ON THE SECRECY CAPACITY OF FADING GAUSSIAN WIRE-TAP CHANNEL

A Thesis
Submitted to the Graduate Faculty
of the
North Dakota State University
of Agriculture and Applied Science

By

Mohammad Kamal Hossan

In Partial Fulfillment of the Requirements
for the Degree of
MASTER OF SCIENCE

Major Department:
Electrical and Computer Engineering

November 2014

Fargo, North Dakota

North Dakota State University
Graduate School

Title

On the Secrecy Capacity of Fading Gaussian Wire-tap Channel

By

Mohammad Kamal Hossan

The Supervisory Committee certifies that this ***disquisition*** complies with North Dakota State University's regulations and meets the accepted standards for the degree of

MASTER OF SCIENCE

SUPERVISORY COMMITTEE:

Dr. Sanjay Karmakar
Chair

Dr. Rajesh Kavasseri

Dr. Ivan T. Lima, Jr.

Dr. Indranil Sengupta

Approved:

11/18/2014 — Date

Dr. Scott C. Smith — Department Chair

ABSTRACT

We consider the so called "wire-tap channel", where a transmitter sends secret information to its receiver in the presence of an eavesdropping receiver with similar signal processing capability as the desired receiver. It is assumed that all the communication links have time varying signal strengths[1] which are only known at the corresponding receivers and not at the transmitter. In this thesis, we address the problem of characterizing the maximum possible rate of secret and reliable information transmission on such a wire-tap channel. We first characterize the secrecy capacity of a corresponding layered abstraction of the channel, and then, we derive an upper bound to the secrecy capacity of the fading wire-tap channel. Finally, we show that the wireless channels in the urban and most of the rural environments belong to a class of channels called *Stochastically degraded channels*, for which we have characterized the exact capacity in this thesis work.

[1]Such communication links are called *fading channels*.

ACKNOWLEDGMENTS

Firstly I would like to express my humble gratitude to my Almighty Allah for His endless blessings on me.

This research work would not have been possible without the guidance, support, motivation that I got from my adviser Dr. Sanjay Karmakar. He provided me immense time explaining information theory in order to understand the research problem in an inside out way. Whenever I got stuck at some point with my research problem, Dr. Karmakar always showed the thread that I should pursue to make progress. I want to thank him from the core of my heart.

I am grateful to Dr. Rajesh Kavasseri, Dr. Ivan T. Lima, Jr., and Dr. Indranil Sengupta to give me inspiration and guidance to achieve my goal.

Finally, I would like to express a special thanks to my family and friends for their support and inspiration.

DEDICATION

To my wife Taslima, and my daughter Laiba.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1. INTRODUCTION

In any form of communication, ranging from the primitive hand-waving signaling to the state of the art wireless communications, the main purpose is to exchange information among interested parties. Better communication system ensures faster information transfer rate with better reliability. Before going into detail discussion of how the rate of information transfer can be maximized, it is necessary to answer the fundamental question first: what is information and how can we measure it?

Intuitively, any outcome that is deterministic does not contain any information. For example, the result of an election where only one candidate is competing has no uncertainty, because anybody can surely predict who is going to win beforehand. Therefore, reveling the fact that the only candidate won the election does not provide any information. On the other hand, consider the toss of a fair coin, the outcome could not be known with certainty before the coin is tossed. As a result, knowing the outcome of the coin reveal some information about the random experiment of tossing the coin. From information transmission point of view, revealing some fact to a person who already knows it, is pointless. Hence, information is always accompanied by some amount of uncertainty to the event of interest.

The best way to model uncertainty and thus information is through Random Variables (RV). Information content of a random variable is related to the amount of the uncertainty associated with that RV. We know that a discrete RV is defined by its Probability Mass Function (PMF), whereas a continuous RV is characterized by its Probability Distribution Function (PDF). So, its not unreasonable to predict that the information content of a RV should be a function of the PMF or PDF of the RV.

Let us call the random variable representing the outcome of tossing a coin Q. The outcome has two possibilities: 1) Head and 2) Tail, with probabilities p and $(1-p)$, respectively. The outcome of the random experiment is most uncertain when

$p = \frac{1}{2}$, and most certain when $p = 0$ or $p = 1$. Hence, from our intuition, it follows that if the random variable Q is equiprobable, the information content of the RV should be maximum, and the information content reduces to zero when the RV assumes one of the possibilities with certainty. A set of such intuitive guidelines are first converted into mathematical constraints which finally yields the mathematical expression for information of a random variable.

In information theory, the information content of a RV is represented by the quantity called *entropy*. Although information theoretic entropy has a quite different definition than that of the thermodynamic entropy, both have similarity in terms of disorderness/randomness of the system. The thermodynamic entropy is a measure of the disorderliness; consequently the thermodynamic entropy of a system increases as the chaos increases. Similarly, the information theoretic-entropy is the measure of the uncertainty the system, and the entropy increases as the system gets more random. In what follows, we shall define the information-theoretic entropy and verify that many properties of entropy corroborates our intuitive idea of a measure of information. The definitions and/or notations of the information-theoretic terms those we state in this chapter are taken from [1].

1.1. Entropy

We first introduce the concept of *entropy*, which is a measure of the uncertainty of a random variable. Let X be a discrete random variable with alphabet $\mathscr{X}$ and its PMF be denoted by $p(x) = Pr\{X = x\},\ x\epsilon\mathscr{X}$. Without loss of generality, we shall assume that $\mathscr{X}$ contains only those realizations of X where the PMF is strictly positive.

Definition 1. *The entropy $H(X)$ of a discrete random variable X is defined by*

$$H(X) = -\sum_{x\epsilon\mathscr{X}} p(x)\log p(x). \tag{1.1}$$

Since the entropy function is not dependent on the exact realizations of the random variable and is a function of the PMF, the entropy is often denoted by $H(p)$, as well. Hereafter, we shall assume that the logarithm is to the base 2 and the resulting entropy value has a unit of *bits*.If the base of the logarithm is b, we denote the entropy as $H_b(X)$. If the base of the logarithm is e, the entropy is measured in *nats*.

Let us get back to the example of RV the X, where it represents the outcome of tossing a coin. The PMF of X is denoted by $P_X(x)$, where $P_X(heads) = p$ and $P_X(tails) = (1 - p)$.

The entropy of RV X is given by,

$$H(X) = -p \log p - (1 - p) \log(1 - p). \tag{1.2}$$

Let us say $p = 1$. Then the entropy is

$$H(X) = -1 \log 1 - (1 - 1) \log(1 - 1) = 0 - 0 = 0 \quad \text{bits}. \tag{1.3}$$

In (1.3), we have used the fact $0 \log 0 = 0$, which is justified by the slower rate of decay of $\log(x)$ than x as x approaches zero. This result agrees with our intuition of information content. $p = 1$ implies that *heads* appear with certainty, which in turn converts the outcome deterministic with zero information content. Anyone can predict the outcome. It is not surprising that the corresponding entropy is zero as well.

Next, let us set $p = \frac{1}{2}$ to examine the information content of RV X. $p = \frac{1}{2}$ implies the event of getting head or tail are equally probable, hence associated uncertainty is of getting head is maximum. Equivalently,we can say that associated uncertainty is of getting tail is maximum which in turns says that the there is no preference over

choosing the outcome as head or tail. Intuitively, the corresponding entropy which is the measure of the information content of the RV should be the highest.

$$H(X) = -\frac{1}{2}\log\frac{1}{2} - (1-\frac{1}{2})\log(1-\frac{1}{2}) \tag{1.4}$$

$$= \frac{1}{2}\log 2 + \frac{1}{2}\log 2 \tag{1.5}$$

$$= \frac{1}{2} + \frac{1}{2} = 1 \quad \text{bits.} \tag{1.6}$$

Again, from our intuition, to convey the outcome of binary RV X, we should not need more than 1 bit. We can describe the outcome of head as 1 and tail as 0, hence, single bit is enough to describe the information content of RV X. The entropy of the RV X with $p = \frac{1}{2}$ agrees with the notion of the measure of the information.

Definition 2. *The differential entropy $h(X)$ of a continuous random variable X with PDF $f_X(x)$ is defined as*

$$h(X) = -\int_S f_X(x)\log f_X(x)dx. \tag{1.7}$$

where S is the support set of the random variable X.

We shall now define two other entropy terms named *joint entropy* and *conditional entropy* which will appear in this paper quite often.

1.2. Joint Entropy and Conditional Entropy

We defined entropy of a single random variable in the last section. We now extend the definition to a pair of random variables. There is nothing really new in this definition because (X, Y) can be considered to be a single vector-valued random variable. Later, we shall see that joint entropy can expanded using chain rule.In the derivation of the capacity for our fading wire-tap channel, joint entropy and conditional entropy, and their relationship will play important role.

Definition 3. *The joint entorpy $H(X,Y)$ of a pair of discrete random variables (X,Y) with a joint distribution $p(x,y)$ is defined as*

$$H(X,Y) = -\sum_{x\epsilon\mathscr{X}}\sum_{y\epsilon\mathscr{Y}} p(x,y)\log p(x,y). \tag{1.8}$$

We also define the conditional entropy of a random variable given another as the expected value of the entropies of the conditional distributions, averaged over the conditioning random variable.

Definition 4. *If $(X,Y) \sim p(x,y)$, the conditional entropy $H(Y|X)$ is defined as*

$$\begin{aligned} H(Y|X) &= \sum_{x\epsilon\mathscr{X}} p(x)H(Y|X=x) &(1.9)\\ &= -\sum_{x\epsilon\mathscr{X}} p(x)\sum_{y\epsilon\mathscr{Y}} p(y|x)\log p(y|x). &(1.10)\end{aligned}$$

We have also the chain rule of entropy.

Definition 5. *Let $X_1,\ldots,X_n$ be drawn according to $p(x_1,\ldots,x_n)$. Then*

$$H(X_1,\ldots,X_n) = \sum_{i=1}^{n} H(X_i|X_{i-1},\ldots,X_n). \tag{1.11}$$

Using the chain rule, we relate entropy, conditional entropy, and joint entropy by

$$H(X,Y) = H(X) + H(Y|X) = H(Y) + H(Y|X). \tag{1.12}$$

The naturalness of the definition of joint entropy and conditional entropy is exhibited by the fact that the entropy of a pair of random variables is the entropy of one plus the conditional entropy of the other.

The concept of entropy plays the central role in information theory. Most of the other information-theoretic terms are built on the definition of the entropy. Next, we

consider another key concepts called *mutual information*. We will see shortly that the *mutual information* between two RVs is actually the possible rate of information transfer through a communication channel.

1.3. Mutual Information

Mutual information is a measure of the amount of information that one random variable contains about another random variable. It is the reduction in the uncertainty of one random variable due to the knowledge of the other.

Definition 6. *Consider two random variables X and Y with a joint PMF $p(x, y)$ and the marginal PMFs $p(x)$ and $p(y)$. The mutual information $I(X;Y)$ is given by*

$$I(X;Y) = \sum_{x \epsilon \mathscr{X}} \sum_{y \epsilon \mathscr{Y}} p(x,y) \log \frac{p(x,y)}{p(x)p(y)}. \tag{1.13}$$

1.4. Relationship between Entropy and Mutual Information

We can rewrite the mutual information $I(X;Y)$ as

$$I(X;Y) = H(X) - H(X|Y). \tag{1.14}$$

Thus, the mutual information $I(X;Y)$ is the reduction in the uncertainty of X due to the knowledge of Y.

By symmetry, it also follows that

$$I(X;Y) = H(Y) - H(Y|X). \tag{1.15}$$

Thus, X says as much about Y as Y says about X.

It follows easily from the definitions of the above quantities that

$$I(X;Y) \leq H(X), \quad I(X;Y) \leq H(Y), \text{and} \quad I(X;Y) \geq 0. \tag{1.16}$$

Figure 1 below depicts the relationship among the aforementioned quantities via a Venn diagram.

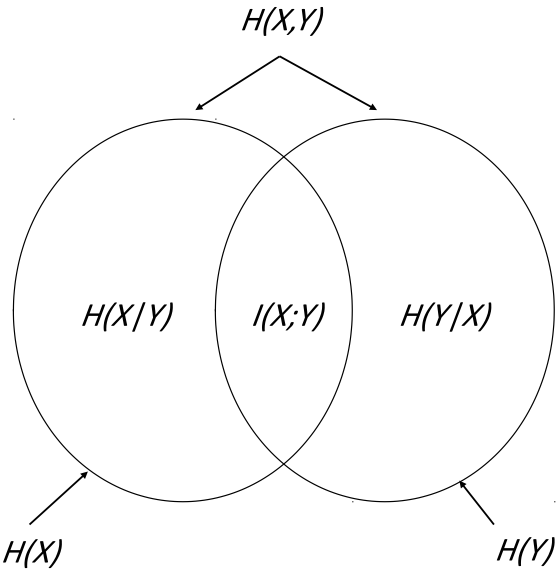

Figure 1. Relationship among *entropy*, *conditional entropy*, and *mutual information*.

