SECRECY RATES OF FINITE-INPUT INTERSYMBOL INTERFERENCE CHANNELS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF ENGINEERING AND SCIENCE
OF BILKENT UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR
THE DEGREE OF
MASTER OF SCIENCE
IN
ELECTRICAL AND ELECTRONICS ENGINEERING

By
Serdar Hanoğlu
October 2016

Secrecy Rates of Finite-Input Intersymbol Interference Channels
By Serdar Hanoğlu
October 2016

We certify that we have read this thesis and that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Tolga Mete Duman (Advisor)

Sinan Gezici

Ali Özgür Yılmaz

Approved for the Graduate School of Engineering and Science:

Ezhan Karaşan
Director of the Graduate School

ABSTRACT

SECRECY RATES OF FINITE-INPUT INTERSYMBOL INTERFERENCE CHANNELS

Serdar Hanoğlu
M.S. in ELECTRICAL AND ELECTRONICS ENGINEERING
Advisor: Tolga Mete Duman
October 2016

Due to the broadcast nature of the communication medium, security is a critical problem in wireless networks. Securing the transmission at the physical layer is a promising alternative or complement to the conventional higher level techniques such as encryption. During the past decade, various studies have been carried out which investigate such possibilities in providing secrecy for different scenarios. On the other hand, secrecy over intersymbol interference (ISI) channels has not received significant attention, and much work remains to be done.

With this motivation, we focus on secrecy rates of finite-input ISI channels for both fixed and fading channel coefficients. We argue that the secrecy rates of ISI channels can be computed by the forward recursion of the BCJR algorithm. Moreover, by utilizing Markov input distributions for transmission over the ISI channels, achievable secrecy rates can be increased. However, the existing iterative method in the literature to obtain the optimal Markov input distribution is computationally complex as many BCJR recursions are needed. Thus, we propose an alternative solution by introducing a codebook based approach. Particularly, among the existing Markov input distributions in the codebook, we propose to select the one which spectrally matches the main channel. Our numerical results reveal that the proposed low complexity approach undergoes a minimal loss with respect to the existing iterative algorithm while offering a considerably reduced complexity.

We also propose injection of artificial noise (AN) to increase the secrecy rates, and show that this is especially useful for moderate and high signal to noise ratio (SNR) values where the use of Markov input distributions is not beneficial. We inject AN to frequencies where the eavesdropper's channel is better than the

main channel. We show that this approach significantly increases the secrecy rates compared to the existing methods. Furthermore, we consider the effect of channel state information (CSI) on the secrecy rates, and demonstrate that availability of eavesdropper's CSI at the transmitter is highly beneficial in terms of the achievable secrecy rates.

Keywords: Physical layer security, intersymbol-interference channels, artificial noise, fading, finite-alphabet inputs, finite state Markov channels, spectral shaping.

ÖZET

SONLU GİRDİ SETİNE SAHİP SİMGELER ARASI GİRİŞİM KANALLARINDAKİ GÜVENLİK SEVİYESİ

Serdar Hanoğlu
Elektrik ve Elektronik Mühendisliği, Yüksek Lisans
Tez Danışmanı: Tolga Mete Duman
Ekim 2016

Dışa açık doğaları gereği kablosuz iletişim ağlarında güvenliğin sağlanması kritik bir öneme sahiptir. Bu güvenliği fiziksel katmanda sağlamak ise üst katmandaki geleneksel şifreleme yöntemlerine hem iyi bir alternatif hem de ilave bir güvenliktir. Son on yıla baktığımızda, bir çok çalışma tarafından fiziksel katmandaki çalışmaların güvenliği sağlama noktasında yapabilecekleri farklı senaryolar için araştırılmıştır. Öte yandan, güvenliğin simgeler arası girişim (Intersymbol Interference - ISI) kanallarında sağlanması yeterince ilgi görmemiştir ve bu konuda araştırmaya açık bir çok yön bulunmaktadır.

Biz bu motivasyonla sonlu girdili ISI kanallarındaki güvenlik seviyesini hem sabit hem de sönümlemeli kanal katsayıları için inceliyoruz. ISI kanallardaki güvenlik seviyesinin BCJR algoritmasının ileri yönlü özyinelemeleri ile hesaplanabildiğini göstermekteyiz. Ayrıca, bu güvenlik seviyesi Markov girdiler yardımı ile artırılabilmektedir. Ancak, optimal Markov girdi değerini bulmak için önerilen literatürdeki mevcut algoritma, BCJR özyinelemesinin defalarca kullanılmasını gerektirdiği için işlemsel olarak yoğundur. Biz bu işlem yoğunluğunu azaltmak için kod defteri temelli bir yaklaşımı alternatif olarak sunuyoruz. Bu yaklaşımımızda, oluşturduğumuz kod defteri içerisindeki Markov girdilerden esas kanala spektral anlamda en uygun olanını seçiyoruz. Elde ettiğimiz nümerik sonuçlar göstermektedir ki önerilen yaklaşım düşük işlem kazancı sunmasının yanında mevcut yinelemeli çözüm ile kıyaslandığında performanstan çok kaybettirmemektedir.

Biz güvenlik seviyesini artırmak için yapay gürültü eklenmesini de önermekteyiz. Bu önerimiz Markov girdilerin fayda sağlamadığı orta ve yüksek sinyal gürültü oranı (Signal to Noise Ratio - SNR) değerlerinde büyük bir öneme

sahiptir. Yapay gürültü tekniği kapsamında gizli dinleyicinin esas kanaldan daha iyi olduğu frekans değerlerine gürültü ekliyoruz. Sonuçlarımız bu yaklaşımın güvenlik seviyesi üzerindeki artırıcı etkisini doğrulamaktadır. Ayrıca, vericideki mevcut kanal durum bilgisinin güvenlik seviyesi üzerindeki etkisini de incelemekte ve bu doğrultuda gizli dinleyicinin kanal durum bilgisinin verici tarafından bilinmesinin ne kadar faydalı olduğunu göstermekteyiz.

Anahtar sözcükler: Fiziksel katmanda güvenlik, simgeler arası girişim kanalları, yapay gürültü, sönümleme, sonlu girdi, sonlu durumlu Markov kanallar, spektral biçimlendirme.

Acknowledgement

First and foremost, I would like to express my sincere gratitude to my supervisor Prof. Dr. Tolga M. Duman for his invaluable guidance and encouragement throughout my M.Sc. study. His wide knowledge and his logical way of thinking have been of great value for me.

I would also like to thank Assoc. Prof. Dr. Sinan Gezici and Prof. Dr. A. Özgür Yılmaz as my examining committee members.

I would like to thank Sina Rezaei Aghdam who helped me in the every part of my work.

I would like to express my thanks to the The Scientific and Technological Research Council of Turkey (TÜBİTAK) for providing financial support during my M.Sc. study under the grant 113E223.

I would like to thank my office mates Kadir Ayhan, Mehdi Dabirnia, Umut Demirhan, Mücahit Gümüş, Mahdi Shakiba Herfeh, Nurullah Karakoç, Alireza Nooraiepour, Ersin Yar and Aras Yurtman.

I would also like to thank my wife, Ebru, and my parents for their invaluable support, motivation and understanding.

I thank all who in one way or another contributed to the completion of this thesis.

Contents

List of Figures

List of Tables

Abbreviations

AB	Alice to Bob
AE	Alice to Eve
AN	Artificial Noise
AWGN	Additive White Gaussian Noise
BPSK	Binary Phase Shift Keying
CSI	Channel State Information
i.i.d.	independent and identically distributed
i.u.d.	independent and uniformly distributed
ISI	Intersymbol Interference Channels
MIMO	Multiple Input Multiple Output
p.m.	performance metric
PSD	Power Spectral Density
QPSK	Quadrature Phase Shift Keying
SNR	Signal to Noise Ratio
w.r.t.	with respect to

Symbols

$\mathbb{Z}$	Set of integer numbers
$I(X;Y)$	Mutual information between the random variables X and Y
$h(X)$	Differential entropy of the random variable X
Pr	Probability
$p(.)$	Probability density function
C_s	Secrecy capacity
R_s	Achievable secrecy rate
$\|.\|$	Absolute value
$\|\|.\|\|$	Euclidean norm
X^n	A vector length n
$[.]^T$	Transpose
$[.]^+$	Maximization function $max\{0,.\}$
$\mathbf{E}[.]$	Expectation

Chapter 1

Introduction

Many communication schemes are vulnerable to undesired eavesdropping due to their open nature. In 1949, Shannon addressed this issue by defining the secrecy capacity as the maximum rate at which the transmission can occur while preventing any inference by the eavesdropper [1]. In traditional systems, security has been provided by cryptographic encryption and decryption techniques in the upper layers of the network [2]. However, there are difficulties in secret key distribution and management [3]. Moreover, cryptographic solutions may be infeasible and breakable by a computationally powerful eavesdropper [4]. These deficiencies motivate a provably unbreakable solution which can also be complemented with the conventional cryptographic methods for additional secrecy. This necessity was the point where physical layer security emerged. The basic principle in physical layer security is to exploit the inherent randomness of noise and communication channels to prevent possible eavesdropping.

In 1975, Wyner [5] proposed the wiretap channel model and studied physical layer security in that setup. Since then, many scenarios have been studied by making different assumptions on the system parameters such as channel type, antenna numbers, power constraints, etc., which brought about many aspects of physical layer security. In our work, we investigate the possibilities at the physical layer in providing secrecy for intersymbol interference (ISI) wiretap channels with

additive white Gaussian noise (AWGN) under a finite input alphabet constraint.

1.1 Literature Review

In his landmark paper [6], Shannon develops a mathematical theory of communication systems. The capacity of discrete-time Gaussian channels are also formulated, and it is shown that capacity achieving input distribution is Gaussian. However, Gaussian distribution is not realizable in real life applications. Thus, more realistic scenarios introduce finite input alphabet constraints, which can decrease the channel capacity significantly.

Above mentioned studies consider scenarios where the communicating sides consist of only legitimate users. In [1], Shannon introduces the concept of information theoretic security in the presence of an eavesdropper channel. Shannon called the communication over the main channel perfectly secure if the mutual information between the message and the eavesdropper's observation goes to zero, which requires use of a long shared secret key. In his seminal work [5], Wyner introduces the notion of weak secrecy, where the communication is secure if the the average mutual information between the message and the eavesdropper's observation goes to zero. In Wyner's degraded wiretap channel model, a sender (Alice) tries to communicate with a legitimate receiver (Bob) over a noisy channel, while an eavesdropper (Eve) overhears a degraded version of the signal received by Bob. He proved that the secrecy capacity of a degraded wiretap channel is the supremum of information rate difference between Bob and Eve optimized over the input probability distribution. Then, the results are extended to broadcast channels with confidential messages by Csiszar and Körner [7] where there is no degradedness assumption. Leung and Hellman [8] find the secrecy capacity of Gaussian wiretap channels. Finite input alphabet constraints for the wiretap channel set-up have been considered in [9] and [10]. In these studies, the secrecy capacity results are characterized for finite input alphabets, and it is shown that secrecy capacity significantly decreases as a result. Moreover, [11–13] study the finite input alphabet constraint with multiple antennas.

All the studies mentioned in the previous paragraphs focus on memoryless channels. However, some practical channels cannot be modeled as memoryless. Thus, it is inevitable to work on channels with memory, such as ISI channels. In [14], Hirt and Massey calculate the capacity of ISI channels with AWGN. They state that mutual information maximizing input distribution is Gaussian and its exact distribution is obtained by water-filling in the frequency domain. For ISI channels with inputs drawn from finite signal constellations, the information rates are estimated by Arnold and Loeliger [15] with the use of BCJR algorithm [16]. However, their solution does not maximize the information rate. In [17], Kavcic maximizes the information rate by adapting the Blahut-Arimoto algorithm [18,19] to their scenario. In addition to these estimation-based methods, for the finite input alphabet case, there are approaches that utilize spectral shaping of the inputs [20, 21].

To the best of our knowledge, the secrecy capacity of ISI wiretap channels with AWGN is not known. However, if the input alphabet is limited to a finite set, there exists a secrecy rate formula involving an auxiliary random variable [22]. If we further assume that main channel is less noisy than the eavesdropper's channel, this secrecy rate formula simplifies to a problem where auxiliary variable vanishes. In [22], the authors solve this simplified problem via an iterative optimization technique and obtain the secrecy rates for less-noisy ISI wiretap channels.

In addition to the fixed channel scenarios, there are some studies which consider fading channels. For memoryless AWGN wiretap channel scenarios, fading setups are first considered in [23] and [24]. In these papers, it is assumed that fading is quasi-static which requires outage based calculations. On the other hand, [25] investigates the secrecy capacity assuming ergodic fading channels. To the best of our knowledge, there is no study considering ISI wiretap channels with fading in the current literature.

1.2 Thesis Contributions

We first state the existing results in the literature and provide numerical examples. Then, we investigate several unsolved problems. The specific contributions of this thesis are as follows:

- There exists an iterative method [15, 17] to find the optimal Markov input distribution for the maximization of ISI channel capacity. There is also a low-complexity alternative based on spectral shaping methods [20, 21]. However, for this spectral shaping method, there are no detailed examples in the literature. We first demonstrate that its performance can compete with the existing iterative method by providing detailed numerical examples.

- In [22], the authors concentrate on secrecy rates of ISI wiretap channels with AWGN under a finite input alphabet constraint. They design an iterative algorithm to find the optimal Markov input distribution, however, they do not provide any numerical examples. We describe their algorithm and provide several numerical examples.

- The existing iterative method in the literature [22] to obtain the optimal Markov input distribution is computationally complex due to necessity of performing many BCJR recursions. Thus, we propose an alternative solution by introducing a codebook based approach. Specifically, among the existing Markov input distributions in the codebook, we propose to select the one which spectrally matches the main channel. Our numerical results reveal that this low complexity approach undergoes a minimal loss with respect to the iterative algorithm while offering a considerably reduced complexity.

- We propose injection of artificial noise (AN) to increase the secrecy rates, and show that this is especially useful for moderate and high SNR (signal to noise ratio) values where the use of Markov input distributions is not beneficial. We inject AN to frequencies where eavesdropper's channel is better

than the main channel. We show that the proposed approach significantly increases the secrecy rates when compared to existing methods.

- Considering the ISI channel scenarios, we demonstrate that availability of eavesdropper's channel state information (CSI) at the transmitter is highly beneficial in terms of achievable secrecy rates.

- We extent our studies to fading ISI channels by considering both quasi-static and ergodic fading channel formulations.

1.3 Thesis Outline

The thesis is organized in five chapters. In Chapter 2, we consider the secrecy capacity of memoryless AWGN wiretap channels. Firstly, capacity of a single channel is investigated. Then, by introducing the finite-alphabet input constraint, more practical scenarios are studied. Finally, numerical results on the secrecy capacity are provided by introducing an eavesdropper in the system model both with and without finite-alphabet input constraints.

Chapter 3 extends the capacity and secrecy capacity results of the previous chapter to channels with memory. For the capacity of ISI channels, scenarios with and without input alphabet constraints are considered by introducing Gaussian and Markov inputs. Then, secrecy capacity of ISI wiretap channels are investigated. After reproducing the existing results in the literature, a power spectral density (PSD) based approach is suggested to exploit channel state information at the transmitter. Current methods optimize the capacity of a single channel by using time-consuming simulation based calculation approach. However, by exploiting the PSD of the channels, the optimization can be performed much faster with the aid of a codebook based design. In addition to this approach, we introduce AN injection to ISI channels to increase the secrecy capacity. We compare the existing methods and our proposals by providing numerical examples. Moreover, performance comparisons with respect to the availability of CSI are also provided.

In Chapter 4, outage and ergodic secrecy rates are studied for wiretap channels with ISI both with quasi-static and block fading. We discuss how fixed channel formulations can be extended to the fading scenarios. Then, numerical examples are provided for various setups to compare the iterative input optimization method with the proposed PSD matching and AN injection approaches.

Finally, Chapter 5 concludes the thesis and presents several directions for future research.

Chapter 2

Secrecy Capacity of Memoryless AWGN Channels

In this chapter, our goal is to provide secrecy capacity formulations and results for memoryless AWGN channels. The chapter is organized as follows. In Section 2.1, we provide the standard capacity results for AWGN channels. In Section 2.2, we note the effects of constraining to inputs to a finite set. In Section 2.3, we consider secrecy capacity of Gaussian wiretap channels, while in Section 2.4, we extend our discussion to the secrecy capacity with finite input constraints. In Section 2.5, we provide a chapter summary.

2.1 Capacity Results of Memoryless AWGN Channels

For a channel coded communication system, as seen in Figure 2.1, the information source (that will be called Alice) produces a message, W, and the transmitter sends a proper signal through the channel. At the other end, receiver reconstructs the message for the destination (that will be called Bob) as $\hat{W}$. Here, $X(k)$ is the channel input and $Y(k)$ is the channel output at time instance k. We denote

probability density functions with $p(.)$ and probabilities with $Pr(.)$.

