $[\gamma_{E,dB}, \gamma_{D,dB}]$ is very likely to be large and the differences between the $\bar{\mathcal{M}}$ of Gray mapping and other mapping schemes are small. On the contrary, when $\Delta\gamma = -5$dB, no positive secrecy rate can be obtained during most of the fading realizations, it is more likely to obtain small $[\gamma_{E,dB}, \gamma_{D,dB}]$ interval, thus, Gray mapping obtains much lower secrecy rate.

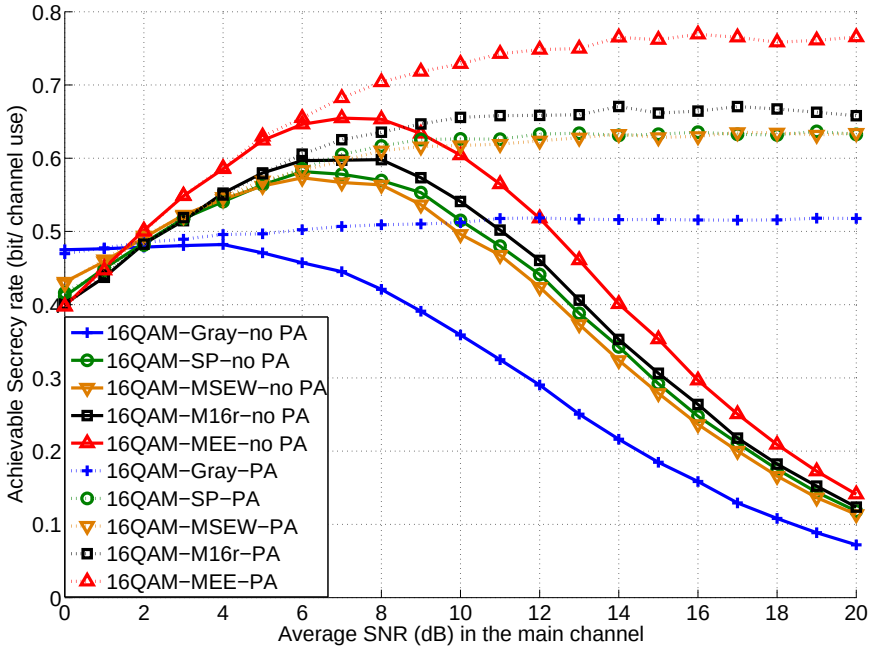

Figure 5.7: The secrecy rate performances of various mappings on 16QAM constellation, the full lines are with flat power allocation, while the dotted lines are with the fast power allocation. The SNR gap $\Delta\gamma = -5dB$

.

5.5.2 Example: secrecy rate performances on 8PSK

In the case of 8PSK, we compare the secrecy rate performances of MEE mapping with Gray, SP and MSEW mappings over Rayleigh fading channels in the following figures with the SNR gap equal to 0dB, 5dB, -5dB, respectively.

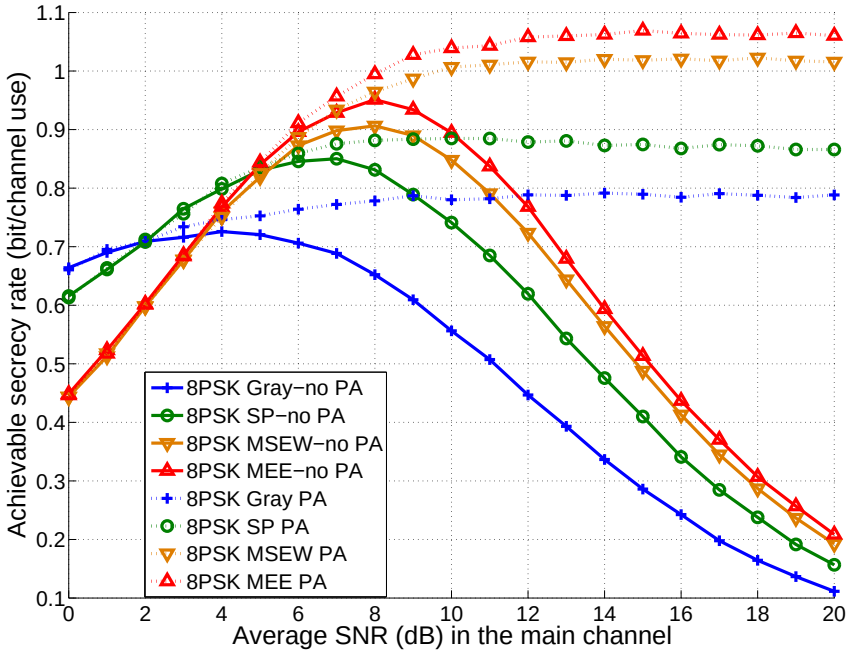

Figure 5.8: The secrecy rate performances of various mappings on 8PSK constellation, the full lines are with flat power allocation, while the dotted lines are with the fast power allocation. The SNR gap $\Delta\gamma = 0dB$

.

In the 8PSK case, we compare Gray, SP, MSEW and MEE mappings in terms of their secrecy rate performances. The SP mapping and MSEW mapping have the same $N(2\alpha)$ value but the $N(\alpha)$ value of MSEW mapping is significantly larger than SP mapping, thus, MSEW mapping obtains higher secrecy rate at high SNR range, The $N(\alpha)$ value of MEE mapping is the largest, however, its $N(2\alpha)$ value is smaller than others, MEE mapping still achieves the highest secrecy rate, but with no significant advantage. Gray mapping achieves the lowest secrecy rate due to the minimum $N(\alpha)$ value of all mappings. To demonstrate that MEE algorithm is applicable to all constellations, the secrecy rate performances on (1,5,10) mapping is simulated.

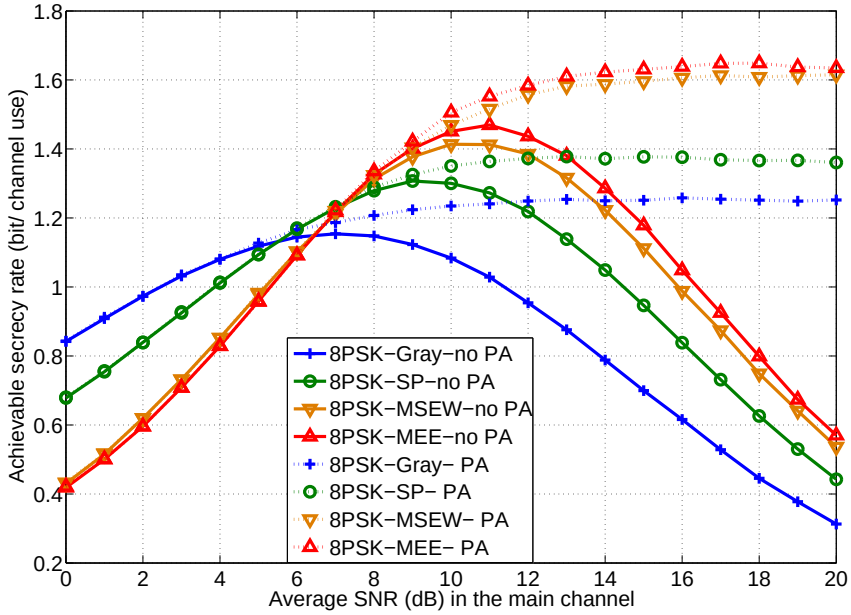

Figure 5.9: The secrecy rate performances of various mappings on 8PSK constellation, the full lines are with flat power allocation, while the dotted lines are with the fast power allocation. The SNR gap $\Delta\gamma = 5dB$

.

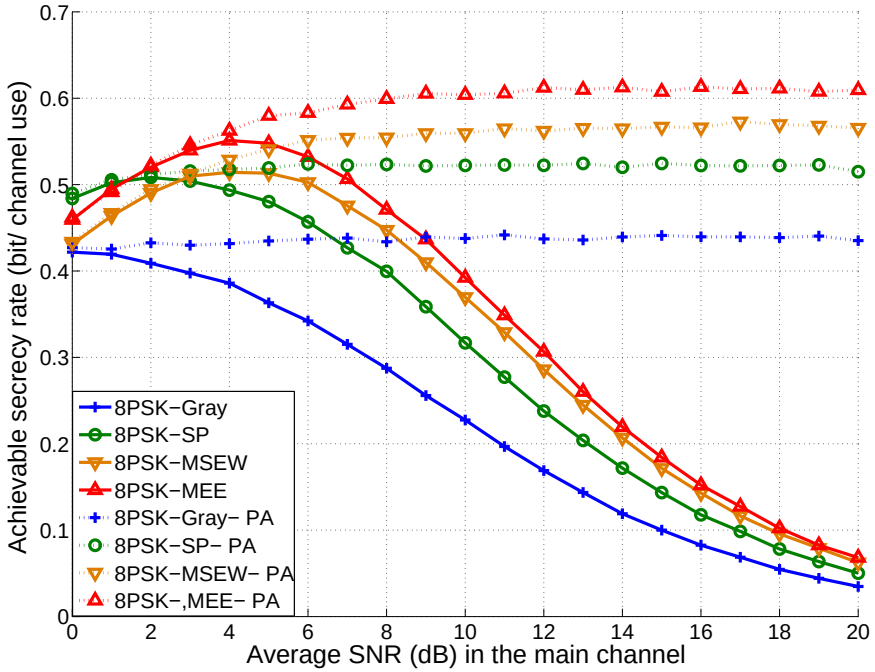

Figure 5.10: The secrecy rate performances of various mappings on 8PSK constellation, the full lines are with flat power allocation, while the dotted lines are with the fast power allocation. The SNR gap $\Delta\gamma = -5dB$

.