Finally, we note that

$$I(X;X) = H(X) - H(X|X) = H(X). \tag{1.17}$$

Thus, the mutual information of a random variable with itself is the entropy of the random variable. This is the reason that entropy is sometimes referred to as *self-information*.

We shall see shortly that the mutual information is actually the rate of information transfer on a channel. To illustrate this connection, let us consider a simple channel model where input to the channel is X and output of the channel is Y. We assume, the channel is noiseless ideal channel, i.e., output uniquely determines the input or input is a function of the output. Another way to say this in a simpler way is that the input is exactly reproduced at the output.

The mutual information becomes

$$I(X;Y) = H(Y) - H(Y|X) = H(X) - H(X|X) = H(X) - 0 = H(X), \qquad (1.18)$$

which is the maximum value that can be attained by mutual information. The term $H(X|X)$ represents the uncertainty remained in X after knowing X, which is zero. On the other hand, let us assume the channel to be worst one (for example a broken wire) such that output Y become independent of X. The mutual information is

$$I(X;Y) = H(Y) - H(Y|X) = H(Y) - H(Y) = 0, \qquad (1.19)$$

which is the minimum value that can be attained by mutual information. The term $H(Y|X)$ represents the uncertainty remained in Y after knowing X, which is equal to $H(Y)$ because knowing X does not reduce any uncertainty of Y since they are independent of each other.

$I(X;Y)$ can also be called as the mutual information of the channel. From the above example, we can predict that the amount of information transferable is dependent on the mutual information of the channel. It turns out that if we send information at a higher rate than the mutual information of the channel, the receiver cannot receive the information *reliably*.

Now, with help of above definitions, we can quantify the aforementioned notions of rate of information transmission and reliability and subsequently, formally define the maximum rate of information transmission with very high reliability, which is popularly known as the *capacity* of a communication channel.

1.5. Channel Capacity

Any well thought transmission scheme shall have a well defined rate of transmission of information on a channel. If in addition, it is possible to make the probability

of decoding error at the receiver arbitrarily small, the corresponding rate is called an *achievable rate* for the channel. Clearly, different transmission schemes will have different achievable rates. The maximum achievable rate on a channel over all possible transmission schemes is called the capacity of the channel. In particular, every choice of the input distribution results in a new transmission scheme. As a result the number of different transmission schemes are infinite.

The typical approach to characterize the capacity is thus to derive upper bounds to the rate of information transmission and then compare with the achievable rates. It is possible to derive different upper-bounds on reliable information transfer rate for a particular channel. Each of these upper bounds serve as an upper bound to all possible *achievable rates* for the channel. If any particular upper-bound coincides with an achievable rate we call it the capacity of the channel.

On one hand, the capacity of the channel is an upper-bound to all achievable rates for the channel but it is the infimum of the all upper-bounds. On the other hand, the capacity is also an achievable rate, but it is the supremum of all achievable rates. This particular explanation of channel capacity will be helpful to understand the derivation of the secrecy capacity for our problem in chapter 3 and chapter 4.

Definition 7. *We define the information channel capacity of a discrete memoryless channel as*

$$C = \max_{p(x)} \big[I(X;Y) \big], \tag{1.20}$$

where the maximum is taken over all possible input distributions $p(x)$*.*

This definition follows for continuous channel with only difference is that now the maximization is carried out over the all possible input PDFs instead of PMFs. Next, we consider few examples of channel capacity for some simplest channels. Those examples will provide the idea how the channel capacity can be computed.

In addition, we shall use some of the results in deriving the channel capacity of our problem.

1.5.1. Noiseless Binary Channel

Suppose that we have a channel where the binary input is reproduced exactly at the output. In this case, any transmitted bit is received without error. Intuitively, one error-free bit can be transmitted per use of the channel, and the capacity should be 1 bit.

Figure 2. Binary noiseless channel.

First,we will compute the rate upper-bound. In information-theoretic terminology, this is know as the converse.

$$R \leq \max I(X;Y) \tag{1.21}$$

$$= \max \big[H(X) - H(X|Y)\big] \tag{1.22}$$

$$= \max \big[H(X)\big] \tag{1.23}$$

$$\leq 1 \quad \text{bit/channel use,} \tag{1.24}$$

because for a binary RV X, $H(X) \leq 1$.

Now, let us consider the achievable rate for a particular input X^* with $p_{X^*}(x) = (\frac{1}{2}, \frac{1}{2})$. The achieved rate R^* for that iput is

$$R^* = I(X^*; Y) \tag{1.25}$$

$$= H(Y) - H(Y|X^*) \tag{1.26}$$

$$= H(X^*) \tag{1.27}$$

Since$H(X^*) = 1$ bit, the achievable rate

$$R^* = H(X^*) = 1 \quad \text{bit/channel use.} \tag{1.28}$$

The upper-bound in (1.24) matches with the achievable rate (1.28). Hence, we can say the capacity of the noiseless binary channel is 1 bit/per channel use.

Finally, we consider one more channel called binary erasure channel because in our work, the capacity of a erasure channel is used to prove the achievability part of the theorem 1 in chapter 3.

1.5.2. Binary Erasure Channel

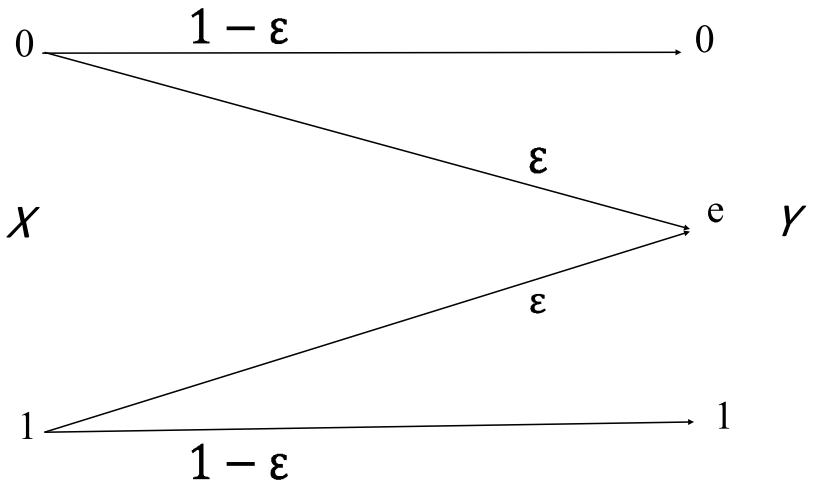

Figure 3. Binary erasure channel.

In this channel, each input bit is erased with probability ϵ. The binary erasure channel has two inputs and three outputs as shown in Figure 3 above, where the erasure event is denoted by the symbol e. It turns out that the capacity of the binary erasure channel is

$$C = 1 - \epsilon \qquad \text{bits/channel use.} \tag{1.29}$$

The expression for the capacity has some intuitive meaning: Since a proportion ϵ of the bits are lost in the channel, we can recover (at most) a proportion $1 - \epsilon$ of the bits. Hence the capacity is at most $1 - \epsilon$.

With the help of definitions and concepts of this chapter, we explain the notion of information-theoretic secret communication, previous works, and finally the outline of our work in next chapter.

CHAPTER 2. INFORMATION-THEORETIC SECRECY

Traditional cryptographic way of secret communication is based on the secret-key generation and exchange between transmitter and receiver. Due to broadcast nature of wireless communication, this approach is vulnerable primarily in two ways: efficient secret-key exchange is not guaranteed due to the fading characteristics of the wireless channel; there is always a chance of breach of the secret-key by the possible wire-taper with very high computing power. In contrast, the information-theoretic secrecy concept is simple: based on the statistics of the legitimate and eavesdropper channels, we can come up with a coding scheme that allows information to be decodable only by legitimate receiver. The secrecy capacity is the highest rate at which one transmitter can communicate a message securely to a receiver with perfect secrecy in the presence of a passive eavesdropper.

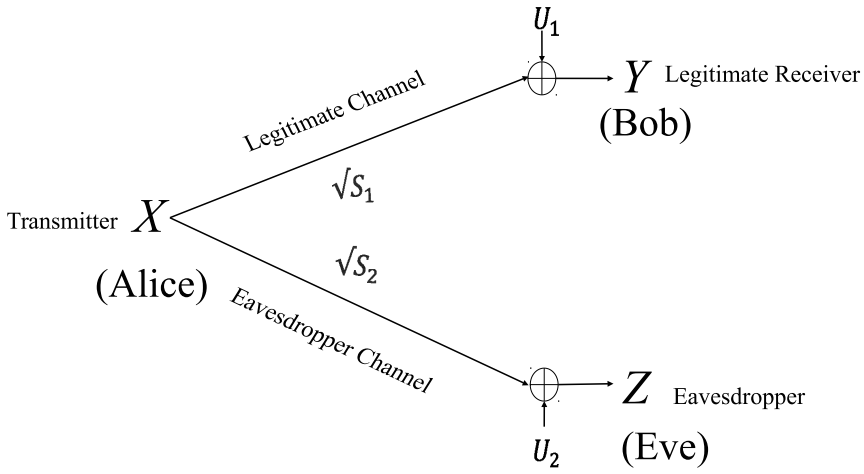

Figure 4. Illustration of a wire-tap channel.

Wire-tap channel model of figure 4 is given by

$$Y = \sqrt{S_1}X + U_1, Z = \sqrt{S_2}X + U_2, \tag{2.1}$$

where X is the transmitted signal by Alice is X, Y and Z are the received signal by Bob and Eve, respectively. U_1, U_2 are additive white noise present at Bob and Eve, respectively. The channel states are given by S_1 for Legitimate channel and S_2 for eavesdropper channel. In information-theoretic terminology, S_1 and S_2 are known as the channel state information (CSI) of the legitimate and eavesdropper channel respectively, and can be constant or time varying depending on the channel characteristics. Bob and Eve can always measure the respective CSI from their received signals. If Bob and Eve feedback the CSI information to Alice, then only Alice can know the instantaneous channel states.

Suppose, Alice wants to communicate with Bob maintaining confidentiality of message from Eve. In this setting, Bob is the legitimate receiver and Eve is the eavesdropper. We call the channel between Alice and Bob as the legitimate channel and the channel between Alice and Eve as the eavesdropper channel. The objective of Alice is to transfer information at the highest possible rate with perfect secrecy. Perfect secrecy is achieved when Eve fails to decode any confidential information no matter what computing power she has. The notion of perfect secrecy precludes use of any cryptographic method because such method fails when the eavesdropper has infinite computing power. Is there any way to achieve perfectly secret communication in presence of an eavesdropper with infinite computing power? The answer is yes and it comes from the information-theoretic approach of achieving secret communication. The 'catch' is that Alice have to send at a lower rate satisfying the secrecy constraint. Let us consider a very simplistic wire-tap channel. For example, suppose both the channels are fixed; the point to point capacity of the legitimate channel is 5 bits per channel use and eavesdropping channel is 2 bits per channel use. Basic information-theoretic results say that a coding scheme can be constructed for perfectly secret communication if rate of the code, i.e., the rate of communication takes place less

than the difference of the capacities of the channels which is 3 bits per channel use for above case. The strategy of constructing of such coding scheme is to insert noise in the encoding process to confuse the eavesdropper totally.