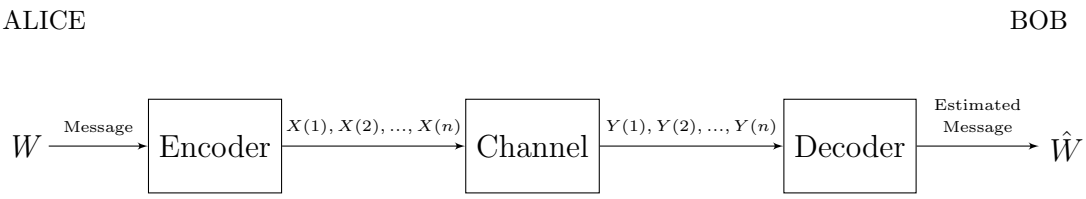

Figure 2.1: Block diagram for a channel coded communication system.

In this context, the fundamental problem is to produce the intended message of the information source at the destination side. However, there is a limit for the information rate that can be achieved with reliable communications. Shannon defined this limit as the channel capacity which is the highest rate in bits per channel use for which information can be sent with an arbitrarily low probability of error over a noisy channel. Mathematically, it can be written for discrete channels with memory (under certain technical assumptions) as [26]

$$C = \lim_{n\to\infty} \frac{1}{n} \max_{p(x^n)} I(X^n; Y^n) \tag{2.1}$$

where X^n is the channel input vector, Y^n is the channel output vector, and the maximization is carried out over all the possible input distributions $p(x^n)$. If the channel is memoryless, this boils down to

$$C = \max_{p(x)} I(X; Y). \tag{2.2}$$

The channel capacity is important to determine the information theoretical limits for reliable communication and to measure the performance of practical coding schemes. However, the solution of (2.1) is known only for certain channels. In this chapter, we only focus on AWGN channels which can be modeled as

$$Y = X + Z \tag{2.3}$$

where X is the complex channel input, Y is the complex channel output and Z is the circularly symmetric Gaussian noise with variance $N_0/2$ per dimension. Moreover, there is a power constraint on the input which requires that $E(X^2) \leq E_s$ where E_s is the energy per symbol. For this setup, the maximizing distribution for (2.2) is Gaussian, and the resulting capacity in *bits/channel use* can be written as [27]

$$C_{AWGN}(E_s/N_0) = \log_2\left(1 + \frac{E_s}{N_0}\right) \tag{2.4}$$

where E_s/N_0 is the SNR.

In practical systems, it is not feasible to create Gaussian inputs and transmit them. Therefore, it is more practical to consider finite input alphabet constraints as discussed in the next section.

2.2 Capacity of Memoryless AWGN Channels with Finite Input Alphabet Constraint

For AWGN channel with a finite input alphabet constraint, the capacity expression in (2.1) must be maximized according to the specified input type. For example, for binary phase shift keying (BPSK), the possible inputs are $+1$ and -1. In this case, one can find that optimal input distribution uses both inputs with equal probabilities, and the constrained capacity is given by [28]

$$I^b(E_s/N_0) = 1 - \sqrt{\frac{1}{\pi}} \int_{-\infty}^{\infty} e^{-\left(\tau - \sqrt{E_s/N_0}\right)^2} \log_2\left(1 + e^{-4\tau\sqrt{E_s/N_0}}\right) d\tau. \tag{2.5}$$

The result extends similarly for other modulation schemes such as quadrature phase shift keying (QPSK), 8 PSK, etc. We provide a comparison of the channel capacity and constrained capacities under different input constraints in Figure 2.2. We observe that the capacity saturates as the SNR increases unlike the case with no finite-alphabet constraints. Moreover, the finite input alphabet constraint decreases the channel capacity considerably for high SNRs, however, for low SNRs, they offer similar rates with the channel capacity (under a power constraint only).

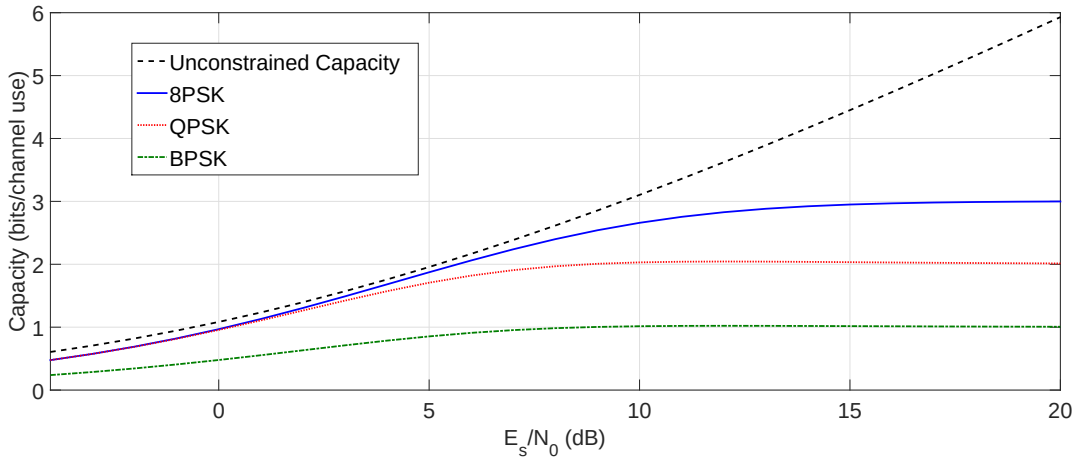

Figure 2.2: Capacity of memoryless AWGN channels with different finite input constellations.

2.3 Secrecy Capacity of Gaussian Wiretap Channels

In the preceding sections, the transmitter and the receiver were the only participants in the communication system. However, in reality, there can be undesired participants eavesdropping the main channel and try to deduce messages. In 1975, Wyner proposed the wiretap channel model and studied the problem of secrecy. Since then, many scenarios have studied the secrecy capacity of wiretap channels in which a transmitter communicates with a legitimate receiver in the

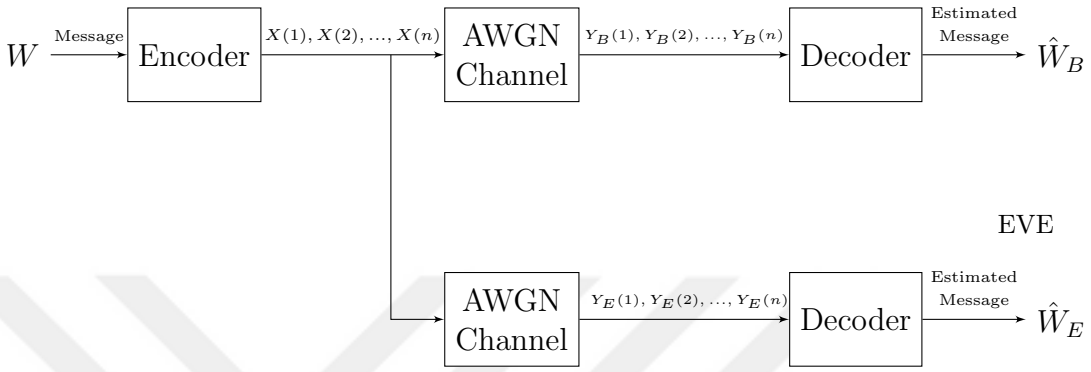

Figure 2.3: Block diagram for the Gaussian wiretap channel.

presence of an eavesdropper overhearing the main channel.

For the Gaussian wiretap channel model, the schematic of the system is provided in Figure 2.3. In the system model, $X(k)$ is the complex channel input, $Y_B(k)$ and $Y_E(k)$ are the complex channel outputs seen by Bob and Eve, respectively, at time instance $k \in \mathbb{Z}$. W denotes the message sent by Alice while $\hat{W}_B$ and $\hat{W}_E$ denote the estimated messages by Bob and Eve, respectively.

Csiszár and Körner [7] formulated the secrecy capacity of a general wiretap channel as

$$C_s = \max_{p(u,x)} (I(U;Y_B) - I(U;Y_E)) \tag{2.6}$$

where U is an auxiliary random variable such that $U \to X \to (Y_B, Y_E)$ forms a Markov chain.

The secrecy capacity of the Gaussian wiretap channels is obtained by $U = X$ where the maximizing input distribution is Gaussian, and it can be expressed as

$$C_s = [C_{AB} - C_{AE}]^+ \tag{2.7}$$

where $C_{AB} = \log_2(1 + SNR_{AB})$ and $C_{AE} = \log_2(1 + SNR_{AE})$. Here, $[.]^+$ denotes the maximization function $max\{0, .\}$.

There is a positive secrecy rate only if the capacity of the main channel is higher than that of the eavesdropper's channel.

2.4 Secrecy Rates of Gaussian Wiretap Channels with Finite Inputs

In regard to physical layer security, much of the literature focuses on results under assumptions of Gaussian signaling. This is unrealistic as no practical communication system employs Gaussian signaling, but instead actual transmissions involve discrete constellations, like QPSK. For secret communication, discrete signaling behaves quite differently from Gaussian signaling. For example, with an increase in power, while the information rate increases monotonically for a Gaussian input distribution, it approaches the saturation value for a finite input alphabet. Thus, for the finite-alphabet case, the information rate approaches a limit for both the main and eavesdropper's channels at high SNRs. As a result, the secrecy capacity drops zero asymptotically. In other words, the effects of using a finite signal constellation should be investigated with care.

The problem of secrecy with finite constellations has been tackled in [9] and [10] for single antenna scenarios. [9] shows that the secrecy capacity with finite inputs as a function of the SNR has a global maximum unlike the case with only a power constraint due to saturation of information rates for both the legitimate user and the eavesdropper. That is, increasing the transmission power beyond the optimal operating point is harmful as the secrecy capacity decreases thereafter. While [9] assumes uniformly distributed inputs, [10] does not make such an assumption and considers the optimization of input distributions and powers jointly. In [11–13], the authors try to maximize the secrecy rates by developing transmission strategies for multi antenna scenarios with finite-alphabet constellations. Their

results show that optimum transmission schemes for the case of finite inputs are different than the ones without this constraint. For example, [11] demonstrates that power allocation strategy based on Gaussian inputs is far from optimal when employed blindly in finite input scenarios. Moreover, [12] shows that the beamforming strategy in MIMOME systems, which is a secrecy capacity achieving approach for Gaussian inputs, does not provide the maximum secrecy rate for the finite input case. In [13], the authors reveal that the achievable secrecy rates with Gaussian inputs increase monotonically with increasing SNR, however, it saturates for finite inputs.

All in all, in these studies, it is shown that finite-alphabet input constraints change the solutions of physical layer secrecy problems significantly, hence study of such problems for this setup requires different approaches. The rest of the thesis will focus on the case of ISI channels with inputs drawn from a discrete constellation.

2.5 Chapter Summary

In this chapter, the capacity of memoryless AWGN channels and the secrecy capacity of memoryless AWGN wiretap channels are reviewed. Then, by comparing the results with and without finite-alphabet input constraints, it is argued that finite signal constellations can change the system performance significantly. To remedy this issue, innovative strategies should be developed. There are existing approaches in the literature addressing these problems, however, the specific setups are limited to the case of memoryless channels. In next chapter, we study channels with memory as a further extension.

Chapter 3

Secrecy Capacity of ISI Channels with AWGN

In Chapter 2, we only considered transmission through AWGN channels with no bandwidth constraints resulting in memoryless channels. However, some practical channels cannot be modeled as memoryless. For example, wireline telephone channels, radio channels and magnetic recording channels are characterized as band-limited linear filters [29]. That is, the received signal is obtained by the convolution of the transmitted signal and the channel response introducing a generally undesirable property: ISI. Therefore, it is of interest to evaluate secrecy rates of ISI channels with AWGN.

The chapter is organized as follows. In Section 3.1, we provide capacity results for ISI channels. In Section 3.2, we note the effects of constraining the channel inputs to a finite set. We discuss calculation of information rates with uniform inputs, and describe the maximization of the mutual information with the use of Markov inputs. Moreover, we propose an alternative approach by introducing a codebook-based design for the maximization. In Section 3.3, we study secrecy capacity of ISI wiretap channels with finite-inputs. In addition to uniform and Markov inputs, we propose injection of AN to increase secrecy rates. Then, we provide several examples to compare the performance of different methods. In

Section 3.4, we provide a chapter summary.

3.1 Capacity of ISI Channels with AWGN

The system model for an ISI channel with m taps and channel coefficients $g(0), \ldots, g(m-1)$ can be written as

$$Y(k) = \sum_{i=0}^{m-1} g(i)X(k-i) + W(k) \tag{3.1}$$

where $X(k)$, $Y(k)$ and $W(k)$ represent the channel input, the channel output and noise sample at time $k \in \mathbb{Z}$, respectively. The noise term, W, is assumed to be circularly symmetric Gaussian with variance $N_0/2$ per dimension. We use normalized channel coefficients so that $\|g\|^2 \triangleq \sum_{i=0}^{m-1} |g(i)|^2 = 1$ and we define the SNR as

$$SNR = \frac{E_s \|g\|^2}{N_0} \tag{3.2}$$

where E_s is the average energy per symbol.

The problem is to find the capacity maximizing input distribution as formulated in (2.1). Hirt and Massey [14] show that the optimum strategy adapts the power following a waterfilling approach. This approach results in the following capacity formulation:

$$C_{ISI} = 2 \int_0^{1/2} \log_2 \Big[max\Big(\Phi |G(f)|^2, 1\Big)\Big] df \tag{3.3}$$

where $G(f)$ is the frequency response of the channel with

$$G(f) = \sum_{i=0}^{m-1} g(i) e^{-2\pi f j i}, \tag{3.4}$$

and the parameter Φ is the waterfilling level that satisfies the power constraint

$$\int_{0,\ G(f)\neq 0}^{0.5} max(\Phi - |G(f)|^{-2}, 0) df = \frac{E_s}{2N_0}. \tag{3.5}$$

The authors show that capacity achieving input distribution is Gaussian with zero mean and covariance given by

$$E\Big[X(i+n)X(i)\Big] = 2\int_0^{1/2} S_x(f) cos(nf) df \tag{3.6}$$

where

$$S_x(f) = \begin{cases} \frac{N_0}{2}\big(\Phi - |G(f)|^{-2}\big), & if \quad \Phi|G(f)|^2 > 1 \quad and \quad |f| \leq 1/2, \\ 0, & otherwise. \end{cases}$$

We provide an example to compare the capacities of standard memoryless channels and ISI channels with the coefficients given in Table 3.1 in Figure 3.1. For this specific example, we observe that capacities of the channels with memory are lower than that of the memoryless channel for high SNRs. On the other hand, in the low SNR region, channels with memory have larger capacities.

Up to now, the obtained results are valid for the scenarios with no finite-alphabet constraints. To study more practical scenarios, we introduce the finite input constraints in the next section.

Table 3.1: Coefficients of the simulated channels for the capacity of ISI channels with AWGN.

Channel Name	g_0	g_1	g_2	g_3	g_4	g_5	g_6
No Memory	1						
Dicode	$1/\sqrt{2}$	$-1/\sqrt{2}$					
EPR4	$1/2$	$1/2$	$-1/2$	$-1/2$			
E2PR4	$1\sqrt{10}$	$2\sqrt{10}$	0	$-2\sqrt{10}$	$-1\sqrt{10}$		
CH6	0.19	0.35	0.46	0.5	0.46	0.35	0.19

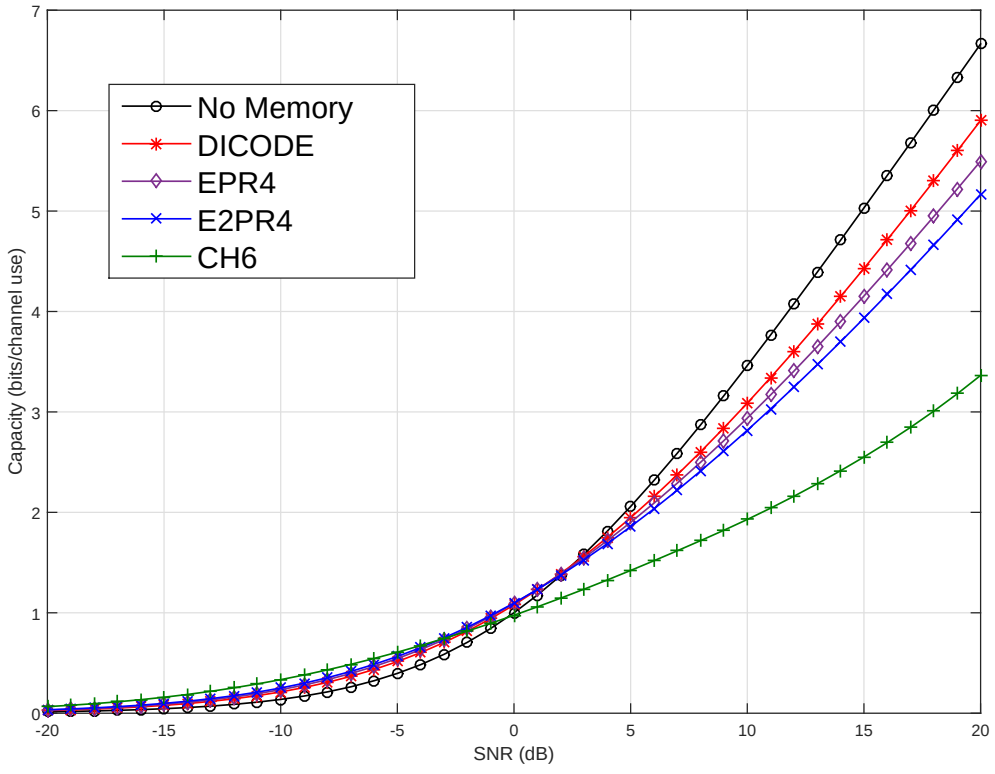

Figure 3.1: Capacities of the ISI channels in Table 3.1.

