PRIVACY RATE

A Thesis
Presented to
The Academic Faculty

By

Seonwoo Lee

In Partial Fulfillment
of the Requirements for the Degree
Master of Science
in
Electrical and Computer Engineering

School of Electrical and Computer Engineering
Georgia Institute of Technology
August 2021

PRIVACY RATE

Approved by:

Dr. Mary Ann Weitnauer, Committee Chair
Professor, School of ECE
Georgia Institute of Technology

Dr. Gregory Durgin
Professor, School of ECE
Georgia Institute of Technology

Dr. Matthieu Bloch
Associate Professor, School of ECE
Georgia Institute of Technology

Date Approved: July 30, 2021

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

A Lower bound of Dave's noise uncertainty interval.

B Upper bound of Dave's noise uncertainty interval.

H_{d} Channel gain between Alice to Dave.

$d[n]$ Dave's received signal.

ϵ An arbitrarily small number.

$\mathbf{G}$ Vector of channel gains between Alice and Dave.

γ Dave's detection threshold.

Γ_{d} Dave's noise power.

$\widehat{\Gamma}_{\mathrm{d}}$ Dave's uncertain noise power.

Γ_{hd} Variance of channel gain between Alice and Dave.

Γ_{hr} Variance of channel gain between Alice and Bob.

Γ_{r} Bob's noise power.

Γ_{s} Alice's transmit power.

$\mathbf{H}$ Matrix of MIMO channel gains between Alice and Bob.

H_{r} Channel gain between Alice and Bob.

P_{D} Probability of Detection.

ξ Probability of Detection Errors = $P_{\mathrm{FA}}+ P_{\mathrm{MD}}$.

ξ’ Robust Probability of Detection Errors with an infinite number of samples.

ξ” ξ’ at 1 sample.

ξ”’ Robust Probability of Detection Errors with a finite number of samples.

P_{FA} Probability of False Alarm.

P_{MD} Probability of Missed Detection.

C_{pr} Privacy capacity.

R_{pr} Privacy rate.

ψ Path loss proportionality constant.

$r[n]$ Bob’s received signal.

r_{d} Distance between Alice and Dave.

r_{r} Distance between Alice and Bob.

$s[n]$ Alice’s transmitted signal.

SUMMARY

In some situations, a user would like to communicate without detection. It has been shown that it is impossible to achieve positive rate while remaining undetectable to a third party. However, that work assumes that the detector is certain about their own noise power, which inherently has uncertainty because that knowledge is based on a measurement. By exploiting this uncertainty the transmitter can achieve a positive rate while remaining undetectable to a third party. This positive rate is quantified in numerous scenarios: Single Input Single Output (SISO) Additive White Gaussian Noise (AWGN) and Rayleigh channels (with channel state information (CSI) and channel distribution information (CDI)), and Multiple Input Multiple Output (MIMO) Rayleigh channels. Finally, building on previous work, it is shown that for a detector to lower their maximum possibility of an error, they should not take as many samples as possible–a counterintuitive result. This is explained in more detail in the last chapter.

CHAPTER 1

INTRODUCTION

1.1 Motivation and Background

In wireless communications there are situations where a user would want to communicate such that his emissions are undetectable to other users—that is, transmit with privacy. One emerging example is underlay cognitive radio (CR) [1], where a secondary user seeks to communicate with such low power as to not interfere with or be detected by primary users. Another example is secure communications where a wireless user does not want to reveal his presence in the spectrum to an eavesdropper. Many attacks on wireless networks are predicated on an attacker's ability to determine that a target is transmitting [2, 3]. By transmitting with sufficiently low power we can avoid potential network attacks and also politely use the spectrum in the presence of primary users. In this thesis we determine the achievable communications rate afforded by the privacy constraint under a variety of eavesdropper and channel assumptions.

To formalize our objective, consider a scenario where two users, Alice and Bob, would like to communicate over a wireless channel without being detected by a detector, Dave. Dave's objective is not to decode Alice's transmissions, but merely to detect the presence of Alice's transmissions. If Alice does not want to reveal her position or even her existence, encrypting her communications is not enough. Bash, Goeckel, and Towsley found that if Alice knows a lower bound of Dave's noise power, $O(\sqrt{N})$ bits can be sent in N channel uses while guaranteeing that Dave's sum of probability of false alarm P_{FA} and missed detection P_{MD} is asymptotically arbitrarily close to one [4].

To make this more clear, we define two terms. $I(N)$, which behaves as $O(\sqrt{N})$, is the number of undetected error-free bits that can be sent in N channel uses. Likewise, $C_{pr} = \lim_{N\to\infty} I(N)/N$ is the error-free privacy channel capacity. The result in [4] means that $C_{pr} = 0$ in Additive White Gaussian Noise (AWGN) channels. While the asymptotic rate is zero, this does not mean no information can be communicated—$I(N)$ is positive so long as the probability of detection is nonzero. Bash, Goeckel, and Towsley's work is the first work that we are aware of that puts information theoretic bounds on low probability of detection communication.

The square root law found in [4] relates to problems in steganography where a fixed-size, finite-alphabet covertext object can be changed to hide a message. Because the covertext object is transmitted noiselessly in steganography, $O(\sqrt{N}\log N)$ bits can be transmitted by modifying $O(\sqrt{N})$ symbols in covertext of size N [5, Ch. 8, Ch. 13]. If we put this in information theory terms of rate over a channel, where covertext of size N is analogous to N channel uses, this is still asymptotically zero rate despite the noiseless transmission because $\lim_{N\to\infty} O(\sqrt{N}\log N)/O(N) = 0$.

However, it is possible to achieve a positive rate when we assume that Dave is uncertain of his noise level and uses a radiometer (energy detector) as his detection test. This improves upon the AWGN case with noise power certainty, where positive privacy rate is not possible with a radiometer detector. However, it is important to note that while a radiometer is the optimal detector for AWGN systems where Dave knows his noise variance, a radiometer is not optimal when Dave does not know his noise variance [6]. Thus, the result we present is not as strong as the one in [4], but our result does demonstrate that in practical situations, a positive rate is possible while still guaranteeing that Dave's $P_{\text{MD}} + P_{\text{FA}} \to 1$.

It is important to distinguish privacy capacity from secrecy capacity, which is the maximum error free rate that Alice can talk to Bob, while preventing an eavesdropper from decoding Alice's transmissions. The constraints of privacy and secrecy, while different, do not actually supersede one another [7].

In this thesis we delve into greater detail the notion of an SNR wall [4], and how Alice can use it to her advantage to communicate without being detected. We also try to estimate what kinds of uncertainty we can reasonably expect and the resultant communication rates that Alice and Bob can achieve over Single Input-Single Output (SISO) and Multiple Input-Multiple Output (MIMO) AWGN and Rayleigh channels. We use several assumptions of channel information: channel state information (CSI) on the Alice-Bob and Alice-Dave channels and CSI on the Alice-Bob channel and channel distribution information (CDI) on the Alice-Dave channel.

1.2 Privacy Capacity

Privacy capacity involves three parties: a transmitter, receiver, and detector. It is dependent not only on the transmitter's choice of coding scheme, but also the detector's detection scheme.

1.2.1 System Setup

Consider the communications scenario in Figure 1 where Alice transmits a circularly symmetric Gaussian signal $s[n]$, where n is the time index, with mean 0 and variance Γ_{s}. Bob is her intended receiver, and Dave is a passive detector. Dave is trying to determine Alice's presence–whether or not she is transmitting. Finally, Bob and Dave experience circularly symmetric Gaussian noise of zero mean and variance Γ_{r} and Γ_{d}, respectively.

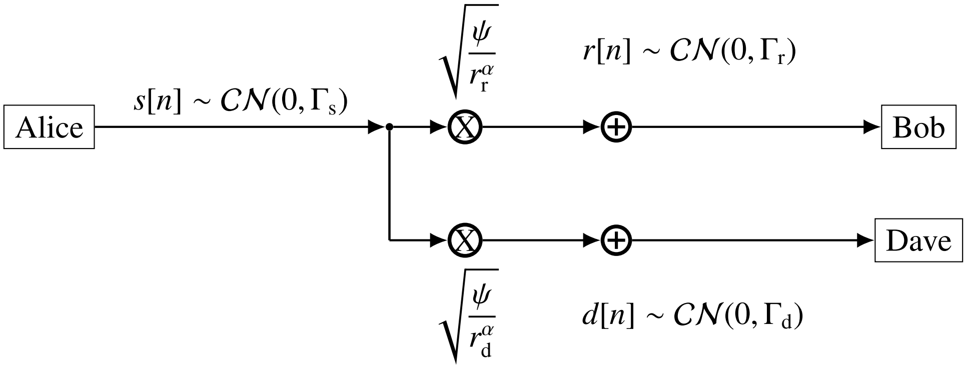

$\sqrt{\frac{\psi}{r_{\mathrm{r}}^{\alpha}}}$
$r[n] \sim \mathcal{CN}(0, \Gamma_{\mathrm{r}})$
$s[n] \sim \mathcal{CN}(0, \Gamma_{\mathrm{s}})$
Alice
Bob
Dave
$\sqrt{\frac{\psi}{r_{\mathrm{d}}^{\alpha}}}$
$d[n] \sim \mathcal{CN}(0, \Gamma_{\mathrm{d}})$

Figure 1: System block diagram.

When a random variable X has a circularly symmetric complex Gaussian distribution with mean μ and variance Γ it is denoted as $X \sim \mathcal{CN}(\mu, \Gamma)$. Bob and Dave are located distances r_{r} and r_{d} from Alice, respectively. All of our signals $s[n]$, $r[n]$, and $d[n]$, are mutually independent. We assume the received signal power, P, is a scaled monomial function of the distance, which is consistent with the free space path loss model where $P \propto 1/r^2$ [8, p. 107], as well as multipath path loss models, where $P \propto 1/r^\alpha$ with α, the path loss exponent, as low as 1.2 and as high as 6.2 [9]. We will let $P = \psi/r^\alpha$ for some proportionality constant ψ. The uncertainty in Dave's noise power measurement is given by $\widehat{\Gamma}_\mathrm{d} \in [A, B]$, where Γ_d is the true noise power. As discussed in Chapter 5, one source of Dave's noise uncertainty Alice can expect and put reasonable bounds on is thermal noise. This is something she can estimate without any knowledge of her channel to Dave.

1.2.2 Detection Metrics

To define privacy capacity, we assume that Dave is trying to distinguish between the following two signal hypotheses,

$$H_0 : x[n] = d[n], \tag{1}$$

$$H_1 : x[n] = \sqrt{\frac{\psi}{r_\mathrm{d}^\alpha}} s[n] + d[n], \tag{2}$$

with $n \in \{1, ..., N\}$ and associated probability distributions $P_0(\mathbf{x})$ and $P_1(\mathbf{x})$, respectively.

The privacy capacity C_pr is defined as the maximum error free rate at which Alice can talk to Bob, while guaranteeing that Dave's sum of probabilities of detection errors is ϵ close to one—that is,

$$\xi = P_\mathrm{MD} + P_\mathrm{FA} > 1 - \epsilon, \tag{3}$$

where P_MD is the probability of missed detection and P_FA is the probability of false alarm for some arbitrarily small ϵ.

It is not immediately obvious that ξ being close to one should be our objective. We are adding two probabilities, which normally results in a value bounded between 0 and 2. However, $P_\mathrm{FA} + P_\mathrm{MD} = P_\mathrm{FA} + 1 - P_\mathrm{D}$, and $P_\mathrm{D} \geq P_\mathrm{FA}$, where P_D is the probability of detection. A detector can always achieve $P_\mathrm{D} = P_\mathrm{FA}$ by ignoring the input data and flipping a coin with probability of heads being P_D, and declaring a detection when it is heads [10]. Hence any algorithm the detector uses should be able to achieve $P_{\mathrm{D}} \geq P_{\mathrm{FA}}$. Additionally, if $P_{\mathrm{D}} < P_{\mathrm{FA}}$, then the detector can simply switch what they declare a detection and a non-event.

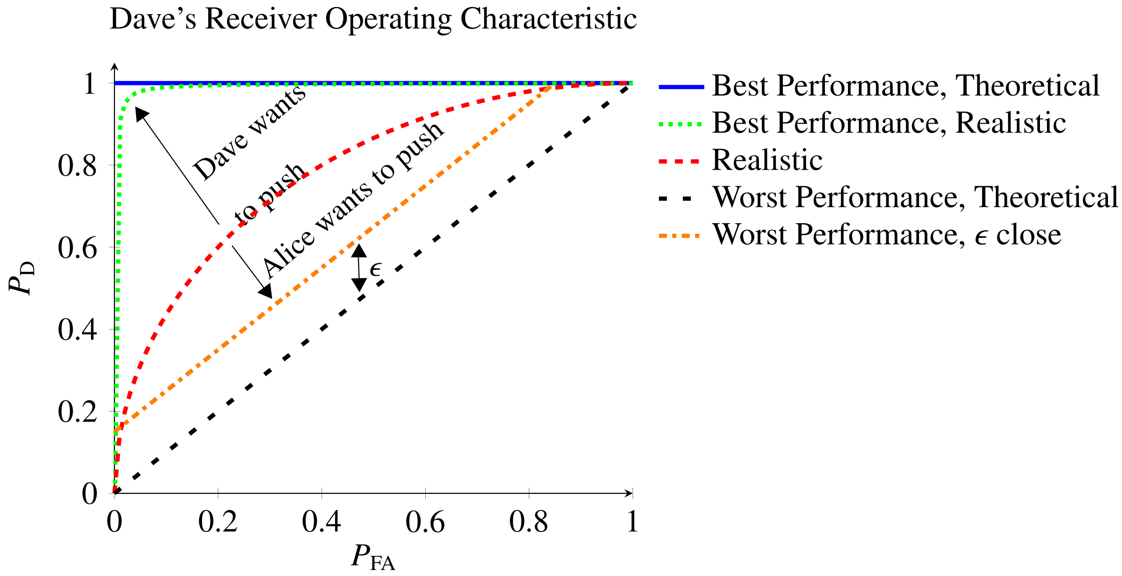


Figure 2: Dave's receiver operating characteristic curves, where best and worst are with respect to Dave.