In information-theoretic terminology, suppose Alice wants to send a secret message $W \in \{1, \ldots, 2^{nR}\}$ to Bob. Alice maps the message index $W(i)$ to a signal codeword $X^n(i) = X_1(i), \ldots, X_n(i)$ where $i \in \{1, \ldots, 2^{nR}\}$ and transmits that codeword in n channel uses. Due to the different channel gains and additive noise at receivers, Bob and Eve will receive different signals. Let us say the legitimate channel output is $Y^n(i) = Y_1(i), \ldots, Y_n(i)$ and eavesdropper channel output is $Z_n(i) = Z_1(i), \ldots, Z_n(i)$. Based on the receive signals, Bob and and Eve try to decode the codeword. After decoding, let us say, they declare the sent message is $\hat{W}(i)$. To have secure communication, two certain things need to be achieved: The decoding error probability at Bob must be arbitrarily small; the uncertainty of the message given eavesdropper output must be arbitrarily close to the uncertainty of the message itself. We say a secrecy rate R is achievable if for any $\epsilon > 0$ there exists a encoder-decoder with rate R for sufficiently large code block length of n, such that, the decoding error probably at legitimate receiver is

$$P\big(W(i) \neq \hat{W}(i)\big) \leq \epsilon, \tag{2.2}$$

and the message uncertainty given the channel output at the eavesdropper is

$$\frac{1}{n} H(W|Z^n) \geq H(W) - \epsilon. \tag{2.3}$$

That is, the reduction of uncertainty of the message W due to the knowledge of Z^n at Eve is not more than ϵ that can be made arbitrarily close to zero, which in turn imply complete secrecy.

2.1. Previous Works

Information-theoretic approach for secret communication first appeared in the Shannon's work [2] . In the pioneering paper on wiretap channel [3], Wyner laid out the mathematical formulation of the information-theoretic secrecy. Wyner considered a discrete memoryless wiretap channel where Eve receives a degraded version of Bob's received signal i.e. the channels form a Markov chain $W \longrightarrow X \longrightarrow Y \longrightarrow Z$. By analyzing each channel as a binary symmetric channel (BSC), Wyner showed perfect secrecy can be achieved if the information is encoded at a rate less than the difference of the point to point capacities of the legitimate and eavesdropper channels.

Csiszár and Körner [4] generalized the Wyner's result for discrete memoryless broadcast channel. Their analysis characterized the secrecy capacity, the highest achievable secrecy rate, which is given by

$$C_s = \max_{W \to V \to X \to Y,Z} \big[I(V;Y) - I(V;Z) \big], \tag{2.4}$$

where V is the auxiliary random variable for prefixing satisfying the Markov chain $W \to V \longrightarrow X \longrightarrow Y, Z$. The maximization is done over all valid joint distributions $P_{V,X}(v,x)$ for the given discrete memeoryless channel $P_{Y,Z|X}$. Although (2.4) characterizes the capacity, it is very difficult to find out the optimal $P_{V,X}(v,x)$. Authors [4] showed that if the channels are fixed and legitimate channel is more capable than the eavesdropper channel, i.e., $I(X;Y) - I(X;Z) \geq 0$ for all X, then the secrecy capacity archiving strategy is to setting $V = X$ which means no need of prefixing auxiliary RV. Hence, the capacity expression reduced to the Wyner's result.Hence, the secrecy capacity of a degraded channel can be written as

$$C_s = \max_{p(x)} \big[I(X;Y) - I(X;Z) \big]. \tag{2.5}$$

Equations (2.4) and (2.5) are also valid for continuous channels because any discrete channel can be seen as the quantized version of the continuous channel where the quantizing interval is arbitrarily small. The detail proof can be found in standard information-theoretic textbooks such as [5].

In [6], Leung-Yan-Cheong and Hellman considered a special case of Wyners results known as the Gaussian wire-tap channel and solved it explicitly. In their wire-tap channel, both the channels have fixed gain and received signals are further corrupted by all white Gaussian noise (AWGN). Suppose, the legitimate and eavesdropper channel have fixed channel gain of a and b respectively,and U_1 and U_2 be the additive Gaussian white noise with unit variance, respectively. For received signals $Y = \sqrt{a}X + U_1$ and $Z = \sqrt{b}X + U_2$, the author proved that Gaussian input without prefixing is optimal that achieve capacity, and with average input power constraint P, i.e., $E[X^2] \leq P$, where $E[.]$ denotes the expectation, the capacity is

$$C_s = \big(\log(1 + aP) - \log(1 + bP)\big)^+, \tag{2.6}$$

where $(x)^+ = \max(x, 0)$. Hence for fixed AWGN channel, the secret communication with positive rate is only possible when the legitimate channel has a better signal to noise ration(SNR).

After those early works, the information-theoretic security issue was in long hibernation due to several reasons, partly because of the unavailability of the practical wire-tap code. In addition, to achieve a positive secrecy rate, the legitimate channel needs to be superior to the eavesdropper channel. Furthermore, public-key cryptography, proposed by Diffie and Hellman, [7] become popular security schemes for its practical feasibility.

In late nineties, there had been a surge of interest in information-theoretic secrecy approach. In combination of cryptographic method and information-theoretic

approach can result in more robust and practical security scheme. More interesting results are coming for wireless channel where time-varying wireless channel provides an opportunity for secret communication. Since, channel state information (CSI) at transmitter is important to exploit the randomness of the channel to obtain physical layer security, previous works mostly focused with the assumptions that CSI is available at the transmitter. But in a fast-fading wireless channel, timely feedback of the channel measurement information by the receiver to the transmitter is a challenging task. Although there are some results for without channel state information at transmitter (CSIT), most of those works were carried out for specific channel state distribution. The capacity of a fast-fading Gaussian wire-tap channel with general fading distribution without CSIT is still to be found.

The secrecy capacity of slow fading channel with single-input multiple-output with CSIT was characterized in [8]. In [9], secure transmission of information over fast fading channel was studies. In that paper, the author considered full CSI where the transmitter has the CSI of the legitimate and eavesdropper receiver both. Secrecy communication for fast Rayleigh fading channel was considered in [10]. In that paper, the legitimate channel is fixed-SNR Gaussian channel and the eavesdropper channel is a Rayleigh fading channel with no CSIT. The author showed that for that channel model, there can be a positive secrecy rate even if the legitimate channel is worse than the eavesdropper channel on the average. The strategy to achieve positive rate is to inject optimal white noise which can be computed from the statistics of the channel states.

2.2. Problem Statement

We consider a fast-fading Gaussian wire-tap channel without CSIT. In our channel model, Alice wants to communicate with Bob with perfect secrecy in presence of a passive eavesdropper Eve. We consider fast fading channel where the instantaneous

channel state is available at the receivers but not at the transmitter. This is the case in many practical wireless communication systems where channel states can only be measured by the receivers which cannot inform the transmitter of the state accurately in a timely manner through a feedback link due to the fast fading. Specifically, we assumes independent fast fading i.e. the channel is changing in each symbol time, where the fading statistics are known to the transmitters, but not the realizations. This paper investigates the ergodic case where the code is designed to perform over a typical realization of the time-varying fading process. We call the Alice-Bob channel as legitimate channel, whereas Alice-Eve channel as the eavesdropper channel. Both Bob and Eve know the instantaneous realizations of their own channels, but the Alice know only the distributions of the legitimate and eavesdropper channels, not the actual realizations. Channel fading state distributions for both channels are arbitrary; we are not restricting for a specific channel distribution. Those assumptions make the problem quite challenging. We address this problem first considering a layered erasure wire-tap channel. Layered erasure model was introduced by [11], in which each component channel is expressed in terms of a binary expansion.While in [11], the model was used in a different communication scenario called the relay channel without secrecy, we use the deterministic layered erasure model approach to obtain insights about Gaussian wire-tap channel. We represent the fading wireless channel by time-varying version of a deterministic model, called the layered erasure model, where the state of a link corresponds to the number of most significant bits not erased. We have complete characterization of secrecy capacity for such class of channel. Using insight from the layered erasure wire-tap channel, we derive an upper bound for Gaussian fast-fading channel and we show for some very interesting practical scenarios, the fading wire-tap channels fall into a class of channels for which the upper-bound can be achieved.

The main contributions of this work are as follows.

1. We derive the complete characterization of the secrecy capacity of the layered erasure wire-tap channel.

2. We derive an upper-bound of secrecy rate for fading Gaussian wire-tap channel with arbitrary fading statistics.

3. For two very important class of practical wireless environment, we derive achievable schemes can meet the aforementioned upper-bound, characterizing the secrecy capacity.

In next chapter, first, we shall show how we can model a Gaussian channel as a layered erasure channel. With that, we shall derive the layered erasure wire-tap channel model for our fading Gaussian wire-tap channel. The secrecy rate upper-bound will be derived for such layered eraser wiretap channel, and then we shall show that the upper-bound is achievable.

CHAPTER 3. LAYERED ERASURE WIRE-TAP CHANNEL

In this chapter, we derive an upper-bound of secrecy rate, and subsequently we show that the upper-bound is achievable for a layered erasure wire-tap channel. Therefore we, in fact, characterize the secrecy capacity of such wiretap channel. The primary motivation behind considering a layered erasure wire-tap channel is because the analysis of such channel can be extended to the actual Gaussian wire-tap channel. We shall briefly outline the concept of layered erasure model as explained in [11]. With that, we shall formulate the layered erasure model for our fast-fading Gaussian wire-tap channel. Using that model, we derive the converse, i.e., the upper-bound for secrecy rate and finally, we prove that the upper-bound is achievable.

3.1. Layered Erasure Deterministic Model

On a communication channel, the Gaussian model is commonly used where along with channel gain, all white Gaussian noise (AWGN) is added at the receiver. The nature of the AWGN makes the Gaussian model difficult to analyze. Due to this reason, the complete characterization of the capacity of most of the Gaussian networks is still unknown except for some simplest networks such as the one-to-many Gaussian broadcast channel (BC) and the many-to-one Gaussian multiple access channel (MAC).Analysis for fading Gaussian channel without CSIT is way more complicated. That is the one reason why it is still an open problem. However, A. Salman Avestimehr et.al. showed a novel layered approach in [11] which can closely mimic the properties of the Gaussian channel with simpler analysis to attack the problem. This layered approach gives the insights about proving the upper bound and potentially successful coding scheme for Gaussian case. To solve our problem, i.e., to find the secrecy capacity of the fading Gaussian wire-tap channel, the layered approach will be instrumental. Hence, we briefly outline how we can have layered

channel for a Gaussian channel as explained [11]. With that deterministic layered model, we shall derive the layered wire-tap channel model for our fading Gaussian wire-tap channel.

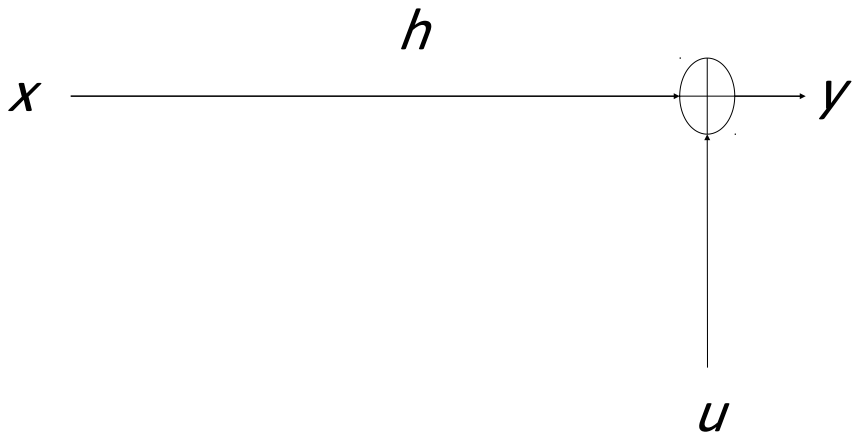

Figure 5. A point-to-point Gaussian channel.

Let us consider a real scalar single-input-single-output (SISO) Gaussian point-to-point channel as shown in the figure 5 , whose input output relation is given by

$$y = hx + u, \tag{3.1}$$

where x, y, h be the input, output, and gain of the channel respectively. u is the AWGN at the receiver with zero mean and unit variance. There is also the average input power constraint $E[|x|^2] \leq 1$ where $E[.]$ denotes the expectation operation taken over the input distribution. The relation between the channel gain and signal-to-noise ratio (SNR) with transmitted power and noise power both normalized to be 1 is given by

$$|h| = \sqrt{SNR}. \tag{3.2}$$

Capacity of the this point-to-point channel is

$$C_{AWGN} = \frac{1}{2}\log(1 + SNR), \tag{3.3}$$

where the base of the logarithm is 2.

For this scalar Gaussian channel, since x, u are all positive real numbers, we can express them in terms of their binary expansions.

Any real positive number a can have a binary expansion

$$a = \sum_{i=1}^{\infty} a_i 2^{-i}, \tag{3.4}$$

where $a_i \in \{0, 1\}$.