3.2 Capacity of ISI Channels with Finite Inputs

For this setup, system model in Section 3.1 is valid with an additional finite input alphabet constraint. For memoryless AWGN channels with BPSK inputs, we have stated the capacity expression in (2.5) which is easy to compute. However, there is no such simple expression for the ISI channels due to memory. Thus, we have to continue with the general capacity formula in (2.1) and evaluate it under the finite input constraints. We will first consider the computation of achievable information rates for given inputs, and then continue with the maximization over the input distribution.

For the calculation of information rates, a simulation based method is developed by Arnold and Loeliger in [15], where information rates are accurately estimated by sampling both a long channel input and the resulting output sequence followed by the forward recursion of the BCJR algorithm [16]. We now explain this simulation based approach.

The information rate term can be divided into differential entropy terms so that

$$\lim_{n\to\infty} \frac{1}{n} I(X^n; Y^n) = \lim_{n\to\infty} \frac{1}{n} (h(Y^n) - h(Y^n|X^n)) \tag{3.7}$$

where $X^n = (X(1), .., X(n))$ and $Y^n = (Y(1), .., Y(n))$.

Furthermore, we know that $h(Y^n|X^n) = h(W^n)$ since the noise term is AWGN and independent of the input. Then, we can write

$$\lim_{n\to\infty} \frac{1}{n} h(W^n) = log(\pi e N_0). \tag{3.8}$$

Hence, we obtain

$$\lim_{n\to\infty}\frac{1}{n}I(X^n;Y^n)=\lim_{n\to\infty}\frac{1}{n}h(Y^n)-log(\pi eN_0). \tag{3.9}$$

Thus, the only term that we need to estimate is $\lim_{n\to\infty}\frac{1}{n}h(Y^n)$, which is nothing but

$$\lim_{n\to\infty}\frac{1}{n}h(Y^n)=-\lim_{n\to\infty}\frac{1}{n}E[\log p(Y^n)]. \tag{3.10}$$

This expectation can be computed via Monte Carlo methods, namely

$$\lim_{n\to\infty}\frac{1}{n}h(Y^n)=-\lim_{n\to\infty}\frac{1}{n}\left(\lim_{T\to\infty}\frac{1}{T}\sum_{l=1}^{T}\log p_l(y^n)\right). \tag{3.11}$$

In this equation, due to the stationarity of the sequence Y^n, Shannon-McMillan-Breiman theorem holds [27]. In other words, a single realization with a large block length n is enough instead of T realizations. It means that we can simplify the equations further as

$$\lim_{n\to\infty}\frac{1}{n}h(Y^n)=-\lim_{n\to\infty}\frac{1}{n}\log\big(p(y^n)\big). \tag{3.12}$$

The last equation states that we need to estimate $p(y^n)$ for large values of the block length n. This is where the forward recursion part of the BCJR algorithm comes into play.

To calculate $p(y^n)$, a trellis diagram that shows the state transitions can be used. For example, trellis diagram of the length two ISI channel with BPSK inputs is provided in Figure 3.2. In this diagram, transition between states occur according to the past two inputs and the current input. Note that solid lines denote the transitions for input $+1$ and dashed lines denote those for input -1.

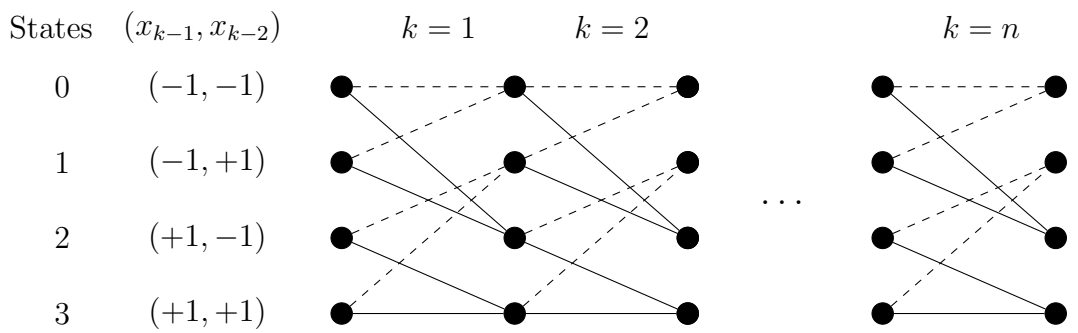

Figure 3.2: Trellis diagram for a BPSK input ISI channel with two taps.

In general, considering a channel with M taps and input alphabet size K, there are K^M states, K incoming and K outgoing paths. We denote the state at time k as S_k. In a trellis diagram, each state transition occurs with respect to corresponding input at time k. To compute $p(y^n)$, we define two additional terms α and γ as

$$\alpha_k(j) = Pr(S_k = j).p(y^k|S_k = j) \tag{3.13}$$

and

$$\gamma_k(i, j) = Pr(S_k = j|S_{k-1} = i) \cdot p(y^k|S_k = j, S_{k-1} = i). \tag{3.14}$$

Note that with these definitions

$$p(y^n) = \sum_{i=1}^{n} \alpha_n(j) \tag{3.15}$$

and

$$
\begin{aligned}
\alpha_k(j) &= p(y^k, S_{k-1} = i, S_k = j) \\
&= \sum_{i=1}^{k} p(y^k | y^{k-1}, S_{k-1} = i, S_k = j) \cdot p(y^{k-1}, S_{k-1} = i, S_k = j) \\
&= \sum_{i=1}^{k} p(y^k | y^{k-1}, S_{k-1} = i, S_k = j) \cdot Pr(S_k = j | S_{k-1} = i) \cdot p(y^{k-1}, S_{k-1} = i) \\
&= \sum_{i=1}^{k} \gamma_k(i, j) \alpha_{k-1}(i).
\end{aligned}
\tag{3.16}
$$

Considering (3.14), it is straightforward to calculate the γ parameter since $Pr(S_k = j | S_{k-1} = i)$ is known by the input distribution and

$$
p(y^k | S_{k-1} = i, S_k = j) = \frac{1}{\pi N_0} e^{-\frac{|y_k - \hat{y}_k|^2}{N_0}} \tag{3.17}
$$

where $\hat{y}_k$ is the corresponding noiseless output fixed by the transition i to j.

Thus, we can calculate the $\gamma_k(i, j)$ values and use them to solve $\alpha_n(j)$ iteratively by (3.16). Then, we can sum all $\alpha_n(j)$ at time n to find $p(y^n)$ as seen in (3.15). In these calculations, one can specify the initial state arbitrarily since the system is ergodic. All in all, the resulting algorithm to estimate $I(X^n; Y^n)$ can be summarized as Algorithm 1. In the next section, we will use this algorithm with uniform input distributions.

Algorithm 1 : Arnold-Loeliger Sum Product Approach to Estimate Mutual Information Rate [15]

Step 1: Pick a large value of n, and create a single long realization of x^n and y^n.

Step 2: Compute $p(y^n)$ by using (3.15) and the iterative procedure.

Step 3: Calculate

$$\begin{aligned} I(X;Y) &= \frac{1}{n} I(X^n;Y^n) \\ &= -\frac{1}{n}\log\left(p(y^n)\right) - log(\pi e N_0) \end{aligned}$$

to estimate the information rate.

3.2.1 Information Rates with Uniform Inputs

The results of the previous section are applicable under general Markov input distributions. Here, we focus on the achievable rate results for independent and uniformly distributed (i.u.d.) inputs whose information rates are provided in Figure 3.3. We use uniformly distributed BPSK symbols, and let $n = 10^5$. The information rates are estimated by Algorithm 1. We observe that capacities of the channels converge to certain finite values due to the finite input constraint. Thus, it is not beneficial to increase the transmit power after a certain point.

If we compare the system performance with the one in Figure 3.1, it can be shown that limitation on the input alphabet decreases the achievable rate. For example, considering the dicode channel at -5 dB, there is an information rate loss of 0.1917 $bits/channel\ use$ due to the finite-alphabet constraint. The loss is increases with SNR as seen in Figure 3.4.

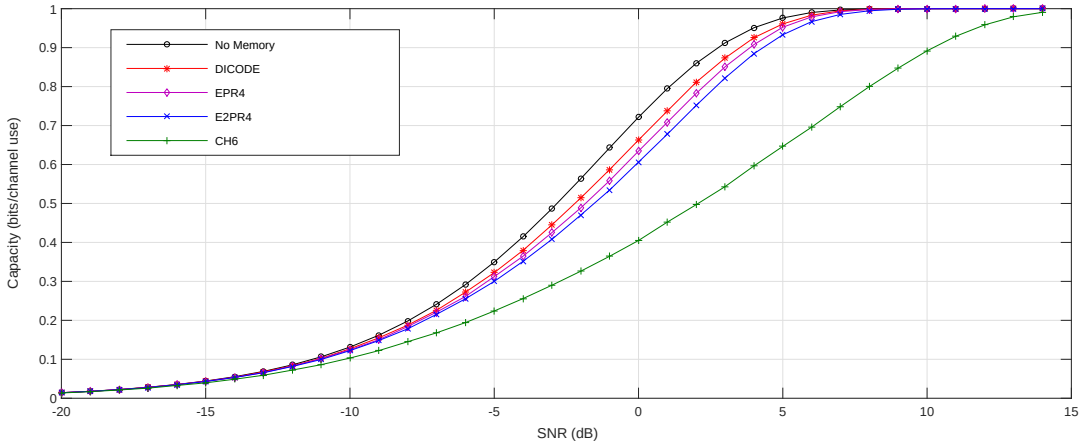

Figure 3.3: Information rates of the ISI channels in Table 3.1 with BPSK inputs.

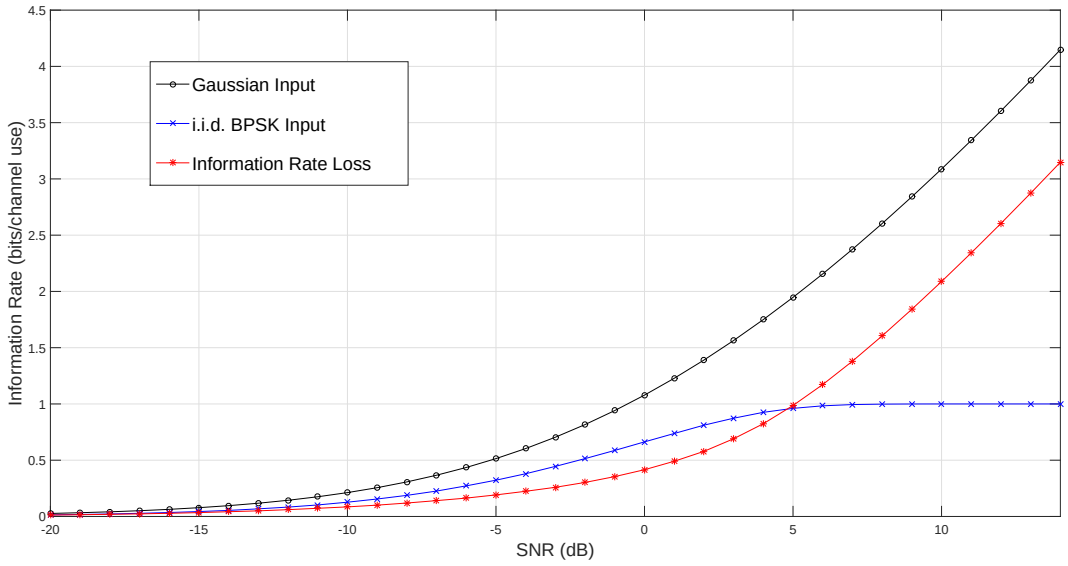

Figure 3.4: Information rates with and without finite-alphabet input constraint for the dicode channel.

3.2.2 Information Rates with Markov Inputs

Memoryless input distribution limits the achievable rates considerably. Instead, we can employ input distributions having memory (of length V) such as Markov

inputs. By implementing Markov inputs, we can exploit the channel characteristics and obtain better rates. However, for this setup, estimating the information rate is not enough. In addition to estimation, we need to select suitable Markov distributions by applying optimization techniques.

Kavcic [17] proposes a method by limiting the input distribution set to Markov sources and reformulating the Blahut-Arimoto algorithm [18, 19] to optimize the Markov transition probabilities. Assume that there exists a discrete memoryless channel with input alphabet $X = 1, 2, ..., G$, and output alphabet $Y = 1, 2, ..., N$, where the channel is specified by the probabilities $p_{i,j} = Pr(Y = j|X = i)$. The aim is to find the input distribution $r_i = Pr(X = i)$ that maximizes the mutual information between the channel input and output. The resulting algorithm is the stochastic version of Blahut-Arimoto algorithm as stated in [17] and given here as Algorithm 2.

Algorithm 2 : The Expectation-Maximization Version of the Blahut-Arimoto Algorithm [17]

Initialization: Pick an arbitrary distribution r_i, such that $0 < r_i < 1$ and $\sum_{i=1}^{G} r_i = 1$.

Repeat until convergence

Step 1 - Expectation: For r_i fixed, compute

$$T_i = E\left[\frac{Pr(X=i|Y)log(Pr(X=i|Y))}{r_i}\right].$$

Step 2 - Maximization: For T_i fixed, find r_i to maximize $\sum_i r_i[log\frac{1}{r_i} + T_i]$, i.e., set $r_i = \frac{2^{T_i}}{\sum_k 2^{T_k}}$.

end

In this algorithm, starting from an arbitrary distribution, the input distribution is updated in a step by step manner. At the end, the maximizing input distribution is obtained. Now, we will use similar approach by converting the actual problem to this format. Remember that the actual problem is to maximize

mutual information $I(X^n;Y^n)$. Since the input vector X^n implicitly determines the state transitions S^n, we can reformulate the mutual information term so that

$$\lim_{n\to\infty}\frac{1}{n}I(X^n;Y^n)=\lim_{n\to\infty}\frac{1}{n}I(S^n;Y^n). \tag{3.18}$$

Applying the chain rule and the Markov property, we can rearrange the terms on the right hand side of (3.18) so that

$$\begin{aligned}\frac{1}{n}I(S^n;Y^n)&=\frac{1}{n}\sum_{k=1}^{n}I(S_k;Y^n|S^{k-1})\\&=\frac{1}{n}\sum_{k=1}^{n}I(S_k;Y^n|S_{k-1})\\&=\frac{1}{n}\sum_{k=1}^{n}h(S_k|S_{k-1})-\frac{1}{n}h(S_k|S_{k-1},Y^n).\end{aligned} \tag{3.19}$$

After this rearrangement, the differential entropy terms can be investigated separately. Using the properties of expectation and Bayes' rule, we can further simplify the expressions. By defining

$$T_{ij}=\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n}E\left[log\frac{Pr(S_{k-1}=i,S_k=j|Y^n)^{\frac{Pr(S_{k-1}=i,S_k=j|Y^n)}{\mu_iP_{ij}}}}{Pr(S_{k-1}=i|Y^n)^{\frac{Pr(S_{k-1}=i|Y^n)}{\mu_i}}}\right] \tag{3.20}$$

where $\mu_i=Pr(S_k=i)$ and $P_{ij}=Pr(S_k=j|S_{k-1}=i)$, the actual problem becomes to find optimal P_{ij} distribution to maximize

$$\lim_{n\to\infty}\frac{1}{n}I(S^n;Y^n)=\sum_{i,j:(i,j)\in T}\mu_iP_{ij}\left[log\frac{1}{P_{ij}}+T_{ij}\right] \tag{3.21}$$

within the valid state transition set $(i,j)\in T$ such that the transition from i to j

is valid. In (3.21), the term T_{ij} can be estimated using the Arnold-Loeliger sum-product approach as shown in the previous derivations. With these formulations, the same expectation-maximization procedure of Algorithm 2 can be adapted to this problem. The resulting iterative optimization procedure is summarized in Algorithm 3.