We can draw this notion of ϵ closeness on a receiver operating characteristic (ROC) curve. In Fig. 2 we've graphed the detector's probability of detection for any given probability of false alarm. The best and worst cases depicted are from Dave's perspective. His absolute best case performance achieves a 100% chance of detecting Alice for any P_{FA}. Of course, in the real world, he can't actually achieve this, but a realistic best case would be the dotted curve in green, where there's a rapid rise in P_{D} as P_{FA} increases from 0 until P_{D} hits 1. In the worst case, Dave ignores the data and flips coins instead, achieving the black dashed line of $P_{\mathrm{D}} = P_{\mathrm{FA}}$. A realistic scenario for Dave is that of the dashed red curve. Dave would like to push this curve out to the upper left corner, where he would have a very large P_{D} for any P_{FA}. Conversely, Alice would like to force Dave's ROC curve to the black dashed line. Practically, Alice can't push Dave's performance that low, but aims to make his curve ϵ close to the worst case (only ϵ greater). In other words, Alice wants

$P_{\mathrm{D}} < P_{\mathrm{FA}} + \epsilon$, which follows from (3).

This ϵ parameter is Alice's notion of outage, which is analogous to how power constrained capacity denotes outage in terms of probability of error.

1.2.3 Theoretical Privacy Capacity

It is possible to bound ξ by bounding the total variation distance between $P_0(x)$ and $P_1(x)$, defined as

$$||P_1 - P_0||_1 = \int |P_1(\mathbf{x}) - P_0(\mathbf{x})| d\mathbf{x}. \tag{4}$$

Under the optimal detector for distinguishing $P_1(x)$ from $P_0(x)$ [11, Ch. 13],

$$\xi = 1 - \frac{1}{2}||P_1 - P_0||_1. \tag{5}$$

Hence, if we force $||P_1 - P_0|| < 2\epsilon$, then Dave's $\xi > 1 - \epsilon$.

1.3 Practical Privacy Rate

Recall that the capacity of an AWGN channel is actually a maximization problem solving for the optimal input distribution while keeping the probability of transmission error less than ϵ. Similarly, to find the privacy capacity under noise uncertainty, we would have to find the input distribution that maximizes the rate of information between Alice and Bob while still keeping $\xi > 1 - \epsilon$. We leave this as an open problem, as the challenge is that for each input distribution Alice could choose, there is a corresponding optimal detector for Dave. A brute force search over all possible input distributions is infeasible as there are infinitely many possible input distributions; to find the optimal input distribution would require a different analytical approach.

We avoid this issue by fixing the detection test to be an energy detector (radiometer), described by

$$T(x) = \frac{1}{N} x^H x = \frac{1}{N} \sum_{n=1}^{N} x[n]^* x[n] > \gamma, \tag{6}$$

where γ is the detection threshold of Dave's choosing and N is the number of samples.

The capacity of an AWGN channel is maximized with a Gaussian input distribution, and the optimal detector for a Gaussian input is a radiometer, so we assume Gaussian signaling for Alice. Under these constraints, we are no longer solving for C_{pr} and instead are solving for an achievable privacy rate R_{pr}. This particular R_{pr} is a lower bound of C_{pr}, as it is an achievable privacy rate with the choice of a particular input distribution (Gaussian) and the optimal detector for that distribution (a radiometer). It is possible that there exists some other input distribution and it's corresponding optimal detector that will result in a higher privacy rate.

The Gaussian input signal is in actuality a shared secret between Alice and Bob. In a traditional AWGN channel without privacy constraints, we know that this achieves and doesn't exceed capacity [12, p. 200].

1.4 SNR Wall

We furthermore assume that Dave is uncertain of his noise power—that is, he only knows his noise $\widehat{\Gamma}_{\text{d}}$ is contained to an interval $I = [A, B]$. In this scenario, Tandra and Sahai showed that robust detection of Alice is impossible [6], even if Dave takes an infinite number of samples. In their proof, they derive

$$P_{\text{FA}} = \max_{\widehat{\Gamma}_{\text{d}} \in [A,\, B]} Q\left(\frac{\gamma - \widehat{\Gamma}_{\text{d}}}{\sqrt{\frac{2}{N}}\widehat{\Gamma}_{\text{d}}} \right) \tag{7}$$

$$P_{\text{MD}} = 1 - \min_{\widehat{\Gamma}_{\text{d}} \in [A,\, B]} Q\left(\frac{\gamma - \Gamma_{\text{s}} - \widehat{\Gamma}_{\text{d}}}{\sqrt{\frac{2}{N}}(\widehat{\Gamma}_{\text{d}} + \Gamma_{\text{s}})} \right), \tag{8}$$

where they have used the Central Limit Theorem (CLT) on the chi square distribution of the test statistic. From this they conclude that Dave cannot detect Alice if she transmits below the SNR wall of $\frac{B-A}{\Gamma_{\text{d}}}$. By maximizing P_{FA} and P_{MD} independently, Dave's true performance is no worse, and with probability 1 better, than if he did not maximize over I. If Dave were to instead just assume one value of $\widehat{\Gamma}_{\text{d}} \in I$, then with probability 1, Dave's assumption about $\widehat{\Gamma}_{\mathrm{d}}$ is incorrect, and his P_{MD} and P_{FA} will be higher than what he calculates.

In Tandra and Sahai's work, when P_{FA} and P_{MD} are maximized independently, B maximizes (7) and A maximizes (8). Because it is obviously impossible for $\widehat{\Gamma}_{\mathrm{d}}$ to be A and B simultaneously, Dave's detection performance can be improved and remain robust. We instead analyze the scenario that Dave maximizes their sum,

$$\xi' = \min_{\gamma} \max_{\widehat{\Gamma}_{\mathrm{d}} \in [A,\, B]} P_{\mathrm{FA}}(\widehat{\Gamma}_{\mathrm{d}}, \gamma) + P_{\mathrm{MD}}(\widehat{\Gamma}_{\mathrm{d}}, \gamma'). \tag{9}$$

Dave performs a min max—for any fixed threshold γ, he has to maximize ξ' over the uncertainty interval for robustness. But he is free to choose any threshold γ, and hence minimizes over his choice of γ to improve detection performance. While we are primarily concerned with this min max, which considers his worst case performance, He. et al studies the implications of taking into account the distribution of noise uncertainty [13].

While in this thesis we only consider that Dave is uncertain about his noise power, Che et. al derive the channel capacity when none of Alice, Bob, or Dave know the noise of both the binary symmetric Alice-Bob channel and the noisier binary symmetric Alice-Dave channel [14].

1.5 Other Means to Overcome the Square Root Law

While in this thesis we only examine exploiting noise power uncertainty to transmit more than $O(\sqrt{n})$ bits in n channel uses, there are other means. For example, Dave's ignorance of when Alice transmits allows her to transmit $O(\min(\sqrt{n \log(T(n))}, n)$ bits in n channel uses, where $T(n)$ is the number of time slots each containing n symbol periods, and Alice may use only a single slot [15]. Another method is the presence of a friendly uninformed jammer, which allows Alice to transmit $O(n)$ bits in n channel uses, thereby achieving a positive rate [16, 17, 18]. A third method is to consider a different channel type not subject to the square root law, such as a continuous time, infinite-bandwidth Poisson channel without a peak power constraint. The privacy capacity of such a channel is infinite [19].

CHAPTER 2
SISO PRIVACY RATE WITH MEASUREMENT UNCERTAINTY

This chapter examines privacy rate for SISO AWGN and Rayleigh channels. Both CSI and CDI are considered for Rayleigh channels.

2.1 AWGN Channel Privacy Rate with Measurement Uncertainty

As is well known, Alice can transmit at a rate of $\log_2(1+\Gamma_\mathrm{s}/\Gamma_r)$ bits per channel use over a AWGN channel when her transmit power is constrained to Γ_s and Bob's noise power is Γ_r [12, Ch 9]. Using this we define the privacy rate as

$$R_\mathrm{pr} = \max_{\Gamma_\mathrm{s}:\ \lim_{N\to\infty}\xi'(N,\Gamma_\mathrm{s})=1} \log_2(1+\tfrac{\psi}{r_\mathrm{r}^\alpha}\tfrac{\Gamma_\mathrm{s}}{\Gamma_\mathrm{r}}), \tag{10}$$

where $\xi'(N,\Gamma_\mathrm{s})$ is the sum of P_FA and P_MD after N observations. By maximizing Γ_s we are maximizing Alice's rate, but we limit ourselves only to the situations where Dave's ξ' approaches 1 as he approaches an infinite number of samples.

2.1.1 Privacy Rate

First we need to establish our P_FA and P_D:

$$\begin{aligned} P_\mathrm{FA} &= Pr(T(x) > \gamma; H_0) \\ &= Pr\left(\frac{1}{N}\sum_{n=1}^{N} d[n]^* d[n] > \gamma\right) \\ &= Q_{\chi^2_{2N}}\left(\frac{2N\gamma}{\widehat{\Gamma}_d}\right) \end{aligned} \tag{11}$$

$$\begin{aligned} P_D &= Pr(T(x) > \gamma; H_1) \\ &= Q_{\chi^2_{2N}}\left(\frac{2N\gamma}{\widehat{\Gamma}_d + \frac{\psi}{r_\mathrm{d}^\alpha}\Gamma_\mathrm{s}}\right) \end{aligned} \tag{12}$$

$$\lim_{N\to\infty} P_{\mathrm{FA}} = \begin{cases} 0, & \text{if } \gamma > \widehat{\Gamma}_{\mathrm{d}} \\ 1, & \text{if } \gamma < \widehat{\Gamma}_{\mathrm{d}} \end{cases}, \tag{13}$$

$$\lim_{N\to\infty} P_D = \begin{cases} 0, & \text{if } \gamma > \widehat{\Gamma}_{\mathrm{d}} + \frac{\psi}{r_{\mathrm{d}}^{\alpha}}\Gamma_{\mathrm{s}} \\ 1, & \text{if } \gamma < \widehat{\Gamma}_{\mathrm{d}} + \frac{\psi}{r_{\mathrm{d}}^{\alpha}}\Gamma_{\mathrm{s}}, \end{cases} \tag{14}$$

where $Q_{\chi^2_{2N}}$ is the tail probability of a chi square distribution of $2N$ samples, and for some choice of $\widehat{\Gamma}_{\mathrm{d}} \in [A, B]$. We want to maximize Alice's signal power while forcing $\xi \to 1$, so we can either force $P_{\mathrm{D}} \to 0$ or $P_{\mathrm{FA}} \to 1$. To do this we need to satisfy

$$\gamma < \widehat{\Gamma}_{\mathrm{d}} \tag{15}$$

or

$$\gamma > \widehat{\Gamma}_{\mathrm{d}} + \frac{\psi}{r_{\mathrm{d}}^{\alpha}}\Gamma_{\mathrm{s}} \tag{16}$$

for all γ and some $\widehat{\Gamma}_{\mathrm{d}} \in [A, B]$ while maximizing Γ_{s}. For $\gamma < B$, we can choose $\widehat{\Gamma}_{\mathrm{d}} = B$ to satisfy (15). For $\gamma \geq B$, we can't satisfy (15) but we can satisfy (16) by choosing $\widehat{\Gamma}_{\mathrm{d}} = A$ and constraining

$$\frac{\psi}{r_{\mathrm{d}}^{\alpha}}\Gamma_{\mathrm{s}} < B - A. \tag{17}$$

Hence, the Signal to Noise Ratio (SNR) wall to force $\xi \to 1$ is

$$\Gamma_{\mathrm{s}} = r_d^{\alpha}(B - A)/\psi. \tag{18}$$

Given this, for Alice to achieve privacy, she should emit less power than (18), resulting in

$$\begin{aligned} R_{pr} &= \lim_{N\to\infty} \log_2(1 + \tfrac{\psi}{r_{\mathrm{r}}^{\alpha}}\tfrac{\Gamma_{\mathrm{s}}}{\Gamma_{\mathrm{r}}}) \\ &= \log_2\left(1 + \left(\tfrac{r_{\mathrm{d}}}{r_{\mathrm{r}}}\right)^{\alpha} \tfrac{B-A}{\Gamma_{\mathrm{r}}}\right). \end{aligned} \tag{19}$$

2.1.2 Lower Bound on SNR Wall

Alice can communicate with a positive rate given by (19) while forcing Dave's detector's $P_{\mathrm{D}} \to 0$ or $P_{\mathrm{FA}} \to 1$ so long as she talks below the SNR wall in (18). Unfortunately, Alice does not know what Dave's uncertainty is, so Alice cannot know with certainty if she is communicating just below the SNR wall to maximize her rate. However, she can lower bound all of the SNR wall parameters under some assumptions.