We express the input and the additive white noise in terms of their binary expansion. Hence the input-output relation of the channel (3.1) can be written as

$$y = h \sum_{i=1}^{\infty} x_i 2^{-i} + \sum_{i=1}^{\infty} u_i 2^{-i}. \tag{3.5}$$

Furthermore (3.2) can be expressed as

$$|h| = \sqrt{SNR} = 2^{\log(\sqrt{SNR}} = 2^{\frac{1}{2}\log SNR}. \tag{3.6}$$

Hence (3.5) becomes

$$y = 2^{\frac{1}{2}\log SNR} \sum_{i=1}^{\infty} x_i 2^{-i} + \sum_{i=1}^{\infty} u_i 2^{-i}. \tag{3.7}$$

Note that the channel gain in (3.7) actually determines the number of the input bit levels that are above the noise floor. If the channel gain is high, we have higher number of most significant bits of input above the noise level.

Substituing $n = \frac{1}{2}\log SNR$ in (3.7), we get

$$y = 2^n \sum_{i=1}^{\infty} x_i 2^{-i} + \sum_{i=1}^{\infty} u_i 2^{-i} \tag{3.8}$$

$$\approx 2^n \sum_{i=1}^{n} x_i 2^{-i} + \sum_{i=1}^{\infty} (x_{i+n} + u_i) 2^{-i}. \tag{3.9}$$

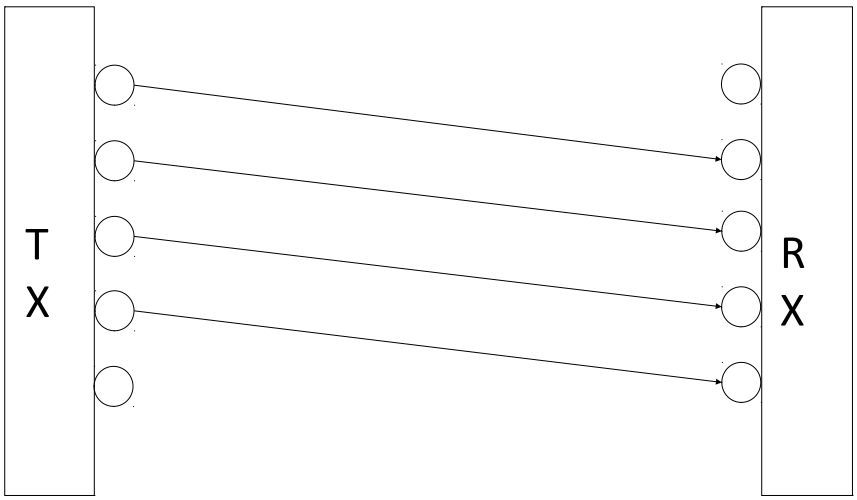

Figure 6. Pictorial view of deterministic layered channel.

If the 1 bit carry-over from the second summation is ignored, It can be said that the receiver gets the n no of bits correctly. Hence the point-to-point Gaussian channel can be approximated as a pipe that truncates the transmitted signal and only passes the bits that are above the noise level. Information can be encoded as a sequence of bits at different signal level up to layer n where the highest layer represent the most significant bit (MSB) and the lowest level as the lowest significant bit (LSB). The receiver can see the up to n most significant bits of x and rest of the bits are completely obliterated by noise.

The parameter n which is function of SNR determines the number of layers which are above the noise floor that can be used for reliable communication. Using

multilevel lattice code in the AWGN channel [12], a coding scheme can be constructed where at each layer up to layer n , can be thought of a noiseless binary channel, hence, the maximum rate at each layer can be achieved is 1 . With coding on n layers, the capacity of the layered channel is approximately equal to n bits per channel use.

3.2. Incorporating Fading in Layered Erasure Deterministic Model

From the above channel model, if the channel state h is constant, the number of layers that can be used for reliable communications is equal to n, and maximum rate of that channel is upper bound by n bits/sec per channel use. However, we consider a fading Gaussian wire-tap, where the channel state is changing in every symbol time. Hence, for each time instance, the value of the number of the layers can be different. Furthermore, we are considering a case where the CSI is not available at the transmitter; therefore, the transmitter cannot adapt the rate of transmission based on the instantaneous channel state. Hence, the deterministic model without little modification cannot be directly used to get the layered model for fading Gaussian channel.

For our fading channel, we represent the number of layers as the channel state at a particular time. And the value of n is changing every symbol time. We consider the channel state as random variable N which takes the different values at different time based on the instantaneous channel state. Since, transmitter does not know the instantaneous channel state, the dynamic coding cannot be used. Rather, we shall consider sufficient long codewords to capture the ergodic realization of the channel to determine the capacity for such channel on the average.

3.3. Channel Model

We consider a layered erasure wire-tap channel model where Alice sends a q-bit length binary sequence to Bob, where $q \in \mathbb{N}$. Channel fading characteristic is incorporated in the layered eraser model as the erasure of the least significant bits. For

example, if the channel is good enough, then the received signal is same q-bit length binary sequence like the original. On the other hand, if the fading state is the worst i.e. the channel state is zero, then the bits thought to be erased and consequently receiver does not receive any single bit.

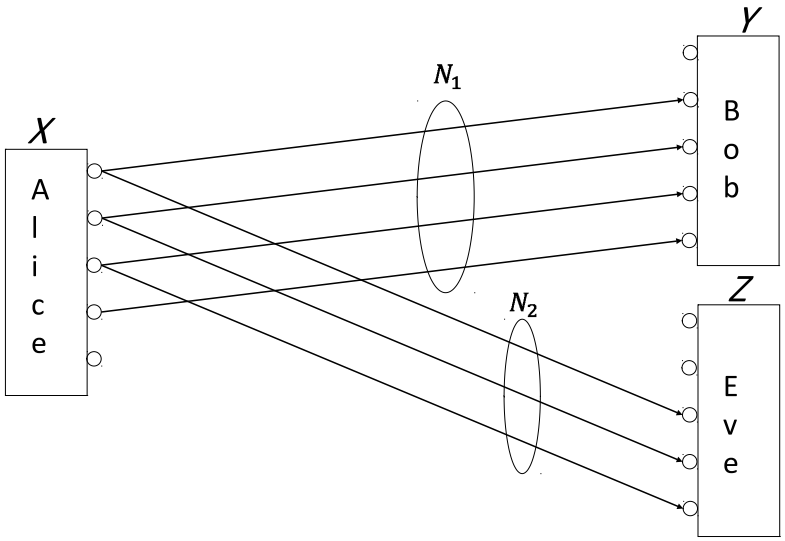

Figure 7. Layered erasure wire-tap channel.

A q-bit layered erasure wire-tap channel, the channel states of the legitimate and eavesdropper are denoted by $N_1(t)$ and $N_2(t)$ random sequences respectively, where $t = 1, 2, 3.....$ is the time index and $N_i(t) \in \{1, 2, 3....q\}$ for $i \in \{1, 2\}$. We assume instantaneous realization of the channel state is known to the respective receiver i.e. $N_1(t)$ is known to Bob and $N_2(t)$ to Eve at time t , whereas the transmitter i.e. Alice knows only the statistical properties of $N_1(t)$ and $N_2(t)$. We assume that the channels are memoryless and channels states are independent and identically distributed (i.i.d.). Hence, without loss of generality, we can ignore the time index for notational convenience.

Before having the formal definition of q-bit layered erasure wire-tap channel, we need few more explanations. The PMF of a random variable N is expressed as $P_N(n) := P[N = n]$.

We define the complementary cumulative distribution function (CCDF) of random variable N as

$$\bar{F}_N(n) := P[N \geq n]. \tag{3.10}$$

Definition 8. *A q-bit layered erasure wire-tap channel has one input $X = X^q \in \mathbb{F}_2^q$, and two outputs, one at legitimate receiver $Y = X^{N_1}$ and the other at eavesdropper $Z = X^{N_2}$ where $N_i \in \{1, 2, 3....q\}$ are the channel states and independent of X^q satisfying $\bar{F}_{N_1}(0) = 1, \bar{F}_{N_2}(0) = 1$ and $\bar{F}_{N_1}(q+1) = 0, \bar{F}_{N_2}(q+1) = 0$.*

For our channel model, the transmitted signal by Alice is

$$X = X^q = [X_1, \ldots, X_q], \tag{3.11}$$

Bob receives

$$Y = X^{N_1} = [X_1, \ldots, X_{N_1}], \tag{3.12}$$

and Eve receives

$$Z = X^{N_2} = [X_1, \ldots, X_{N_2}]. \tag{3.13}$$

Now we shall state the main results of analysis to find out the secrecy capacity for the layered erasure wire-tap channel as explained above.

Theorem 1. *The secrecy capacity of q-bit layered erasure wire-tap channel (N_1, N_2) is given by,*

$$C_s = \sum_{n:\alpha_n > 0} \big(\bar{F}_{N_1}(n) - \bar{F}_{N_2}(n)\big), \tag{3.14}$$

where $\alpha_n := \bar{F}_{N_1}(n) - \bar{F}_{N_2}(n)$ and $n \in \{1, \ldots, q\}$.

The proof, like any other information-theoretic proof, is consisted of two parts. Firstly, we shall prove the converse, i.e., the upper-bound for the secrecy rate; later, the achievability which means the secrecy rate upper-bound can be achieved.

3.4. Layered Erasure Wire-tap Channel: Converse

The secrecy capacity for a degraded wire-tap channel can be derived from [4], which is

$$C_s = \max \big[I(X;Y) - I(X;Z) \big], \tag{3.15}$$

the maximization being carried out over all possible input distribution.

Since our wire-tap channel is the general one, we cannot use this results directly. To make progress, we enhance the legitimate channel to make it a degraded wire-tap channel. As we are enhancing the legitimate channel, the resultant secrecy capacity will be always higher than or at least equal to that of the original channel.

We enhance the legitimate channel by enhancing channel state N_1 to $\tilde{N}_1$ such that

$$\bar{F}_{\tilde{N}_1}(n) = \max \big[\bar{F}_{N_1}(n), \bar{F}_{N_2}(n) \big]. \tag{3.16}$$

With lthe lemma from [16], the q-bit layered erasure wiretap channel $(\tilde{N}_1, N_2)$ is a degraded wiretap channel. We are restating the lemma here, the proof of the lemma can be found in [16].

Lemma 1. *The q-bit layered erasure wire-tap channel* (N_1, N_2) *satisfying* $N_1 \geq_{st} N_2$ *is a degraded wire-tap channel.*

As a result of lemma 1, our fading Gaussian wire-tap channel $(\tilde{N}_1, N_2)$ is a degraded wire-tap channel. Hence we can apply (3.15) to get an upper-bound on the secrecy rate of the enhanced channel, which is a better channel than the original channel. Therefore any upper bound to the enhanced channel also serves as an upper bound to the original channel as well. However, we shall show that the secrecy-rate upper-bound for the enhance one is tight which means the upper-bound for the enhanced channel can be achieved for the original channel. Hence, although we are deriving the secrecy rate upper-bound for the enhanced degraded layered erasure

wire-tap channel, such upper-bound equally works as a tight upper-bound for general layered erasure wire-tap channel.

$$R_s \leq \max I(X;\tilde{Y},\tilde{N}_1) - I(X;Z,N_2) \tag{3.17}$$

$$= \max \big[I(X^q;X^{\tilde{N}_1},\tilde{N}_1) - I(X^q;X^{N_2},N_2)\big] \tag{3.18}$$

$$= \max \big[I(X^q;\tilde{N}_1) + I(X^q;X^{\tilde{N}_1}|\tilde{N}_1) - I(X^q;N_2) - I(X^q;X^{N_2}|N_2)\big] \tag{3.19}$$

$$= \max \big[I(X^q;X^{\tilde{N}_1}|\tilde{N}_1) - I(X^q;X^{N_2}|N_2)\big] \tag{3.20}$$

$$= \max \big[H(X^{\tilde{N}_1}|\tilde{N}_1) - H(X^{\tilde{N}_1}|X^q,\tilde{N}_1) - H(X^{N_2}|N_2) + H(X^{N_2}|X^q,N_2)\big] \tag{3.21}$$

$$= \max \big[H(X^{\tilde{N}_1}|\tilde{N}_1) - H(X^{N_2}|N_2)\big] \tag{3.22}$$

$$= \max \big[\sum_{n=1}^{q} P_{\tilde{N}_1}(n)H(X^n|\tilde{N}_1=n) - \sum_{n=1}^{q} P_{N_2}(n)H(X^n|N_2=n)\big] \tag{3.23}$$

$$= \max \big[\sum_{n=1}^{q}\sum_{j=1}^{n} P_{\tilde{N}_1}(n)H(X_j|X^{j-1}) - \sum_{n=1}^{q}\sum_{j=1}^{n} P_{N_2}(n)H(X_j|X^{j-1})\big] \tag{3.24}$$

$$= \max \big[\sum_{j=1}^{q}\sum_{n=j}^{q} P_{\tilde{N}_1}(n)H(X_j|X^{j-1}) - \sum_{j=1}^{q}\sum_{n=j}^{q} P_{N_2}(n)H(X_j|X^{j-1})\big] \tag{3.25}$$

$$= \max \big[\sum_{j=1}^{q} \bar{F}_{\tilde{N}_1}(j)H(X_j|X^{j-1}) - \sum_{j=1}^{q} \bar{F}_{N_2}(j)H(X_j|X^{j-1})\big] \tag{3.26}$$

$$= \max \Big[\sum_{j=1}^{q} \big(\bar{F}_{\tilde{N}_1}(j) - \bar{F}_{N_2}(j)\big)H(X_j|X^{j-1})\Big]. \tag{3.27}$$

(3.19) follows from the chain rule of entropy. Since, channel state is independent of the input, both the mutual information terms, $I(X^q;\tilde{N}_1)$ and $I(X^q;N_2)$, are zero resulting (3.20). By expanding mutual information in terms of entropy, we get (3.21). Given channel state and input, the out put is known. Hence, both the entropy terms, $H(X^{\tilde{N}_1}|X^q,\tilde{N}_1)$ and $H(X^{N_2}|X^q,N_2)$, in (3.21) are zero resulting (3.22). (3.23) is because we are calculating the average entropy. In (3.24), inner summations of both the entropy terms appear due the chain rule of entropy. By changing order of the summations, we get (3.25). (3.26) follows directly from the definition of the CCDF.