Algorithm 3 : The Expectation-Maximization for Optimizing Markov Process Transition Probabilities to Maximize Capacity [17]

Initialization: Pick an arbitrary distribution P_{ij} within the valid state transition set $(i,j) \in T$, such that

1) $if (i,j) \in T$ then $0 < P_{ij} < 1$, otherwise $P_{ij} = 0$ and

2) for any i, $\sum_j P_{ij} = 1$

Repeat until convergence

Step 1 - Expectation: While keeping all P_{ij} fixed, compute

$$T_{ij} = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} E\left[log \frac{Pr(S_{k-1}=i, S_k=j|Y^n)^{\frac{Pr(S_{k-1}=i,S_k=j|Y^n)}{\mu_i P_{ij}}}}{Pr(S_{k-1}=i|Y^n)^{\frac{Pr(S_{k-1}=i|Y^n)}{\mu_i}}} \right].$$

Step 2 - Maximization: While keeping all T_{ij} fixed, find all P_{ij} and the corresponding μ_j to achieve the maximization of (3.21) , i.e., set

$$[P_{ij}] = \arg\max_{[P_{ij}]} \sum_{i,j:(i,j)\in T} \mu_i P_{ij} \left[log \frac{1}{P_{ij}} + T_{ij} \right].$$

end

We now need to solve the maximization problem in Step 2 of Algorithm 3, which can be done by using the Lagrangian. The objective function is

$$\sum_{i,j:(i,j)\in T} \mu_i P_{ij} \left[log \frac{1}{P_{ij}} + T_{ij} \right] \tag{3.22}$$

under the constraints

$$\sum_{i,j:(i,j)\in T} P_{ij} = 1, \tag{3.23}$$

$$\sum_{i} \mu_i P_{ij} = \mu_j \quad \forall (i,j) \in T, \tag{3.24}$$

$$\sum_{i} \mu_i = 1. \tag{3.25}$$

With this objective function and constraints, the Lagrangian can be written as

$$L = \sum_{i,j:(i,j)\in T} \mu_i P_{ij} \Big[log \frac{1}{P_{ij}} + T_{ij} \Big] + \sum_{i,j:(i,j)\in T} \lambda_i P_{ij} + \sum_{i,j:(i,j)\in T} \lambda_j^{'} \Big(\mu_i P_{ij} - \mu_j \Big) + \lambda^{''} \sum_{i} \mu_i. \tag{3.26}$$

where λ, $\lambda^{'}$ and $\lambda^{''}$ are the Lagrange multipliers for the corresponding constraints.

After taking the derivatives, the result shows that the optimal P_{ij} values are

$$P_{ij} = \frac{\hat{b}_j}{\hat{b}_i} \cdot \frac{\hat{A_{ij}}}{\hat{U}_{max}} \tag{3.27}$$

where

$$\hat{A}_{ij} = \begin{cases} 2^{T_{ij}} & if (i,j) \in T, \\ 0, & otherwise. \end{cases}$$

Here, $\hat{U}_{max}$ and $\hat{b} = [\hat{b}_j \quad \hat{b}_i]^T$ are the maximal eigenvalue and the corresponding eigenvector of $\hat{A}_{ij}$, respectively. Considering the optimization results, we update Algorithm 3 and obtain the procedure given in Algorithm 4.

Algorithm 4 : The Expectation-Maximization for Optimizing Markov Process Transition Probabilities to Maximize Capacity (including the optimization method) [17]

Initialization: Pick an arbitrary distribution P_{ij} within the valid state transition set $(i,j) \in T$, such that

1) $if (i,j) \in T$ then $0 < P_{ij} < 1$, otherwise $P_{ij} = 0$ and

2) for any i, $\sum_j P_{ij} = 1$.

Repeat until convergence

Step 1 - Expectation: While keeping all P_{ij} fixed, compute

$$T_{ij} = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} E\left[log \frac{Pr(S_{k-1}=i, S_k=j|Y^n) \frac{Pr(S_{k-1}=i, S_k=j|Y^n)}{\mu_i P_{ij}}}{Pr(S_{k-1}=i|Y^n) \frac{Pr(S_{k-1}=i|Y^n)}{\mu_i}} \right].$$

Step 2 - Maximization: While keeping all T_{ij} fixed, find all P_{ij} and the corresponding μ_j to achieve the maximization of (3.21), i.e., set

$$P_{ij} = \frac{\hat{b}_j}{\hat{b}_i} \cdot \frac{\hat{A_{ij}}}{\hat{U}_{max}} \text{ where } \hat{A}_{ij} = \begin{cases} 2^{T_{ij}} & if (i,j) \in T, \\ 0, & otherwise, \end{cases}$$

where $\hat{U}_{max}$ and $\hat{b} = [\hat{b}_1 \quad \hat{b}_2]^T$ are the maximal eigenvalue and the corresponding eigenvectors of $\hat{A}_{ij}$, respectively.

end

We now provide a numerical example for the dicode channel where the information rates are maximized by using Markov inputs. In Figure 3.5, it is shown that information rate increases with Markov BPSK inputs when compared to i.u.d. BPSK case. Considering the order of Markov inputs, using $V = 1$ increases the information rate considerably. However, this effect fades away for higher memory orders. For order 2 and order 3, the improvements of the information rate are almost the same. Thus, for the sake of complexity, it may be sufficient to use a Markov input of order 1 for this example.

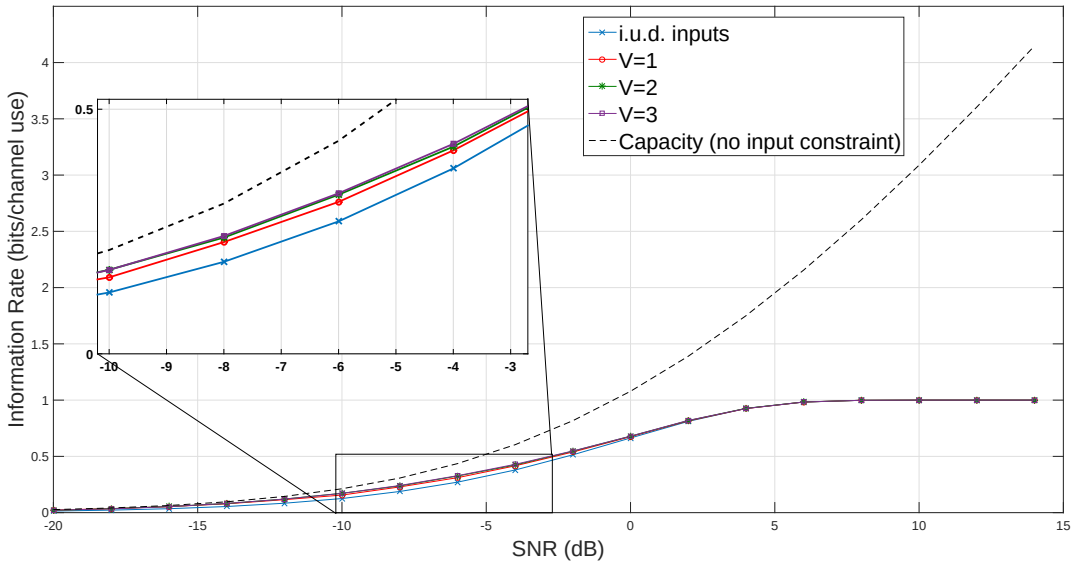

Figure 3.5: Maximized information rates of the dicode channels with the Markov inputs order V and BPSK input alphabet.

3.2.3 Markov Input Solution with Spectrum Match Based Optimization (PSD Approach)

The iterative search algorithm described in the previous section has a computational complexity as many BCJR recursions are needed. Here, we propose an alternative solution by introducing a codebook based design similar to the approach in [21]. First, we create a codebook which consists of arbitrarily generated Markov transition matrices. Then, we select the one which spectrally matches the main channel since it is shown that frequency response of the channels and the PSD of the input distribution should match for the maximization of information rates [20]. We calculate similarity levels by defining a suitable performance metric (p.m.) as

$$p.m. = -\sqrt{\int_{-0.5}^{0.5} \Big(|G(f)|^2 - S_x(f)\Big)^2 df} \tag{3.28}$$

where $G(f)$ represents channel frequency response and $S_x(f)$ represents the PSD of the corresponding Markov process in the codebook. After computing the performance metrics of the input distributions (codes), we select the one with the highest similarity as the optimal solution.

We now provide numerical examples to demonstrate that the PSD based approach works well to maximize the information rates of noisy channels. We compare the PSD based approach with the iterative method of Algorithm 4 for Markov inputs order of 1. We use a codebook of size 1000. We provide the dicode channel's frequency response, the PSD of a matching code and a non-matching one along with the corresponding information rates at $SNR = -10\ dB$ in Figure 3.6. We illustrate that the code which spectrally matches the channel outperforms the non-matching code in terms of the information rates. We also observe that the information rate increases considerably when the performance metric increases as provided in Figure 3.7.

Next, the same methodology is employed for all SNR values, and the corresponding information rates are obtained. In Figure 3.8, it is shown that the PSD based approach works well when compared to the previous method of Algorithm 4, especially, for low SNR values. In that region, two methods improve the system performance almost equally, however, the PSD based method is computationally much less complicated compared to the alternative of iterative search algorithm.

As a result, we argue that the PSD based approach can be a low-complexity alternative to (approximately) maximize the information rates over a channel. We consider the use of the PSD based approach over the wiretap channel in the next section.

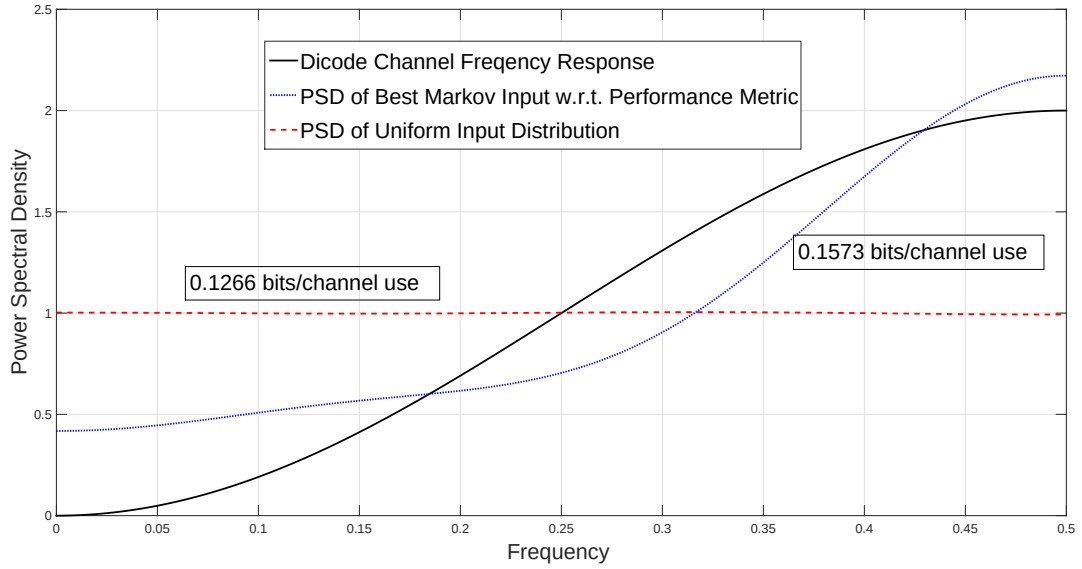

Figure 3.6: Spectral matching of the PSD of the Markov inputs and dicode channel response for $SNR = -10\ dB$ and $V = 1$ along with the corresponding information rates.

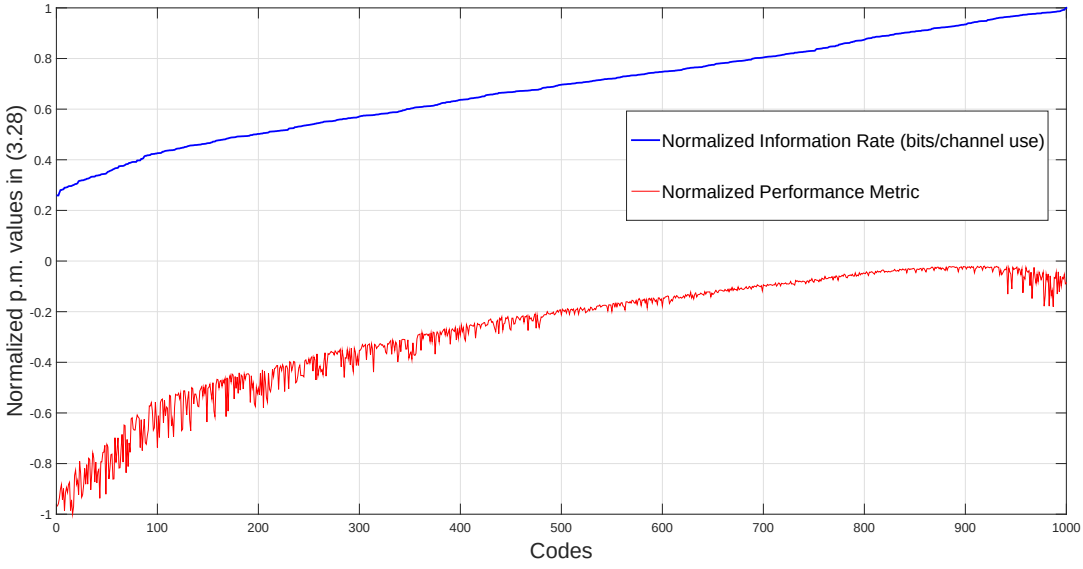

Figure 3.7: Information rate and performance metric relation for the codebook of size 1000 when $SNR = -10\ dB$ and $V = 1$.

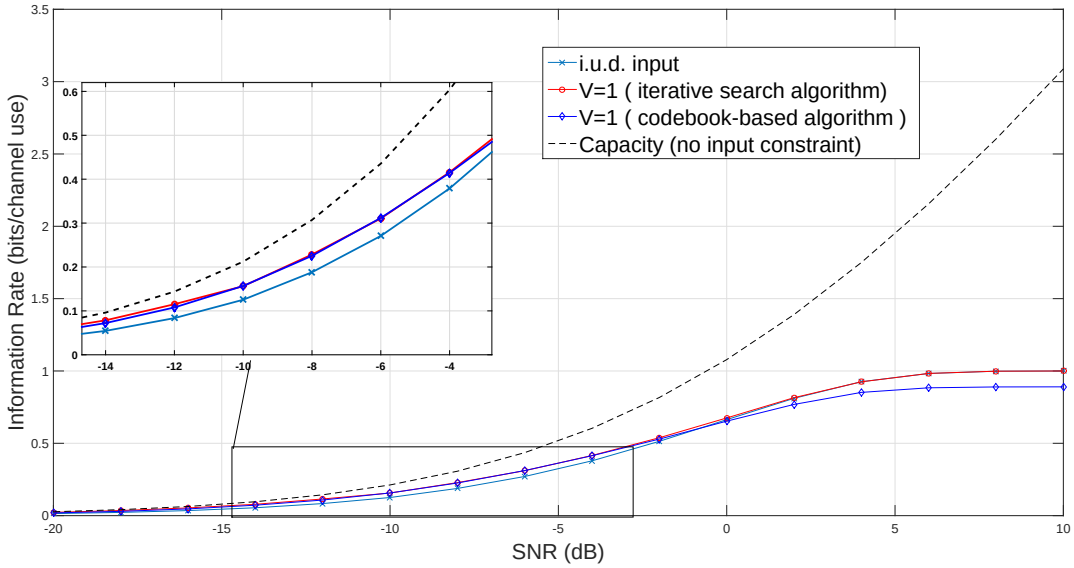

Figure 3.8: Comparison of Algorithm 4's search method and our codebook-based PSD method for the maximization of information rates of the dicode channels with the Markov inputs order $V = 1$.

3.3 Secrecy Rates of ISI Wiretap Channels with Finite Inputs

An expression for the secrecy capacity of AWGN wiretap channel with ISI is known, however, it is not feasible to compute it numerically. Here, we propose a lower bound (i.e., an achievable rate), and evaluate performance of secure transmission schemes using this lower bound.

3.3.1 System Model and the Problem Description

The system model of a wiretap ISI channel with AWGN can be expressed as

$$
\begin{aligned}
Y_B(k) &= \sum_{i=0}^{m_{AB}-1} g_{AB}(i)X(k-i) + W_{AB}(k), \\
Y_E(k) &= \sum_{i=0}^{m_{AE}-1} g_{AE}(i)X(k-i) + W_{AE}(k),
\end{aligned}
\tag{3.29}
$$

where $X(k)$ is the channel input at time instant $k \in \mathbb{Z}$. $Y_B(k)$ and $Y_E(k)$ represent the channel outputs at Bob and Eve, respectively. Similarly, g_{AB} and g_{AE} denote the fixed complex ISI channel coefficients. m_{AB} and m_{AE} are the number of propagation paths over the main and the eavesdropper's channels, respectively. The noise terms W_{AB} and W_{AE} are assumed to be circularly symmetric Gaussian complex random variables with variances $N_{AB}/2$ and $N_{AE}/2$ per dimension, respectively. The channel gains are normalized so that $\|g_{AB}\|^2 = 1$ and $\|g_{AE}\|^2 = 1$. We define the SNRs as

$$
SNR_{AB} = \frac{E_s\|g_{AB}\|^2}{N_{AB}}, \tag{3.30}
$$

$$
SNR_{AE} = \frac{E_s\|g_{AE}\|^2}{N_{AE}}, \tag{3.31}
$$

where E_s is the symbol energy constraint. We assume that input is constrained to a finite set. Particularly, BPSK input set is employed for all the numerical examples throughout the section.