5.5.3 Example: secrecy rate performances on (1,5,10) constellation

The secrecy rate of various mappings on (1, 5, 10) constellation with SNR gap equal to -5dB, 0dB and 5dB are compared in this section.

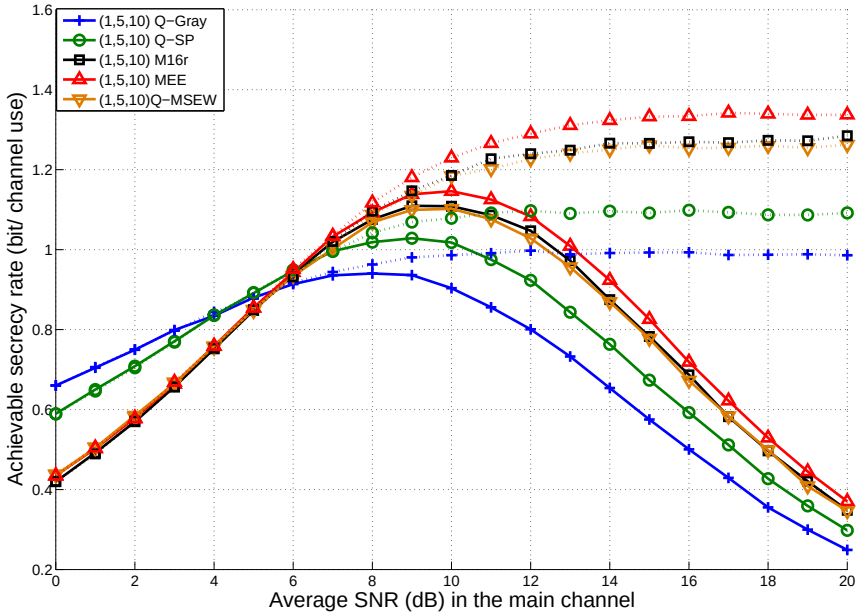

Figure 5.11: The secrecy rate performances of various mappings on (1,5,10) constellation, the full lines are with flat power allocation, while the dotted lines are with the fast power allocation. The SNR gap $\Delta\gamma = 0dB$

.

Fig. 5.11, Fig. 5.12 and Fig. 5.13 show the mutual information performance of various mapping schemes when the average SNR in the main channel is 0dB, 5dB and -5dB higher than the wiretap channel. The MEE mapping obtains maximum secrecy rate value at a high SNR range in all figures. MEE mapping has the maximum $N(\alpha)$ value among all mapping schemes, thus MEE mapping obtains the maximum secrecy rate at a medium SNR range. It is illustrated that M16^r and MSEW mapping obtain a very similar secrecy rate across the entire SNR range. In terms of $N(\alpha)$ value, both MSEW and M16^r have $N(\alpha) = 0.75$, this demonstrates that they show similar secrecy rate performance. Gray mapping achieves the maximum secrecy rate at a much lower SNR than other mappings, but at the cost of the secrecy rate performance at high SNR. SP mapping achieves higher secrecy rate than Gray mapping, but a lower secrecy rate than MSEW, M16^r and MEE mapping.

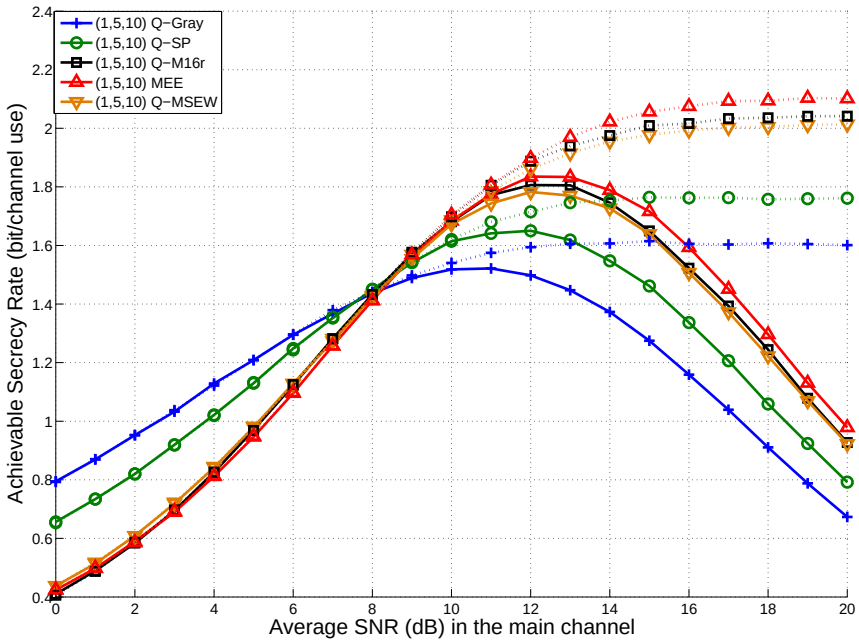

Figure 5.12: The secrecy rate performances of various mappings on (1,5,10) constellation, the full lines are with flat power allocation, while the dotted lines are with the fast power allocation. The SNR gap $\Delta\gamma = 5dB$

.

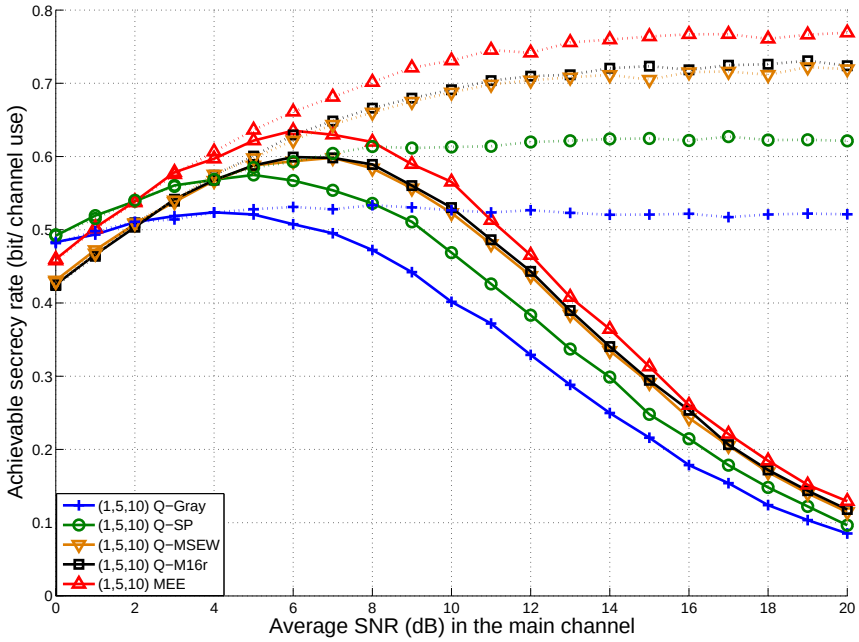

Figure 5.13: The secrecy rate performances of various mappings on (1,5,10) constellation, the full lines are with flat power allocation, while the dotted lines are with the fast power allocation. The SNR gap $\Delta\gamma = -5dB$

.

5.6 Conclusion

In this section, a new mapping algorithm is proposed as the optimal mapping rule under secrecy constraint, the generated mapping, namely MEE mapping, achieves the highest secrecy rate among all mappings. The distance spectrum is the critical parameter in the MEE mapping searching steps. The secrecy rate of Gray, SP, MSEW, M16^r and MEE mappings are compared on 16QAM and (1,5,10) constellation, while Gray, SP, MSEW and MEE mappings are compared on 8PSK in three cases: equal average channel SNR of both channels, the main channel is less noisy than the wiretap channel on average and the main channel is noisier than the wiretap channel on average. Considering the transmission power consumption and secrecy rate performance, we draw conclusions from two aspects: on one hand, Gray mapping achieves lowest secrecy rate at high SNR range, MEE performs at a significantly higher secrecy rate than other mappings at a high SNR range for all cases that are considered in this chapter. On the other hand, Gray mapping achieves maximum secrecy rate at a much lower SNR than the other mappings, and its secrecy rate performance at low SNR is optimal.

Chapter 6

Secrecy capacity maximization for BICM wiretap channel with a trustful relay employing decode-and-forward strategy

6.1 Introduction

The secrecy rate of the Wyner wiretap channel model when all terminals are equipped with single input single output (SISO) is studied in chapter 4. We show that the maximum secrecy rate is a linear function of the SNR gap of both channels in decibel. However, the study also indicates that positive secrecy rate is obtained only when the main channel is less noisy than the wiretap channel. If both channels inhabit Rayleigh fading, the transmission has to stop when the instantaneous SNR of main channel γ_D is smaller than the wiretap channel γ_E. This limitation on the confidential message transmission seriously decreased the transmission speed seriously.