Let us define

$$\tilde{\alpha}_n := \bar{F}_{\tilde{N}_1}(n) - \bar{F}_{N_2}(n). \tag{3.28}$$

It follows from the our choice of $\bar{F}_{\tilde{N}_1}$, the difference between the two CCDFs in above is always nonnegative. Hence we can maximize the rate upper bound by maximizing the entropy term. We get

$$R_s \leq \max \big[\sum_{j=1}^{q} \tilde{\alpha}_j H(X_j|X^{j-1}) \big] \tag{3.29}$$

$$\leq \sum_{j=1}^{q} \tilde{\alpha}_j \tag{3.30}$$

$$= \sum_{j=1}^{q} \big(\bar{F}_{\tilde{N}_1}(j) - \bar{F}_{N_2}(j) \big), \tag{3.31}$$

where the first step follows from the fact that conditional entropy can not be larger than unconditional entropy, which in turn is upper bounded by 1, since $X_j,\ \forall j$ are binary random variables.

Let us define

$$\alpha_n := \bar{F}_{N_1}(n) - \bar{F}_{N_2}(n). \tag{3.32}$$

Note that, by definition $\tilde{\alpha}_n \geq 0$. Comparing equations (3.28) and (3.32) it is evident that for any given $1 \leq j \leq q$,

$$\tilde{\alpha}_j = \begin{cases} \alpha_j, & \text{if } \alpha_j > 0, \\ 0, & \text{if } \alpha_j \leq 0. \end{cases} \tag{3.33}$$

Using these facts it is easy to see that

$$\sum_{j=1}^{q} \tilde{\alpha}_j = \sum_{j:\alpha_j>0} \alpha_j. \tag{3.34}$$

Hence, the final upper-bound for layered erasure wire-tap channel in terms of CCDFs is

$$R_s \leq \sum_{j:\alpha_j>0} \big(\bar{F}_{N_1}(j) - \bar{F}_{N_2}(j)\big). \tag{3.35}$$

3.5. Layered Erasure Wire-tap Channel: Achievability

To prove the achievability, first we consider a simple scenario using single layer erasure wire-tap channel i.e. $q = 1$ to have the insight, and then we shall derive our achievable rate for general layered erasure wire-tap channel. Finally, we conclude the proof of theorem 1 by showing that the upper-bound is achievable.

For single layer case, the channel states N_i can take value 0 and 1 where $i \in 1, 2$. When channel state takes value of 1, it implies the transmitted bit is received by the receiver correctly. On the other hand, when the channel state takes value of 0, it implies the bit is completely erased by the channel.

Let us define, the probability of receiving the bit correctly at the legitimate receiver as

$$P[N_1 = 1] = \bar{F}_{N_1}(1) = \bar{\epsilon}_1, \tag{3.36}$$

and the probability that the bit is erased at the legitimate receiver as

$$P[N_1 = 0] = 1 - P[N_1 = 1] = 1 - \bar{F}_{N_1}(1) = \epsilon_1. \tag{3.37}$$

Similar way we define, the probability of receiving the bit correctly at the eavesdropper as

$$P[N_2 = 1] = \bar{F}_{N_2}(1) = \bar{\epsilon}_2, \tag{3.38}$$

and the probability that the bit is erased at the eavesdropper as

$$Pr[N_2 = 0] = 1 - Pr[N_2 = 1] = 1 - \bar{F}_{N_2}(1) = \epsilon_2. \tag{3.39}$$

Hence, our single layer erasure wire-tap channel can be viewed as the aggregation of two binary erasure channels: One is the legitimate binary erasure channel with erasure probability ϵ_1 and the other is the eavesdropper binary erasure channel with erasure probability ϵ_2 . We can compute the capacity of the individual binary erasure channel using the basic information-theoretic identity. And if the legitimate channel has higher capacity than the eavesdropper one, we can achieve a secrecy rate which is the difference between the capacities of the two channels. This is due to the fact that when the legitimate channel has higher capacity than that of the eavesdropper one, the single layered erasure wire-tap channel becomes a degraded wire-tap channel.

Note that, in our upper bound expression in (3.35) ,only those layers are present where $\bar{F}_{N_1}(n) - \bar{F}_{N_2}(n) > 0$. For single layer case, this condition implies that the upper-bound is non zero only when $\bar{F}_{N_1}(1) > \bar{F}_{N_2}(1)$, i.e., $\bar{\epsilon}_1 > \bar{\epsilon}_2$. Otherwise, the upper-bound is zero.

From our achievability standpoint, let us assume $\bar{\epsilon}_1 > \bar{\epsilon}_2$. Otherwise the proof is trivial because the upper-bound is zero.

We know from the basic information-theoretic result (1.29) stated in chapter 1 that the capacity of a binary erasure channel with erasure probability ϵ_1 is $1 - \epsilon_1$ and that is achieved when the input has i.i.d. Bernoulli ($p = 1/2$) distribution.

Hence the maximum achievable rate of the legitimate binary erasure channel is

$$r_1 = 1 - \epsilon_1 = \bar{\epsilon}_1 = \bar{F}_{N_1}(1). \tag{3.40}$$

Similarly, the maximum achievable rate of eavesdropper binary erasure channel is

$$r_2 = 1 - \epsilon_2 = \bar{\epsilon}_2 = \bar{F}_{N_2}(1). \tag{3.41}$$

Since, from our assumption, $\bar{F}_{N_1}(1) \geq \bar{F}_{N_2}(1)$, using Wyner's results [3] for

degraded wire-tap channel, we can say the achievable secrecy rate for single layer erasure wire-tap channel is

$$r_s = r_1 - r_2 \tag{3.42}$$

$$= (1 - \epsilon_1) - (1 - \epsilon_2) \tag{3.43}$$

$$= \bar{\epsilon}_1 - \bar{\epsilon}_2 \tag{3.44}$$

$$= \bar{F}_{N_1}(1) - \bar{F}_{N_2}(1). \tag{3.45}$$

This concludes the proof of theorem 1 for single layer case.

Now, our achievability for the general layer erasure wire-tap channel follows exactly same line of argument as presented in the single layer case. First, we partition the bit levels based on the distribution of the channel states of the receivers. We use only those layers for which we have $\alpha_n > 0$ is satisfied. Furthermore we use independent signaling on each layers i.e. $X_1, ..., X_q$ are i.i.d. Bernoulli ($p = 1/2$) random variables.

Suppose layer n is used for secret communication. We can consider the layer n channel as two independent binary erasure channels. The erasure probability of the legitimate channel on layer n is $1 - \bar{F}_{N_1}(n)$, and that of the eavesdropper channel at layer n is $1 - \bar{F}_{N_2}(n)$. We Apply the channel capacity of binary erasure channel to get the following results.

Hence, the legitimate channel can have a rate of communication at layer n

$$r_1(n) = \bar{F}_{N_1}(n), \tag{3.46}$$

and the eavesdropper can have rate of communication at layer n

$$r_2(n) = \bar{F}_{N_2}(n). \tag{3.47}$$

Therefore,the achievable secret communication rate at layer n is

$$r_s(n) = r_1(n) - r_2(n) \tag{3.48}$$

$$= \bar{F}_{N_1}(n) - \bar{F}_{N_2}(n). \tag{3.49}$$

Using independent signaling on each layer $n : \alpha_n > 0$, the achievable secrecy rate for general layered erasure wire-tap channel is

$$R_s^* = \sum_{n:\alpha_n>0} r_1(n) - r_2(n) \tag{3.50}$$

$$= \sum_{n:\alpha_n>0} \big(\bar{F}_{N_1}(n) - \bar{F}_{N_2}(n)\big). \tag{3.51}$$

It is clear that this rate coincide with the upper-bound (3.35). This concludes the proof the theorem 1.

Next, we provide an example to illustrate further.

Example 1. *Consider the following layered erasure wire-tap channel with PMFs of the channel states N_1, N_2 are defined by*

$$P_{N_1}(n) = \begin{cases} \frac{1}{3}, & n = 0 \\ 0, & n = 1 \\ \frac{1}{3}, & n = 2 \\ \frac{1}{3}, & n = 3 \end{cases} \tag{3.52}$$

$$P_{N_2}(n) = \begin{cases} \frac{1}{4}, & n = 0 \\ \frac{1}{4}, & n = 1 \\ \frac{1}{4}, & n = 2 \\ \frac{1}{4}, & n = 3 \end{cases} \tag{3.53}$$

in which the legitimate channel seems stronger at bit level 2 *and* 3 *whereas the eavesdropper channel looks stronger at bit level* 1*. Hence the resulting layered erasure wire-tap channel is neither degraded nor more capable. The corresponding CCDFs are given by*

$$\bar{F}_{N_1}(n) = \begin{cases} 1, & n = 0 \\ \frac{2}{3}, & n = 1 \\ \frac{2}{3}, & n = 2 \\ \frac{1}{3}, & n = 3 \end{cases} \tag{3.54}$$

$$\bar{F}_{N_2}(n) = \begin{cases} 1, & n = 0 \\ \frac{3}{4}, & n = 1 \\ \frac{1}{2}, & n = 2 \\ \frac{1}{4}, & n = 3 \end{cases} \tag{3.55}$$

Hence, the usable layers for secret communication are bit levels 2 3*. The resulting secrecy capacity is*

$$C_s = \sum_{n\in\{2,3\}} \left(\bar{F}_{N_1}(n) - \bar{F}_{N_2}(n)\right) \tag{3.56}$$

$$= \left(\bar{F}_{N_1}(2) - \bar{F}_{N_2}(2)\right) + \left(\bar{F}_{N_1}(3) - \bar{F}_{N_2}(3)\right) \tag{3.57}$$

$$= 0.25 \quad \textit{bit per channel use.} \tag{3.58}$$

In next chapter, we shall consider the fading Gaussian wire-tap channel.

CHAPTER 4. FADING GAUSSIAN WIRE-TAP CHANNEL

With the insights from the layered erasure wire-tap channel, we shall derive an upper bound for Gaussian fading wire-tap channel. In this scenario, the channel states can take any value, and the CSI is not known at the transmitter. We use the similar technique of channel enhancement to create a degraded fading Gaussian wire-tap channel and then applying (2.5) we l get an upper-bound. Although we do not have a general achievable scheme to attain that upper-bound, we show that for some distributions, the upper-bound can be achieved.

4.1. Channel Model

Let $X(t), Y(t), Z(t)$ the transmitted signal by Alice, received signal at Bob, and received signal at Eve respectively at time t.