The secrecy capacity for this setup can be expressed as [22]

$$
C_s = \left[\max_{P(u^n,x^n)} \lim_{n\to\infty} \frac{1}{n}\Big(I(U^n;Y_B^n) - I(U^n;Y_E^n) \Big) \right]^+ \tag{3.32}
$$

where U^n is a sequence of auxiliary random variables such that $U^n \to X^n \to (Y_B^n, Y_E^n)$ form a Markov chain. In other words, the random variable U represents the channel prefixing. This capacity expression is the vectorized form of the memoryless wiretap channel's secrecy capacity (2.6). Intuitively, for large n, the input and output of the ISI channels can be considered as the input and output of a ("large") memoryless channel, hence the difference of usual mutual information terms becomes the secrecy capacity.

Assuming $U = X$ (no prefixing), we obtain the following lower bound on the capacity as an achievable secrecy rate:

$$R_s = \left[\max_{P(x^n)} \lim_{n\to\infty} \frac{1}{n} \Big(I(X^n; Y_B^n) - I(X^n; Y_E^n) \Big) \right]^+. \tag{3.33}$$

We limit ourselves to the case of Markov input distributions. By expressing the information rate terms in terms of differential entropies, we obtain the following equivalent formulation:

$$\begin{aligned} R_s &= \left[\max_{P_{ij}:(i,j)\in T} \lim_{n\to\infty} \frac{1}{n} \left(I(X^n; Y_B^n) - I(X^n; Y_E^n) \right) \right]^+ \\ &= \left[\max_{P_{ij}:(i,j)\in T} \lim_{n\to\infty} \frac{1}{n} \left(h(Y_B^n) - h(Y_B^n|X^n) - h(Y_E^n) + h(Y_E^n|X^n) \right) \right]^+ \\ &= \left[\max_{P_{ij}:(i,j)\in T} \sum_{i,j:(i,j)\in T} \mu_i P_{ij} \left(log \frac{1}{P_{ij}} + T_{ij}^{(1)} + T_{ij}^{(2)} + T_{ij}^{(3)} \right) \right]^+, \end{aligned} \tag{3.34}$$

where

$$T_{ij}^{(1)} = \frac{1}{n} \sum_{k=1}^{n} \left[log \frac{Pr(S_{k-1} = i, S_k = j|y_B^n)^{\frac{Pr(S_{k-1}=i, S_k=j|y_B^n)}{\mu_i P_{ij}}}}{Pr(S_{k-1} = i|y_B^n)^{\frac{Pr(S_{k-1}=i|y_B^n)}{\mu_i}}} \right],$$

$$T_{ij}^{(2)} = \frac{log\ p(y_E^n)}{n\mu_i P_{ij}} \left(\frac{1}{n} \sum_{k=1}^{n} Pr(S_{k-1} = i, S_k = j|y_E^n) \right), \tag{3.35}$$

$$T_{ij}^{(3)} = -\frac{log\ p(y_E^n|x^n)}{n\mu_i P_{ij}} \left(\frac{1}{n} \sum_{k=1}^{n} Pr(S_{k-1} = i, S_k = j|y_E^n) \right).$$

The problem is to maximize the achievable secrecy rate in (3.34) over the Markov input distributions. In [22], the authors propose a suboptimal solution by providing an iterative search algorithm. Here, we also propose a suboptimal

solution, however, by using a codebook based design approach where the input power spectral densities and channel frequency responses are employed. The codebook design is more advantageous than the iterative search algorithm in terms of computational complexity. In addition, we provide secrecy rate results with the use of iterative search algorithm and the newly proposed codebook based design, and make comparisons.

We first consider the calculation of secrecy rates and obtain results with uniformly distributed inputs. Then, we apply the proposed algorithms, and compare their performance via numerical examples.

3.3.2 Different Transmission and Optimization Strategies for the Maximization of Secrecy Rates

3.3.2.1 Secrecy Rates with Uniform Inputs

For uniform input distributions, the only problem is the calculation of achievable secrecy rates. Since we know that T_{ij}'s in (3.34) can be calculated with the aid of a trellis diagram through the BCJR algorithm, it is straightforward to calculate the resulting secrecy rates.

For the maximization of achievable secrecy rates, uniform input distribution may not be the optimal choice. For example, we can employ Markov input distributions to better match the channel characteristics. In this case, the problem is to find the optimal Markov input distribution that maximizes the achievable secrecy rate. We offer two different suboptimal solutions to do this. The first one is the iterative optimization method of [22], and the second one is the newly proposed spectral matching based optimization method.

3.3.2.2 Iterative Optimization of Markov Inputs to Increase Secrecy Rates

The iterative optimization method is based on the expectation-maximization procedure similar to Algorithm 3. By applying this algorithm to the secrecy problem, Algorithm 5 is obtained to find the optimal Markov input distribution that maximizes the achievable secrecy rate.

We have explained the details of the information rate calculations in Section 3.2. Here, the problem is the maximization in Step 2. [22] provides a suboptimal solution (given in Algorithm 6) by applying the Lagrangian method similar to Algorithm 4.

3.3.2.3 Spectrum Matching Based Solution (the PSD Approach)

The optimization problem in Algorithm 5 is difficult to solve directly. Instead, we propose another solution which combines a codebook based design, the PSD of the input distribution and the frequency responses of the main user's and the eavesdropper's channels. We create a codebook which consists of arbitrarily generated Markov transition matrices. Then, we calculate similarity levels of the frequency responses of the channels and the input PSDs by using the performance metric (p.m.) in (3.28). We compute two performance metrics where the first one is for the main channel and the second one is for the eavesdropper's channel. Finally, in Algorithm 7, we combine these two metrics to find the best code which matches the main channel while mismatching the eavesdropper's channel.

Algorithm 5 : The Expectation-Maximization for Optimizing Markov Process Transition Probabilities to Maximize the Achievable Secrecy Rates [22]

Initialization: Pick an arbitrary distribution P_{ij} within the valid state transition set $(i,j) \in T$, such that

1) $if (i,j) \in T$ then $0 < P_{ij} < 1$, otherwise $P_{ij} = 0$ and,

2) for any i, $\sum_j P_{ij} = 1$.

Repeat until convergence

Step 1 - Expectation: While keeping all P_{ij} fixed, compute

$$T_{ij}^{(1)} = \frac{1}{n} \sum_{k=1}^{n} \left[log \frac{Pr(S_{k-1}=i, S_k=j|y_B^n) \frac{Pr(S_{k-1}=i, S_k=j|y_B^n)}{\mu_i P_{ij}}}{Pr(S_{k-1}=i|y_B^n) \frac{Pr(S_{k-1}=i|y_B^n)}{\mu_i}} \right],$$

$$T_{ij}^{(2)} = \frac{log\ p(y_E^n)}{n \mu_i P_{ij}} \left(\frac{1}{n} \sum_{k=1}^{n} Pr(S_{k-1}=i, S_k=j|y_E^n) \right),$$

$$T_{ij}^{(3)} = -\frac{log\ p(y_E^n|x^n)}{n \mu_i P_{ij}} \left(\frac{1}{n} \sum_{k=1}^{n} Pr(S_{k-1}=i, S_k=j|y_E^n) \right).$$

Step 2 - Maximization: While keeping all T_{ij}s fixed, find all P_{ij} and the corresponding μ_j to achieve the maximization of (3.21), i.e., set

$$[P_{ij}] = \arg\max_{[P_{ij}]} \sum_{i,j:(i,j)\in T} \mu_i P_{ij} \left[log \frac{1}{P_{ij}} + T_{ij}^{(1)} + T_{ij}^{(2)} + T_{ij}^{(3)} \right]^+.$$

end

Algorithm 6 : The Expectation-Maximization for Optimizing Markov Process Transition Probabilities to Maximize Secrecy Rates (the suboptimal iterative solution) [22]

Initialization: Pick an arbitrary distribution P_{ij} within the valid state transition set $(i,j) \in T$, such that

1) $if (i,j) \in T$ then $0 < P_{ij} < 1$, otherwise $P_{ij} = 0$ and,

2) for any i, $\sum_j P_{ij} = 1$.

Repeat until convergence

Step 1 - Expectation: While keeping all P_{ij} fixed, compute

$$T_{ij}^{(1)} = \frac{1}{n}\sum_{k=1}^{n}\left[log\frac{Pr(S_{k-1}=i,S_k=j|y_B^n)^{\frac{Pr(S_{k-1}=i,S_k=j|y_B^n)}{\mu_i P_{ij}}}}{Pr(S_{k-1}=i|y_B^n)^{\frac{Pr(S_{k-1}=i|y_B^n)}{\mu_i}}}\right],$$

$$T_{ij}^{(2)} = \frac{log\ p(y_E^n)}{n\mu_i P_{ij}}\left(\frac{1}{n}\sum_{k=1}^{n} Pr(S_{k-1}=i, S_k=j|y_E^n)\right),$$

$$T_{ij}^{(3)} = -\frac{log\ p(y_E^n|x^n)}{n\mu_i P_{ij}}\left(\frac{1}{n}\sum_{k=1}^{n} Pr(S_{k-1}=i, S_k=j|y_E^n)\right).$$

Step 2 - Maximization: While keeping all T_{ij}s fixed, find all P_{ij} and the corresponding μ_j to achieve the maximization of (3.21), i.e., set

$$P_{ij} = \frac{\hat{b}_j}{\hat{b}_i}\cdot\frac{\hat{A_{ij}}}{\hat{U}_{max}} \text{ where } \hat{A}_{ij} = \begin{cases} 2^{T_{ij}^{(1)}+T_{ij}^{(2)}+T_{ij}^{(3)}} & if (i,j) \in T \\ 0, & otherwise \end{cases}$$

where $\hat{U}_{max}$ and $\hat{b} = [\hat{b}_1 \quad \hat{b}_2]^T$ are the maximal eigenvalue and the corresponding eigenvectors of $\hat{A}_{ij}$, respectively.

end

Algorithm 7 : The PSD Based approach for Optimizing Markov Process Transition Probabilities to Maximize Secrecy Rates

Initialization: Create a codebook C of size $|C|$ whose elements P_{ij}s are arbitrarily distributed within the valid state transition set $(i,j) \in T$, such that

1) $if (i,j) \in T$ then $0 < P_{ij} < 1$, otherwise $P_{ij} = 0$ and,
2) for any i, $\sum_{j} P_{ij} = 1$.

Step 1 - Performance Metric Calculation: For each $P \in C$, compute the corresponding performance metric by using the main channel frequency response $G_{AB}(f)$ and Markov process PSD $S_x(f)$:

$$pm_{AB} = -\sqrt{\int_{-0.5}^{0.5} \Big(|G_{AB}(f)|^2 - S_x(f)\Big)^2 df}.$$

If the eavesdropper's CSI exists at the transmitter **then**

Step 2 - Selection of the Candidate Codes w.r.t. Main Channel: Among all the codes, choose the highest 10 ones in terms of their pm_{AB}. These are the candidate codes.

Step 3 - Performance Metric Calculation for the Candidates: For each candidate code, compute the corresponding performance metric by using the eavesdropper's channel frequency response $G_{AE}(f)$ and Markov process PSD $S_x(f)$:

$$pm_{AE} = -\sqrt{\int_{-0.5}^{0.5} \Big(|G_{AE}(f)|^2 - S_x(f)\Big)^2 df}.$$

Step 4 - Selection of the Code w.r.t. Eve's Channel: Among the candidate codes, choose the lowest one in terms of their performance metrics and return it.

else

Step 5 - Selection of the Codes w.r.t. Main Channel: Among all the codes, choose the highest one in terms of their pm_{AB} and return it.

3.3.2.4 Artificial Noise Solution for the Secrecy Rates with Uniform Inputs

In this section, we propose an AN-aided strategy for improving the achievable secrecy rates over finite input ISI channels. The system block diagram is shown in Figure 3.9. Unlike the most AN-aided schemes in the literature which consider transmissions via multiple antennas and offer beamforming based approaches to span the null space of the main channel [30], our AN injection is carried out by a single antenna. We propose to inject a colored noise whose power spectral density has the least match with the spectrum of the main channel, and therefore, the information rate over the main channel undergoes a minimal loss. On the other hand, we demonstrate through numerical examples that this AN injection may suppress the information rates at the eavesdropper leading to considerable improvements in the achievable secrecy rates.

For the design of the filter generating colored Gaussian AN, we employ a codebook based strategy similar to the PSD based approach in Section 3.2.3. We create a codebook which consists of various filters. Then, by calculating the similarities between their frequency responses and the main channel we decide on the best one. We only use the main CSI and choose the least harmful filter within the codebook for the main channel information rate.

The information rate terms in the secrecy rate of ISI channels are computed by the Arnold-Loeliger sum-product algorithm [15]. This simulation-based computation is applicable if the Gaussian terms are i.i.d. Hence, we apply whitening to the received signals to obtain i.i.d. Gaussian noise terms before employing the simulation based information rate estimation. The mutual information terms of the new system are equivalent to the initial one as the whitening operation is invertible.

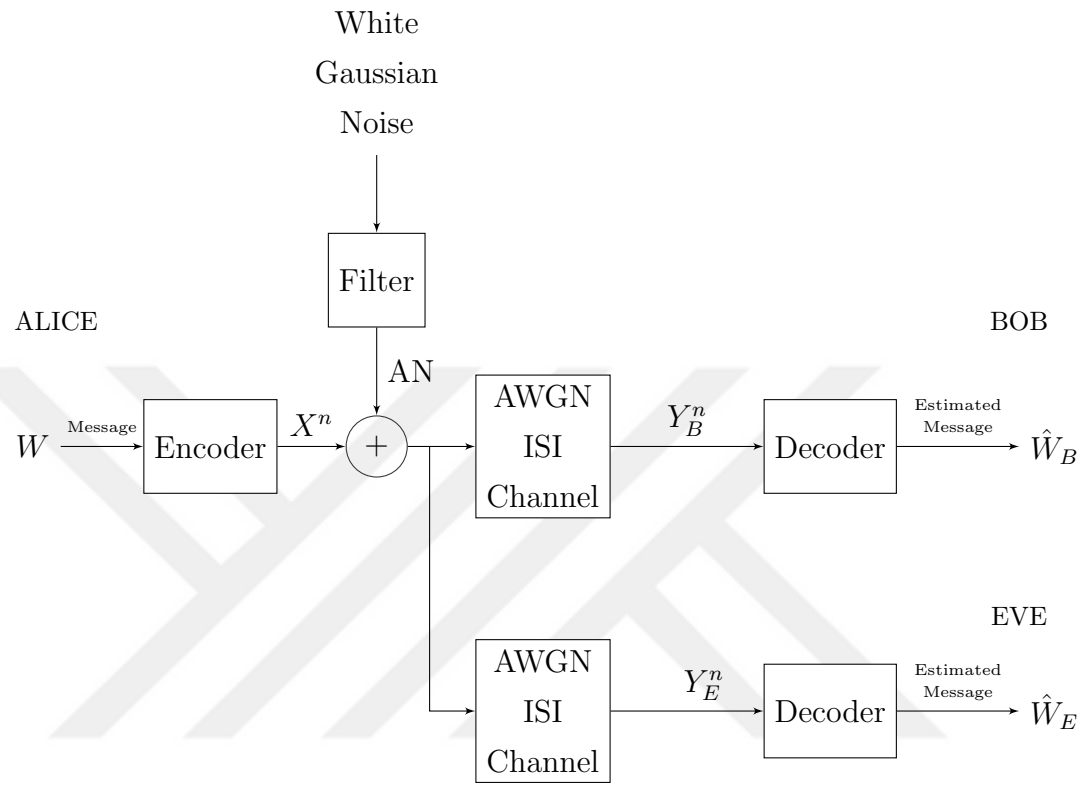

Figure 3.9: Block diagram for ISI wiretap channels with AWGN and AN injection.

We provide an example to illustrate the performance of the AN-aided scheme. We use a codebook of 100 filters. Channel coefficients are chosen as $g_{AB} = [0.6320,\ 0.7750]$ and $g_{AE} = [-0.6803,\ 0.7330]$. We assume that $SNR_{AB} = 5\ dB$ and $SNR_{AE} = 0\ dB$. As provided in Figure 3.10, the frequency responses of the channels are different. We inject a colored noise after filtering the white Gaussian noise. We show that injected AN degrades the performance of the eavesdropper's channel more than performance of the main channel, hence increasing the secrecy rate.

We inject different levels of AN by changing its ratio and tabulate the results in Table 3.2. It is obvious that AN injection increases the secrecy rate considerably when compared to the uniform input case without AN. Furthermore, AN ratio is an important parameter that should be considered carefully.