One solution to $\gamma_D < \gamma_E$ is to equip multiple antennas on the transmitter, namely a multiple input single output (MISO) or multiple input multiple output (MIMO) strategy to increase the channels between the source to both destination and eavesdropper. Each antenna between the source and the destination/eavesdropper establishes a communication antenna pair. By using multiple antenna transmission, it is possible to obtain positive secrecy rate if one or more sub-channels in the main

channel is less noisy than the sub-channels in the wiretap channel. The research on Gaussian input case indicates that secrecy capacity can be optimized by using the convex optimization technique to obtain positive secrecy capacity.

Another solution is to apply cooperative communication by introducing a trustful helper relay to the communication party. In the this model, a pair of relay-destination and relay-eavesdropper channels are established. When the original source-destination and source-eavesdropper channel pair cannot achieve positive secrecy rate, the relay-destination and relay-eavesdropper channel pair may achieve positive secrecy rate instead. The use of multiple relays in the wiretap channel is studied in [80] [81] [75] [82], the relays can either work cooperatively to enhance the secrecy rate, or based on the requirements of secrecy rate and the channel state information the best relay is selected.

In this chapter, we focus on the advantages of cooperative communication over the classical wiretap channel model. Due to optimal power allocation (PA) requiring exhaustive searching, an alternative computation resource saving PA algorithm is introduced and the secrecy rate is computed.

6.2 The general channel model of decode and forward relay wiretap channel

In the DF scheme, the system model consists of one message source, one legitimate destination, one eavesdropper and L relays. Two stage transmission is applied. In the first stage, the source broadcasts the confidential message to all users, including the relays, intended destination and the eavesdropper. In the second stage, the i-th relay decodes the received signals from the source and re-encodes in the same fashion as the source and sends signals to the destination and the eavesdropper. Fig. 6.1 shows the wiretap channel model with L helping DF relays. The full lines denote that the transmission happened in the first stage, while the dashed lines represent the second stage transmission from the relay to the destination and the eavesdropper. The notation $h_D, h_E, h_{R,i}$ are the channel coefficients between source to destination, source to eavesdropper and source to the i-th relay, respectively, while g_D and g_E are the channel coefficients of the relay to destination channel and the relay to eavesdropper channel, respectively. As the relay only forwards the infor-

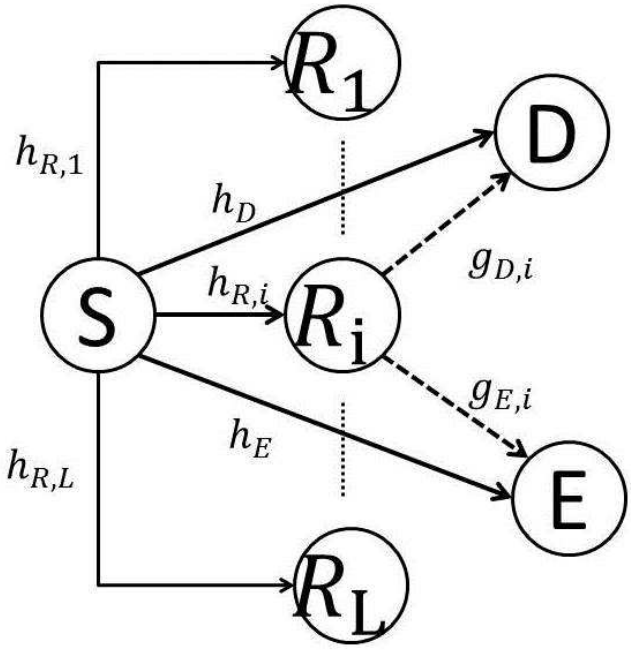

Figure 6.1: The system model of relay helped wiretap channel with DF strategy.

mation decodes from the source message but not generate its own information, the throughput of the relay-to-destination channel is always smaller than the throughput of the source-to-relay channel. In the DF scheme, the information rate transmitted in the channel between relay and destination is given by [76]:

$$C_M = \min\{I(SNR_{SR}), I(SNR_{RD})\}, \tag{6.1}$$

where $I(SNR_{SR})$ denotes the mutual information in the source to relay channel and $I(SNR_{RD})$ is the mutual information in the relay to destination channel. If $I(SNR_{SD}) \leq I(SNR_{RD})$, the relay can not forward all of the information that it received from the source, which normally should be avoided.

6.3 No direct link between source and destination

To start with, we consider a special case, which is that there is only one relay and the direct links between the source and destination/eavesdropper are very weak compared to the relay to destination/eavesdropper links. The relay in this model can be regarded as a message source but with some power constraints. This assumption models the case that destinations are of long distances from the source. The secrecy rate and power allocation policy for this model is similar to the direct transmission case. The maximum information rate at the destination receiver and the eavesdrop-

per receiver are given by $\min\{I(\gamma_D), I(\gamma_R)\}$ and $\min\{I(\gamma_E), I(\gamma_R)\}$, respectively. We define the total available power as P_T, the transmission power at the source is denoted as P_S and the transmission power at the relay is denoted as P_R. We assume the noises at destination and eavesdropper are Gaussian distributed with zero mean, unit variance. The secrecy rate maximization problem is formulated to

$$\max\ C_S$$

s.t.

$$P_S + P_R \leq P_T. \tag{6.2}$$

The ideal solution to this problem is to set γ_{opt} in the center of $[\gamma_{E,dB}, \gamma_{D,dB}]$, which indicates $\frac{\gamma_{D,dB}+\gamma_{E,dB}}{2} = \gamma_{opt}$. The values of $\gamma_{D,dB}$ and $\gamma_{E,dB}$ given by

$$\gamma_{D,dB} = 10\log_{10}(P_R|g_D|^2) \tag{6.3}$$

$$\gamma_{E,dB} = 10\log_{10}(P_R|g_E|^2) \tag{6.4}$$

the minimum P_S is given by $P_S|h_R|^2 = P_R|g_D|^2$, thus the computed minimum total transmission power $\hat{P_T}$ is given by

$$\hat{P_T} = \frac{10^{0.1\gamma_{opt}}}{\sqrt{|g_D|^2|g_E|^2}}(1 + \frac{|g_D|^2}{|h_R|^2}), \tag{6.5}$$

and the optimal values for P_S and P_R are given by

$$P_S = \sqrt{\frac{|g_D|^2}{|h_R|^4|g_E|^2}}10^{0.1\gamma_{opt}} \tag{6.6}$$

$$P_R = \sqrt{\frac{1}{|h_D|^2|g_E|^2}}10^{0.1\gamma_{opt}} \tag{6.7}$$

if $\hat{P_T} \leq P_T$, the secrecy rate is maximized by using partial of the available power, however, if $\hat{P_T} > P_T$, the secrecy rate maximization problem is formulated to

$$\max \frac{\gamma_{D,dB}+\gamma_{E,dB}}{2} \tag{6.8}$$

s.t.

$$P_S + P_R = P_T.$$

$$P_S|h_R|^2 \geq P_R|g_D|^2.$$

This condition is satisfied when $P_S|h_R|^2 = P_R|g_D|^2$, thus, the optimal solution is given by

$$P_S = \frac{|g_D|^2}{|g_D|^2 + |h_R|^2} P_T, \tag{6.9}$$

$$P_R = \frac{|h_R|^2}{|g_D|^2 + |h_R|^2} P_T. \tag{6.10}$$

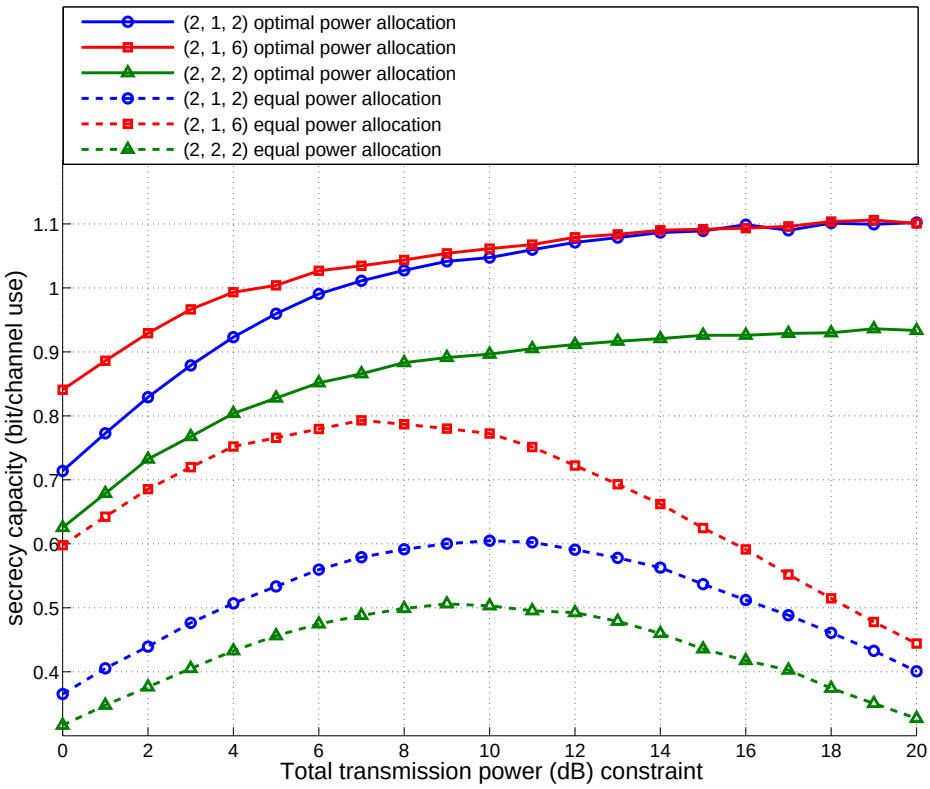

Figure 6.2: secrecy rate performances of BICM scheme wiretap channel with one DF relay helper and no direct source to destination links, the legends are representing $(E[10\log_{10}|g_D|^2], E[10\log_{10}|g_E|^2], E[10\log_{10}|h_R|^2])$

Fig. 6.2 shows that the secrecy rate performances of the proposed PA algorithm are much higher than the equal PA algorithm. When the value of P_T increases, the secrecy capacities with the proposed PA remain at high values while the secrecy rate of the equal PA decreases to zero. The $|h_R|^2$ affects the minimum value of $\hat{P}_T$, larger $|h_R|^2$ value results in smaller $\hat{P}_T$, thus improving secrecy rate performance and saving energy at the same time.