In most situations there is at least some area in which Alice can be certain that there is no eavesdropper, such as her immediate vicinity or her building. She can use this to lower bound r_d. Dave's noise level depends on the temperature, so Alice can also lower bound $B - A$ by assuming a temperature uncertainty that is less than what is available in highly-accurate thermometers. The noise level Γ_d can also be lower bounded by assuming a temperature in Dave's receiver and some noise figure. The path loss exponent α can be lower bounded as well based on the propagation environment characteristics.

With these lower bounds, Alice can achieve private communication—that is, she can pick a rate $R < R_{pr} = \log_2\left(1 + \left(\frac{r_\mathrm{d}}{r_\mathrm{r}}\right)^{\alpha} \frac{B-A}{\Gamma_\mathrm{r}}\right)$. Numerical results are discussed in Chapter 5.

Goeckel et. al examine the implications when Dave has the full collection of channel observations, instead of abstracting Dave's error to the noise level only being known between A and B [20]

2.2 Rayleigh Fading Channel Privacy Rate with Measurement Uncertainty

Privacy rate can be applied to other channels as well. Here we examine how Rayleigh fading, under both CSI and CDI, affects our privacy rate.

2.2.1 Problem Statement

We can also apply similar analysis to Rayleigh fading channels with complex valued symbols as depicted in Fig. 3. All other aspects of the scenario are the same as the AWGN setup. For simplicity, the channel gains H_d and H_r are assumed to be static over the signaling period.

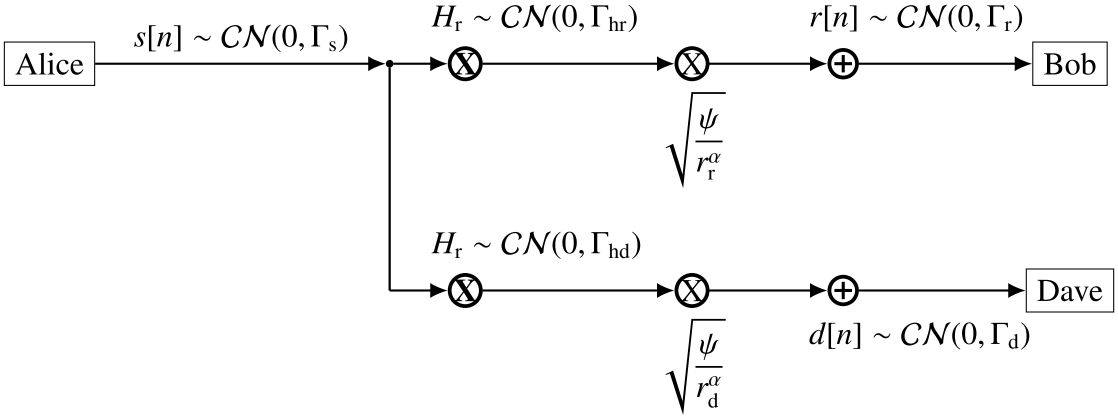

Alice
$s[n] \sim \mathcal{CN}(0, \Gamma_{\mathrm{s}})$
$H_{\mathrm{r}} \sim \mathcal{CN}(0, \Gamma_{\mathrm{hr}})$
$r[n] \sim \mathcal{CN}(0, \Gamma_{\mathrm{r}})$
Bob
$\sqrt{\frac{\psi}{r_{\mathrm{r}}^{\alpha}}}$
$H_{\mathrm{r}} \sim \mathcal{CN}(0, \Gamma_{\mathrm{hd}})$
Dave
$d[n] \sim \mathcal{CN}(0, \Gamma_{\mathrm{d}})$
$\sqrt{\frac{\psi}{r_{\mathrm{d}}^{\alpha}}}$

Figure 3: System block diagram.

For detection the two hypotheses are:

$$H_0 : x[n] = d[n] \tag{20}$$

$$H_1 : x[n] = \sqrt{\frac{\psi}{r_{\mathrm{d}}^{\alpha}}} H_d s[n] + d[n]. \tag{21}$$

When Alice has CSI for the Alice-Dave channel, Dave and Alice's objectives are the same as the AWGN case. We use the same strategy to analyze the privacy rate in this scenario. This is an unlikely scenario in practice because Dave and Alice do not cooperate in any way, but the resulting privacy rate gives us an idea of the best case privacy rate Alice can hope to achieve.

When Alice only has CDI for the Alice-Dave channel, Dave's objective is the same as the AWGN case. However, Alice can no longer guarantee that $\xi' \to 1$ because she will not know the instantaneous value of the channel fade. Accordingly, we have to change the constraint in the privacy rate definition to be $E[\lim_{N\to\infty} \xi'(\Gamma_{\mathrm{s}}, N)] > 1 - \epsilon$.

2.2.2 Privacy Rate Under Alice-Dave CSI

Under CSI with a static channel gain, the channel is still characterized as a AWGN channel with a known scalar multiplier, so we assume Gaussian signaling for Alice. Dave uses the same detection test as the AWGN case and hence the same detection threshold. The probability of detection is now

$$\begin{aligned} P_D &= Pr(T(x) > \gamma; H_1), \\ &= Q_{\chi^2_{2N}}\left(\frac{2N\gamma}{\widehat{\Gamma}_d + \frac{\psi}{r_{\mathrm{d}}^{\alpha}}|H_d|^2\Gamma_{\mathrm{s}}}\right). \end{aligned} \tag{22}$$

We quickly see that aside from the addition of a new scale factor $|H_d|^2$ everywhere there is $\frac{\psi}{r_{\mathrm{d}}^{\alpha}}$, our equations for the Rayleigh fading CSI case will be the same as the AWGN case. Hence Alice should talk below

$$\Gamma_{\mathrm{s}} = \frac{(B-A)r_d^{\alpha}}{|H_d|^2\psi}. \tag{23}$$

Using the SNR from (23),

$$\begin{aligned} R_{pr}|H_d, H_r &= \lim_{N\to\infty} \log_2(1 + \tfrac{\psi}{r_{\mathrm{r}}^{\alpha}}\tfrac{\Gamma_{\mathrm{s}}}{\Gamma_{\mathrm{r}}}) \\ &= \log_2(1 + \left(\tfrac{r_{\mathrm{d}}}{r_{\mathrm{r}}}\right)^{\alpha} \tfrac{|H_r|^2}{|H_d|^2}\tfrac{B-A}{\Gamma_{\mathrm{r}}}). \end{aligned} \tag{24}$$

Assuming $H_d \sim \mathcal{CN}(0, \Gamma_{hd})$ and $H_r \sim \mathcal{CN}(0, \Gamma_{hr})$, we have

$$R_{pr} = \log_2(1 + \left(\tfrac{r_{\mathrm{d}}}{r_{\mathrm{r}}}\right)^{\alpha} \Omega\tfrac{\Gamma_{hr}}{\Gamma_{hd}}\tfrac{B-A}{\Gamma_{\mathrm{r}}}), \tag{25}$$

where $\Omega \sim F(2, 2)$, that is, an F-distribution. With this, the ergodic rate is

$$\begin{aligned} R_{pr,erg} &= \int_0^{\infty} \log_2\left(1 + \left(\tfrac{r_{\mathrm{d}}}{r_{\mathrm{r}}}\right)^{\alpha} \tfrac{\Gamma_{\mathrm{hr}}}{\Gamma_{\mathrm{hd}}}\tfrac{B-A}{\Gamma_{\mathrm{r}}}x\right) f_x(x)dx \\ &= \int_0^{\infty} \log_2(1 + \left(\tfrac{r_{\mathrm{d}}}{r_{\mathrm{r}}}\right)^{\alpha} \tfrac{\Gamma_{\mathrm{hr}}}{\Gamma_{\mathrm{hd}}}\tfrac{B-A}{\Gamma_{\mathrm{r}}}x)(1+x)^{-2}dx \\ &= \tfrac{D}{D-1}\log_2(D), \end{aligned} \tag{26}$$

where $D = \frac{\Gamma_{\mathrm{hr}}}{\Gamma_{\mathrm{hd}}}\frac{B-A}{\Gamma_{\mathrm{r}}}\left(\frac{r_{\mathrm{d}}}{r_{\mathrm{r}}}\right)^{\alpha}$.

We can also find the outage rate

$$\begin{aligned} Pr(R_{pr} < c) &= Pr\left(F(2, 2) \leq \frac{2^c - 1}{D}\right) \\ &= \frac{(2^c - 1)}{(2^c - 1) + D} \end{aligned} \tag{27}$$

as shown in Figure 4.

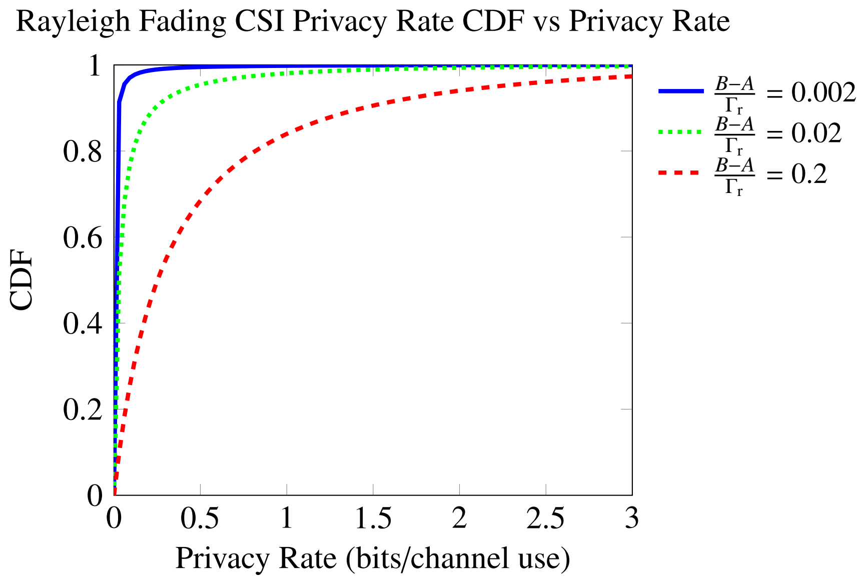


Figure 4: Rayleigh Privacy Rate under CSI for various values of $\frac{B-A}{\Gamma_r}$. Other parameter ratios - $\frac{\Gamma_{hr}}{\Gamma_{hd}}$ and $\left(\frac{r_d}{r_r}\right)^{\alpha}$ - are 1.

2.2.3 Analysis of Privacy Rate under CSI

Alice can communicate with a positive rate and ξ arbitrarily close to 1 so long as she talks below the SNR wall in (23). If we compare the privacy rates of the Rayleigh fading and AWGN channels,

$$Pr(\text{Privacy Rate}_{\text{Rayleigh}} < \text{Privacy Rate}_{\text{AWGN}}) = \frac{1}{1+\frac{\Gamma_{hr}}{\Gamma_{hd}}}.$$

we can see that if the channel gains have identical distributions, then the probability that the Rayleigh fading channel under CSI has a greater privacy rate than the AWGN channel is actually one half. There is a small probability that the channel gain ratio will be very large in Alice's favor, and this causes the ergodic privacy rate under CSI to increase over the rate of the AWGN channel. This phenomenon is similar to what occurs in physical layer security - by sending at a high rate when the channel is in Alice's favor, Alice can achieve a higher ergodic secrecy capacity under fading channels than under a AWGN channel [21]. A plot of the outage rate can be found in Fig. 4. We discuss numerical results are discussed in Chapter 5.