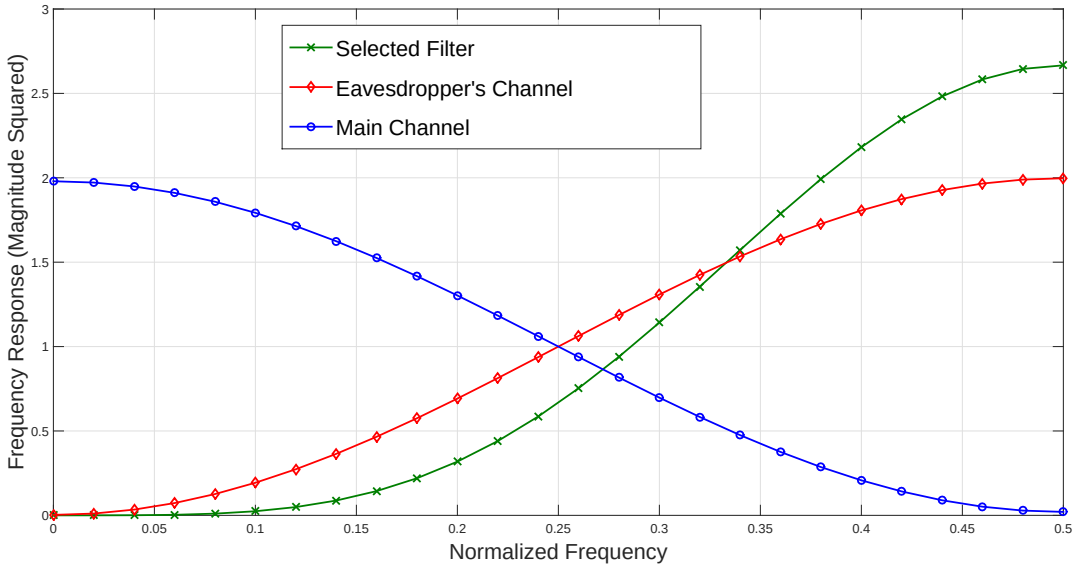

Figure 3.10: Frequency responses of the channels and the selected filter.

Table 3.2: Secrecy and information rate (in bits/channel use) results for the artificial noise approach with uniform input. $SNR_{AB} = 5\ dB$ and $SNR_{AE} = 0\ dB$. Channel coefficients are $g_{AB} = [0.6320,\ 0.7750]$ and $g_{AE} = [-0.6803,\ 0.7330]$.

AN power ratio (%)	R_s	I_{AB}	I_{AE}
0	0.2972	0.9626	0.6654
10	0.3648	0.9340	0.5692
20	0.4103	0.8933	0.4830
35	0.4380	0.8111	0.3731
50	0.4262	0.7034	0.2772
80	0.2835	0.3878	0.1043

3.3.3 Detailed Numerical Examples

We provide numerical examples for the iterative optimization approach of [22], the proposed PSD based optimization, and the AN-aided transmission approaches. We consider both the main CSI and full CSI scenarios.

a) Iterative Optimization Approach with Markov Inputs

We provide numerical examples for the iterative optimization approach of [22], given in Algorithm 6. We assume that $SNR_{AB} = 0\ dB$ and $SNR_{AE} = -5\ dB$. BPSK is used. Markov inputs order of 1 are selected to reduce the computational complexity.

For the first example, the channel coefficients are

$$g_{AB} = [-0.10 - 0.05j,\ 0.78 + 0.53j,\ -0.11 + 0.30j],$$

$$g_{AE} = [0.76 + 0.25j,\ -0.49 - 0.26j,\ -0.15 + 0.17j].$$

The results are provided in Table 3.3. Three different scenarios are compared with the corresponding information and secrecy rates. It can be observed that a suitable Markov input distribution improves the secrecy rate. Furthermore, the eavesdropper's CSI at the transmitter is clearly beneficial. Optimization with only main CSI maximized the main channel information rate while increasing Eve's information rate unintentionally. On the contrary, optimization with full CSI focuses on the difference between the main channel and the eavesdropper's channels resulting in improved rates.

For the second example, the channel coefficients are chosen as

$$g_{AB} = [0.02 - 0.64j,\ 0.06 - 0.46j,\ 0.52 - 0.33j],$$

$$g_{AE} = [-0.67 - 0.08j,\ -0.62 - 0.07j,\ -0.38 - 0.07j].$$

The results are provided in Table 3.4. For the full CSI case, we observe that the use of uniform input distribution results in higher secrecy rates than the use of Markov input distribution obtained by the iterative approach. We attribute this to the convergence of the iterative algorithm to a local optimum. Actually, one may initialize the input distribution of the iterative algorithm to a uniform input distribution so that such a behavior is not obtained.

Table 3.3: Secrecy and information rate results for the iterative optimization approach with Markov inputs. $SNR_{AB} = 0\ dB$ and $SNR_{AE} = -5\ dB$. Channel coefficients are $g_{AB} = [-0.10 - 0.05j,\ 0.78 + 0.53j,\ -0.11 + 0.30j]$ and $g_{AE} = [0.76 + 0.25j,\ -0.49 - 0.26j,\ -0.15 + 0.17j]$.

Scenarios	Rates (in bits/channel use)		
	R_s	I_{AB}	I_{AE}
Uniform Input	0.3859	0.7210	0.3351
Iterative Optimization (only main CSI)	0.3921	0.7228	0.3307
Iterative Optimization (full CSI)	0.4113	0.6804	0.2691

Table 3.4: Secrecy and information rate results for the iterative optimization approach with Markov inputs. $SNR_{AB} = 0\ dB$ and $SNR_{AE} = -5\ dB$. Channel coefficients are $g_{AB} = [0.02-0.64j,\ 0.06-0.46j,\ 0.52-0.33j]$ and $g_{AE} = [-0.67-0.08j,\ -0.62 - 0.07j,\ -0.38 - 0.07j]$.

Scenarios	Rates (in bits/channel use)		
	R_s	I_{AB}	I_{AE}
Uniform Input	0.3702	0.6748	0.3046
Iterative Optimization (only main CSI)	0.3564	0.6822	0.3258
Iterative Optimization (full CSI)	0.3572	0.6816	0.3244

b) The PSD Based Approach

We now provide numerical examples for Algorithm 7 under the assumptions that $SNR_{AB} = 0\ dB$, $SNR_{AE} = -5\ dB$, and BPSK is used. Markov inputs of order 1 are employed. Both full CSI and only main CSI cases are studied using a codebook of size $|C| = 1000$.

For the first example, the channel coefficients are

$$g_{AB} = [0.36 - 0.74j,\ 0.11 + 0.34j, 0.23 + 0.37j],$$

$$g_{AE} = [0.52 + 0.59j,\ 0.44 + 0.17j,\ 0.25 - 0.32j].$$

The achievable rate results are provided in Table 3.5. It is observed the PSD based approach increases the secrecy rates compared to the uniform input distribution. For main CSI-only case, the PSD based approach increases the secrecy rate by decreasing Eve's rate, however, this behavior is not universal as it depends on the exact channel characteristics. For the full CSI case, the algorithm works better.

While Bob's information rate decreases, Eve's information rate decreases more dramatically, which results in higher secrecy rates than the one with uniform input distributions.

Table 3.5: Secrecy and information rate results for the PSD based approach with Markov inputs. $SNR_{AB} = 0\ dB$ and $SNR_{AE} = -5\ dB$. Channel coefficients are $g_{AB} = [0.36 - 0.74j,\ 0.11 + 0.34j, 0.23 + 0.37j]$ and $g_{AE} = [0.52 + 0.59j,\ 0.44 + 0.17j,\ 0.25 - 0.32j]$.

Scenarios	Rates (in bits/channel use)		
	R_s	I_{AB}	I_{AE}
Uniform Input	0.3616	0.6926	0.3310
PSD Approach (only main CSI)	0.3737	0.6940	0.3203
PSD Approach (full CSI)	0.3803	0.6880	0.3077

As a second example, we use the channels

$$g_{AB} = [-0.31 + 0.54j,\ -0.27 - 0.06j,\ 0.64 - 0.35j],$$

$$g_{AE} = [-0.21 + 0.13j,\ 0.36 - 0.17j,\ -0.28 + 0.84j].$$

If we examine the achievable rate results in Table 3.6, it can be seen that the PSD based approach with only main CSI performs better than the one with full CSI. This is attributed to the fact that the algorithm for matching the PSDs are ad-hoc, and the resulting solutions are suboptimal. Moreover, uniform input distribution is more beneficial than the Markov inputs provided by the PSD based approach, hence uniform input distribution is preferable for this channel realizations.

Table 3.6: Secrecy and information rate results for the PSD based approach with Markov inputs. $SNR_{AB} = 0\ dB$ and $SNR_{AE} = -5\ dB$. Channel coefficients are $g_{AB} = [-0.31 + 0.54j,\ -0.27 - 0.06j,\ 0.64 - 0.35j]$ and $g_{AE} = [-0.21 + 0.13j,\ 0.36 - 0.17j,\ -0.28 + 0.84j]$.

Scenarios	Rates (in bits/channel use)		
	R_s	I_{AB}	I_{AE}
Uniform Input	0.3570	0.6872	0.3302
PSD Approach (only main CSI)	0.3429	0.6883	0.3454
PSD Approach (full CSI)	0.3551	0.6886	0.3335

c) Comparison of Iterative and PSD Based Solutions

We provide numerical examples to compare the performance of the proposed algorithms with Markov inputs. We use BPSK inputs and a codebook of size 1000. We assume that $SNR_{AB} = 0\ dB$ and $SNR_{AE} = -5\ dB$. Moreover, the main and eavesdropper's CSI are known at the transmitter.

For the first example, channel coefficients are

$$g_{AB} = [-0.08 - 0.71j,\ 0.38 + 0.39j,\ -0.42 + 0.17j],$$

$$g_{AE} = [0.09 - 0.84j,\ -0.10 - 0.49j,\ -0.06 + 0.18j].$$

The results are provided in Table 3.7. It is observed that the PSD based approach outperforms the iterative optimization based approach. As a result, for this specific ISI channel, it is better to use the newly proposed algorithm for these SNR values.

Table 3.7: Secrecy rate results for the comparison of iterative optimization and the PSD based approach with Markov inputs. $SNR_{AB} = 0\ dB$ and $SNR_{AE} = -5\ dB$. Channel coefficients are $g_{AB} = [-0.08-0.71j,\ 0.38+0.39j,\ -0.42+0.17j]$ and $g_{AE} = [0.09 - 0.84j,\ -0.10 - 0.49j,\ -0.06 + 0.18j]$.

Scenarios	Rates (in bits/channel use)		
	R_s	I_{AB}	I_{AE}
Uniform Input	0.3471	0.6841	0.3370
Iterative Optimization (full CSI)	0.3771	0.6945	0.3174
PSD Approach (full CSI)	0.3961	0.6703	0.2742

For the second example, we specify the channel coefficients as

$$g_{AB} = [-0.64 + 0.53j,\ 0.06 - 0.42j,\ 0.23 - 0.31j],$$

$$g_{AE} = [0.14 + 0.75j,\ -0.15 + 0.38j,\ -0.37 + 0.34j].$$

By looking the results in Table 3.8, it can be said that the performance of the PSD based approach is not as good as the iterative optimization based approach. All in all, it is clear that our algorithm can be beneficial for some scenarios while the iterative optimization algorithm offers higher secrecy rates for others. On the

other hand, the PSD based solution is significantly less complex, hence it may be preferable.

Table 3.8: Secrecy rate results for the comparison of iterative optimization and the PSD based approach with Markov inputs. $SNR_{AB} = 0\ dB$ and $SNR_{AE} = -5\ dB$. Channel coefficients are $g_{AB} = [-0.64 + 0.53j,\ 0.06 - 0.42j,\ 0.23 - 0.31j]$ and $g_{AE} = [0.14 + 0.75j,\ -0.15 + 0.38j,\ -0.37 + 0.34j]$.

Scenarios	Rates (in bits/channel use)		
	R_s	I_{AB}	I_{AE}
Uniform Input	0.3735	0.7017	0.3282
Iterative Optimization (full CSI)	0.4069	0.6817	0.2748
PSD Approach (full CSI)	0.3849	0.7001	0.3152

d) Artificial Noise Aided Transmission with Uniform Inputs

We now provide a numerical example to illustrate the performance of the AN-aided transmission scheme. A BPSK alphabet with uniform distribution is used as the channel input. The channel coefficients are $g_{AB} = [0.6320,\ 0.7750]$ and $g_{AE} = [-0.6803,\ 0.7330]$. We set $SNR_{AB} = 5\ dB$ and calculate the achievable secrecy rates for different SNR_{AE} values and AN power ratios as provided in Figure 3.11. The first observation is that AN injection increases the secrecy rates compared to the case without AN. The increase in secrecy rate is impressive especially for high SNR_{AE} values. Secondly, the AN power ratio is critical to maximize the achievable secrecy rates. We observe that the optimal AN power ratio increases by increasing SNR_{AE}. This implies that the importance of AN increases when the eavesdropper becomes more powerful. On the other hand, it is better to use much of the power for the message transmission when the SNR_{AE} is low. This observation is in line with the results in [13] where it is shown for a MIMO wiretap channel driven by finite inputs that the higher the SNR, the higher should the optimal fraction of power allocated to the AN be.

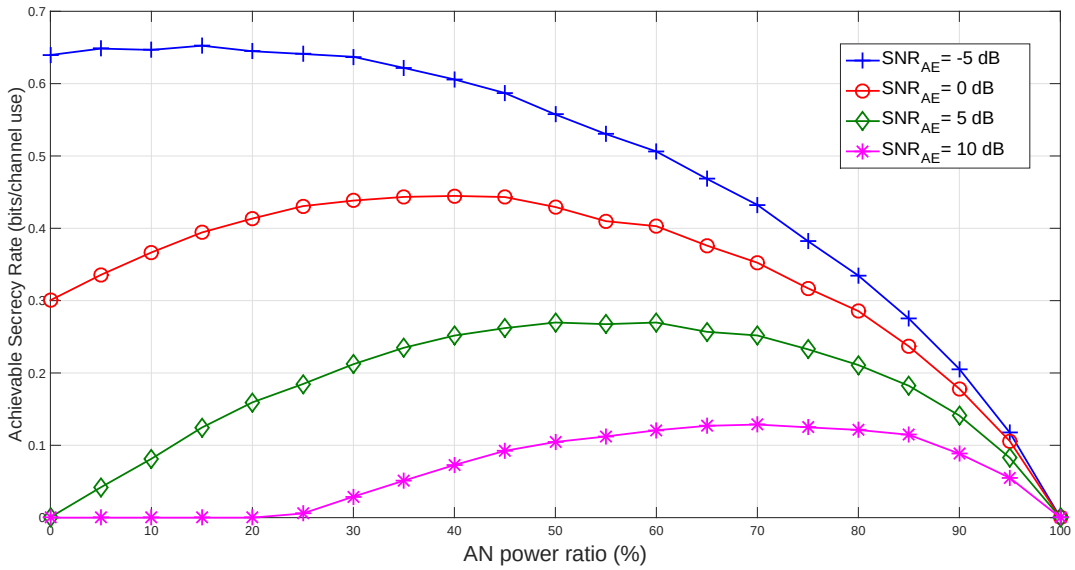

Figure 3.11: Achievable secrecy rate results for different AN power ratios and SNR_{AE} values when $SNR_{AB} = 5\ dB$, $g_{AB} = [0.6320,\ 0.7750]$ and $g_{AE} = [-0.6803,\ 0.7330]$.

e) Comparison of Artificial Noise-Aided Transmission with the Iterative and PSD Optimization Methods

We compare all the transmission strategies for the same channel realizations $g_{AB} = [0.6320,\ 0.7750]$ and $g_{AE} = [-0.6803,\ 0.7330]$. BPSK inputs are used. For the Markov input based strategies, the input order is selected as 1. We use the optimal AN power ratio for each SNR value to maximize the secrecy rates.

For the first example, we set $SNR_{AE} = -5\ dB$ and increase the main channel SNR step by step. If we consider the results in Figure 3.12, it can be said that Markov input based transmission strategies are effective for low SNR values. However, their solutions converge to the one with uniform input distributions when the SNR increases. On the other hand, the AN-aided transmission scheme provides significant secrecy rate increases for high SNRs while not being effective in the low SNR regime.

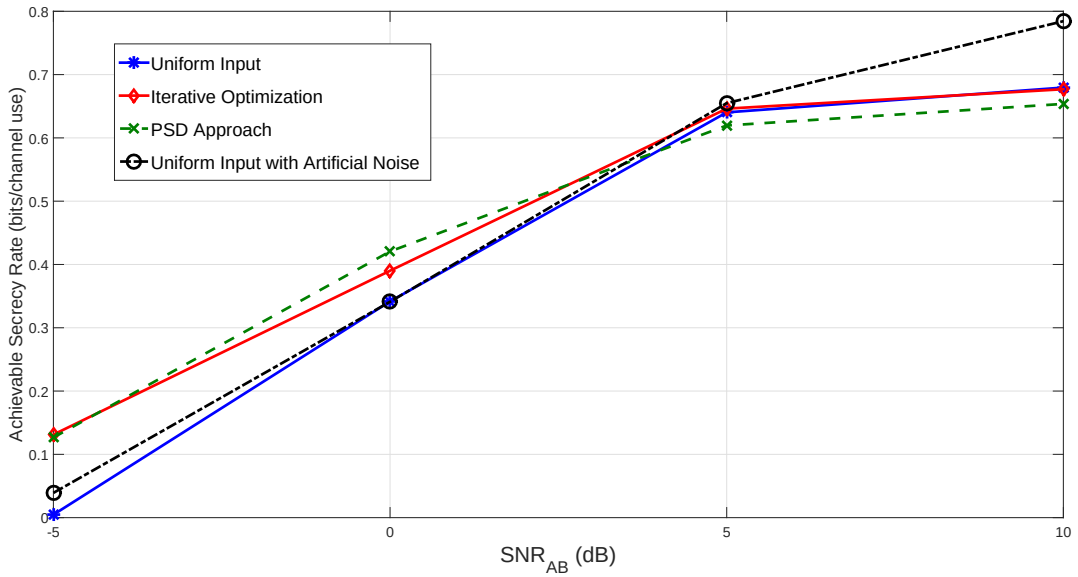

Figure 3.12: Achievable secrecy rate results for different transmission strategies when $SNR_{AE} = -5\ dB$, $g_{AB} = [0.6320,\ 0.7750]$ and $g_{AE} = [-0.6803,\ 0.7330]$.