6.4 The direct link between source and destination is not ignorable

Having analyzed the no direct link case, we now consider a more popular DF model, where the direct links between source and destination/eavesdropper are not ignorable. In this case, the use of a relay is to cope with $|h_D| < |h_E|$ in order to achieve positive secrecy rate, or enhance the secrecy rate performance. The two time slots transmission scheme is introduced, at the first time slot, all receivers listen to the source, the source broadcasts the confidential message to the relay and the relay performs decoding process; at the second time slot, the transmitter stops sending message, meanwhile, the relay sends the re-encoded message to the destination. The channel outputs are given by

$$y_D = \sqrt{P_S} h_D x + \sqrt{P_R} g_{D,i} x + n_D, \tag{6.11}$$

$$y_E = \sqrt{P_S} h_E x + \sqrt{P_R} g_{E,i} x + n_E, \tag{6.12}$$

where n_D and n_E are the Gaussian noises of measured at the destination receiver and the eavesdropper receiver, respectively. For convenience, we assume $n_D \sim \mathcal{CN}(0,1)$, $n_E \sim \mathcal{CN}(0,1)$. The channel SNR of the main channel (source and relay to the destination) and the eavesdropper channel (source and relay to the eavesdropper) are given by

$$\gamma_{D,i}^{DF} = P_S |h_D|^2 + P_{R,i} |g_{D,i}|^2, \tag{6.13}$$

$$\gamma_{E,i}^{DF} = P_S |h_E|^2 + P_{R,i} |g_{E,I}|^2. \tag{6.14}$$

The maximum transmission power at each fading realization is P_T, the transmission power P_S and P_R satisfies $P_S + P_R \leq P_T$.

Since in the DF scheme, the relay R_i has to successfully decode the message received from the source S before forwarding the re-encoded message to the destination, thus, the amount of information transmitted by the relay is less or equal to the amount of information received at the relay R_i, which is written as

$$\log_2(1 + |h_{R,i}|^2 P_S) > \log_2(1 + |h_{R,i}|^2 P_{R,i}), \tag{6.15}$$

thus we have the relationship between P_S and $P_{R,i}$

$$|h_{R,i}|^2 P_S > |g_{D,i}|^2 P_{R,i} \tag{6.16}$$

The maximum information rate in the source to relay channel and relay to destination channel is affected by P_S and P_R and computed by the mutual information of the corresponding channels. If the mutual information of the source to destination channel $I(\gamma_{SR})$ is smaller than the mutual information of the relay to destination channel $I(\gamma_{RD})$, the value of $I(\gamma_{RD})$ is equal to $I(\gamma_{SR})$ no matter how good the channel quality is. To this end, we have the following relationships:

$$C_{RD} = min\{I\gamma_{SR}, I(\gamma_{RD})\}, \tag{6.17}$$

$$C_{RE} = min\{I\gamma_{SR}, I(\gamma_{RE})\}, \tag{6.18}$$

where C_{RD} and C_{RE} denote the maximum information rate in the relay to destination channel and the maximum information rate in the relay to eavesdropper channel, respectively. When both C_{RD} and C_{RE} equal to $I(\gamma_{SR})$, the relay provides zero secrecy, which should be avoided.

6.5 Equal power allocation

One straightforward power allocation strategy in the relay network is to divide the total transmission power equally onto the transmitter and the chosen relay. In this thesis, the relay with maximum $I(\gamma_{SR})$ while satisfying $I(\gamma_{RD}) > I(\gamma_{RE})$ is chosen. Assume the source and the relays have perfect knowledge of global CSI. The P_S and P_R are given by

$$P_S = P_R = \frac{P_T}{2}. \tag{6.19}$$

The maximum information rate transmitted by the source while the relay can decode without error is defined by $\log_2(1 + |h_{R,i}|^2 \frac{P}{2})$, which is the upper limit of the information rate in relay to destination channel. The SNR gap in dB between the destination and the eavesdropper is given by

$$\begin{aligned} \Delta\gamma_{dB} &= \gamma_{D,dB} - \gamma_{E,dB} \\ &= 10\log_{10}\frac{|h_{D,i}|^2 + |g_{D,i}|^2}{|h_{E,i}|^2 + |g_{E,i}|^2}. \end{aligned} \tag{6.20}$$

The SNR gap in dB remains constant when the transmission power varies during on transmission block. The secrecy rate is maximized by setting γ_{opt}, which is the SNR in dB that maximizes the transformed MMSE $\mathcal{M}(\gamma_{dB})$ introduced in chapter 4, at the center of $[\gamma_{E,dB}, \gamma_{D,dB}]$. The secrecy rate of the relay helped wiretap channel is approximated by

$$\begin{aligned} C_S &\approx \mathcal{M}(\gamma_{opt})(\gamma_{D,dB} - \gamma_{E,dB}) \\ &= \mathcal{M}(\gamma_{opt})(10\log_{10}\frac{|h_{D,i}|^2 + |g_{D,i}|^2}{|h_{E,i}|^2 + |g_{E,i}|^2}). \end{aligned} \tag{6.21}$$

The maximum secrecy rate is achieved by setting P_T as

$$\frac{\gamma_{E,dB} + \gamma_{D,dB}}{2} = \gamma_{opt} \tag{6.22}$$

the optimal P_T is given by

$$P_T = \sqrt{2\frac{10^{0.1\gamma_{opt}}}{(|h_{D,i}|^2 + |g_{D,i}|^2)(|h_{E,i}|^2 + |g_{E,i}|^2)}}. \tag{6.23}$$

The optimal transmission power is easy to compute in an equal power allocation strategy. However, the positive secrecy rate can only be obtained if and only if

$$|h_{D,i}|^2 + |g_{D,i}|^2 > |h_{E,i}|^2 + |g_{E,i}|^2, \tag{6.24}$$

where we assume $h_{D,i} < h_{E,i}$, therefore, $g_{D,i}$ has to be far larger than $g_{E,i}$. In the next section, we investigate an alternative fast power allocation policy that maximises the secrecy rate.

6.6 Suboptimal power allocation strategy for DF wiretap channel

The closed-form optimal power allocation policy to maximize secrecy rate is unknown. However, similar to the PCP introduced in Chapter 4, a suboptimal power allocation policy for DF wiretap channel can be obtained in closed-form. The trans-

mission power of the source P_S and P_R satisfies the following conditions

$$P_S + P_{R,i} \leq P_T, \tag{6.25}$$

$$|h_{R,i}|^2 P_S > |g_{D,i}|^2 P_{R,i}. \tag{6.26}$$

In the case of Gaussian input, the secrecy rate is given by

$$C_S^G = \log_2(\frac{1 + P_S|h_D|^2 + P_R|g_{D,i}|^2}{1 + P_S|h_E|^2 + P_R|g_{E,i}|^2}). \tag{6.27}$$

Hereby, we prove that the optimal transmission strategy of Gaussian input wiretap channel is to let $P_S + P_R = P_T$.

Initially we assume that $\frac{|h_D|^2}{|g_{D,i}|^2} = a$, $\frac{|h_E|^2}{|g_{E,i}|^2} = b$ and $a \geq b$. The secrecy rate is given by

$$\begin{aligned} C_S^G &= \bar{\mathcal{M}}(\gamma_{D,dB} - \gamma_{E,dB}) \\ &= 10\bar{\mathcal{M}} \log_{10}(\frac{P_S|h_D|^2 + P_R|g_{D,i}|^2}{P_S|h_E|^2 + P_R|g_{E,i}|^2}) \\ &= 10\bar{\mathcal{M}} \log_{10}(\frac{a|h_E|^2 P_S + b|g_{E,i}|^2 P_R}{P_S|h_E|^2 + P_R|g_{E,i}|^2}) \\ &\leq 3.3 \log_{10}(\frac{a|h_E|^2 P_T}{|h_E|^2 P_T}) \\ &= 10\bar{\mathcal{M}} \log_{10}(a). \end{aligned} \tag{6.28}$$

where $\bar{\mathcal{M}}$ value is increased as the SNR raises and achieves the maximum value at $SNR \to \infty$.

Otherwise, if $a < b$, $P_{R,i}$ needs to be maximized, the optimal $P_{R,i}$ value satisfies

$$P_S + P_{R,i} = P_T, \tag{6.29}$$

$$|h_{R,i}|^2 P_S = |g_{D,i}|^2 P_{R,i}. \tag{6.30}$$

In summary, in the Gaussian input case, the optimal power allocation policy requires the system to allocates all available power for transmission.