2.2.4 Privacy Rate under Alice-Dave CDI

Next we study the privacy rate when only CDI is known about the Alice-Dave channel. We still assume CSI for the Alice-Bob channel. We assume that Alice's signal is uncorrelated with the channel gain to Dave: $E[s[n]^* H_d] = 0\ \forall n$. Otherwise the system setup is the same as the CSI case. However, Alice can no longer guarantee that $\xi' \rightarrow 1$ because she no longer knows the exact value of H_d when she transmits. Hence, we have to modify our definition of privacy rate to

$$\tilde{R}_{pr,\epsilon} = \max_{\lim_{N\to\infty} E[\xi'(\Gamma_{\mathrm{s}},N)]\geq 1-\epsilon} \log_2(1 + \tfrac{\psi}{r_{\mathrm{r}}^{\alpha}}\tfrac{\Gamma_{\mathrm{s}}}{\Gamma_{\mathrm{r}}}). \tag{28}$$

While P_{FA} remains the same, we must further analyze P_{D}.

$$\lim_{N\to\infty} P_{\mathrm{D}}|H_d = \begin{cases} 0, \text{if } \gamma' > \widehat{\Gamma}_{\mathrm{d}} + \dfrac{\psi}{r_{\mathrm{d}}^{\alpha}}|H_d|^2\Gamma_s \\ 1, \text{if } \gamma' < \widehat{\Gamma}_{\mathrm{d}} + \dfrac{\psi}{r_{\mathrm{d}}^{\alpha}}|H_d|^2\Gamma_s \end{cases} \tag{29}$$

$$\lim_{N\to\infty} E[P_{\mathrm{D}}] = \begin{cases} 0, \quad \text{with probability } 1 - Q_{\chi_2^2}\left(\dfrac{\gamma - \widehat{\Gamma}_{\mathrm{d}}}{\frac{\psi}{r_{\mathrm{d}}^{\alpha}}\Gamma_{\mathrm{s}}\Gamma_{hd}/2}\right) \\ 1, \quad \text{with probability } Q_{\chi_2^2}\left(\dfrac{\gamma - \widehat{\Gamma}_{\mathrm{d}}}{\frac{\psi}{r_{\mathrm{d}}^{\alpha}}\Gamma_{\mathrm{s}}\Gamma_{hd}/2}\right). \end{cases} \tag{30}$$

When we analyze ξ' we can see that the worst case scenario for Alice is when Dave picks $\gamma = B$, which maximizes P_D. For any $\gamma < B$, we choose $\widehat{\Gamma}_{\mathrm{d}} = B$. Hence to have $\lim_{N\to\infty} \mathrm{E}[\xi'(N,\Gamma_{\mathrm{s}})] \geq 1 - \epsilon$, we need

$$P_{\mathrm{FA}} + P_{\mathrm{MD}} \geq 1 - \epsilon$$

$$1 - Q_{\chi_2^2}\left(\frac{B - A}{\frac{\psi}{r_{\mathrm{d}}^{\alpha}}\Gamma_{\mathrm{s}}\Gamma_{hd}/2}\right) \geq 1 - \epsilon. \tag{31}$$

Thus, to maximize rate under the constraint, Alice should transmit with power

$$\Gamma_{\mathrm{s}} = \frac{B - A}{\frac{\psi}{r_{\mathrm{d}}^{\alpha}} Q_{\chi_2^2}^{-1}(\epsilon)\Gamma_{hd}/2}.$$

Assuming CSI on the Alice-Bob channel, we have

$$\tilde{R}_{pr,\epsilon}|H_r = \log_2\left(1 + \frac{|H_r|^2}{\Gamma_{hd}/2}\frac{B - A}{\Gamma_r}\left(\frac{r_d}{r_r}\right)^{\alpha}\frac{1}{Q_{\chi_2^2}^{-1}(\epsilon)}\right). \tag{32}$$

Because $|H_r|^2 \sim \frac{\Gamma_{hr}}{2}\chi_2^2$, we can find the ergodic rate

$$\begin{aligned}\tilde{R}_{pr,\epsilon,erg} &= \int_0^\infty \log_2(1+Gx)\frac{e^{-x/2}}{2}dx \\ &= \frac{1}{\ln(2)}\exp\left(\frac{1}{2G}\right)\mathrm{E}_1\left(\frac{1}{2G}\right) \end{aligned} \tag{33}$$

where $E_1(x) = \int_x^\infty \frac{e^{-t}}{t}dt$ and $G = \left(\frac{r_\mathrm{d}}{r_\mathrm{r}}\right)^\alpha \frac{B-A}{\Gamma_\mathrm{r}}\frac{\Gamma_\mathrm{hr}}{\Gamma_\mathrm{hd}}\frac{1}{Q^{-1}_{\chi_2^2}(\epsilon)}$. The derivation of the integral can be found in the appendix.

We can also find the outage rate

$$\begin{aligned}Pr(\tilde{R}_{pr,\epsilon} \leq c) &= Pr\left(\chi_2^2 \leq (2^c-1)\frac{1}{G}\right) \\ &= 1 - Q_{\chi_2^2}\left((2^c-1)\frac{1}{G}\right). \end{aligned} \tag{34}$$

2.2.5 Comparison of Privacy Rates Under Different Channels

A plot of the privacy rates can be found in Fig. 5 with all parameter ratios set to one (that is, $\frac{\Gamma_{hr}}{\Gamma_{hd}} = \frac{r_r}{r_d} = 1$). As we previously observed, the ergodic privacy rate of a Rayleigh channel under CSI is greater than that of a AWGN channel because of the small probability of having a channel gain ratio in Alice's favor. We also observe that the ergodic privacy rate for a Rayleigh channel under CDI is lower than that of an AWGN channel, with only small increases in privacy rate for orders of magnitude increases in ϵ.

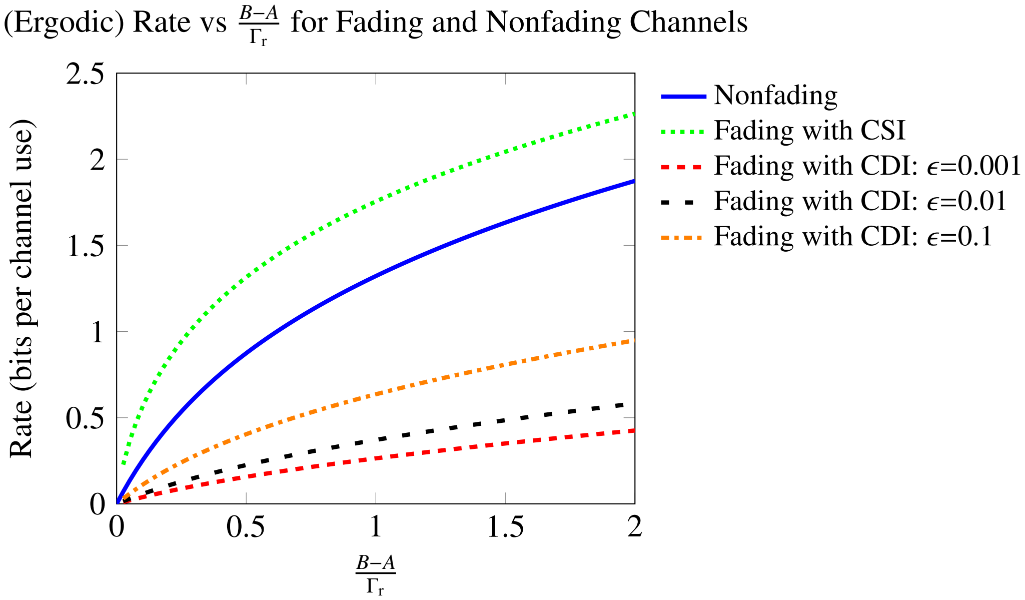
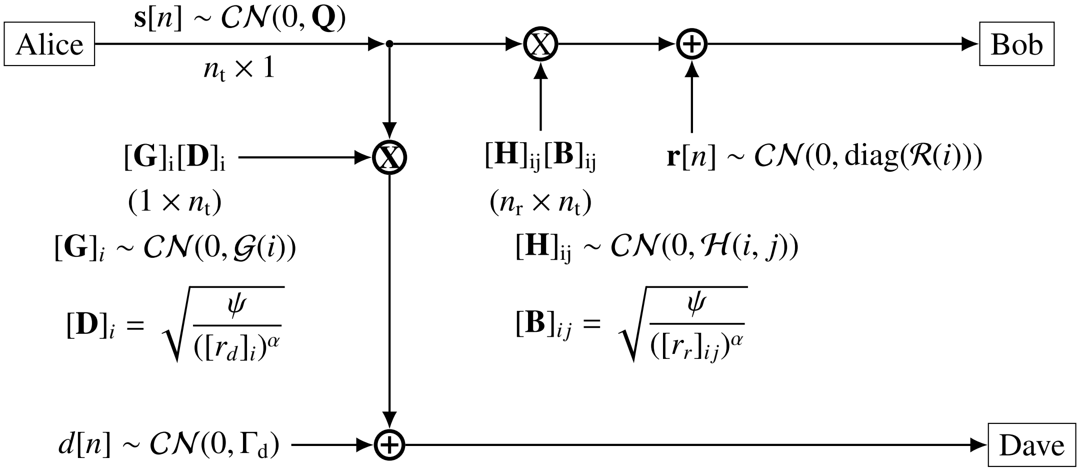


Figure 5: Comparison of Rate or Ergodic Rate vs $\frac{B-A}{\Gamma_r}$. All parameter ratios are 1. The ergodic rate under CDI increases with ϵ.

CHAPTER 3

MIMO RAYLEIGH PRIVACY RATE

We also extend our results to MIMO Rayleigh fading channels with complex valued symbols (Fig. 6). We also assume that while Alice and Bob have multiple antennas, Dave only has one antenna.



Alice
$\mathbf{s}[n] \sim \mathcal{CN}(0, \mathbf{Q})$
$n_t \times 1$
Bob
$[\mathbf{G}]_i[\mathbf{D}]_i$
$(1 \times n_t)$
$[\mathbf{G}]_i \sim \mathcal{CN}(0, \mathcal{G}(i))$
$[\mathbf{D}]_i = \sqrt{\frac{\psi}{([r_d]_i)^\alpha}}$
$[\mathbf{H}]_{ij}[\mathbf{B}]_{ij}$
$(n_r \times n_t)$
$[\mathbf{H}]_{ij} \sim \mathcal{CN}(0, \mathcal{H}(i, j))$
$[\mathbf{B}]_{ij} = \sqrt{\frac{\psi}{([r_r]_{ij})^\alpha}}$
$\mathbf{r}[n] \sim \mathcal{CN}(0, \text{diag}(\mathcal{R}(i)))$
$d[n] \sim \mathcal{CN}(0, \Gamma_d)$
Dave

Figure 6: The circle multiplication symbols denote matrix multiplication.

Let a bolded quantity represent a vector or matrix. Let $\mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{\Xi})$ denote a vector of circularly symmetric complex jointly Gaussian random variables with mean $\boldsymbol{\mu}$ and covariance matrix $\boldsymbol{\Xi}$. Let n_t and n_r denote the number of transmit and receive antennas, respectively. Let the $[\mathbf{v}]_i$ operator be the ith entry of a vector $\mathbf{v}$, and let the $[\mathbf{M}]_{ij}$ operator be the row i, column j entry of a matrix $\mathbf{M}$. Let $\mathcal{H}$ denote the set of all variances of the matrix $\mathbf{H}$, with $\text{Var}([\mathbf{H}]_{ij}) = \mathcal{H}(i, j)$. Let the diag operator denote a diagonal matrix with the diagonal entries given by the argument.

Alice sends signal $\mathbf{s}[n]$ at time index n. Bob and Dave experience noise $\mathbf{r}[n]$ and $d[n]$, respectively. Bob's jth antenna is located $[\mathbf{r_r}]_{ij}$ away from Alice's ith antenna, and Dave's antenna is located $[\mathbf{r_d}]_i$ away from Alice's ith antenna. Bob and Dave experience channel gains $\mathbf{H}$ and $\mathbf{G}$, respectively. We denote the diagonal entries of $\mathbf{Q}$, the covariance matrix of our signal $\mathbf{s}[n]$, as $\mathcal{S}(i)$. For simplicity, the channel gains $\mathbf{H}$ and $\mathbf{G}$ are assumed to be static over the signaling period.

Dave's detection hypotheses are

$$H_0 : x[n] = d[n] \tag{35}$$

$$H_1 : x[n] = \sum_{i=1}^{n_t} \sqrt{\frac{\psi}{([r_d]_i)^\alpha}}[\mathbf{G}]_i[\mathbf{s}[n]]_i + d[n]. \tag{36}$$

Alice's objective is to find the maximum error-free rate at which she can communicate to Bob while forcing $\xi \geq 1 - \epsilon$.

3.1 Privacy Rate under Alice-Dave Channel Distribution Information (CDI)

We assume Dave uses the same detection test from (6). Let $L[n] = \sum_{i=1}^{n_t} \sqrt{\frac{\psi}{([r_d]_i)^\alpha}}[\mathbf{G}]_i[\mathbf{s}[n]]_i + d[n]$, and let $l = \sum_{i=1}^{n_t} \frac{\psi}{([r_d]_i)^\alpha}|[\mathbf{G}]_i|^2\Gamma_{si} + \widehat{\Gamma}_d$. Therefore $L[n] \sim \mathcal{CN}(0, l)$. Then we can find Dave's detection probability

$$\begin{aligned} P_D &= Pr\left(\frac{1}{N}\sum_{n=1}^{N}(L[n]^* L[n]) > \gamma'\right) \\ &= Q_{\chi^2_{2N}}\left(\frac{2N\gamma'}{\sum_{i=1}^{n_t} \frac{\psi}{([r_d]_i)^\alpha}|[\mathbf{G}]_i|^2\mathcal{S}(i) + \widehat{\Gamma}_d}\right). \end{aligned} \tag{37}$$

Dave's asymptotic P_{D} and P_{FA} are [22]

$$\lim_{N\to\infty} P_{\mathrm{FA}} = \begin{cases} 0, & \gamma' > \widehat{\Gamma}_d \\ 1, & \gamma' < \widehat{\Gamma}_d \end{cases} \tag{38}$$

$$\lim_{N\to\infty} P_{\mathrm{D}} = \begin{cases} 0, & \gamma' > \sum_{i=1}^{n_t} \frac{\psi}{([r_d]_i)^\alpha}|[\mathbf{G}]_i|^2\mathcal{S}(i) + \widehat{\Gamma}_d \\ 1, & \gamma' < \sum_{i=1}^{n_t} \frac{\psi}{([r_d]_i)^\alpha}|[\mathbf{G}]_i|^2\mathcal{S}(i) + \widehat{\Gamma}_d \end{cases} \tag{39}$$

For Dave to robustly detect Alice he should choose the γ' that maximizes ξ'. Forcing $\xi' \to 1$ is equivalent to forcing $P_{\mathrm{D}} \to 0$ for $\widehat{\Gamma}_d = B$ [22]. However, we can only lower bound $Pr(\xi' \to 1)$ because under CDI the $[\mathbf{G}]_i$'s are random. Hence

$$Pr\left(\sum_{i=1}^{n_t} \frac{\psi}{([r_d]_i)^\alpha}|[\mathbf{G}]_i|^2\mathcal{S}(i) < B - A\right) \geq 1 - \epsilon. \tag{40}$$

Ideally we would use a generalized chi square distribution (the $|[\mathbf{G}]_i|^2$ are χ_2^2 distributed) and calculate the set $\mathcal{S}$ that satisfies (40). However, we are unable to find an analytical solution. Instead, we use the Lyapunov Central Limit Theorem (LCLT) for an approximate analytical solution (see Chapter 3.1.1), and also compute the constraint numerically (see Chapter 3.1.2).