As a second example, we consider the same setup with different SNR values. The results are provided in Figure 3.13. It can be said that Markov input solutions provide almost the same secrecy rates since their solution converge to the one with uniform input distributions for this example. We observe that the AN-aided transmission scheme significantly increases the secrecy rates. The improvement is further increased for high SNR_{AE} values.

For the third example, we set $SNR_{AB} = 5\ dB$ and change the SNR_{AE} values. In Figure 3.14, we show that the AN-aided transmission scheme increases the secrecy rates considerably when compared to the other strategies. Even when zero secrecy rates are obtained by the Markov input based solutions, the AN solution provides significant (positive) secrecy rates.

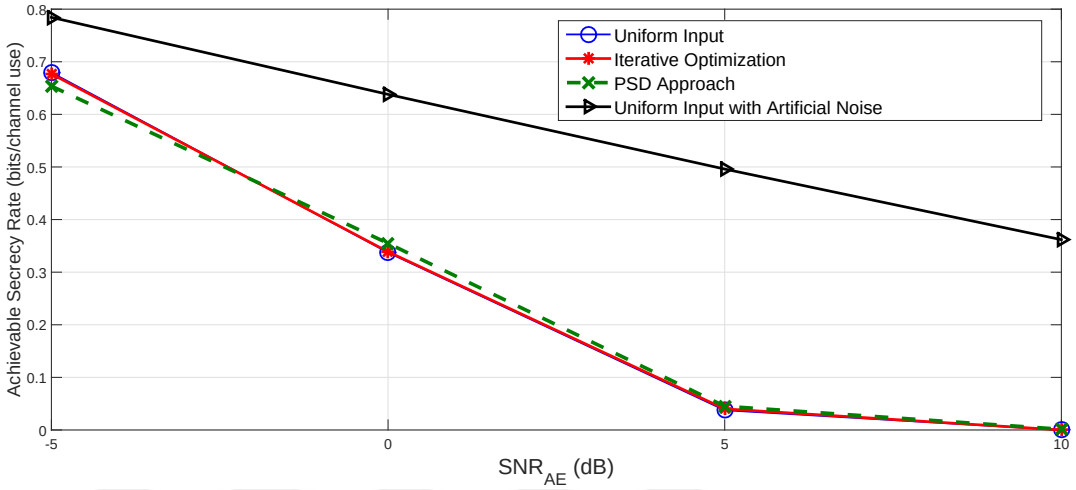

Figure 3.13: Achievable secrecy rate results for different transmission strategies when $SNR_{AB} = 10\ dB$, $g_{AB} = [0.6320,\ 0.7750]$ and $g_{AE} = [-0.6803,\ 0.7330]$.

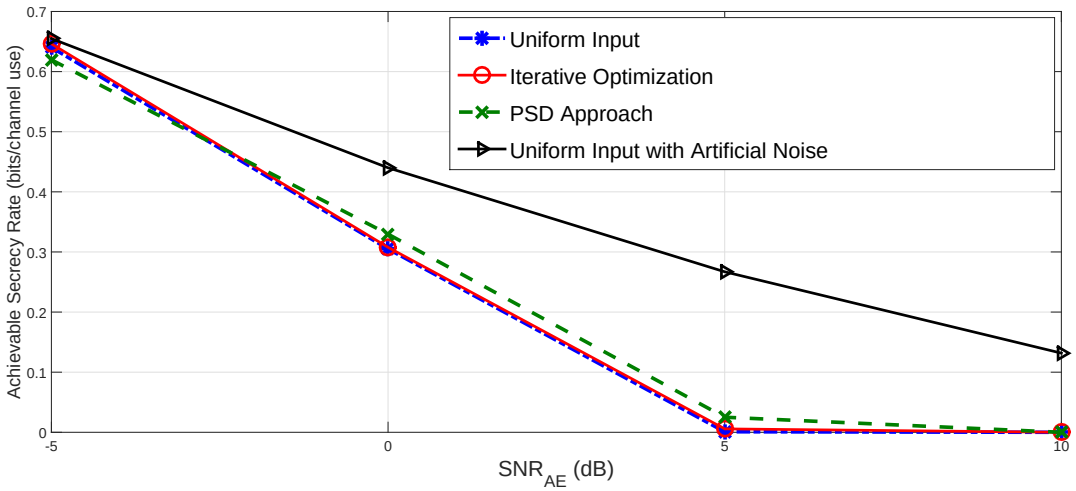

Figure 3.14: Achievable secrecy rate results for different transmission strategies when $SNR_{AB} = 5\ dB$, $g_{AB} = [0.6320,\ 0.7750]$ and $g_{AE} = [-0.6803,\ 0.7330]$.

3.4 Chapter Summary

In this chapter, we first provide standard capacity results for ISI channels, and remark the consequences of constraining to inputs to a finite set. Then, we discuss calculation of information rates with uniform inputs, and describe the maximization of the mutual information with the use of Markov inputs. We describe the existing iterative optimization approach, and propose a PSD based approach by introducing a codebook-based design for the maximization of mutual information. We then extend our discussion to the secrecy capacity of ISI wiretap channels with finite inputs. We also propose injection of AN to increase secrecy rates. Finally, we compare the performance of the existing and proposed algorithms.

Our investigations establish the following results. First of all, ISI channels with finite inputs should be investigated with care due to the saturation of information rates at high SNRs. Secondly, the proposed PSD based solution can be a low-complexity alternative to the existing iterative optimization of the information rates. Furthermore, considering the secrecy rates, the proposed PSD based algorithm can be beneficial for some scenarios while the iterative optimization algorithm provides increased information rates for others. On the other hand, the PSD based solution is significantly less complex, hence it may be preferable. Beyond these solutions, the proposed AN-aided transmission scheme provides secrecy rate increases compared to the PSD based and iterative optimization based solutions, especially, in the high SNR regime for finite input ISI wiretap channels.

Chapter 4

Secrecy Rates of Fading Channels with ISI

In Chapter 3, we considered AWGN channels with a constant attenuation and delay. However, in wireless communication systems, a more accurate model is necessary since transmitted signals are received through multiple paths with different attenuations and delays, and there are time variations, resulting in received signals with random fluctuations due to what is called *fading*. To the best of our knowledge, there are very limited number of studies that consider ISI channels with fading in the context of physical layer security, see [31] for one example. With this motivation, in this chapter, we focus on secrecy rates of ISI fading channels with finite inputs. Particularly, we study two different fading scenarios, namely quasi-static fading for which outage formulations are needed, and ergodic fading channels.

The organization of the chapter as follows. In Section 4.1, we provide the system model for fading wiretap channels with ISI. In Section 4.2, we consider secrecy over quasi-static fading ISI channels, while in Section 4.3, we discuss secrecy over ergodic fading ISI channels. We provide several numerical examples for both fading channels by implementing the transmission strategies in Chapter 3. In Section 4.4, we conclude with a chapter summary.

4.1 System Model for ISI Channels with Fading

The system model of fading wiretap channels with ISI and AWGN can be expressed as

$$\begin{aligned} Y_B(k) &= \sum_{i=0}^{m_{AB}-1} g_{AB}(i)X(k-i) + W_{AB}(k), \\ Y_E(k) &= \sum_{i=0}^{m_{AE}-1} g_{AE}(i)X(k-i) + W_{AE}(k), \end{aligned} \tag{4.1}$$

where $X(k)$ is the input at time instant $k \in \mathbb{Z}$. The input alphabet is constrained to a finite set, specifically, to BPSK for the examples throughout the chapter. $Y_B(k)$ and $Y_E(k)$ represent the channel outputs at Bob and Eve, respectively. For simplicity, we assume that $g_{AB}(i)$ and $g_{AE}(i)$ are (real) Gaussian random variables with zero mean and their variances are determined according to the corresponding multipath delay profiles.[1] m_{AB} and m_{AE} are the number of propagation paths over the main and the eavesdropper's channels, respectively. The noise terms W_{AB} and W_{AE} are assumed to be (real) Gaussian random variables with variances $N_{AB}/2$ and $N_{AE}/2$, respectively. We define the SNRs as

$$SNR_{AB} = \frac{E_s \ \mathbf{E}[\|g_{AB}\|^2]}{N_{AB}}, \tag{4.2}$$

$$SNR_{AE} = \frac{E_s \ \mathbf{E}[\|g_{AE}\|^2]}{N_{AE}}, \tag{4.3}$$

where E_s is the symbol energy constraint. The channel coefficients are normalized so that $\mathbf{E}[\|g_{AB}\|^2] = 1$ and $\mathbf{E}[\|g_{AE}\|^2] = 1$.

We now consider two different slow-fading scenarios, namely quasi-static and ergodic fading channels.

[1] In reality, for bandpass communication systems, these would be complex quantities. For simplicity, however, we take them as real throughout this chapter. The general methodology will work for the complex case in exactly the same way.

4.2 Secrecy over Quasi-static Fading ISI Channels

For quasi-static fading channels, the codeword durations are smaller than coherence time of the channel [23,24]. This results in constant channel coefficients over the entire symbol transmission. In this case, secrecy capacity is zero in the Shannon sense, because secure communication cannot be guaranteed for any positive rate. Hence, a more convenient performance metric is the outage secrecy rate, which is the achievable secrecy rate for a given positive error probability [24].

The outage probability is given by

$$P_{out}(\tau) = Pr(R_s < \tau) \tag{4.4}$$

where τ is the minimum desired secrecy rate, and R_s is the instantaneous secrecy rate which can be estimated by the techniques in Section 3.3.

4.2.1 Numerical Examples

Throughout the simulations, we generate 1000 pairs of 3-tap channels and evaluate the secrecy outage rates by the use of (4.4). We use BPSK inputs, and assume that $\tau = 0.1$ *bits/channel use*. In other words, system is in outage for the secrecy rates below 0.1 *bits/channel use*. All the Markov input based approaches in the previous chapter are studied for the same channel realizations. We take the codebook size $|C| = 1000$ and Markov input order $V = 1$. Furthermore, we assume that the main and eavesdropper's CSI are known at the transmitter. Multipath delay profiles of the channels are provided in Figure 4.1.

For the first example, we let $SNR_{AE} = -5$ *dB* and sweep the main channel SNR value from -10 *dB* to 0 *dB*. The results are provided in Figure 4.2. We observe that the use of suitable Markov input distributions improve the secrecy

rates by decreasing the probability of outage. Among the proposed approaches, it is better to employ the iterative optimization approach since it outperforms the newly proposed PSD approach in Chapter 3. On the other hand, the PSD based solution is significantly less complex.

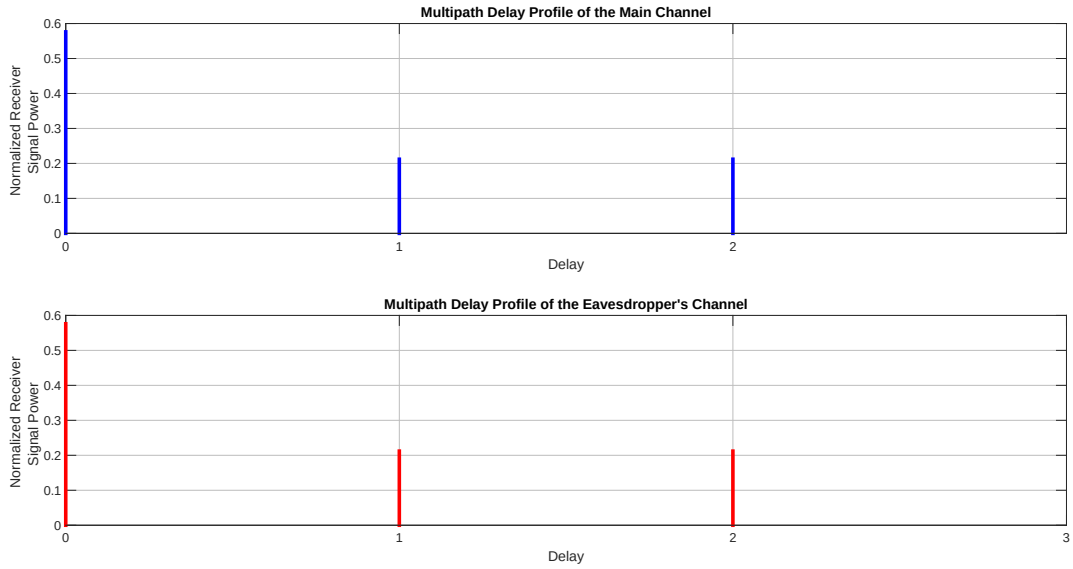

Figure 4.1: Multipath delay profiles of the considered 3-tap ISI channels.

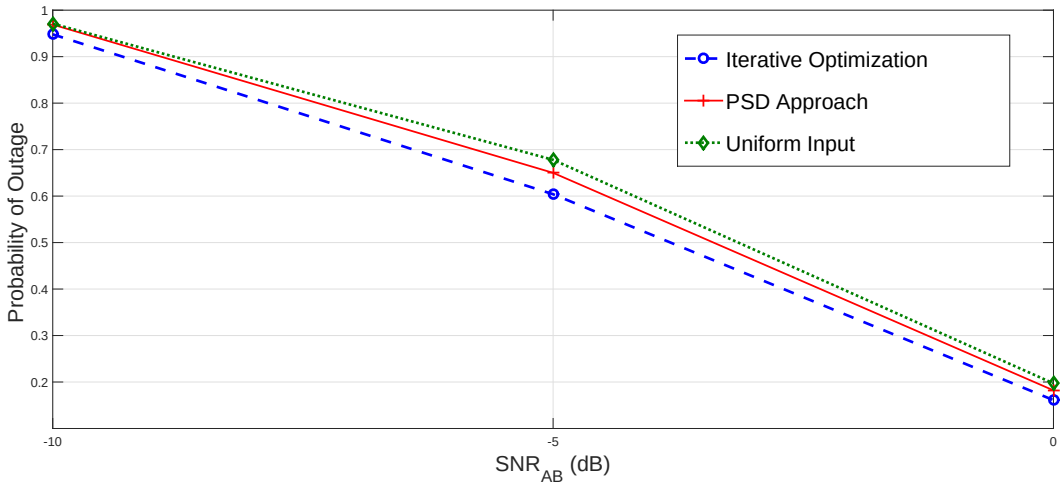

Figure 4.2: Probability of outage results for ISI fading channels when $SNR_{AE} = -5\ dB$ and $\tau = 0.1\ bits/channel\ use$. Multipath delay profiles of the channels are provided in Figure 4.3.

For the second example, we let $SNR_{AE} = 0\ dB$ and sweep the main channel SNR value from $-5\ dB$ to $5\ dB$. The results are provided in Table 4.1. We observe that the conclusions of the previous example are still valid for low SNR values. However, performance of the PSD based approach is worse than the one with uniform input distribution for high SNRs. For example, when $SNR_{AB} = 5\ dB$, the use of uniform input distribution outperforms the use of Markov input distribution that is offered by the PSD based approach. Thus, it may be desirable to use the PSD based approach as a low-complexity alternative only for low SNRs.

Table 4.1: Probability of outage results for ISI fading channels when $SNR_{AE} = 0\ dB$ and $\tau = 0.1\ bits/channel\ use$.

Scenarios \ SNR_{AB}	-5 dB	0 dB	5 dB
Uniform Input	0.9320	0.6220	0.2360
Iterative Optimization (full CSI)	0.9160	0.5980	0.2330
PSD Approach (full CSI)	0.9260	0.6220	0.2510

4.2.2 Numerical Examples with Artificial Noise

We now provide numerical examples to demonstrate the performance of the AN-aided transmission scheme for quasi-static fading channels. We set the number of channel realizations to 500. Outage threshold is $\tau = 0.1\ bits/channel\ use$. Markov input based approaches are employed similar to the previous section. For the AN-aided approach, the filter codebook size is 100. We use %25 of the power for AN injection and the rest for the message transmission. Power distributions over the channel coefficients are chosen arbitrarily in each realization with respect to the multipath delay profiles of the channels in Figure 4.3.