However, in the finite-alphabet input case, $\bar{\mathcal{M}}$ achieves maximum value at medium SNR range and $\bar{\mathcal{M}}$ is 0 at high SNR range, which implies that the increment of transmission power may result in a decrement of secrecy rate. Thus, the transmission

power constraint of finite-alphabet input case is given by

$$P_S + P_{R,i} \leq P_T, \tag{6.31}$$

$$|h_{R,i}|^2 P_S \geq |g_{D,i}|^2 P_{R,i}. \tag{6.32}$$

In order to maximize the secrecy rate, the optimal relay and the transmission power $P_S, P_{R,i}$ is selected based on the following rules

$$\max_{P_S, P_{R,i}} C_S \tag{6.33}$$

s.t.

$$P_S + P_{R,i} \leq P_T$$

$$|h_{R,i}|^2 P_S > |g_{D,i}|^2 P_{R,i},$$

Depending on the CSI of the channels, the power allocation policy for BICM to maximize the secrecy rate is also considered in two cases: $a \geq b$ or $a < b$. In the following sections, the terms source links and relay links specify the channels between source to destination/eavesdropper and the channels between relay to destination/eavesdropper.

6.6.1 The source links have a larger SNR gap than the relay links

In this case, the use of relay will inevitably decrease the throughput as the relay links can not achieve higher secrecy rate than the source links providing the same transmission power. The optimal transmission strategy is to abandon the two time slots algorithm but use normal direct link transmission scheme, in fact, the optimal PA is presented in 4.23. We will focus in the other case that the relay links have larger SNR gap than the source links as it has potential to enhance the secrecy rate performance by allocating transmission power onto the relay. As it is mentioned in the previous chapter that the total power can be more than the required transmission power to achieve maximum secrecy performance, the additional power can be used for energy harvesting.

6.6.2 The relay links have larger SNR gap than the source links

It is very common that a carefully chosen relay provides larger SNR gap than the source links. In this case, where $\frac{|h_D|^2}{|h_E|^2} < \frac{|g_{D,i}|^2}{|g_{E,i}|^2}$, the SNR gap is increased when $\frac{P_S}{P_R}$ decreases. However, the decreased P_S value means that a smaller information rate that relay can successfully decoded by the relay. The minimum P_S is given by taking equality for $P_S|h_{R,i}|^2 \geq P_R|g_{D,i}|^2$, in this case, the SNR gap is maximized, which is given by

$$\begin{aligned}\max \Delta\gamma = & \ 10\log_{10} P_R(|h_D|^2\frac{|g_{D,i}|^2}{|h_{R,i}|^2} + |g_{D,i}|^2) - 10\log_{10} P_R(|h_E|^2\frac{|g_{D,i}|^2}{|h_{R,i}|^2} + |g_{E,i}|^2) \\ = & \ 10\log_{10}(|h_D|^2\frac{|g_{D,i}|^2}{|h_{R,i}|^2} + |g_{D,i}|^2) - 10\log_{10}(|h_E|^2\frac{|g_{D,i}|^2}{|h_{R,i}|^2} + |g_{E,i}|^2). \quad (6.34)\end{aligned}$$

Assume the optimal solution for transmission powers to maximize secrecy rate are given by $\hat{P}_S$ and $\hat{P}_R$. We start the analysis by considering two cases: the first case is $P_T \geq \hat{P}_T$, the other case is $P_T < \hat{P}_T$, where $\hat{P}_T = \hat{P}_S + \hat{P}_R$.

The $\hat{P}_S$ and $\hat{P}_R$ obtained by solving

$$\begin{aligned}&\frac{\gamma_{D,dB} + \gamma_{E,dB}}{2} = \gamma_{opt}, \quad (6.35)\\ &\text{s.t.}\\ &\hat{P}_S|h_{R,i}|^2 \geq \hat{P}_R|g_{D,i}|^2,\\ &\hat{P}_T = \hat{P}_S + \hat{P}_R,\end{aligned}$$

the $\hat{P}_T$ is given by

$$\hat{P}_T = 10^{0.1\gamma_{opt}}\sqrt{\frac{|g_{D,i}|^2 + |h_{R,i}|^2}{(|h_D|^2|g_{D,i}|^2 + |h_{R,i}|^2|g_{D,i}|^2)(|h_E|^2|g_{D,i}|^2 + |h_{R,i}|^2|g_{E,i}|^2)}}. \quad (6.36)$$

If $\hat{P}_T < P_T$, which indicates that both values of $\bar{\mathcal{M}}$ and $\Delta\gamma$ can be maximized, the optimal P_S and P_R values are given by

$$P_S = \frac{|g_{D,i}|^2}{|g_{D,i}|^2 + |h_{R,i}|^2}\hat{P}_T, \quad (6.37)$$

$$P_S = \frac{|h_{R,i}|^2}{|g_{D,i}|^2 + |h_{R,i}|^2}\hat{P}_T. \quad (6.38)$$

The secrecy rate achieved in this case is the global maximum value.

In the other case, the total transmission power P_T is not enough for the source and relay to cooperate to achieve the global maximum of secrecy rate, following similar steps in the section 6.6.1, the adaptive searching method is used to find the optimal solution for P_S and P_R.

Firstly, we start by computing the maximum value of $\frac{\gamma_{D,dB}+\gamma_{E,dB}}{2}$, which is given by

$$\max \frac{\gamma_{D,dB}+\gamma_{E,dB}}{2} \tag{6.39}$$

s.t.

$$P_S + P_R = P_T,$$
$$|h_{R,i}|^2 P_S \geq |g_{D,i}|^2 P_R.$$

If the maximum value of $\frac{\gamma_{D,dB}+\gamma_{E,dB}}{2} < \gamma_{opt}$, the optimal transmission power is given by

$$P_S = \frac{|g_{D,i}|^2}{|g_{D,i}|^2 + |h_{R,i}|^2} P_T, \tag{6.40}$$
$$P_R = \frac{|h_{R,i}|^2}{|g_{D,i}|^2 + |h_{R,i}|^2} P_T. \tag{6.41}$$

The secrecy rate achieved in this case is denoted as $C_S = \bar{\mathcal{M}} \max_{P_R,P_S} \Delta\gamma$.

If the maximum value of $\frac{\gamma_{D,dB}+\gamma_{E,dB}}{2} > \gamma_{opt}$, according to

$$\max_{\hat{P}_S,\hat{P}_R} \{\bar{\mathcal{M}}\Delta\gamma_{dB}\} \geq \max\{\bar{\mathcal{M}}\}\Delta\gamma, \tag{6.42}$$
$$\max_{\hat{P}_S,\hat{P}_R} \{\bar{\mathcal{M}}\Delta\gamma_{dB}\} \geq \bar{\mathcal{M}} \max\{\Delta\gamma\}. \tag{6.43}$$

we find the P_S and P_R values that maximizes $\bar{\mathcal{M}}$, according to the following constraints:

$$\frac{\gamma_{D,dB}+\gamma_{E,dB}}{2} - \gamma_{opt} = 0, \tag{6.44}$$
$$P_S + P_R = P_T, \tag{6.45}$$
$$|h_{R,i}|^2 P_S \geq |g_{D,i}|^2 P_R. \tag{6.46}$$

If there is at least one positive real root, the P_R value is given by the minimum

positive real root of the equation array and it is the minimum value to achieve area maximum secrecy rate, we denote it by $\dot{P}_R$.

The optimal (P_S, P_R) pair is obtained by using the adaptive searching algorithm presented in Table **??** but setting $P_{R,min} = \dot{P}_R$ and $P_{R,max} = \frac{|h_{R,i}|^2}{|g_{D,i}|^2+|h_{R,i}|^2} P_T$.

In the case that there is no real root for P_R, which means γ_{opt} is not achievable for any pair of (P_S, P_R), the $P_{R,min}$ is obtained by

$$\max_{P_S,P_R} \frac{\gamma_{D,dB}+\gamma_{E,dB}}{2}, \tag{6.47}$$

s.t

$$P_S + P_R = P_T,$$

$$|h_{R,i}|^2 P_S \geq |g_{D,i}|^2 P_R. \tag{6.48}$$

The optimal (P_S, P_R) pair is obtained by adaptive searching algorithm using the same steps as the previous case.

6.7 Numerical results

In this section, the simulation results of secrecy rate of BICM schemes with DF relay are presented. The direct links between the source to the destination/eavesdropper are not ignorable. Firstly, we compare the secrecy rate performances with using DF relays and direct transmission technique.

In Fig.6.2, the secrecy rate performances of the no direct link case are compared. In terms of secrecy rate performance, the proposed PA algorithm greatly outperforms the equal PA algorithm. It also indicates that the maximum secrecy rate is determined by the SNR gap between relay to the destination and relay to the eavesdropper, while a larger value of source to relay SNR improves the secrecy rate performance when the total transmission power is low. The (2,1,2) and (2,1,6) curves imply that the secrecy rate performance is only affected by the SNR difference between relay to destination channel and relay to eavesdropper channel.