Once we have the set of valid power allocations,

$$R_{pr} = \max_{\substack{\mathbf{Q}: \begin{array}{c}\mathcal{S} \text{ satisfies (40), } [\mathbf{Q}]_{ii} \le \mathcal{S}(i)\ \forall i, \\ \mathbf{Q} \text{ positive semidefinite}\end{array}}} \log_2 |\mathbf{I} + \mathbf{H}\mathbf{Q}\mathbf{H}^H|. \tag{41}$$

3.1.1 Analytic Solution to Privacy Rate under Alice-Dave CDI

For this solution we assume $[\mathbf{r_d}]_i = r_d, [\mathbf{G}]_i = \Gamma_g, \mathcal{R}(i) = \Gamma_r, [\mathbf{r_r}]_{ij} = r_r, \mathcal{H}(i,j) = \Gamma_h\ \forall i, j$. These parameter uniformity assumptions allow us to use the Marchenko-Pastur (MP) law [23]. We also assume $n_t = n_r = \tilde{n}$, but these results can be generalized to $n_t \neq n_r$.

We use the LCLT, which unlike the classical CLT allows for the random variables to not be identically distributed but requires some extra bounds on their means and variances. The LCLT allows us to avoid the problem of using the inverse tail of a generalized chi square distribution $Q^{-1}_{\chi_2^2;\mathcal{S}}(\cdot)$, where the function itself depends on $\mathcal{S}$, the values we are trying to solve for. By applying the LCLT to (40),

$$\sum_{i=1}^{\tilde{n}} \frac{\psi}{r_{\mathrm{d}}^{\alpha}} \Gamma_g \mathcal{S}(i) + Q^{-1}(\epsilon) \sqrt{\sum_{i=1}^{\tilde{n}} \left(\frac{\psi}{r_{\mathrm{d}}^{\alpha}} \Gamma_g \mathcal{S}(i) \right)^2} \le B - A. \tag{42}$$

At first glance this equation seems like a solution to bypass the difficulty of an analytical solution. However, the application of the LCLT in this instance assumed that $\tilde{n}$, the number of Alice's (and Bob's) antennas, approaches infinity. Additionally, we have assumed that all of Alice's antennas are equidistant to Dave. This would require that all of Alice's antennas be placed on a circle (or sphere), with the center at Dave. However, we will see in Chapter 3.1.2 that the combination of the LCLT's $\tilde{n} \to \infty$ assumption with the following constraint results in a good approximation of privacy rate.

To simplify (42), we use the norm property that for $a_i \geq 0$,

$$\sqrt{\sum_i a_i^2} \leq \sum_i a_i, \tag{43}$$

giving us the new constraint function

$$\sum_{i=1}^{n_t} \mathcal{S}(i) \leq \frac{B - A}{(1 + Q^{-1}(\epsilon))\frac{\psi}{r_{\mathrm{d}}^{\alpha}}\Gamma_g}. \tag{44}$$

To understand (43), observe that the unit ball described by setting the right hand side (RHS) of (43) to one is a strict subset of the unit ball described by setting the left hand side of (43) to one. Hence by using the RHS, we have restricted the valid set of power allocations that we are maximizing over.

From this point forward we use the MP distribution. The MP law tells us the distribution of the eigenvalues of a matrix $\mathbf{JJ^H}$ when $[\mathbf{J}]_{ij} \sim \mathcal{CN}(0, 1)$ [23]. The parameter uniformity assumptions allow us to write our new channel matrix $\tilde{\mathbf{H}} = \sqrt{\Gamma_h}\mathbf{JJ}^H$. If the distribution of the eigenvalues for the general $\mathbf{H}$ were known, that distribution could be used.

If we take the singular value decomposition (SVD) of $\tilde{\mathbf{H}} = \sqrt{\Gamma_h}\mathbf{U\Sigma V}^H$ where $\mathbf{\Sigma} = \mathrm{diag}(\sigma_i)$ and let $\mathbf{Q} = \mathbf{VSV}^H$ where $\mathbf{S} = \mathrm{diag}(\frac{\mathcal{S}(i)}{\Gamma_r})$ then our privacy rate approximation is

$$R_{pr,CLT} = \max_{\substack{\mathcal{S}: \ \mathcal{S}(i) \geq 0 \ \forall i, \\ \mathcal{S} \text{ satisfies (44)}}} \sum_{i=1}^{\tilde{n}} \log_2 \left(1 + \sigma_i^2 \frac{\Gamma_h \psi \mathcal{S}(i)}{r_r^{\alpha}\Gamma_r}\right) \tag{45}$$

where $\sigma_i^2 = \lambda_i$ are the eigenvalues of $\mathbf{JJ}^H$. Our numerical solution in 3.1.2 considers the off diagonal elements of $\mathbf{Q}$.

By using Lagrange multipliers and Kuhn-Tucker conditions, we can find the optimal power allocation as

$$\mathcal{S}(i) = \left(\frac{\theta}{(1 + Q^{-1}(\epsilon))\frac{\psi}{r_{\mathrm{d}}^{\alpha}}\Gamma_g} - \frac{\Gamma_r r_r^{\alpha}}{\psi\Gamma_h\lambda_i}\right)^+ \quad \forall i \tag{46}$$

where θ is a water filling parameter chosen such that

$$\frac{B - A}{1 + Q^{-1}(\epsilon)} = \sum_{i=1}^{\tilde{n}} \left(\frac{\theta}{1 + Q^{-1}(\epsilon)} - \left(\frac{r_r}{r_d}\right)^{\alpha} \frac{\Gamma_r\Gamma_g}{\lambda_i\Gamma_h}\right)^+ \tag{47}$$

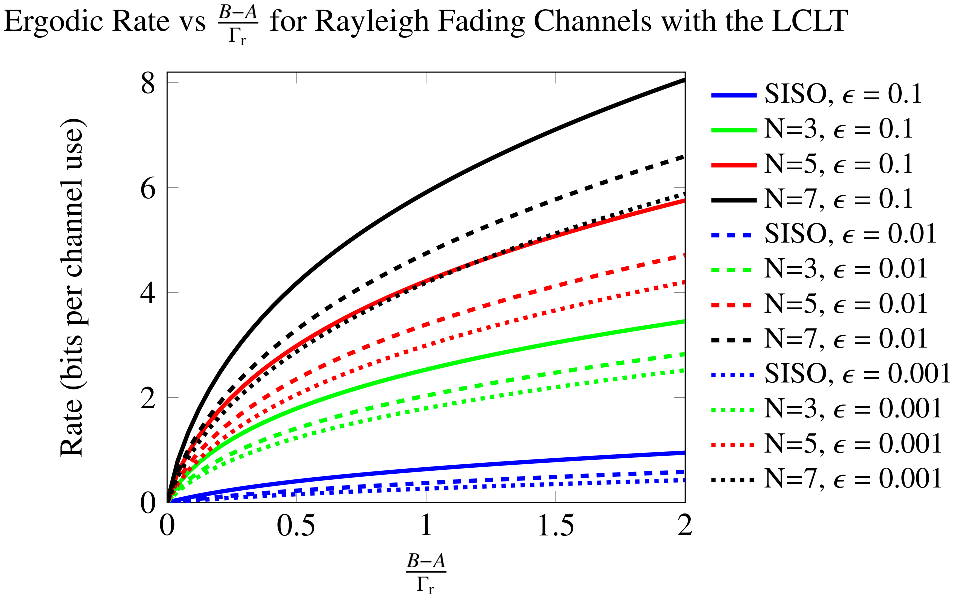


Figure 7: Privacy rates vs $\frac{B-A}{\Gamma_r}$ under the LCLT model. Rates increase with ϵ and number of antennas

The familiar water filling solution follows from the fact that applying the LCLT and (43) changes our constraint function (44) to a total power constraint.

While the eigenvalue distribution of $\tilde{\mathbf{H}}$ converges asymptotically with the number of antennas, it converges very quickly. By using equations (15), (19), (20), and (21) in [23] with

$$P_0 = \frac{B-A}{\Gamma_r}\frac{1}{1+Q^{-1}(\epsilon)}\frac{\Gamma_h}{\Gamma_g}\left(\frac{r_d}{r_r}\right)^{\alpha} \tag{48}$$

we get an analytical approximation of the privacy rate. The complete equations are not particularly insightful but have been included in the appendix.

If $n_t \neq n_r$, the rate bound can be found numerically by evaluating (15) in [23]. The privacy rates are plotted in Fig. 7 for 1, 3, 5, and 7 antennas, with $\epsilon = 0.001, 0.01,$ and 0.1.

This privacy rate differs to that found in [24], which also analyzed a MIMO setup between Alice and Bob. Hero derives $C_{pr} = \mathrm{E}\left[\log\left(\frac{1}{2}\sqrt{1+\mu\lambda_i^2}\right)\right]$ where λ_i are the eigenvalues of $\mathbf{H}^H\mathbf{H}$ and μ is a water-filling parameter. However, the low probability of detection (LPD) constraint in [24] is different from ours, instead constraining the Chernoff exponent, which limits how quickly Dave's detection errors decay exponentially to zero. This Chernoff exponent constraint acknowledges that while Dave's detection will be asymptotically perfect with noise power certainty, it is still possible to transmit a finite amount of data with a reasonably high ξ for Dave. Our result differs because we assume noise power uncertainty and a radiometer for Dave.

3.1.2 Numerical Solution to Privacy Rate under Alice-Dave CDI

Again, we are interested in maximizing Alice's rate under the constraint given by (40). By using the generalized χ_2^2 distribution [25], we plot valid power allocations for arbitrary values of ψ, $\frac{B-A}{\Gamma_r}, \mathcal{G}, \Gamma_d$ and r_d, with $\tilde{n} = 3$.

Because the rate monotonically increases with power, we are only interested in power allocations at the boundary of our constraint function. The discrete points in Fig. 8 come from (40), whereas the surface plot is that of an ellipsoid, as $(\frac{x}{\mathcal{S}(1)})^2 + (\frac{y}{\mathcal{S}(2)})^2 + (\frac{z}{\mathcal{S}(3)})^2 = 1$, where $\mathcal{S}$ can be found by solving $\mathcal{S}(i) = \frac{B-A}{\frac{\psi}{([r_d]_i)^\alpha} Q_{\chi_2^2}^{-1}(\epsilon)\mathcal{G}(i)/2}$, the maximum power allowed for that antenna if only that antenna were used [22]. The model match can be evaluated by calculating the average of $(\frac{x}{\mathcal{S}(1)})^2 + (\frac{y}{\mathcal{S}(2)})^2 + (\frac{z}{\mathcal{S}(3)})^2$, which is approximately 0.9 for the plotted values and for thirty other sets of arbitrarily chosen parameters. Additionally, all the points are strictly interior to the corresponding ellipsoid. As a side note, consider that the constraint surface for total power-constrained MIMO is a plane in the first hyperoctant.

When just accounting for thermal noise, we have a low resultant transmit power, as we will see in Chapter 5. Under the traditional sum power constraint, maximizing MIMO capacity at low SNR involves beamforming. The optimal beamforming covariance matrix is $\mathbf{Q} = P\mathbf{v}\mathbf{v}^H$, where P is the power constraint and $\mathbf{v}$ is the right singular vector of $\mathbf{H}$ that corresponds to its largest singular value. We can employ this same method for the MIMO privacy rate. However it is important to note that while precoding with the right singular vectors is optimal under the sum power constraint, it is not optimal under a per-antenna power constraint [26]. Finding the privacy rate can be reformulated as finding the maximum of the capacities with per-antenna power constraints for each valid power allocation in Fig.