The channel model is

$$Y(t) = \sqrt{S_1(t)}e^{j\theta_1(t)}X(t) + U_1(t) \tag{4.1}$$

$$Z(t) = \sqrt{S_2(t)}e^{j\theta_2(t)}X(t) + U_2(t), \tag{4.2}$$

where $\big(S_1(t), \theta_1(t)\big)$ and $\big(S_2(t), \theta_2(t)\big)$ denotes the channel gains and phases of the legitimate and eavesdropper channel respectively, and $U_1(t), U_2(t)$ are independent circular symmetric complex Gaussian(CSCG) random variable with unit variance at time t. Since, our wire-tap channel is memoryless and changing independently at each symbol time, we can omit the time index for simpler notation.

Hence our channel model becomes

$$Y = \sqrt{S_1}e^{j\theta_1}X + U_1 \tag{4.3}$$

$$Z = \sqrt{S_2}e^{j\theta_2}X + U_2. \tag{4.4}$$

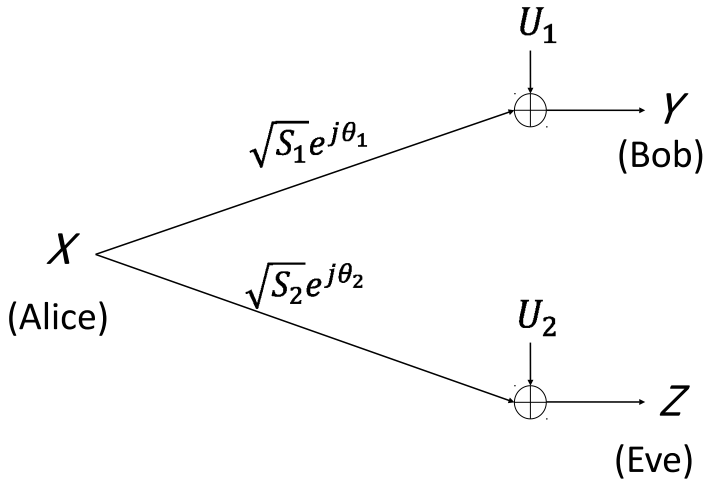

Figure 8. Gaussian fading wire-tap channel.

We consider a complex Gaussian wire-tap channel i.e. Alice transmits a complex baseband signal $X = (X_I + jX_Q)/\sqrt{2}$ with unit power constraint. The phases θ_i is known to the respective receiver, both the legitimate receiver and eavesdropper can post rotate the signal phases by $-\theta_i$ to get rid of the phase component.

Hence, the received signal at Bob can be represented in terms of real and quadrature components Y_I and Y_Q

$$Y_I + jYQ = \sqrt{2}e^{-j\theta}Y \tag{4.5}$$

$$= \sqrt{2}e^{-j\theta}\sqrt{S_1}e^{j\theta_1}(X_I + jX_Q)/\sqrt{2} + \sqrt{2}U_1e^{-j\theta} \tag{4.6}$$

$$= \sqrt{S_1}(X_I + jX_Q) + U_{1,I} + jU_{1,Q} \tag{4.7}$$

$$= (\sqrt{S_1}X_I + U_{1,I}) + j(\sqrt{S_1}X_Q + U_{1,Q}). \tag{4.8}$$

Simillar way, the received signal by Eve can be represented as in-phase and quadrature components

$$Z_I + jZQ = (\sqrt{S_2}X_I + U_{2,I}) + j(\sqrt{S_2}X_Q + U_{2,Q}). \tag{4.9}$$

Thus, the complex channel can be treated as a pair of identical real channels independent of each other. If we compute the achievable rate for one channel, same can be achieved for the other channel.

Now onward we shall consider only the real-valued Gaussian wiretap channel. The capacity of the original complex Gaussian wire-tap channel is just double of the capacity we get for the real-valued channel.

Hence our final channel model becomes,

$$Y = \sqrt{S_1}X + U_1, Z = \sqrt{S_2}X + U_2, \tag{4.10}$$

where X is the transmitted signal by Alice with unit power constraint, Y and Z are the received signal by Bob and Eve respectively, U_1 and U_2 are additive noise at respective receiver and normally distributed with zero mean and unit variance. We call the (4.10) as the fading Gaussian wire-tap channel (S_1, S_2).

When either of the legitimate or eavesdropper channel is in state s, the receiver observes a output identically distributed as

$$Y^{(s)} := \sqrt{s}X + U, \tag{4.11}$$

where the $U \sim \mathcal{N}(0, 1)$ is identically distributed as each U_i . For a fading channel where the fading state is a random process S, the ergodic capacity of the point-to-point fading channel (4.11) with unit transmit power is

$$C_e(S) := \frac{1}{2}E_S\big[\log(1 + s)\big] = \frac{1}{2}\int_0^\infty f_S(s)\log(1 + s)ds, \tag{4.12}$$

and the capacity is achieved with Gaussian input [14][15]. (4.12) represent the ergodic capacity of a point-to-point real fading channel.

Now, we state the main results of the secrecy rate of the fading Gaussian wire-tap channel defined by (4.3) and (4.4). We define the complementary CDF of a random variable S as $\bar{F}_S(s) := P[S \geq s]$.

Theorem 2. *Any achievable secrecy rate, R_s, on an fast fading Gaussian wire-tap channel defined by (4.3) and (4.4) with arbitrary fading statistics and instantaneous channel realizations known only at the corresponding receivers, is upper bounded as*

$$R_s \leq \log e \int_{I_1} \big(\bar{F}_{S_1}(s) - \bar{F}_{S_2}(s)\big) \frac{1}{1+s} ds, \tag{4.13}$$

where $I_1 := \big\{s \geq 0 | \bar{F}_{S_1}(s) > \bar{F}_{S_2}(s)\big\}$.

On a typical communication channel, finding good upper-bounds turns out to be more challenging than finding good achievable coding schemes. However, on a wire-tap channel, since any achievable scheme need to make sure that the eavesdropper can not extract any information, finding effective achievable schemes are as challenging as the converse. In contrast to the layered case, it seems unlikely that one achievable scheme will be capacity achieving for all channel statistics. Therefore, while we do not have an achievable scheme which meets the upper bound of the above Theorem for general channel statistics, for two very important class of practical wireless channels,namely fading wire-tap channels in urban and rural wireless environments, we prescribe achievable schemes which can. As a result for these class of channels we have exact secrecy capacity characterization. To the best of our knowledge, this is the first capacity result on ergodic fading wiretap channel.

In the sequel, we shall show that these aforementioned practical channels belong to a rather interesting class of channels which we hereafter refer to as the class of *Stochastically degraded channels*. Next we define the stochastically degraded wire-tap channel for which our theorem can be used to compute the exact secrecy capacity.

Definition 9 (Stochastically degraded channel)**.** *We call a fast fading wire-tap channel described by equations (*4.3*) and (*4.4*) a stochastically degraded channel if* $\bar{F}_{S_1}(s) \geq \bar{F}_{S_2}(s),\ \forall s \geq 0$*. In what follows, we shall use the notation* $S_1 \geq_{st} S_2$ *to denote a stochastically degraded wiretap channel.*

Theorem 3 below is a special case of the general upper-bound described in Theorem 2 and will later be useful to characterize the capacity of stochastically degraded class of wire-tap channels.

Theorem 3. *The secrecy capacity of a stochastically degraded fading Gaussian wire-tap channel described by (*4.3*) and (*4.4*), is given by*

$$C_s = \log e \int_0^\infty \big(\bar{F}_{S_1}(s) - \bar{F}_{S_2}(s)\big)\frac{1}{1+s}ds. \tag{4.14}$$

Next, we prove theorem 2 and 3. First, we derive the upper-bound.

4.2. Fading Gaussian Wire-tap Channel: Upper-Bound

We follow the similar approach as in the layered case to enhance the legitimate channel to make it a degraded wiretap channel. The secrecy rate upper-bound for the enhanced channel is naturally an upper-bound for the original (S_1, S_2) , The secrecy capacity of original channel cannot be larger than that of the enhanced one.

We define,

$$\bar{F}_{\tilde{S}_1}(s) = \max\big[\bar{F}_{S_1}(s), \bar{F}_{S_2}(s)\big]. \tag{4.15}$$

We need following lemma taken from [16] to prove that resulting fading Gaussian wire-tap channel $(\tilde{S}_1, S_2)$ is a degraded wire-tap channel.

Lemma 2. *The fading Gaussian wiretap channel* (S_1, S_2) *satisfying* $S_1 \geq_{st} S_2$ *is a degraded wiretap channel.*

As a result of lemma, now we can apply (2.5) to get the upper bound

$$R_s \leq \max\big[I(X;\tilde{Y},\tilde{S}_1) - I(X;Z,S_2)\big] \tag{4.16}$$

$$= \max\big[I(X;\tilde{S}_1) + I(X;\tilde{Y}|\tilde{S}_1) - I(X;S_2) - I(X;Z|S_2)\big] \tag{4.17}$$

$$= \max\big[I(X;\tilde{Y}|\tilde{S}_1) - I(X;Z|S_2)\big] \tag{4.18}$$

$$= \max\big[h(\tilde{Y}|\tilde{S}_1) - h(\tilde{Y}|X,\tilde{S}_1) - h(Z|S_2) + h(Z|X,S_2)\big] \tag{4.19}$$

$$= \max\big[h(\tilde{Y}|\tilde{S}_1) - h(U_1) - h(Z|S_2) + h(U_2)\big] \tag{4.20}$$

$$= \max\big[h(\tilde{Y}|\tilde{S}_1) - h(Z|S_1)\big] \tag{4.21}$$

$$= \max\big[\int_0^\infty f_{\tilde{S}_1}(s)h(\sqrt{s}X+U|\tilde{S}_1=s)ds - \int_0^\infty f_{S_2}(s)h(\sqrt{s}X+U|S_2=s)ds\big] \tag{4.22}$$

$$= \max\big[\int_0^\infty f_{\tilde{S}_1}(s)h(\sqrt{s}X+U)ds - \int_0^\infty f_{S_2}(s)h(\sqrt{s}X+U)ds\big] \tag{4.23}$$

$$= \max\Big[\int_0^\infty \big(f_{\tilde{S}_1}(s) - f_{S_2}(s)\big)h(Y^{(s)})ds\Big]. \tag{4.24}$$

(4.17) follows from the chain rule of mutual information. Since, we assume no CSI at transmitter, hence the input and channel states are independent to each other. Therefore, the mutual information between input and channel state is zero and we have (4.18). We express the mutual information in terms of entropy in (4.19). Since, $U_1, U_2 \sim \mathcal{N}(0,1)$, the differential entropies of them are same and cancel each other resulting (4.21). Using (4.11), we derive the average differential entropy in (4.22). Note that in (4.24),finally we get the difference of the two PDFs which is always non-negative.

Let us define

$$\bar{F}_d(s) := \bar{F}_{\tilde{S}_1}(s) - \bar{F}_{S_2}(s). \tag{4.25}$$

Note that $\bar{F}_d(s)$ is defined as the difference of two CCDFs. However, $\bar{F}_d(s)$ itself is not a CCDF.

Differentiating (4.25), we get

$$\frac{d}{ds}F_d(s) = \frac{d}{ds}\big(\bar{F}_{\tilde{S}_1}(s) - \bar{F}_{S_2}(s)\big) \tag{4.26}$$

$$= -f_{\tilde{S}_1}(s) + f_{S_2}(s). \tag{4.27}$$

By denoting, $f_d(s) := -\frac{d}{ds}F_d(s)$, we can write (4.27) as

$$f_d(s) = f_{\tilde{S}_1}(s) - f_{S_2}(s). \tag{4.28}$$

Substituting (4.28) in (4.24) , we get

$$R_s \leq \max\big[\int_0^\infty f_d(s)h(Y^{(s)})ds\big]. \tag{4.29}$$

Using integration by parts, we get

$$\int_0^\infty f_d(s)h(Y^{(s)})ds = \big[h(Y^{(s)})\int f_d(s)ds\big]_0^\infty - \int_0^\infty \big[\frac{d}{ds}h(Y^{(s)})\int f_d(s)ds\big]ds \tag{4.30}$$

$$= \bar{F}_d(0)h(U) - \bar{F}_d(\infty)h(\infty X + U) + \int_0^\infty \bar{F}_d(s)\frac{d}{ds}h(Y^{(s)})ds \tag{4.31}$$

$$= \int_0^\infty \bar{F}_d(s)\frac{d}{ds}h(Y^{(s)})ds. \tag{4.32}$$

From the defintion of $\bar{F}_d(s)$ in (4.25), we have $\bar{F}_d(0) = \bar{F}_{\tilde{S}_1}(0) - \bar{F}_{S_2}(0) = 1-1 = 0$ and $\bar{F}_d(\infty) = \bar{F}_{\tilde{S}_1}(\infty) - \bar{F}_{S_2}(\infty) = 0 - 0 = 0$ which results (4.32). Consider the term $\bar{F}_d(\infty)h(\infty X + U)$ in (4.32), where the CCDF is a decreasing function of its argument and the differential entropy increases logarithmically with variance of the RV. The rate of decrease of the CCDF is faster than the rate of increase of the differential entropy. Hence the combined term results zero.