In Fig.6.3, It is shown that when $P_T < 0.1$dB, the secrecy rate performances of the proposed PA and equal gain PA are similar. However, as the P_T value increases, the proposed PA outperforms equal gain PA for all channel condition cases. To demonstrate the poor source links case, the average channel gain of the source to destination is chosen lower than the average channel gain of source to

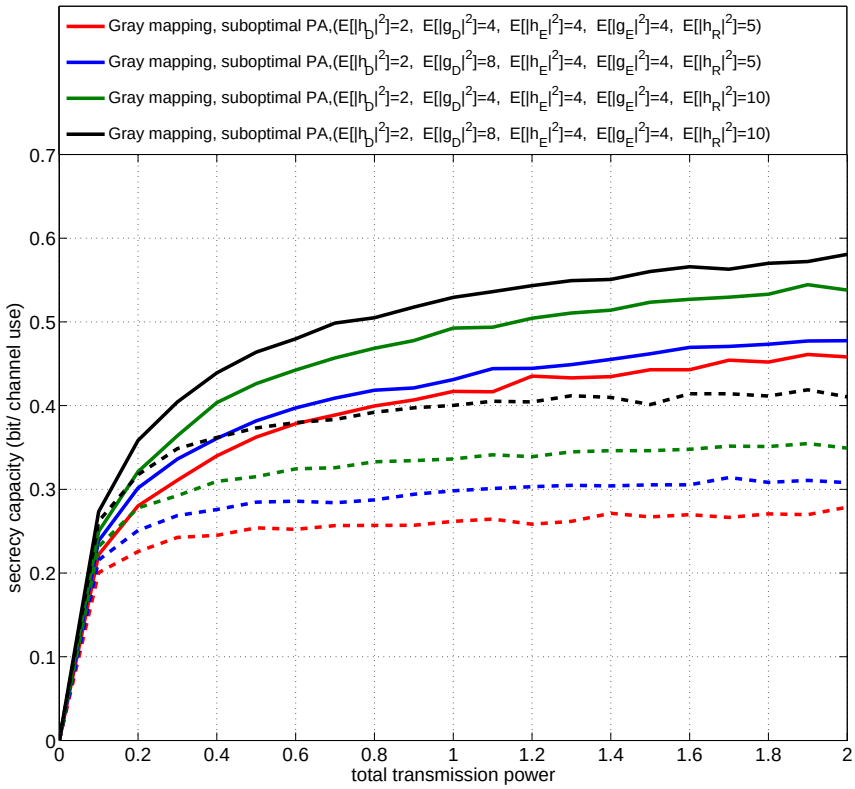

Figure 6.3: The secrecy rate performances comparison between the wiretap channel employing equal PA and the proposed PA, the average channel gains are listed on the legends. The number of relays is 1, the BICM scheme employs Gray mapping. The full lines indicates the secrecy rate performances of various channel gain cases with suboptimal PA algorithm, while the dotted lines are the secrecy rate performances of corresponding cases with equal PA algorithm.

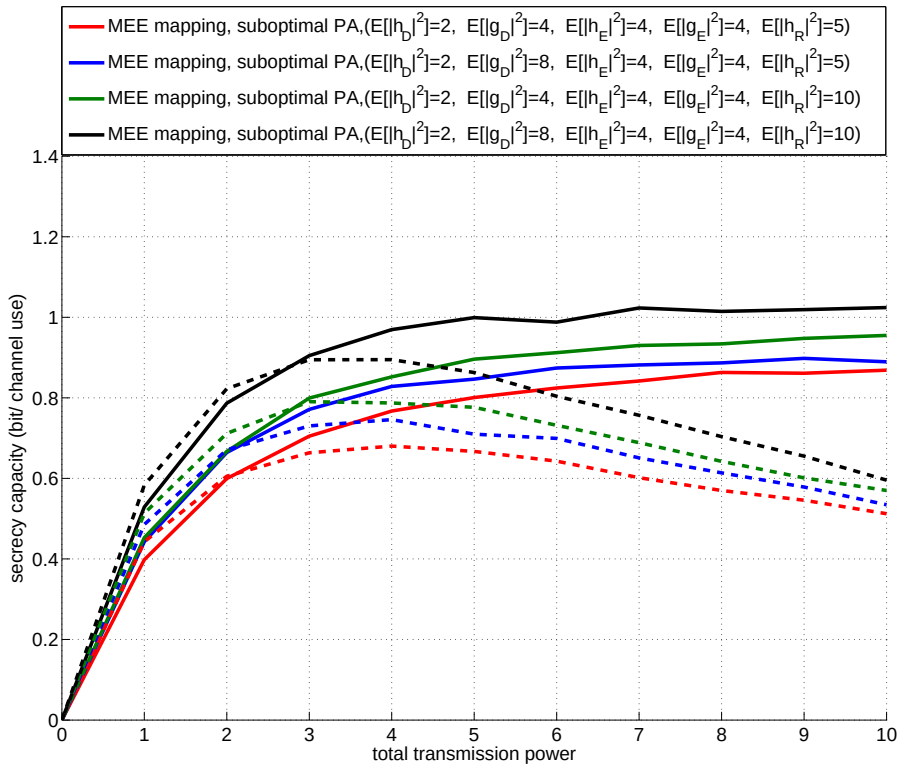

Figure 6.4: The secrecy rate performances comparison between the wiretap channel employing equal PA and the proposed PA, the average channel gains are listed on the legends. The number of relays is 1, the BICM scheme employs MEE mapping. The full lines indicates the secrecy rate performances of various channel gain cases with suboptimal PA algorithm, while the dotted lines are the secrecy rate performances of corresponding cases with equal PA algorithm.

eavesdropper. For the relay to destination/eavesdropper channels, we assume that the relay is well positioned and the average SNR of the relay to destination channel is higher than the relay to eavesdropper channel. The simulation results show that the secrecy rate is increased as the $E[10\log_{10}|g_D|^2] - E[10\log_{10}|g_E|^2]$ value raises. As it has been demonstrated that the source to relay mutual information determines the maximum value of the relay to destination mutual information, we compare the secrecy rate with $E[|h_R|^2] = 5$ and $E[|h_R|^2] = 10$. The simulation results show that significant improvements on the secrecy rate performances are achieved by increasing the $E[|h_R|^2]$ value.

In Fig.6.4, we investigate the secrecy rate of MEE mapping. The proposed PA obtains much higher secrecy rate values than the equal PA algorithm when P_T is large. However, when P_T is small, equal gain PA performs slightly better than proposed PA, this is because the closed-form approximation of the secrecy rate of MEE mapping is only accurate around $SNR = \gamma_{opt}$, thus, the secrecy rate performance obtained by proposed PA algorithm at low SNR is not optimal for MEE mapping. Comparing with the Gray mapping case, for the same amount of maximum input power constraint P_T, the MEE mappping achieves significantly higher secrecy rate values, which has also been demonstrated in the SISO wiretap channel case. In order to show the secrecy rate performance at high SNR, the secrecy rate performances with input power constraint from 0dB to 10dB are simulated. It is shown that with equal PA, the secrecy rate decreases after P_T increases higher than 3dB, while the secrecy rate performances with the proposed PA remain at maximum values. Despite the poor performance at the small P_T value range, the proposed PA algorithm maximizes the secrecy rate over a wide range of P_T values.

6.8 Conclusion

In this chapter, the secrecy rate of wiretap channels with a helper relay employing DF strategy is studied. We show that optimal power allocation strategy can be written in closed-form in most cases, while others need to use the adaptive searching method due to the complexity of mathematical expression. By using the closed-form approximation of the secrecy rate of BICM schemes, the computational cost is considerably low. The secrecy rate performances of the proposed PA algorithm are compared with the equal PA algorithm, it is shown that the secrecy rate of proposed PA algorithm greatly out performed equal PA algorithm, especially when there is a large amount of total available transmission power. We also show that optimal secrecy rate and low energy cost can be simultaneously achieved as BICM schemes obtains optimal secrecy rate performance at a certain finite value of total input power, with the value depending on the channel conditions and the mapping technique applied.

Chapter 7

Conclusions and future work

7.1 Conclusion

In this thesis, the secrecy capacity exhibiting additive Gaussian noise with finite-alphabet input schemes is studied. Firstly, a closed-form solution to the secrecy capacity of is obtained by introducing logarithm transformations to the MMSE, the simulation matches up to real system performances very well when the SNR gap is small. Secondly, we introduce a fast, closed-form PCP algorithm to optimize the secrecy capacity on medium to high SNRs, different to the Gaussian input case, we show that the optimal secrecy capacity performance is achieved at a finite value of input transmission power, by using the proposed PCP, secrecy capacity at high SNR maintains high performance. Additionally, an EH algorithm is introduced with the purpose of saving energy while achieving the target secrecy rate. Thirdly, the mapping effects on secrecy capacity are investigated, a new mapping algorithm is proposed as the optimal mapping rule under secrecy constraint, the generated mapping, namely MEE mapping, achieves the highest secrecy rate among all mappings. The distance spectrum is the critical parameter in the MEE mapping searching steps. The secrecy capacity performance of MEE mapping is compared with Gray, SP, MSEW and M16^r mappings on 16QAM, 8PSK and (1,5,10) constellations under various channel conditions. We show that Gray mapping has the lowest secrecy capacity at high SNR, while MEE mapping achieves maximum secrecy capacity with an additional cost of transmission power. Finally, the secrecy capacity of a DF relay helped wiretap channel is studied, the optimal PA algorithm is introduced in various cases, the simulation on secrecy capacity performance shows that the proposed PA

algorithm greatly outperforms equal PA algorithm, especially at high SNR range.