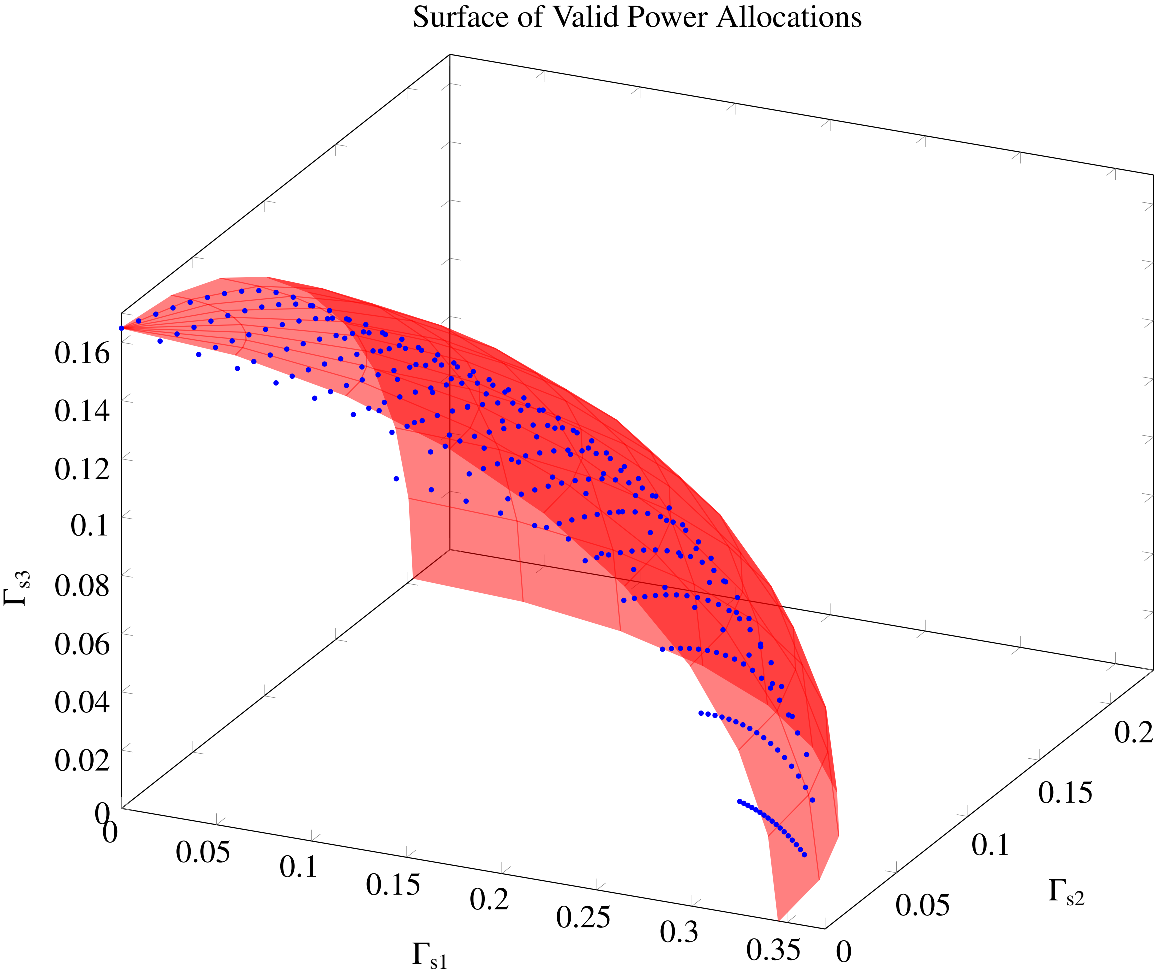


Figure 8: Boundary surface of valid power allocations for arbitrary ψ, $\frac{B-A}{\Gamma_r}$, ϵ, ρ, Γ_g, r_d. All points below the surface in the first octant are also valid. The discrete points are the true boundary, whereas the background surface is an ellipsoid.

8. The advantage of using the right singular vectors is that it is computationally inexpensive - it only involves finding the SVD of $\mathbf{H}$ and then scaling the vector out to the boundary of the valid power allocation surface. Additionally, the beamforming approach does not require the parameter uniformity assumptions, unlike the LCLT approach.

By using only one eigenchannel and sending only one symbol $x \sim \mathcal{CN}(0, \sigma_x^2)$, we precode $\hat{\mathbf{x}} = \mathbf{v}x$. Defining $\mathbf{\Gamma_s} = (\mathcal{S}(1), \mathcal{S}(2), \ldots, \mathcal{S}(n_t))^T$, our power allocation is $\mathbf{\Gamma_s} = \sigma_x^2 \tilde{\mathbf{v}}$, where $\tilde{\mathbf{v}}$ is the vector such that $[\tilde{\mathbf{v}}]_i = |[\mathbf{v}]_i|^2$. We find the scalar σ_x^2 such that $\mathbf{\Gamma_s}$ is at the boundary of the set of valid power allocations. Having found σ_x^2 and λ_1, the largest eigenvalue of $\mathbf{H}\mathbf{H}^H$,

$$R_{pr,\text{beamforming}} = \log_2\left(1 + \tfrac{\sigma_x^2 \lambda_1}{\Gamma_r}\right). \tag{49}$$

We then use a Monte-Carlo simulation to find the ergodic rate. Additionally, we do a brute force search to find the true ergodic privacy rate. In our Monte Carlo simulation, for every realization of $\mathbf{H}$ we discretize the space of valid power allocations, calculate the per antenna power constrained (PAPC) capacity at each allocation [26], and then pick the maximum across all power allocations. Because calculating the PAPC capacity is computationally expensive at low power allocations [26], we also present a lower bound which sets the channel covariance matrix as the diagonal matrix with the per antenna power constraints along the diagonal.

We compare the LCLT, beamforming, grid search, and grid search lower bound methods under the parameter uniformity assumptions (as required by the LCLT) in Fig. 9. We see that at 3 antennas the computationally fast LCLT method provides a good approximation of the privacy rate. However, we see increasing the number of antennas increases the error in the LCLT approximation. There are three factors affecting the error approximation: the use of the LCLT which assumes $\tilde{n} \to \infty$, the use of the MP law which also assumes $\tilde{n} \to \infty$ but converges quite rapidly, and the use of inequality (43). All three factors together combine to result in an approximation that lower bounds the true privacy rate, and becomes worse as the number of antennas increases.

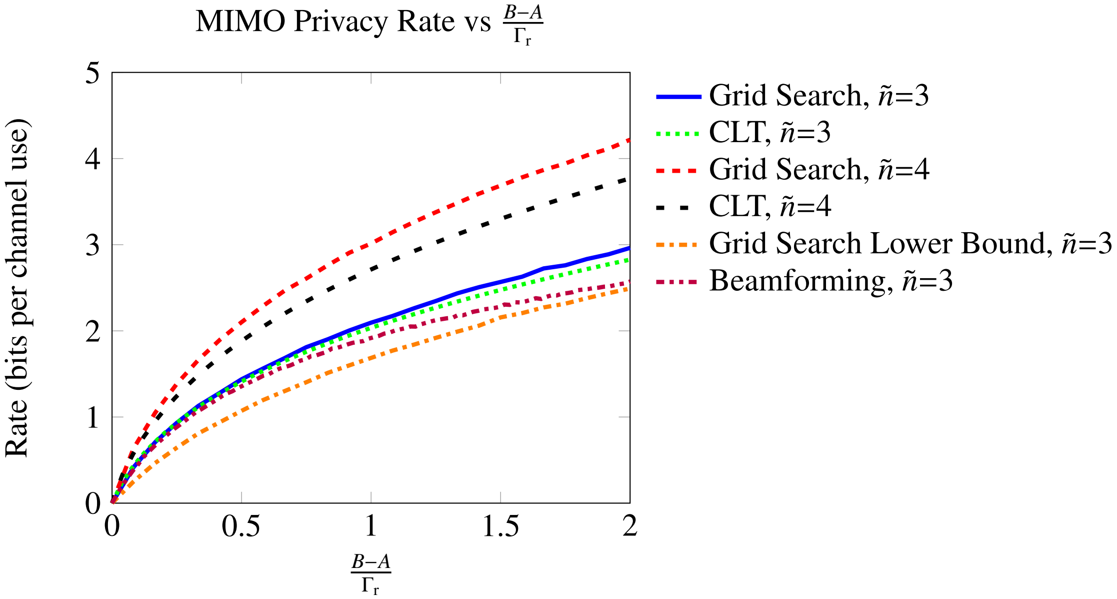


Figure 9: Comparison of privacy rates vs $\frac{B-A}{\Gamma_r}$ under different models

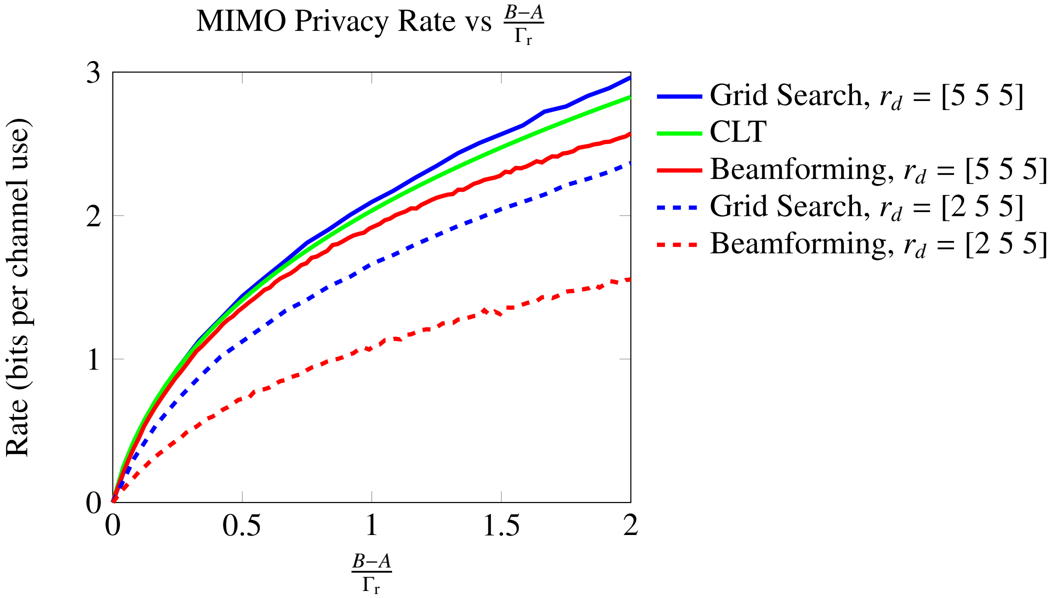


Figure 10: Privacy rates vs $\frac{B-A}{\Gamma_r}$. in skewed vs not skewed

The beamforming solution performs well with parameter uniformity, but as the privacy constraint region becomes skewed, the approximation error grows (Fig. 10). With parameter uniformity, the privacy constraint region is symmetric and represents the best case scenario for the beamforming solution, allowing it to perform well despite using only one eigenchannel and the wrong precoding matrix.

We can apply all these results to look at some hypothetical numbers on privacy rates.

CHAPTER 4

DAVE'S OPTIMAL NUMBER OF SAMPLES

In most detection problems we assume that the detector should take as many samples as possible. This chapter will examine is this is still the case if the noise power is uncertain.

4.1 Worst case scenario

So far we have assumed that Dave's detection performance increases with the number of samples he takes, despite being forced to have $\xi' > 1 - \epsilon$ [22]. We showed that asymptotically, Dave's ξ' is either 0 or 1, depending on Alice's transmit power. However, the assumption that more samples is better is actually incorrect, given constraint (9). To see this, we define ξ" to be ξ' at 1 sample,

$$\xi'' = \min_{\gamma'} \max_{\widehat{\Gamma}_{\mathrm{d}} \in [A,\, B]} \left[\exp\left(\frac{-\gamma'}{\widehat{\Gamma}_d + \frac{\psi}{r_{\mathrm{d}}^{\alpha}} \Gamma_s} \right) - \exp\left(\frac{-\gamma'}{\widehat{\Gamma}_d} \right) \right]. \tag{50}$$

We can plainly see that because $\frac{\psi}{r_{\mathrm{d}}^{\alpha}}\Gamma_s > 0$, $\xi' > 0$ at $N = 1$. Also, $\xi' < 1$ because an exponential with a negative exponent must be less than 1. However, we showed that at an infinite number of samples, Dave's $\xi' = 1$, provided Alice's transmit power is low enough. Because ξ' is a continuous function over N, there must exist some finite N where ξ' is minimized for Dave, and we revise (9) to

$$\xi''' = \min_{N} \min_{\gamma'} \max_{\widehat{\Gamma}_{\mathrm{d}} \in [A,\, B]} \left[P_{\mathrm{FA}}(\widehat{\Gamma}_{\mathrm{d}}, \gamma', N) + P_{\mathrm{MD}}(\widehat{\Gamma}_{\mathrm{d}}, \gamma', N) \right]. \tag{51}$$

This result initially seems counterintuitive. In any detection scenario, the detector is at worst no better off, and almost always better off by gathering more samples. In this scenario, the detector is actually better off ignoring samples past the optimal number (or just collecting that many samples in the first place). However, if we look at (51), we see that Dave is trying to account for the worst case scenario when he maximizes $\widehat{\Gamma}_d$ over I. As Dave collects more samples, there is a chance that he will observe a rare event that represents his worst case. Because his test statistic is cumulative, he will eventually accumulate

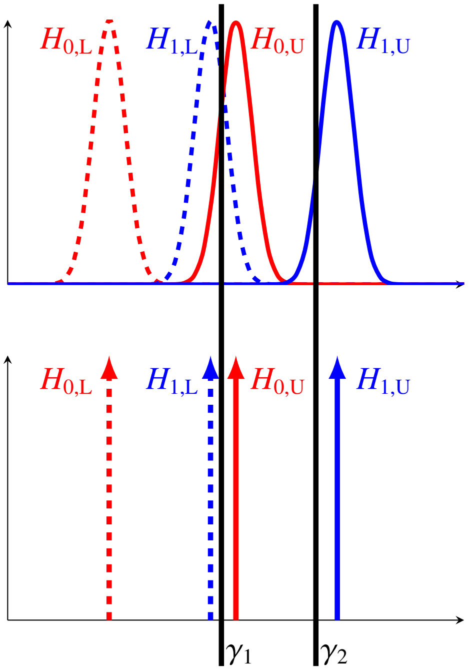


Figure 11: PDFs of test statistics at finite (top graph) and infinite (bottom graph) samples. The dotted PDFs are those at the lower end of the uncertainty interval.

enough rare events that decrease his detection performance.