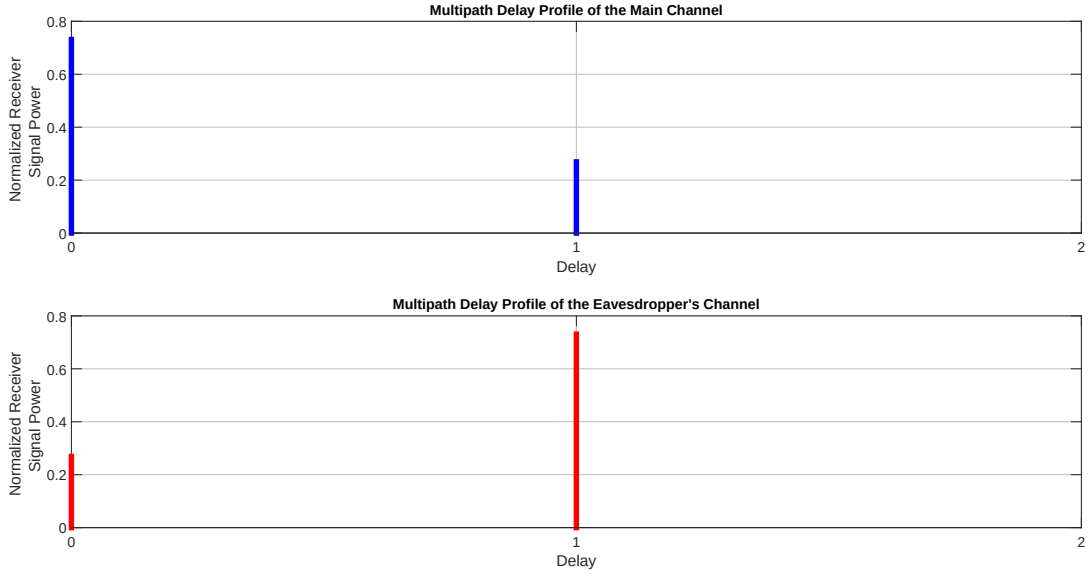

Figure 4.3: Multipath delay profiles of the considered 2-tap ISI channels.

For the first example, we let $SNR_{AE} = 0\ dB$ and sweep the main channel SNR value from $-5\ dB$ to $10\ dB$. We provide the results obtained in Table 4.2. We observe that the AN injection is not beneficial in the low SNR regime, where it is more favorable to spend energy for the message transmission. On the other hand, the AN-aided transmission increases the secrecy for moderate and high SNR values. Furthermore, it can be said that Markov input solutions provide almost the same secrecy rates since their solution converges to the one with uniform input distributions for this example.

As a second example, we provide the results obtained for $SNR_{AE} = 5\ dB$ in Table 4.3. The same observations of the previous example are also valid for this case, however, the AN injection is more beneficial compared to the previous case since Eve is more prone to noise for higher SNRs.

Table 4.2: Probability of outage results for $SNR_{AE} = 0\ dB$.

Scenarios \ SNR_{AB}	-5 dB	0 dB	5 dB	10 dB
Uniform Input	0.7980	0.5680	0.3540	0.2260
Iterative Optimization (only main CSI)	0.7740	0.5520	0.3380	0.2240
Iterative Optimization (full CSI)	0.7780	0.5420	0.3380	0.2160
PSD Approach (only main CSI)	0.7780	0.5620	0.3600	0.2340
PSD Approach (full CSI)	0.7780	0.5640	0.3600	0.2340
AN with Uniform Input (only main CSI)	0.8080	0.5720	0.2980	0.1300

Table 4.3: Probability of outage results for $SNR_{AE} = 5\ dB$

Scenarios \ SNR_{AB}	-5 dB	0 dB	5 dB	10 dB
Uniform Input	0.9100	0.7960	0.6460	0.5560
Iterative Optimization (only main CSI)	0.9060	0.7860	0.6380	0.5560
Iterative Optimization (full CSI)	0.9020	0.7820	0.6320	0.5500
PSD Approach (only main CSI)	0.9140	0.7960	0.6560	0.5760
PSD Approach (full CSI)	0.9100	0.7940	0.6540	0.5680
AN with Uniform Input (only main CSI)	0.9160	0.7700	0.5460	0.3480

4.3 Secrecy over Ergodic Fading ISI Channels

We now consider ergodic fading wiretap channels with ISI where both channels experiencing ergodic fading. In this case, the channel taps remain constant during each coherence interval and change independently from one codeword to the next. Furthermore, the fading coefficients are independent of each other, and we assume that the number of channel use within each coherence interval is large enough to allow random coding arguments so that the results of [25] are valid.

4.3.1 Numerical Examples

We now provide numerical examples to illustrate the performance of the Markov input based transmission strategies for the ergodic fading scenarios. Throughout the simulations, we generate 500 pairs of 2-tap channels and evaluate the ergodic achievable secrecy rates by averaging R_s over these realizations. The codebook size $|C| = 1000$, and the Markov input order $V = 1$. We also let $SNR_{AE} = -5\ dB$ and sweep the main channel SNR value from $-10\ dB$ to $10\ dB$.

For the first example, variances of the channel coefficients are chosen arbitrarily in each realization with respect to the multipath delay profile of the channels in Figure 4.3. The ergodic secrecy rates of all the proposed Markov input based approaches are compared for the same channel realizations, and the results are provided in Table 4.4. Considering the results of the iterative optimization approach, we observe that suitable Markov input distributions improve the ergodic secrecy rates. Furthermore, having the eavesdropper's CSI at the transmitter is beneficial. For the newly proposed PSD based approach, we first observe that its performance is compatible to the other techniques for low SNR values. However, its performance degrades drastically with increasing SNRs. Moreover, the eavesdropper's CSI is not utilized in a positive manner. Despite these, it can be used as a less-complexity alternative method, especially, for low SNR values.

Table 4.4: Ergodic secrecy rates (in bits/channel use) with the use of Markov inputs for 2-tap channels when $SNR_{AE} = -5\ dB$.

Scenarios \ SNR_{AB}	-10 dB	-5 dB	0 dB	5 dB	10 dB
Uniform Input	0.0117	0.0883	0.3095	0.5708	0.6584
Iterative Optimization (only main CSI)	0.0157	0.0959	0.3158	0.5726	0.6593
Iterative Optimization (full CSI)	0.0167	0.0978	0.3191	0.5748	0.6625
PSD Approach (only main CSI)	0.0142	0.0925	0.2984	0.5367	0.6157
PSD Approach (full CSI)	0.0136	0.0920	0.2968	0.5326	0.6082

We consider 3-tap channels for the second example, where multipath delay profile of the channels are chosen as in Figure 4.1. Ergodic secrecy rates of all the Markov input based approaches are provided in Table 4.5. The conclusions for the

previous example are also valid for this specific example with slight differences. The most important difference is that the PSD based approach now utilizes the knowledge of eavesdropper's CSI in a positive manner compared to the 2-tap case. However, the increase in secrecy rates is very small and valid only for low SNRs. Moreover, performance degradation is still observed for PSD based approach with increasing SNRs. As a result, it is better to use PSD based approach only for low SNR values.

Table 4.5: Ergodic secrecy rates (in bits/channel use) with the use of Markov inputs for 3-tap channels when $SNR_{AE} = -5\ dB$.

Scenarios \ SNR_{AB}	-10 dB	-5 dB	0 dB	5 dB	10 dB
Uniform Input	0.0068	0.0912	0.3322	0.5885	0.6735
Iterative Optimization (only main CSI)	0.0117	0.1052	0.3415	0.5909	0.6736
Iterative Optimization (full CSI)	0.0114	0.1074	0.3448	0.5940	0.6771
PSD Approach (only main CSI)	0.0089	0.0942	0.3125	0.5383	0.6179
PSD Approach (full CSI)	0.0092	0.0951	0.3120	0.5341	0.6104

4.3.2 Numerical Examples with Artificial Noise

We now provide numerical examples to illustrate the performance of the AN-aided transmission scheme for ergodic fading channels. We set the number of channel realizations to 500. Markov input based approaches are employed similar to the previous section. For the AN-aided approach, the filter codebook size is 100. We use %25 of the power for AN injection and the rest for the message transmission. The multipath delay profiles of the channels are as given in Figure 4.3.

For the first example, we let $SNR_{AE} = 0\ dB$ and sweep the main channel SNR value from $-5\ dB$ to $10\ dB$. We provide the results in Table 4.6. We observe that AN injection increases the secrecy rates, especially, for high SNR values. On the other hand, the other methods are beneficial in the low SNR regime. We can say that our low-complexity PSD based approach can be an alternative for the low SNR regime. In addition, we illustrate that having the eavesdropper's CSI at the transmitter is beneficial to increase secrecy rates.

For the second example, we increase the SNR_{AE} to 5 dB. The results are provided in Table 4.7. The same conclusions for the previous example are also valid for this case. However, the AN-aided approach contributes more compared to the previous case since Eve is more prone to noise in higher SNRs.

Table 4.6: Ergodic secrecy rates (in bits/channel use) with the use of AN for $SNR_{AE} = 0$ dB

Scenarios \ SNR_{AB}	-5 dB	0 dB	5 dB	10 dB
Uniform Input	0.0621	0.1784	0.3263	0.4217
Iterative Optimization (only main CSI)	0.0692	0.1863	0.3302	0.4232
Iterative Optimization (full CSI)	0.0701	0.1885	0.3331	0.4262
PSD Approach (only main CSI)	0.0619	0.1663	0.2981	0.3865
PSD Approach (full CSI)	0.0630	0.1692	0.3040	0.3941
AN with Uniform Input (only main CSI)	0.0524	0.1649	0.3396	0.4823

Table 4.7: Ergodic secrecy rates (in bits/channel use) with the use of AN for $SNR_{AE} = 5$ dB.

Scenarios \ SNR_{AB}	-5 dB	0 dB	5 dB	10 dB
Uniform Input	0.0245	0.0827	0.1594	0.2143
Iterative Optimization (only main CSI)	0.0268	0.0856	0.1617	0.2151
Iterative Optimization (full CSI)	0.0278	0.0868	0.1640	0.2175
PSD Approach (only main CSI)	0.0250	0.0767	0.1455	0.1962
PSD Approach (full CSI)	0.0254	0.0783	0.1492	0.2008
AN with Uniform Input (only main CSI)	0.0213	0.0808	0.1894	0.2979

4.4 Chapter Summary

In this chapter, we provide secrecy rates of quasi-static and ergodic fading channels with ISI under finite input constraints. We illustrate our results via several examples. We observe that the newly proposed PSD based approach provides a low-complexity solution compared to existing iterative optimization approach for low SNR values. Furthermore, we show that AN injection increases the secrecy

rates significantly for moderate and high SNRs, while Markov input distribution based approaches are not beneficial for these SNR ranges (at least for the examples considered). In addition, we demonstrate that the availability of eavesdropper's CSI at the transmitter is beneficial in terms of the ergodic secrecy rates. However, the newly proposed PSD based approach does not put this to good use, calling for a more reliable algorithm for the case with full CSI.

Chapter 5

Conclusions and Future Work

We have studied physical layer security over ISI channels both with constant and fading coefficients with inputs selected from finite signal constellations.

We first showed that channels with finite inputs should be investigated with care due to the saturation of information rates at high SNRs. Then, we discussed calculation of information rates with uniform inputs, and described the maximization of the mutual information with the use of Markov inputs. Particularly, we described an existing iterative optimization method, and proposed a PSD based approach by introducing a codebook-based design for the optimization of Markov transition probabilities. We demonstrated that the newly proposed PSD based solution can be a low-complexity alternative to the existing iterative optimization solution for the maximization of information rates. Secondly, we extended our discussion to the secrecy capacity of ISI wiretap channels with finite inputs, and showed that the proposed PSD based algorithm can be beneficial for some scenarios while the iterative optimization algorithm is more preferable in others. On the other hand, the PSD based solution is significantly less complex. We also proposed injection of AN to increase secrecy rates, and showed that the proposed AN-aided transmission scheme provides higher secrecy rates compared to the PSD based and the iterative optimization based solutions, especially, in the high SNR regime.

We also considered secrecy rates of quasi-static and ergodic fading channels with ISI under finite input constraints, and provided several numerical examples. We revealed that the proposed low complexity approach undergoes a minimal loss with respect to the existing iterative algorithm while offering a considerably reduced complexity for low SNRs. Furthermore, we showed that the AN-aided transmission increases the secrecy rates significantly for moderate and high SNRs, while Markov input distribution based approaches are not very beneficial. In addition, we demonstrated that the availability of eavesdropper's CSI at the transmitter is beneficial in terms of the ergodic secrecy rates. However, we showed that the newly proposed PSD based approach does not utilize the availability of eavesdropper's CSI fully.

As a further work, one may consider the following research directions. Firstly, the considered approaches do not take the SNR values into account while applying spectral shaping. Thus, one can possibly obtain improved results by utilizing the SNR values within the algorithms as well. Secondly, AN injection was applied based only on the main channel CSI, however, one can include eavesdropper's CSI if it exists at the transmitter as well. Furthermore, AN was injected with a fixed AN power ratio in fading scenarios. On the other hand, the use of optimal AN power ratios can be utilized with respect to the SNR values and specific channel realizations. Lastly, all the considered setups consider single-input single-output scenarios, however, it is possible to increase the number of antennas or introduce more legitimate users or eavesdroppers into the system model and develop new results.

Bibliography

[1] C. E. Shannon, "Communication theory of secrecy systems," *The Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] J. L. Massey, "An introduction to contemporary cryptology," *Proc. IEEE*, vol. 76, no. 5, pp. 533–549, May 1988.

[3] B. Schneier, "Cryptographic design vulnerabilities," *Computer*, vol. 31, no. 9, pp. 29–33, Sep. 1998.

[4] A. Biryukov, A. Shamir, and D. Wagner, *Real Time Cryptanalysis of A5/1 on a PC.* Berlin, Heidelberg: Springer, 2001, pp. 1–18.

[5] A. D. Wyner, "The wire-tap channel," *The Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[6] C. E. Shannon, "A mathematical theory of communication," *The Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul. 1948.

[7] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[8] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[9] G. D. Raghava and B. S. Rajan, "Secrecy capacity of the Gaussian wire-tap channel with finite complex constellation input," [Online]. Available: http://arxiv.org/abs/1010.1163

[10] M. R. D. Rodrigues, A. Somekh-Baruch, and M. Bloch, "On Gaussian wiretap channels with M-PAM inputs," in *European Wireless Conf.*, Lucca, Italy Apr. 2010, pp. 774–781.

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

[12] Y. Wu, C. Xiao, Z. Ding, X. Gao, and S. Jin, "Linear precoding for finite-alphabet signaling over MIMOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2599–2612, Jul. 2012.

[13] S. R. Aghdam and T. M. Duman, "Low complexity precoding for MIMOME wiretap channels based on cut-off rate," in *Proc. IEEE Int. Symp. Infor. Theory*, Barcelona, Spain, Jul. 2016, pp. 2988–2992.

[14] W. Hirt and J. L. Massey, "Capacity of the discrete-time Gaussian channel with intersymbol interference," *IEEE Trans. Inf. Theory*, vol. 34, no. 3, pp. 380–388, May 1988.

[15] D. Arnold and H. A. Loeliger, "On the information rate of binary-input channels with memory," in *IEEE Int. Conf. Commun.*, Helsinki, Finland, vol. 9, 2001, pp. 2692–2695.

[16] L. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Trans. Inf. Theory*, vol. 20, no. 2, pp. 284–287, Mar. 1974.

[17] A. Kavcic, "On the capacity of Markov sources over noisy channels," in *IEEE Global Telecommun. Conf.*, San Antonio, TX, vol. 5, 2001, pp. 2997–3001.

[18] R. Blahut, "Computation of channel capacity and rate-distortion functions," *IEEE Trans. Inf. Theory*, vol. 18, no. 4, pp. 460–473, Jul. 1972.

[19] S. Arimoto, "An algorithm for computing the capacity of arbitrary discrete memoryless channels," *IEEE Trans. Inf. Theory*, vol. 18, no. 1, pp. 14–20, Jan. 1972.

[20] D. N. Doan and K. R. Narayanan, "Design of good low-rate coding schemes for ISI channels based on spectral shaping," *IEEE Trans. Wireless Commun.*, vol. 4, no. 5, pp. 2309–2317, Sep. 2005.

[21] D. Kumar, "Optimal finite alphabet sources over partial response channels," M.S. Thesis, Dept. Elect. Eng., Texas A&M Univ., College Station, TX, 2003.

[22] Y. Sankarasubramaniam, A. Thangaraj, and K. Viswanathan, "Finite-state wiretap channels: Secrecy under memory constraints," in *IEEE Inform. Theory Workshop*, Volos, Greece, Oct. 2009, pp. 115–119.

[23] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. Inform. Theory*, Adelaide, Australia, Sep. 2005, pp. 2152–2155.

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

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

[26] R. Gallager, Information Theory and Reliable Communication. New York, NY: Wiley, 1968.

[27] T. M. Cover and J. A. Thomas, Elements of Information Theory, 2nd ed. Hoboken, NJ: Wiley, 2006.

[28] T. M. Duman and A. Ghrayeb, *Coding for MIMO Communication Systems*. West Sussex, UK: Wiley, 2007.

[29] B. Vasic and E. M. Kurtas, Coding and Signal Processing for Magnetic Recording Systems. Boca Raton, FL: CRC, 2004, ch. 12.

[30] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Veh. Technol. Conf.*, Dallas, TX, vol. 3, Sep. 2005, pp. 1906–1910.

[31] K. Ayhan, "Physical layer security over frequency selective fading channels," M.S. Thesis, Dept. Elect. and Electronics Eng., Bilkent Univ., Ankara, Turkey, 2016.