7.2 Future research

As it is shown repeatedly in this thesis, the secrecy capacity performance of finite-alphabet input is very different to the Gaussian input secrecy capacity. It is interesting and greatly important to extend the research in this thesis for the purpose of practical application.

In this work, we have shown that BICM has the potential to achieve higher secrecy capacity than Gaussian input by using MEE mapping if the SNR gap is small. It has been proved that signal shaping on BICM can optimize the mutual information performance, thus, secrecy capacity performance can also be optimized by using signal shaping techniques. It is fascinating to study the effects of signal shaping on secrecy capacity to further improve the secrecy capacity performance.

The Amplify-and-forward (AF) algorithm is a widely used relay strategy for cooperative communication, different to the DF algorithm, the relay in AF algorithm does not decode the source message but amplify the received signal and forward to the destination. It is clearly that the noise of the source link has been amplified through this process, however, as the secrecy communication aims to maximize the difference of mutual information between channels, the amplification of the noise in AF has the potential advantage to achieve high secrecy performance as this process can be regards as adding artificial noise to both receivers. Future work will be focusing on the optimal PA algorithm for AF scheme under secrecy constraint.

The multiple antenna technique is widely applied in modern communication. In this thesis, SISO and MISO wiretap channel models are studied and the optimal PA algorithm is presented. However, the optimal beamforming algorithm for BICM remains unstudied and considered the complexity of the transceiver design, designing a computational cost saving, secrecy capacity maximization beamforming algorithm is necessary. The successful design of MIMO wiretap channel beamforming can greatly enhance the secrecy capacity performance and reduce the probability that the main channel is more noisy than the wiretap channel. Future work will be focusing on the secrecy capacity maximization and total transmission power minimization over the MIMO wiretap channel model.

Throughout this thesis, perfect CSI knowledge of the wiretap channel is assumed

at the transmitter. However, it is common that the eavesdropper is passive and the transmitter is unable to obtain accurate wiretap CSI. Due to the imperfect CE of the wiretap channel, the strict secrecy capacity is unobtainable. Instead, it is common to measure the outage probability (OP) of the wiretap channel. The OP measures the probability of the information rate that is higher than the secrecy capacity. Since the closed-form approximation of the BICM capacity has been obtained, future work is recommended to study the outage probability under the assumption of imperfect wiretap CSI.

Although it can be established in theory that the confidential message can be perfectly secured provided the information rate is smaller than the secrecy capacity, the capacity approaching code is essential to achieve the secure throughput. As it has been demonstrated in the previous chapters that the finite-alphabet input schemes achieve the maximum secrecy capacity "around" SNR=γ_{opt}dB, it is intriguing to investigate the code design algorithm and generate the code with a "waterfall" BER performance at SNR=γ_{opt}dB for the power adaptive, constant code rate system. The future work will focus on designing capacity approaching code (LDPC code, Turbo code) to maximize the secure throughput for finite-alphabet input.

References

[1] C. E. Shannon, "communication theory in secrecy systems ," *The Bell System Technical Journal*, vol. 27, pp. 350-355 and 623-656, Mar. 1948.

[2] ——, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 28, pp. 656-715, Mar. 1949.

[3] A. Wyner, "The Wire-tap channel," *Bell System Technical Journal*, vol. 54, no.8, pp.1355-1387, 1975.

[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339348, May. 1978.

[5] S. Lueng Yan Cheong and M. E.Hellman,"The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, no. 4, vol. IT-24, PP. 451-456, Jul. 1978.

[6] P. K. Gopala, L. Lai and H. E. Gamal,"On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, no. 10, vol. 54, PP. 4687-4698, Oct. 2008.

[7] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels", in *Proc. IEEE Int. Symp. Information Theory,* Adelaide, Australia, pp. 2152-2155 Jul. 2006.

[8] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels", in *Proc. IEEE Int. Symp. Information Theory,* Seattle, WA, Jul. pp. 356-360, 2006.

[9] M. Bloch, J. Barros, M. R. D. Rodrigues and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, no. 6, vol. 54, PP. 2515 - 2534, Jun. 2008.

[10] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, no. 6, vol. 54, PP. 2470-2492, Jun. 2008.

[11] Y. Liang AND H. V. Poor, "Secure communication over fading channels", IN *Proc. Allerton conf. Communication, control and Computing*, Monticello, IL, Sep. 2006.

[12] Z. Li, R. Yates and W. Trappe, "Secure communication over wireless channels", in *Proc. Information Theory and Application Workshop*, La Jolla, CA, Jan. 2007.

[13] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, no. 8, vol. 57, PP. 4961-4972, Aug. 2011.

[14] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," *ISIT2007, Nice, France*, Jun., 2007.

[15] H. Joen, N. Kim, J. Choi, H. Lee and J. Ha, "Bounds on Secrecy Capacity Over Correlated Ergodic Fading Channels at High SNR", *IEEE Trans. Inf. Theory*, no. 4, vol. 57, pp.1975-1983 , Apr., 2011.

[16] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: the misome wiretap channel," *IEEE Trans. Inf. Theory*, no. 7, vol. 56, PP. 3088-3104, Jul. 2010.

[17] ——, "Secure transmission with multiple antennas II: the mimome wiretap channel," *IEEE Trans. Inf. Theory*, no. 11, vol. 56, PP. 5515-5532, Nov. 2010.

[18] A. Khisti, G. W. Wornell and Y. Eldar, "On the gaussian mimo wiretap channel," *presented at the Proc. IEEE Int. Symp. Information Theory*, Nice, France, 2007.

[19] M. Z. I. Sarkar and T. Ratnarajah, "Bounds on the secrecy capacity with diversity combining techniques," *IWCNC2012: Mobile and Wireless Networks.*

[20] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4005-4019, Sep. 2008.

[21] Z. Han, N. Marina and A. Hjøungnes, "Physical layer security game: Interaction between source, eavesdropper and friendly jammer," *Speical issue on physical-layer security*, Jun., 2009.

[22] O. Simeone and P. Popovski, "Secure communications via cooperating base stations,." *IEEE Commun. Lett.*, no. 3, vol. 12, pp. 188-190, Mar., 2008.

[23] P. Popovski and O. Simeone, "Wireless secrecy in cellular systems with infrastructure-aided cooperation,." *IEEE Trans. Inf. Forensics Security*, no. 2, vol. 4, pp. 242-256, Jun., 2009.

[24] Z. Ding, K. K. Leung, D. L. Goeckel and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE J. Sel. Areas Commun.*, no. 2, vol. 30, pp. 359-368, Feb., 2012.

[25] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, no. 10, vol. 59, pp. 4871-4884, Oct., 2011.

[26] E. Tekin and A. Yener, "The General Gaussian Multiple-Access and Two-Way Wiretap Channels: Achievable Rates and Cooperative Jamming" , *IEEE Trans. Inf. Theory*, no. 6, vol. 54, pp. 2735-2751, Jun., 2008.

[27] D. Fang, N. Yang, M. Elkashlan, P. L. Yeoh and J. Yuan, "Cooperative jamming protocals in two hop amplify-and-forward wiretap channels," *IEEE ICC 2013, Communication and Information Systems Security Symposium*

[28] L. Dong, Z. Han, Athina P. Petropulu and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, no. 3, vol. 58, pp. 1975-1888, Mar., 2010.

[29] X. He and A. Yener, "On the equivocation region of relay channels with orthogonal components," *in Proc. 41st Asilomar Conf. Signals, Syst. Comput.*,Monterey, CA, Nov. 2007.

[30] Y. Oohama, "Relay channels with confidential messages," *IEEE Trans. Inf. Theory*, 2007, [Online]. Available: http://arxiv.org/abs/cs.IT/0611125.

[31] M. Yuksel and E. Erkip, "Secure communication with a relay helping the wiretapper," *in Proc. 2007 IEEE Information Theory Workshop*, Lake Tahoe, CA, Sep. 2007.

[32] H. M. Wang, F. Liu and X. G. Xia, "Joint source- relay precoding and power allocation for secure amplify-and-forward MIMO relay networks," *IEEE Trans. Inf. Forensics Security*, no. 8, vol. 9, pp. 1240-1250, Aug., 2014.

[33] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, no. 10, vol. 59, pp. 4985-4997, Oct., 2011.

[34] J. A. Thomas and T. M. Cover, *Elements of information theory.* John Wiley and Sons, Inc, 1991.

[35] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Trans. Inform. Theory*, no. 28, vol. 1, pp. 55-67, Jan., 1982.

[36] D. Divsalar and M. Simon, "Trellis coded modulation for 4800-9600 bits/s transmission over a fading mobile satellite channel," *IEEE Commun. Mag.*, no. 27, vol. 12, pp. 11-19, July, 1989.

[37] M. Simon and D. Divsalar, "The performance of trellis coded multilevel dpsk on a fading mobile satellite channel," *IEEE J. Select. Areas Commun.*, vol. SAC-5, pp. 162-175, Feb, 1989.

[38] ——, "The design of trellis coded modulation for mpsk for fading channels : Set partitioning for optimum code design," *IEEE Trans. Commun.*, vol. 36, pp. 1013-1021, Sep., 1988.