Substituting (4.32) in (4.29) , we get

$$R_s \leq \max\Big[\int_0^\infty \bar{F}_d(s)\frac{d}{ds}h(Y^{(s)})ds\Big]. \tag{4.33}$$

Since $I(X;Y^{(s)}) = h(Y^{(s)}) - h(U)$, we have $\frac{d}{ds}I(X;Y^{(s)}) = \frac{d}{ds}h(Y^{(s)})$. Substituting this in (4.33) we get

$$R_s \leq \max\Big[\int_0^\infty \bar{F}_d(s)\frac{d}{ds}I(X;Y^{(s)})ds\Big]. \tag{4.34}$$

It was shown in [17] that

$$\frac{d}{ds}I(X;Y^{(s)}) = \frac{\log e}{2}\text{mmse}(s), \tag{4.35}$$

where minimum mean square error (mmse) is given by

$$\text{mmse}(s) := E\Big[\big(X - E[X|Y^{(s)}]\big)^2\Big]. \tag{4.36}$$

Furthermore, we have an upper bound for mmse [16], which is given by

$$\text{mmse}(s) \leq \frac{1}{1+s}. \tag{4.37}$$

This upper-bound of *mmse* can be achieved with Gaussian input.

We define

$$\tilde{I}_1 := \big\{s \geq 0 | \bar{F}_d(s) > 0\big\}. \tag{4.38}$$

Hence, our upper bound becomes

$$R_s \leq \frac{\log e}{2}\int_{\tilde{I}_1} \bar{F}_d(s)\frac{1}{1+s}ds. \tag{4.39}$$

Since $s \in I_1$ implies $\bar{F}_{\tilde{S}_1}(s) = \bar{F}_{S_1}(s)$, we can set the partition of the SNR $\tilde{I}_1 = I_1$ where $I_1 := \{s \geq 0 | \bar{F}_{S_1}(s) > \bar{F}_{S_2}(s)\}$.

Hence, the upper-bound can be written as

$$R_s \leq \frac{\log e}{2} \int_{I_1} \big(\bar{F}_{S_1}(s) - \bar{F}_{S_2}(s)\big) \frac{1}{1+s} ds. \tag{4.40}$$

If we consider signaling for both in-phase and quadrature component channels, the final upper-bound can be written as

$$R_s \leq \log e \int_{I_1} \big(\bar{F}_{S_1}(s) - \bar{F}_{S_2}(s)\big) \frac{1}{1+s} ds. \tag{4.41}$$

4.2.1. Special Case: Upper-bound for a Degraded Channel

Clearly, for a stochastically degraded wire-tap channel, the partition of channel states would not be required. We have proved that in Lemma 2 that for a stochastically degraded wire-tap channel, $\bar{F}_{S_1}(s) \geq \bar{F}_{S_2}(s), \forall s$. Hence the partition of SNR is valid for all values of channel state, i.e., $I_1 = \{s \geq 0\}$

Hence for a for a stochastically degraded fading Gaussian wire-tap channel, the secrecy rate upper-bound is given by

$$R_{sd} \leq \log e \int_{0}^{\infty} \big(\bar{F}_{S_1}(s) - \bar{F}_{S_2}(s)\big) \frac{1}{1+s} ds. \tag{4.42}$$

4.3. Fading Gaussian Wire-tap Channel: Achievability

Our achievability scheme for fading Gaussian wire-tap channel follows a different approach than that of the layered case. We cannot use the layered decoding argument for Gaussian case, because we cannot just dictate the eavesdropper to obey the decoding rule as we instruct. The eavesdropper can have arbitrary decoding technique, hence the layered achievability argument for Gaussian case fails.

Instead, we shall derive the achievable scheme directly from the capacity expression for some familiar input distributions which have the potential to be the optimal. Then, we compare those achievable rates to the upper-bound (4.41) to see how close they are.

We have capacity expression for a discrete memoryless channel wire-tap channel which is given by (2.4). We are restating the expression here.

$$C_s = \max_{V \to X \to Y,Z} \big[I(V;Y) - I(V;Z) \big] \tag{4.43}$$

C_s is maximum secrecy rate where the maximization is taken over all possible joint distributions of $P_{V,X}(v,x)$. Instead of looking for the optimal V, X that gives the maximum secrecy rate (in fact, nobody has found the optimal V, X. That is why the secrecy capacity of Gaussian channel is open for so many years) , rather we would avoid the complicated maximization problem by choosing some specific distributions of V, X . The rate we get for a specific distribution is an achievable rate and (4.43) serves as an upper-bound for all achievable rates. We carefully choose V, X that have potential to be optimal. Since for most of the channel, Gaussian input is optimal, we shall choose V, X both to be Gaussian in our achievable scheme.

4.3.1. Achievable Rate with $V = X \sim \mathcal{N}(0,1)$

We shall evaluate the achievable rate for input with Gaussian distribution and set the auxiliary random variable V equal to the input. In this setting, we have $V = X = X^G$ where $X^G \sim \mathcal{N}(0,1)$. We denote this achievable secrecy rate as R_s^G.

From (4.43), we have

$$R_s^G = I(X^G;Y|S_1) - I(X^G;Z|S_2) \tag{4.44}$$

$$= E_{S_1}\big[\log(1+s_1)\big] - E_{S_2}\big[\log(1+s_2)\big]. \tag{4.45}$$

In (4.45), we have used the ergodic rate of point-to-point fading channel with Gaussian input as given by (4.12) for a complex channel. We can simplify

$$E_{S_1}\big[\log(1+s_1)\big] = \int_0^\infty f_{S_1}(s)\log(1+s)ds \tag{4.46}$$

$$= \big[\log(1+s)\int f_{S_1}(s)ds\big]_0^\infty - \int_0^\infty \big[\frac{d}{ds}\log(1+s)\int f_{S_1}(s)ds\big]ds \tag{4.47}$$

$$= -\log(1)\bar{F}_{S_1}(0) + \log(\infty)\bar{F}_{S_1}(\infty) - \log e\int_0^\infty \big[-\frac{1}{1+s}\bar{F}_{S_1}(s)\big]ds \tag{4.48}$$

$$= \log e\int_0^\infty \frac{1}{1+s}\bar{F}_S(s)ds. \tag{4.49}$$

Similar way we have

$$E_{S_2}[\log(1+s_2)] = \log e\int_0^\infty \frac{1}{1+s}\bar{F}_{S_2}(s)ds. \tag{4.50}$$

Substituting the results of (4.49) and (4.50) in (4.45), we get

$$R_s^G = \log e\int_0^\infty \frac{1}{1+s}\bar{F}_{S_1}(s)ds - \log e\int_0^\infty \frac{1}{1+s}\bar{F}_{S_2}(s)ds \tag{4.51}$$

$$= \log e\int_0^\infty \big(\bar{F}_{S_1}(s) - \bar{F}_{S_2}(s)\big)\frac{1}{1+s}ds. \tag{4.52}$$

For a general wire-tap channel, the difference between the CCDF is not necessarily non-negative for $\forall s \geq 0$. Hence, the achievable secrecy rate for Gaussian input cannot achieve the upper-bound. But if the wire-tap channel is a stochastically degraded wire-tap channel, we can say that Gaussian input without prefixing is optimal, i.e., the secrecy rate R_s^G for Gaussian input matches the upper bound (4.42).

In the next chapter, we apply secrecy capacity result to derive the secrecy capacity of two popular class of wireless channels.

CHAPTER 5. PRACTICAL APPLICATIONS OF OUR RESULTS

In this research work, we found that Gaussian input is secrecy capacity achieving for stochastically degraded wire-tap channels.There are many practical wireless communication systems where, the channels are either stochastically degraded or reversely degraded. In those cases, the general converse (4.41) naturally yields the converse for the special case (4.42). For those class of wire-tap channels, our theorem 3 in chapter 4 can be readily used to compute the secrecy capacities. We shall consider two of such class of channels: channels with Rayleigh fading distribution and Richian fading distribution.

5.1. Secrecy Capacity of Fading Wire-tap Channel in Urban Area

To model the wireless environment in an urban area, cellular wireless networks generally use the Rayleigh fading model to represent the random channel coefficients [18]. This is because Rayleigh fading model works better for the heavily built-up urban area where there is no dominant line of sight propagation and the obstacles to wireless signals are more or less uniformly distributed between the transmitters and the receivers.

For Rayleigh fading, the channel gain $\sqrt{s}$ is Rayleigh distributed and the s has an exponential distribution which has a PDF $f_S(s) = \lambda e^{-s\lambda}$, and corresponding CDF is $F_S(s) = e^{-s\lambda}$ where the SNR of the channel is given by E[s] $= \frac{1}{\lambda}$.

Hence the CCDF of the channel is

$$\bar{F}_S(s) = e^{-s\lambda}. \tag{5.1}$$

We plot the CCDF against channel strength for different values of λ. Note that in the figure 9, the graph the CCDF with high variance is always remains high for

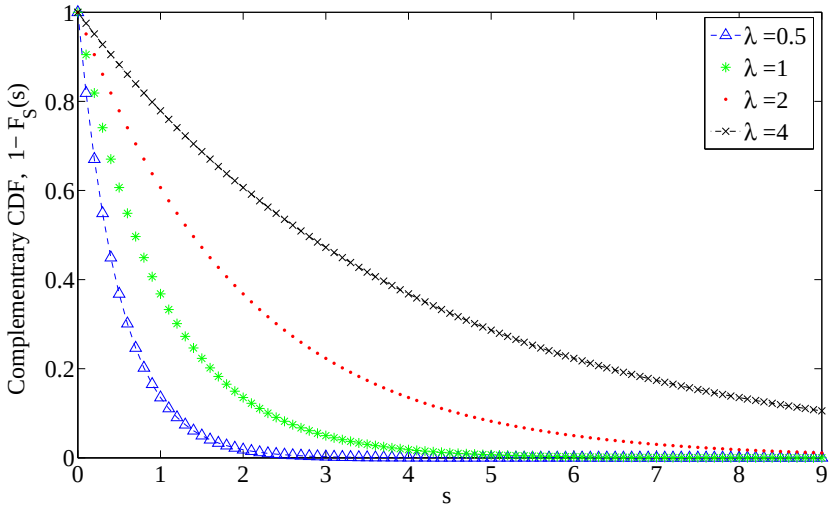

Figure 9. CCDFs vs channel state for different values of λ for Rayleigh fading.

all value of channel strength. Since, the Rayleigh fading model is the most accurate model for urban setting, therefore the wire-tap channel in a cellular wireless network environment is either stochastically degraded or reversely degraded.Therefore, the general converse and the degraded case converse have the same expression because of the fact that there is no partition of SNR. For those class of channels, our general converse is tight and achievable. Hence, we can apply theorem 2 to compute the secrecy capacity.

Consider a Rayleigh fading Gaussian wire-tap channel. The CCDF of the legitimate channel is

$$\bar{F}_{S_1}(s) = e^{-s\lambda_1}, \tag{5.2}$$

and the CCDF of the evaesdropper is

$$\bar{F}_{S_1}(s) = e^{-s\lambda_2}. \tag{5.3}$$

We assume $\lambda_1 \leq \lambda_2$. Otherwise, computing secrecy capacity is trivial because, in that case, the capacity is zero.

The secrecy capacity is given by Theorem 2

$$C_s^{urban} = \log e \int_0^{\infty} \left(e^{-s\lambda_1} - e^{-s\lambda_2}\right) \frac{1}{1+s} ds. \tag{5.4}$$

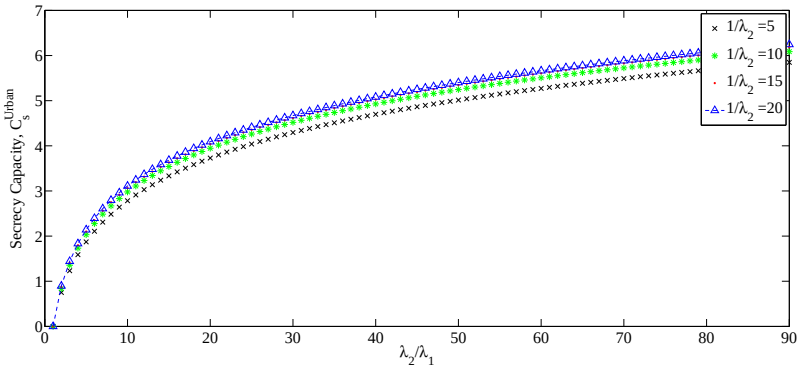

Figure 10. Secrecy Capacity vs λ_2/λ_1 for different values of $1/\lambda_2$ for fading Gaussian wire-tap channel with Rayleigh fading.