Another way to analyze this situation is with the test statistic probability density function (pdf)'s themselves.

At a large number of samples, by the CLT, the pdf of the test statistic under each hypothesis converges to a Gaussian distribution, and with an infinite number of samples the Gaussian distribution converges to a delta function at the mean of the distribution. The red deltas in Figure 11 represent the null hypothesis of Alice not transmitting. $H_{0,l}$ represents the null hypothesis pdf with $\widehat{\Gamma}_d = A$, and $H_{0,u}$ represents the null hypothesis pdf with $\widehat{\Gamma}_d = B$. Conversely, the blue deltas represent the alternate hypothesis that Alice is transmitting, with $H_{1,l}$ representing the alternate hypothesis pdf with $\widehat{\Gamma}_d = A$, and $H_{1,u}$ representing the alternate hypothesis pdf with $\widehat{\Gamma}_d = B$.

If Dave considers any detection threshold less than $H_{0,U}$, such as γ_1, by the robustness criterion in (51), he chooses $\widehat{\Gamma}_d = B$. This means the PDFs of his test statistic are $H_{0,U}$ and $H_{1,U}$, implying he will have 100% false alarms. If Dave considers any detection threshold greater than $H_{1,L}$, such as γ_2, by the robustness criterion in (51), he chooses $\widehat{\Gamma}_d = A$. This means the PDFs of his test statistic are $H_{0,L}$ and $H_{1,L}$, implying that he will have 100% misses. Thanks to Alice's power constraint in (17) here does not exist a threshold that Dave can choose that will allow his asymptotic ξ to be less than 1, and hence it would seem that Alice can communicate while forcing Dave's ξ'' to asymptotically approach 1.

However, if we analyze the finite sample case, we see that the assumption that Dave should take as many samples as possible is not valid. For simplicity we have assumed enough samples for the CLT to be valid, but the results hold if we use the true chi square distribution instead.

The strategy employed in the infinite sample case no longer works because the PDFs now have a support that is not infinitesimal. Dave can choose any detection threshold he desires, as long as he satisfies the robustness criterion in (51). Dave could choose the threshold γ_1, in which case there is no choice of $\widehat{\Gamma}_d$ and the corresponding PDFs that will force his ξ''' to be arbitrarily close to 1. From Fig. 11, with γ_1 as Dave's choice of detection threshold, his worst case ξ over the choice of $\widehat{\Gamma}_d$ would be on the order of 15%. Previously, for *any* choice of γ for Dave, the worst case ξ'' was asymptotically 1.

In order for Dave to actually compute the optimal N, γ', and $\widehat{\Gamma}_d$ in (51), Dave needs to know Alice's Γ_s. Because we are assuming that Alice and Dave are not cooperative, it is not realistic to assume that Dave has this information. However, if Alice assumes that Dave knows Γ_s, then Alice will be assuming the best case detection performance for Dave under the constraints he is given, and Alice will be guaranteed to communicate with privacy.

As we can see in Fig. 12, there is a dramatic decrease in privacy rate when we assume Dave uses the optimal number of samples. This is the robust assumption to take, because if Dave doesn't use the optimal number of samples, Alice could transmit with more power. However, the fact that private communication is even possible, given our assumptions, is of great significance.

The optimal number of samples decreases as $\frac{B-A}{\Gamma_r}$ increases, as seen in Fig. 13.

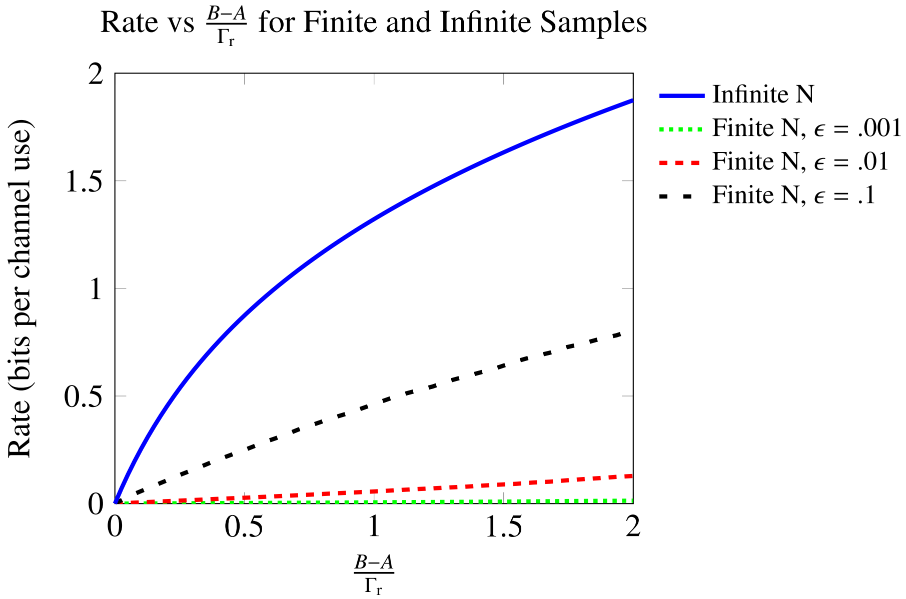


Figure 12: Rate vs $\frac{B-A}{\Gamma_r}$ for finite and infinite samples. Rate increases with ϵ

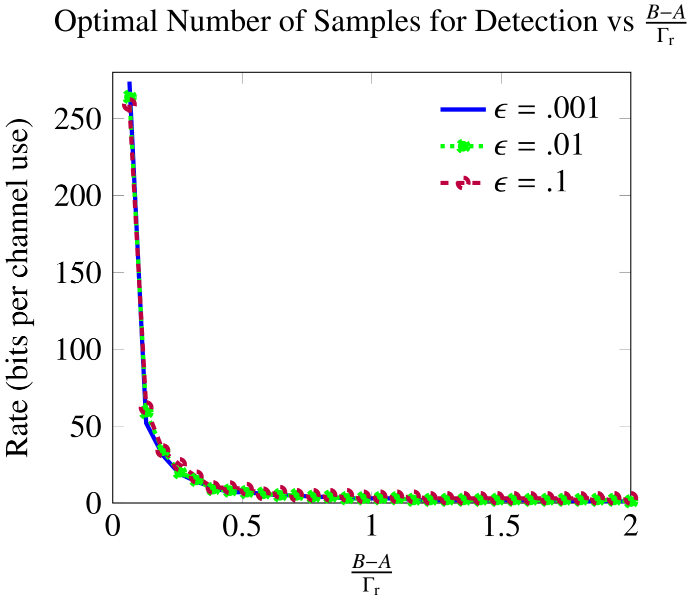


Figure 13: Alice's privacy rate assuming the optimal number of samples for Dave. ϵ has little effect. Rate becomes difficult to compute at low values of $\frac{B-A}{\Gamma_r}$

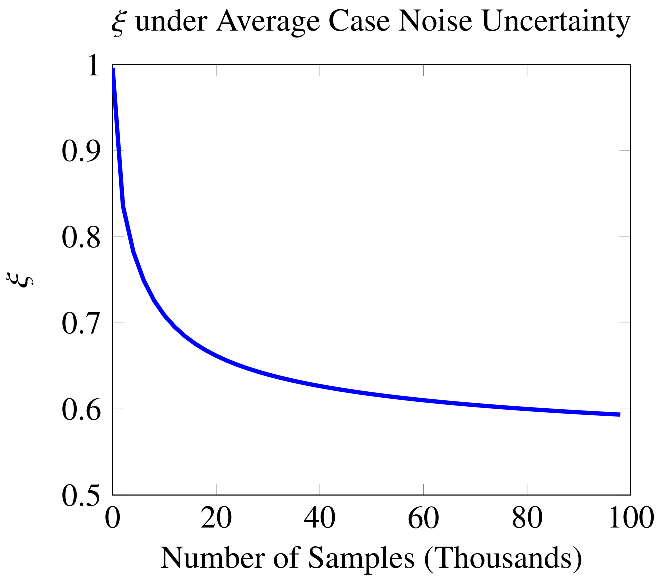


Figure 14: Sum of detection error probabilities for the average case, vs number of samples

4.2 Average Case Scenario

The intuition behind why more samples isn't always better for Dave in the previous scenario was that he was maximizing his worst case for robustness. So if instead, Dave targeted the average case, intuition would be that we would return to the standard situation of more samples is better, or at the very least, not worse. And in fact, we see that this is the case.

While we were not able to show this analytically, we did numerically compute the average case

$$\hat{\xi} = \min_{N} \min_{\gamma'} \int_{A}^{B} \left[P_{\mathrm{FA}}(\widehat{\Gamma}_d, \gamma', N) + P_{\mathrm{MD}}(\widehat{\Gamma}_d, \gamma', N) \right] f_{\widehat{\Gamma}_d}(\widehat{\Gamma}_d) d\widehat{\Gamma}_d \tag{52}$$

where $f_{\widehat{\Gamma}_d}$ is the pdf of $\widehat{\Gamma}_d$. Assuming a uniform distribution on $\widehat{\Gamma}_d$, we can see in Fig. 14 that ξ'' decreases monotonically with respect to N, assuming that the optimal threshold γ'_{opt} has been chosen.

This scenario is not entirely realistic because we are assuming that Dave has knowledge about $f_{\widehat{\Gamma}_d}$, and more importantly that he is not trying to be robust about his detection method. This detection metric would allow for his calculated ξ'' to be not be his true sum of detection errors because $\widehat{\Gamma}_d$ is only going to be one value in I. However, analyzing this scenario does provide some more intuition for the initially counterintuitive result for the worst case scenario.

4.3 Further Extension of Finite Sample Results

We leave this finite sample analysis as an open problem for the other types of channels we consider: SISO and MIMO Rayleigh channels. While we didn't conduct the finite sample analysis on such channels, the fact that we can overcome the square root law in [4] by assuming noise uncertainty, radiometer use, and Dave's taking of a finite number of samples, is the important aspect in this work.

CHAPTER 5
PRACTICAL RATES

One concern in achieving these rates in practice is that Alice will not be certain of where the SNR wall is, especially under the Rayleigh fading case as the SNR wall is random. To give some practical rates we can assume some reasonable lower bounds.

For the non-fading case let us assume Dave is at least 5 meters away because she can see at least 5m in her immediate vicinity that there are no eavesdroppers. We adopt a free space propagation model with isotropic antennas. The measurement uncertainty can be lower bounded by Dave's temperature uncertainty. Thermal noise power can be written as

$$\Gamma_d = k_B \widehat{T} B, \tag{53}$$

where k_B is Boltzman's constant, $\widehat{T}$ is an uncertain temperature in Kelvin in the range $[T_A, T_B]$ and B is bandwidth. An accurate thermometer provides readings within 0.015 K at 298 K [27]. For propagation loss, we will adopt a free space propagation model, which sets $\alpha = 2$. Using these values Alice can compute a worst case SNR wall. For her privacy rate, we will assume that the noise power in the Alice-Dave channel and the Alice-Bob channel are the same. We will also assume that Alice knows her distance to Bob. For the transmission frequency we will assume Alice is transmitting at 900 MHz. Finally, Alice needs to know a lower bound on Γ_d, so she will take the lower end of the uncertainty range for thermal noise power. These values are summarized in Table 1.

Table 2 gives the MIMO and SISO rates for the common bandwidths of 1, 10, and 20 MHz. For the MIMO case, we assume three antennas at each of Alice and Bob, we use the parameter uniformity assumptions so all of Alice's antennas are the same distance away from Dave's antennas, and we assume all the noise variances on the channels from Alice to Dave are the same. While these bitrates found in Table 2 are low, if Alice can obtain better estimates of the noise uncertainty by taking into account interference sources or other factors, this privacy rate can increase.

Table 1: Assumed values

True Temperature (T)	298 K
Temperature Range	297.985 K - 298.015 K
Detector Distance (r_d)	5 meters
Receiver Distance (r_r)	20 meters
Propagation Parameter (α)	2
Alice-Dave Noise Power	Alice-Bob Noise power
Wavelength	333 mm

Table 2: Privacy Rates

Bandwidth	MIMO R_{pr}	SISO R_{pr}
1 MHz	98.1 bits/s	9.07 bit/s
10 MHz	981.2 bits/s	90.7 bit/s
20 MHz	1962.3 bits/s	181.4 bits/s

The MIMO privacy rates are 2.7 times greater than having four individual SISO channels. It is important to remember that the search space for power allocation is not a plane like the standard total power constrained capacity problem—the search space is ellipsoidal in nature, as we see in Fig. 8. This non-planar shape allows us to increase our capacity by a factor beyond the number of antennas.

If Bob gets closer to Alice, the private rate can increase dramatically, as shown in Fig. 15. We previously saw in Fig 7 that we can also increase the privacy rate if Dave's noise uncertainty were to increase.

5.1 Other Sources of Noise Uncertainty

Up to this point we assumed that Dave's noise uncertainty is not affected by Alice's behavior. However, Alice could set up interference sources that turn on and off at random intervals. This interference can create more noise uncertainty for Dave and increase Alice's privacy rate. Also, because Alice set up the interference sources herself, she can estimate Dave's uncertainty from these sources.