[39] M. K. Simon and D. Divsalar, "The design of trellis coded modulation for mpsk for fading channels: Performance criteria," *IEEE Trans. Veh. Technol.*, no. 2, vol. 37, pp. 78-91, May, 1988.

[40] T. M. Cover and A. E. Gamal, "Capacity theorem for the relay channels," *IEEE Trans. Inform. Theory*, no. 5, vol. 25, pp. 572-584, Sep., 1979.

[41] E. Zehavi, "8-psk trellis codes for a rayleigh fading channel," *IEEE Trans. Commun.*, vol. 40, pp. 873-884, May, 1992.

[42] G. Caire, G. Taricoo and E. Biglieri, "Bit-interleaved coded modulation," *IEEE Trans. Inform. Theory*, no. 3, vol. 44, pp. 927-946, May, 1998.

[43] E. Agrell, J. Lassing, E. G. Ström and T. Ottosson,"On the optimality of Binary reflected Gray code", *IEEE Trans. Inform. Theory*, no. 12, vol. 50, pp. 3170-3182, Dec., 2004.

[44] E. Agrell and A. Alvarado,"Optimal alphabets and binary labelings for BICM at low SNR,"*IEEE Trans. Inf. Theory*, no. 10, vol. 57, pp. 6650-6672, Oct. 2011.

[45] J. Tan and G. L. Stüber, "Analysis and Design of Symbol Mappers for Iteratively Decoded BICM", *IEEE Trans. Wireless Commun.*, no. 2, vol. 4, pp. 662-672, Mar. 2005.

[46] C. Stierstorfer and R. F. H. Fisher, "Mappings for bicm in uwb scnarios,"*International ITG conference on SCC*, pp. 1-6, Jan., 2008.

[47] A. Chindapol and J. A. Ritcey, "Design, analysis and performance evaluation for BICM-ID with square QAM constellation in Rayleigh fading channels," *IEEE J. Sel. Areas Commun.*, no. 11, vol. 19, pp. 944-957, May, 2001.

[48] X. Li, A. Chindapol and J. A. Ritcey, "Bit-interleaved coded modulation with iterative decoding and 8PSK signaling, *IEEE Trans. Commun.* no. 8, vol. 50, pp. 1250-1257, Aug., 2002.

[49] F. Schereckenbach, N. Gortz, J. Hagenauer and G. Bauch, "Optimzed symbol mappings for bit-interleaved coded modulation with iterative decoding," *IEEE Globecom Conference, San Francisco*, pp. 3316-3320, Dec., 2003.

[50] S. Pfletschinger and F. Sanzi, "Error floor removal for bit-interleaved coded modulation with iterative detection," *IEEE Trans. Wireless Commun.*, no. 11, vol. 5, pp. 3174-3181, Nov, 2006.

[51] C. Berrou, A. Glavieux and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo codes", *ICC'93 Conf. Geneva*, pp.1064-1070, May, 1993.

[52] Le Goff S, Glavieux A, C.Berrou, "Turbo codes and high spectral efficiency modulation", *International Conference on Communications (ICC), New Orleans, Louisiana, USA*, 1994.

[53] S. Y. L. Goff, "Signaling constellation for power-efficient bit-interleaved coded modulation schemes," *IEEE Trans. Inf. Theory*, no. 1, vol. 49, pp. 307-313, Jan, 2003.

[54] T. Kailath,"A note on least squares estimates from likelihood ratios, *Inf. Contr.*, vol. 13, pp. 534540, 1968.

[55] T. Kailath, "A general likelihood-ratio formula for random signals in Gaussian noise, *IEEE Trans. Inf. Theory*, vol. IT-15, no. 2, pp. 350361, May 1969.

[56] T. Kailath, "A further note on a general likelihood formula for random signals in Gaussian noise, *IEEE Trans. Inf. Theory*, vol. IT-16, no. 4, pp. 393396, Jul. 1970.

[57] A. G. Jaffer and S. C. Gupta, "On relations between detection and estimation of discrete time processes, *Inf. Contr.*, vol. 20, pp. 4654, 1972.

[58] R. Esposito, "On a relation between detection and estimation in decision theory, *Inf. Contr.*, vol. 12, pp. 116120, 1968.

[59] C. P. Hatsell and L. W. Nolte, Some geometric properties of the likelihood ratio, *IEEE Trans. Inf. Theory*, vol. IT-17, no. 5, pp. 616618, Sep. 1971.

[60] R. R. Mazumdar and A. Bagchi, On the relation between filter maps and correction factors in likelihood ratios, *IEEE Trans. Inf. Theory*, vol. 41, no. 3, pp. 833836, May 1995

[61] S. Bashar and C. Xiao, "On secrecy rate analysis of MIMO wiretap channels driven by finite-alphabet input,"*IEEE Trans. Commun.* no. 12, vol. 60, pp. 3816-3825, Dec., 2012.

[62] Y. Wu, C. Xiao, Z. Ding, X. Gao and S. Jin, "Linear precoding for finite-alphabet signaling over MIMEMO wiretap channels,"*IEEE Trans. Veh. Technol.* no. 6, vol. 61, pp. 3816-3825, Jul., 2012.

[63] S. Vishwakarma and A. Chockalingam, "Decode-and-forward relay beamforming for secrecy with finite-alphabet input,."*IEEE Commun. Lett.*, no. 5, vol. 17, pp. 912-915, May, 2013.

[64] S. Verdú, "Spectral efficiency in the wideband regime," *IEEE Trans. Inform. Theory*, no. 6, vol. 48, pp. 13191343, Jan, 2002.

[65] A. Alvarado, F. Brännström and E. Agrell, "High SNR Bounds for the BICM Capacity", *2011 IEEE Information Theory Workshop*, pp. 360-364, Oct. 2011.

[66] A. Martinez, A. G. i Fàbregas, G. Caire and F. W. J. Willems, "Bit-Interleaved Coded Modulation in the Wideband Regime," *IEEE Inf. Theory*, no. 12, vol. 54, Dec. 2008.

[67] S. Y. Le Goff, "Signal constellations for bit-interleaved coded modulation", *IEEE Trans. Inf. Theory*, no. 1, vol. 40, pp. 307-313, Jan., 2003.

[68] D. Guo, S. Shamai, S. Verdú, "Mutual information and minimum mean-square error in Gaussian channels," *IEEE Trans. Inform. Theory*, no. 4, vol. 51, pp. 1261-1282, Apr., 2005.

[69] D. P. Palomar and S. Verdú, "Gradient of mutual information in linear vector Gaussian channels,." *IEEE Trans. Inform. Theory*, no. 1, vol. 52, pp. 141-154, Jan., 2006.

[70] A. Lozano, A. M. Tulino and S. Verdú, "Optimal power allocation for parallel Gaussian channels with arbitrary input distributions," *IEEE Trans. Inform. Theory*, no. 7, vol. 52, pp. 3033-3051, Jul., 2006.

[71] M. Abouelseoud and A. Nosratinia, "Opportunistic Wireless Relay Networks: Diversity-Multiplexing Tradeoff," *IEEE Trans. Inform. Theory*, no. 10, vol. 57, pp. 6514-6538, Oct., 2011.

[72] V. Prelov and S. Verdú, "Second-order asymptotics of mutual information," *IEEE Trans. Inform. Theory*, no. 8, vol. 50, pp. 15671580, Aug, 2004.

[73] F. D. Neeser and J. L. Massey, "Proper complex random processes with applications to information theory," *IEEE Trans. Inform. Theory*, no. 4, vol. 39, pp. 12931302, Jul., 1993.

[74] E. C. van der Meulen, "Three-terminal communication channels," *Advances in Applied Probability*, vol. 3, pp. 121, 1971.

[75] G. Zheng, J. Li, K. Wong, A. P. Petropulu and B. Ottersten, "Using simple relays to improve physical-layer security," *2012 1st IEEE International Conference on Communications in China* (ICCC), pp. 329 - 333, Aug. 2012.

[76] J. N. Laneman, D. N. C. Tse, and G. W. Wornell,"Cooperative diversity in wireless networks: Efficient protocols and outage behavior, *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062-3080, Dec. 2004.

[77] L. R. Varshney, "Transporting information and energy simultaneously," *In Proc.* 2008 IEEE Int. Symp. Inf. Theory.

[78] P. Grover and A. Sahai, "Shannon meets tesla: wireless information and power transfer,"*in Proc.* 2010 IEEE Int. Symp. Inf. Theory.

[79] A. J. Viterbi, J. K. Wolf, E. Zehavi and R.Padovani, "A pragmatic approach to trellis-coded modulation," *IEEE Commun. Mag.*, no. 7, vol. 27, pp. 11-19, July 1989.

[80] M. Abouelseoud and A. Nosratinia, "Opportunistic wireless relay networks: Diversity-multiplexing trade-off," *IEEE Trans. Inf. Theory*, no. 10, vol. 57, pp. 6514-6538, Oct. 2011.

[81] Z. Ding, K. K. Leung D. L. Goeckel and D. Towsley, "Opportunistic relaying for secrecy communications: Cooperative jamming vs relay chatting,"*IEEE Trans. Wireless Commun.*, no. 10 vol. 6, pp. 1725 - 1729, Jun. 2011.

[82] Y. Zou, X. Wang and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, no. 10 vol. 31, pp. 2099 - 2111, Oct. 2013.