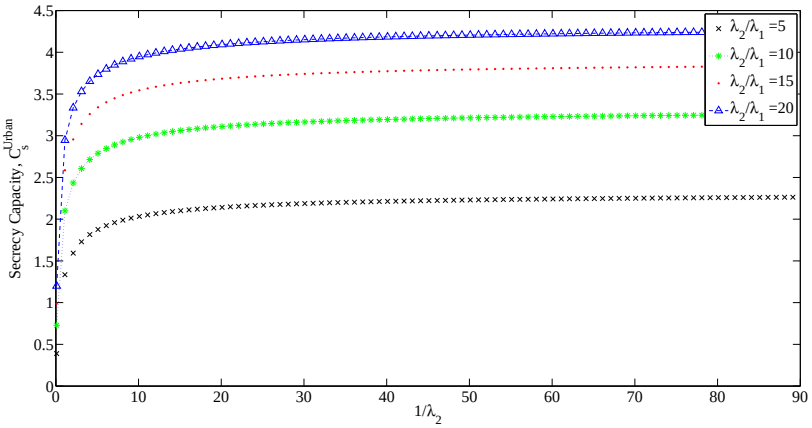

Figure 11. Secrecy Capacity vs $1/\lambda_2$ for different value of λ_2/λ_1 for fading Gaussian wire-tap channel with Rayleigh fading.

Figure 10 and figure 11 show the relationship between secrecy capacity C_s^{urban} and different values of λ_1, λ_2.

5.2. Secrecy Capacity of Fading Wire-tap Channel in Rural Area

Unlike Rayleigh model, Rician model is used for wireless environment where there is dominant path of propagation along with other multipath propagation for

signal. Usually, cellular network in the countryside or along the highway exhibits Rician model like behavior.

Let us assume the channel state s has Rician distribution. Hence the PDF is $f_S(s) = \frac{x}{\sigma^2} e^{\left(\frac{-(x^2+v^2)}{2\sigma^2}\right)} I_0(\frac{sv}{\sigma^2})$, where $I_0(.)$ is the modified Bessel function of the first kind with zero order. The corresponding CDF is $F_S(s) = 1 - -Q_1(\frac{v}{\sigma}, \frac{s}{\sigma})$, where Q_1 is the Marcum Q-function. Variance is a increasing function of v for a particular value of σ.

Hence the CCDF of the channel is

$$\bar{F}_S(s) = Q_1(\frac{v}{\sigma}, \frac{s}{\sigma}). \tag{5.5}$$

We plot the CCDF against channel state for different values of v with $\sigma = 1$. Note that, in the figure 12, we can have either stochastically degraded or reversely

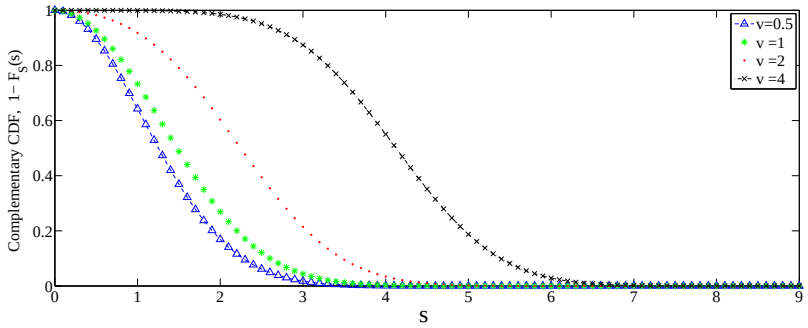

Figure 12. CCDFs vs channel state for different values of v for Rician fading.

degraded wire-tap channel for Rician distribution as well. Consider the CCDF of the legitimate channel is

$$\bar{F}_{S_1}(s) = Q_1(\frac{v_1}{\sigma}, \frac{s}{\sigma}), \tag{5.6}$$

and the CCDF of the eavesdropper is

$$\bar{F}_{S_1}(s) = Q_1(\frac{v_2}{\sigma}, \frac{s}{\sigma}). \tag{5.7}$$

Again,we assume $v_1 > v_2$. Otherwise, computing secrecy capacity is trivial because in that case, the capacity is zero.

The secrecy capacity is given by Theorem 2

$$C_s^{rural} = \log e \int_0^{\infty} \big(Q_1(\frac{v_1}{\sigma}, \frac{s}{\sigma}) - Q_1(\frac{v_2}{\sigma}, \frac{s}{\sigma})\big) \frac{1}{1+s} ds. \tag{5.8}$$

Figure 13 and figure 14 show the relationship between secrecy capacity C_s^{urban} and different value of v_1, v_2.

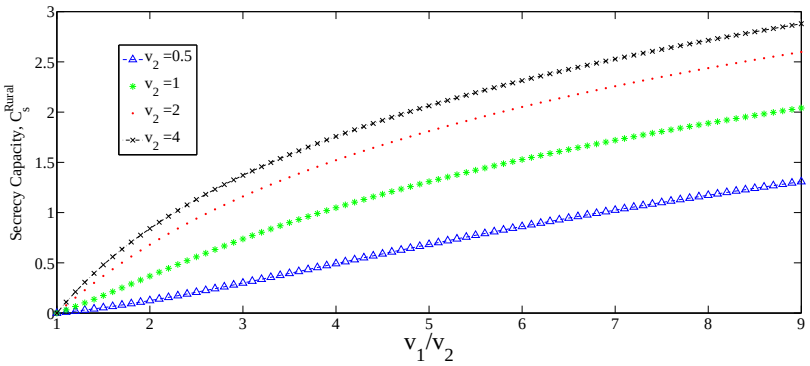

Figure 13. Secrecy Capacity vs v_1/v_2 for different values of v_2 for fading Gaussian wire-tap channel with Rician fading.

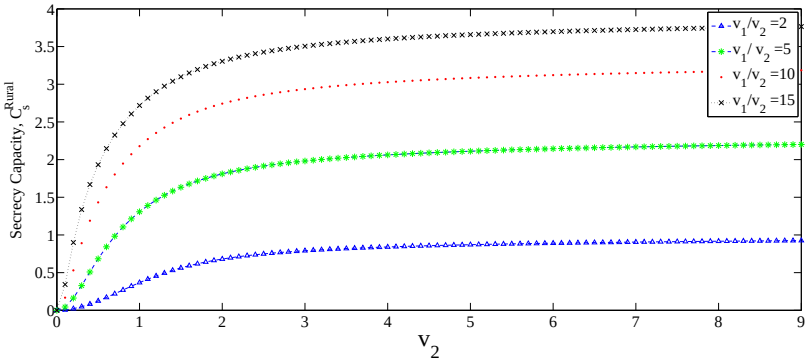

Figure 14. Secrecy Capacity vs v_2 for different value of v_1/v_2 for fading Gaussian wire-tap channel with Rician fading.

Remark 1. *Note that for two of the most predominant wireless environments, namely the urban setting and the rural setting, the capacity characterization of this thesis*

provides complete answer to the secrecy capacity question. For more general fading environments, Theorem 2 *provides an upper-bound to the secrecy capacity and finding achievable schemes which can achieve this upper-bound constitutes a very interesting topic for future research.*

CHAPTER 6. CONCLUSION

We have considered the problem of communicating secret information to a desired receiver through a wireless medium in the presence of a eavesdropping receiver. Time varying channel strength is a very critical issue in wireless channels. Earlier research towards characterization of the secrecy capacity assume the knowledge of this time varying channel strength at the transmitter. For any communication link, the corresponding channel strength is generally measured at the receivers and feed back to the transmitters. Thus for the wireless wiretap channel the availability of channel state information (CSI) at transmitters is not a reasonable assumption, because that would mean the eavesdropper informs the transmitter about its channel strength continuously.

In this work, we assume that the channel states are not available at the transmitter and are known only at the corresponding receivers. To gain insight we first consider a layered abstraction of channels with real channel coefficients and exactly characterize the secrecy capacity of this layered model. The insight revealed from this layered model enable us to derive an outer bound to the capacity of the real channel where the time varying channel coefficients of both the main and eavesdropper channel can assume arbitrary statistics. We then identify a rather broad class of channels - called *stochastically degraded channels* here - for which we characterize the secrecy capacity of the channel. To establish this later result, in addition to the previously mentioned upper bound, we also needed an achievable scheme which can attain a rate same as the upper bound. We show that a Gaussian distributed input can achieve a rate same as the upper bound. This rate thus also represents the secrecy capacity of the channel. Moreover, to illustrate the application of the result of this thesis work in practical scenarios in chapter 5 we have shown that it can be used to characterize the secrecy capacity of two very important and often encountered wireless environments,

namely the urban and the rural environments. In other wireless settings, the general upper bound to capacity provides the first step and paves the way to future research towards exact secrecy capacity characterization.

BIBLIOGRAPHY

[1] Thomas M. Cover and Joy A. Thomas, *Elements of Information Theory*, 2nd edition, John Wiley and Sons, New Jersy, 2006.

[2] C. Shannon, "Communication theory of secrecy systems," *Bell. syst. Tech. J.,* vol. 29, 1949, pp. 656-715.

[3] A. Wyner, "The wire-tap channel," *Bell. syst. Tech. J.,* vol. 54(8), Jan., 1975, pp. 1355-1387.

[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. on Inform. Th.,* vol. 24(3), May, 1978, pp. 339-348.

[5] R. G. Gallager, *"Information Theory and Reliable Communications"*, John Wiley and Sons, New York, 1968.

[6] S.K. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. on Inform. Th.,* vol. 24, no. 4, Jul., 1978, pp. 451-456.

[7] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. on Inform. Th.,* vol. 22, Nov., 1976, pp. 644-652.

[8] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channel," *In IEEE Int. Symp. Inf. Theory,* Sep., 2005, pp. 2152-2155.

[9] P.K. Gopala and L. Lai, and H. El-Gamal., "On the secrecy capacity of fading channels," *IEEE Trans. on Inform. Th.,* vol. 54 ,no. 10, Oct., 2008, pp. 4687-4698.

[10] Z. Li and R.D. Yates, and W. Trappe, "Achieving secret communication for fast Rayleigh fading channels," *IEEE Trans. on Inform. Th.,* vol. 9, no. 9, Sep., 2010, pp. 2792-2799.

[11] A. Avestimehr and D. Digg and D. Tse, "Wireless netowrk information flow: A deterministic approach," *IEEE Trans. on Inform. Th.,* vol. 57 (4), Apr., 2011, pp. 1872-1905.

[12] C. Fragouli and E. Soljanin, "Network coding fundamentals," *Foundations and Trends in Networking,* vol. 2, no. 1, 2007, pp. 1-133.

[13] Y. Liang and V. H.H. Poor, and S. Shamai (Shitz), "Secure communication over fading channels ," *IEEE Trans. on Inform. Th.,*,vol. 54, no. 6, Jun., 2008, pp 2470-2492.

[14] G. Caire and S. Shamai, "On the capacity of some channels with state information," *IEEE Trans. on Inform. Th.,* vol. 45, no. 6 ,Sep., 1999, pp. 2007-2019.

[15] A.J. Goldsmith and P. P. Varaiya, "Capacity of fading channels with side information," *IEEE Trans. on Inform. Th.,* vol. 43, no. 6 ,Nov., 1997, pp. 1986-1992.

[16] David N. C. Tse and Roy D. Yates, "Fading broadcast channels with state information at the receivers," *IEEE Trans. on Inform. Th.,* vol. 58, no. 6 ,Jun., 2012, pp. 3453-3471.

[17] D. Guo and S. Shamai and S. Verdu, "Mutual information and minimum mean-square error in Gaussian channels ," *IEEE Trans. on Inform. Th.,* vol. 51, Apr., 2005, pp. 1261-1282.

[18] D. Tse and P. Viswanath, *"Fundamentals of Wireless Communication"*, Cambridge University press, New York, 2005.