Additionally, there can be other noise sources present that are not in collusion with Alice. In the extreme underlay scenario, the primary user could be seen as an interference

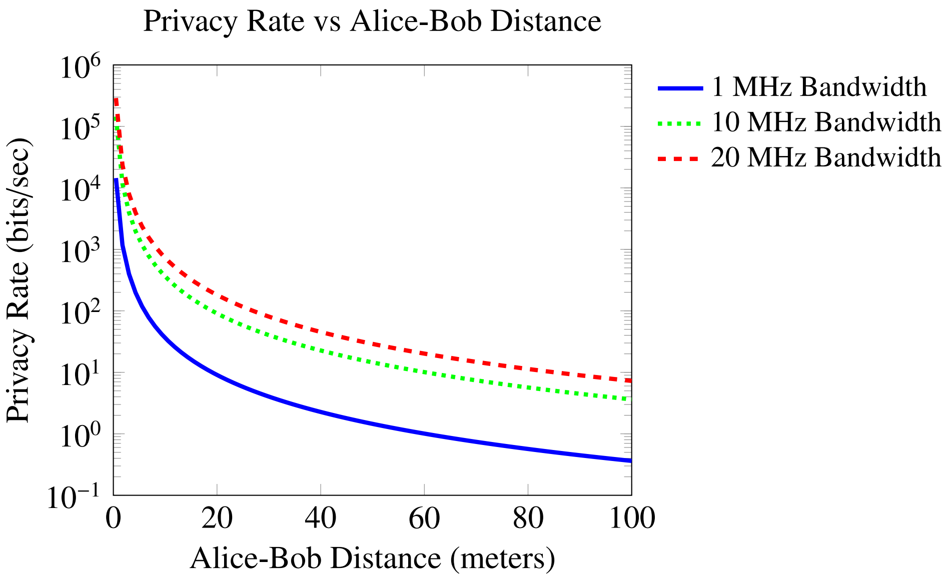


Figure 15: Privacy rates vs Alice-Bob distance.

source that increases Dave's noise uncertainty. However, Bob has to be able to reject the noise for this to increase his rate, because otherwise his noise increases as well and offsets the gain in allowable transmit power.

We leave further study into these areas as an open problem.

CHAPTER 6
CONCLUSION

It is possible to overcome the square root law of private communication if two assumptions are made: the detector is uncertain of its noise level and the detector uses a radiometer. We showed that the detector should only take into account a finite number of samples, and that while the detector cannot actually calculate the optimal number of samples without knowing the transmitter's power, the detector does know that the optimal number of samples decreases as its uncertainty about the noise increases. Further work would be to analyze Rayleigh SISO and MIMO channels to confirm that a finite number of samples is optimal in those cases as well.

APPENDIX

In equation (33) we use the integral

$$\int_0^\infty \log_2(1+Gx)\frac{e^{-x/2}}{2}dx = \frac{1}{\ln(2)}\exp\left(\frac{1}{2G}\right)\mathrm{E}_1\left(\frac{1}{2G}\right)$$

where $E_1(x) = \int_x^\infty \frac{e^{-t}}{t}dt$ (and therefore $\frac{d}{dx}E_1(x) = -\frac{e^{-x}}{x}$). We first need to show that

$$\int \log_2(1+Gx)\frac{e^{-x/2}}{2}dx \overset{?}{=} \frac{1}{\ln(2)}\left(-\exp\left(\frac{1}{2G}\right)\mathrm{E}_1\left(\frac{x}{2}+\frac{1}{2G}\right) - \exp\left(-\frac{x}{2}\right)\ln(Gx+1)\right) + C$$

$$\frac{d}{dx}\int \log_2(1+Gx)\frac{e^{-x/2}}{2}dx \overset{?}{=} \frac{1}{\ln(2)}\frac{d}{dx}\left(-\exp\left(\frac{1}{2G}\right)\mathrm{E}_1\left(\frac{x}{2}+\frac{1}{2G}\right) - \exp\left(-\frac{x}{2}\right)\ln(Gx+1)\right)$$

$$\begin{aligned}\log_2(1+Gx)\frac{e^{-x/2}}{2} &\overset{?}{=} \frac{1}{\ln(2)}\left(\exp\left(\frac{1}{2G}\right)\frac{\exp\left(-\frac{x}{2}-\frac{1}{2G}\right)}{\frac{x}{2}+\frac{1}{2G}}\frac{1}{2} + \frac{1}{2}\exp\left(-\frac{x}{2}\right)\ln(Gx+1)\right.\\ &\qquad\left.-G\frac{\exp\left(-\frac{x}{2}\right)}{Gx+1}\right)\end{aligned}$$

$$\log_2(1+Gx)\frac{e^{-x/2}}{2} \overset{?}{=} \frac{1}{\ln(2)}\left(\frac{G\exp\left(-\frac{x}{2}\right)}{Gx+1} + \frac{1}{2}\exp\left(-\frac{x}{2}\right)\ln(Gx+1) - G\frac{\exp\left(-\frac{x}{2}\right)}{Gx+1}\right)$$

$$\log_2(1+Gx)\frac{e^{-x/2}}{2}dx \overset{?}{=} \frac{1}{\ln(2)}\left(\frac{1}{2}\exp\left(-\frac{x}{2}\right)\ln(Gx+1)\right)$$

$$\log_2(1+Gx)\frac{e^{-x/2}}{2} = \log_2(1+Gx)\frac{e^{-x/2}}{2}$$

By plugging in our integral bounds, we have

$$\begin{aligned}&\frac{1}{\ln(2)}\left(-\exp\left(\frac{1}{2G}\right)\mathrm{E}_1\left(\frac{x}{2}+\frac{1}{2G}\right)\Bigg|_0^\infty - \exp\left(-\frac{x}{2}\right)\ln(Gx+1)\Bigg|_0^\infty\right)\\ &= \frac{1}{\ln(2)}\left(\exp\left(\frac{1}{2G}\right)\left(E_1\left(\frac{1}{2G}\right) - E_1(\infty)\right)\right)\\ &= \frac{1}{\ln(2)}\exp\left(\frac{1}{2G}\right)E_1\left(\frac{1}{2G}\right) \qquad (54)\end{aligned}$$

The equation for ergodic MIMO capacity as derived in [23] is

$$C \approx gn_r\log_2\left[\frac{a^2 n_t P_0 + n_r\int_{\mu_{cut}}^\infty d\mu' f_r(\mu')\frac{1}{\mu'}}{gn_r}\right] + n_r\int_{\mu_{cut}}^\infty du f_r(\mu)\log_2(\mu)$$

where

$$g = \frac{L}{n_r} \approx \int_{\mu_{cut}}^\infty d\mu f_r(u),$$

is the fraction of the channel modes used by the transmitter,

$$\mu_{cut} = \frac{r\int_{\mu_{cut}}^{\infty} d\mu' f_r(\mu')}{a^2 P_0 + r\int_{\mu_{cut}}^{\infty} d\mu f_r(\mu)\frac{1}{\mu}}$$

is the minimum eigenvalue used by the transmitter,

$$f_r(\mu) = \begin{cases} \dfrac{\sqrt{(\mu - a_r)(b_r - \mu)}}{2\pi\mu r}, & a_r \leq \mu \leq b_r \\ 0, & \text{otherwise} \end{cases},$$

$$a_r = (\sqrt{r} - 1)^2,$$

$$b_r = (\sqrt{r} + 1)^2,$$

$$r = \frac{n_r}{n_t},$$

and a in the large matrix limit asymptotically approaches the root mean square transmit to receive attenuation.

When $r = 1$, we have the results

$$\int_{\mu_{cut}}^{\infty} d\mu f_1(\mu) = 1 - \frac{\sqrt{(4 - \mu_{cut})\mu_{cut}} + 4\arcsin\left(\frac{\sqrt{\mu_{cut}}}{2}\right)}{2\pi}$$

$$\int_{\mu_{cut}}^{\infty} d\mu f_1(\mu)\frac{1}{\mu} = -\frac{1}{2} + \frac{1}{\pi}\sqrt{\frac{4 - \mu_{cut}}{\mu_{cut}}} + \frac{1}{\pi}\arcsin\left(\frac{\sqrt{\mu_{cut}}}{2}\right)$$

$$\int_{\mu_{cut}}^{\infty} d\mu f_1(\mu)\log_2(\mu) = \left\{4\,{}_3F_2\left(\left[\tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}\right], \left[\tfrac{3}{2}, \tfrac{3}{2}\right], \tfrac{\mu_{cut}}{4}\right) + \left(\sqrt{4 - \mu_{cut}} - \frac{4}{\mu_{cut}}\operatorname{arcsec}\left[\frac{2}{\sqrt{\mu_{cut}}}\right]\right) \times \left(1 - \ln(\mu_{cut}) - \frac{2\pi}{\sqrt{\mu_{cut}}}\ln(\mu_{cut})\right)\right\}\frac{\sqrt{\mu_{cut}}}{\pi\ln(4)}$$

BIBLIOGRAPHY

[1] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinvasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proceedings of the IEEE*, vol. 97, pp. 894–914, May 2009.

[2] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Mobile Ad Hoc Networking and Computing, Proc. of the 6th ACM International Symposium on*, pp. 46–57, 2005.

[3] L. Lazos, S. Liu, and M. Krunz, "Mitigating control-channel jamming attacks in multi-channel ad hoc networks," in *Wireless Network Security, Proc. of the Second ACM Conference on*, pp. 169–180, 2009.

[4] B. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *Selected Areas in Communications, IEEE Journal on*, vol. 31, pp. 1921–1930, September 2013.

[5] J. Fridrich, *Steganography in Digital media: Principles, Algorithms, and Applications.* MIT Press, 2 ed., 2001.

[6] R. Tandra and A. Sahai, "SNR walls for signal detection," *Selected Topics in Signal Processing, IEEE Journal of*, vol. 2, pp. 4–17, Feb 2008.

[7] J. Hou and G. Kramer, "Effective secrecy: Reliability, confusion and stealth," in *2014 IEEE International Symposium on Information Theory*, pp. 601–605, 2014.

[8] T. Rappaport, *Wireless Communications.* Upper Saddle River, NJ: Prentice Hall, 2 ed., 2002.

[9] S. Alexander, "Characterising buildings for propagation at 900 MHz," *Electronics Letters*, vol. 19, pp. 860–, September 1983.

[10] K. S, *Fundamentals of Statistical Signal Processing Detection Theory.* Prentice Hall, Inc., Upper City River, New Jersey, 2 ed., 1998.

[11] E. Lehmann and J. Romano, *Testing Statistical Hypotheses.* NY: Springer, 3 ed., 2005.

[12] T. M. Cover and J. A. Thomas, *Elements of Information Theory.* John Wiley & Sons, Hoboken, NJ, 2 ed., 2002.

[13] B. He, S. Yan, X. Zhou, and V. K. N. Lau, "On covert communication with noise uncertainty," *IEEE Communications Letters*, vol. 21, no. 4, pp. 941–944, 2017.

[14] P. H. Che, M. Bakshi, C. Chan, and S. Jaggi, “Reliable deniable communication with channel uncertainty,” in *2014 IEEE Information Theory Workshop (ITW 2014)*, pp. 30–34, 2014.

[15] B. A. Bash, D. Goeckel, and D. Towsley, “Covert communication gains from adversary’s ignorance of transmission time,” *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8394–8405, 2016.

[16] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, “Covert communication in the presence of an uninformed jammer,” *IEEE Transactions on Wireless Communications*, vol. 16, no. 9, pp. 6193–6206, 2017.

[17] D. Goeckel, A. Sheikholeslami, T. Sobers, B. A. Bash, O. Towsley, and S. Guha, “Covert communications in a dynamic interference environment,” in *2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 1–5, 2018.

[18] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, “Covert communications on continuous-time channels in the presence of jamming,” in *2017 51st Asilomar Conference on Signals, Systems, and Computers*, pp. 1697–1701, 2017.

[19] L. Wang, “The continuous-time poisson channel has infinite covert communication capacity,” in *2018 IEEE International Symposium on Information Theory (ISIT)*, pp. 756–760, 2018.

[20] D. Goeckel, B. Bash, S. Guha, and D. Towsley, “Covert communications when the warden does not know the background noise power,” *IEEE Communications Letters*, vol. 20, no. 2, pp. 236–239, 2016.

[21] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, “Wireless information-theoretic security,” *Information Theory, IEEE Transactions on*, vol. 54, pp. 2515–2534, June 2008.

[22] S. Lee and R. J. Baxley, “Achieving positive rate with undetectable communication over AWGN and Rayleigh channels,” in *Communications (ICC), 2014 IEEE International Conference on*, pp. 780–785, June 2014.

[23] D. Bliss, K. Forsythe, and A. Yegulalp, “MIMO communication capacity using infinite dimension random matrix eigenvalue distributions,” in *Signals, Systems and Computers, 2001. Conference Record of the Thirty-Fifth Asilomar Conference on*, vol. 2, pp. 969–974 vol.2, Nov 2001.

[24] A. Hero, “Secure space-time communication,” *Information Theory, IEEE Transactions on*, vol. 49, pp. 3235–3249, Dec 2003.

[25] D. Hammarwall, M. Bengtsson, and B. Ottersten, “Acquiring partial CSI for spatially selective transmission by instantaneous channel norm feedback,” *Signal Processing, IEEE Transactions on*, vol. 56, pp. 1188–1204, March 2008.

[26] M. Vu, “MIMO capacity with per-antenna power constraint,” in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, pp. 1–5, Dec 2011.

[27] ICL Calibration Laboratories, *Dostmann D795-PT*, 2013.