Achieving Positive Rate With Undetectable Communication Over AWGN and Rayleigh Channels

Seonwoo Lee
School of Electrical and Computer Engineering
Georgia Institute of Technology
Atlanta, Georgia 30332

Robert J. Baxley
Georgia Tech Research Institute
250 14th Street
Atlanta, Georgia 30332

***Abstract*—In this paper we consider the problem of achieving a positive error-free communications rate without being detected by an eavesdropper—we coin this the *privacy rate*. Specifically, we present the privacy rate over Additive White Gaussian Noise (AWGN) and Rayleigh channels when an eavesdropper employs a radiometer detector and has uncertainty about her noise variance. Leveraging recent results on the phenomenon of an Signal to Noise Ratio (SNR) wall when there is eavesdropper noise power measurement uncertainty, we show that a non-zero privacy rate is possible. We also find the SNR wall under Rayleigh fading. We conclude by presenting realizable privacy rates for several practical scenarios.**

I. Introduction

In wireless communications there are several 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, e.g. [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 paper we determine the achievable communications rate afforded by the privacy constraint under a variety of eavesdropper and channel assumptions. It should be noted that privacy capacity is different from secrecy capacity, which constrains an eavesdropper's rate of receiving information to zero as opposed to preventing detection by an eavesdropper.

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 an eavesdropper, Eve. If Alice does not want to reveal her position or even her existence, encrypting her communications is not enough. Bash, Goeckel, and Towsley [5] found that if Alice knows a lower bound on the noise power on the channel between Bob and Alice, $O(\sqrt{N})$ bits can be sent in N channel uses while guaranteeing that Eve asymptotically has the sum of her probability of false alarm P_{FA} and missed detection P_{MD} arbitrarily close to one.

To make this more clear, we define two terms. $I(N)$ is the number of undetected error-free bits that can be sent in N channel uses. Likewise, $R = \lim_{N\to\infty} I(N)/N$ is the error-free channel rate. The result in [5] means that $R = 0$ in AWGN channels. It is important to note that despite zero asymptotic rate, 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 [5] 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 [10, 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 $\lim_{N\to\infty} O(\sqrt{N}\log N)/O(N) = 0$.

Our goal in this work is to expand on [5] by analyzing different channel conditions and different assumptions on Eve's knowledge of her noise power. Encouragingly, we show that if Eve uses a radiometer detector and is uncertain about her noise variance, positive rate is possible while guaranteeing that Eve's $P_{MD} + P_{FA} \to 1$. 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 point out that while a radiometer is the optimal detector for AWGN systems where Eve knows her noise variance, a radiometer is not optimal when Eve does not know her noise variance [6]. Thus, the result we present is not as strong as the one in [5], but our result does demonstrate that in practical situations, a positive rate is possible while still guaranteeing that Eve's $P_{MD} + P_{FA} \to 1$.

In this paper, we have a slightly different justification for the SNR wall in Section II. We analyze the privacy rate under AWGN channels in Section III and Rayleigh fading channels in Section IV. Numerical results on realizable rates are discussed in Section V, and Section VI analyzes their implications of these results.

II. SNR Wall

The primary element that allows positive rate is the fact that Eve is unable to exactly determine her noise power. This idea of detection noise power uncertainty was discussed in great detail by Tandra and Sahai [6] as an SNR wall. In the uncertainty model, Eve only knows the range of possible noise

power values for Alice-Eve channel. That is, her noise power estimate follows $\widehat{\Gamma}_d \in [1/\rho\Gamma_d, \rho\Gamma_d]$, where Γ_d is the true noise power, and $\rho > 1$. The distribution of $\widehat{\Gamma}_d$ in this interval is not important because while the distribution of $\widehat{\Gamma}_d$ may be heavily concentrated in a small subinterval of $[1/\rho\Gamma_d, \rho\Gamma_d]$, Eve still needs to consider the entire interval to achieve robust detection. Mismatch between Eve's estimate of the noise power and the true noise power can be attributed to calibration inaccuracies. Given this model, Tandra and Sahai showed that if $\rho - 1/\rho >$ SNR, robust detection by the secondary user is impossible, where SNR = Γ_s/Γ_r, with Γ_s as the transmitted signal power and Γ_r as the receiver's (Bob's) noise power. This result is troubling in the context of cognitive radios, for which their paper was written. However for secure communication, this result is of great advantage and allows us to overcome the square root law of information transfer in [5].

We look at the SNR wall when Eve is considering her sum of probabilities of detection errors

$$\xi = \max_{\widehat{\Gamma}_d \in [1/\rho\Gamma_d, \rho\Gamma_d]} P_{FA}(\widehat{\Gamma}_d) + P_{MD}(\widehat{\Gamma}_d). \tag{1}$$

The difference in this approach to that in [6] is that the $\widehat{\Gamma}_d$ chosen from the uncertainty interval is not allowed to be different for P_{FA} and P_{MD}. The definition of nonrobust in [6] is a detection algorithm is *nonrobust* for a fixed SNR if the algorithm cannot robustly achieve every pair (P_{FA}, P_{MD}) in U, where $U = \{(P_{FA}, P_{MD}) : 0 < P_{FA} < 1/2, 0 < P_{MD} < 1/2\}$, even when N is made arbitrarily large. A thorough definition of robust can be found in [6]. Under our paradigm we have expanded U to be $\{(P_{FA}, P_{MD}) : 1 - P_{MD} > P_{FA}\}$. The SNR wall is still the same under this approach, as we will see in (14).

It is important to note that ξ is bounded between 0 and 1, which follows from the fact that $P_D \geq P_{FA}$, where P_D is the probability of false alarm. A detector can always achieve $P_D = P_{FA}$ by ignoring the input data and flipping a coin with probability of heads being P_D, and declaring a detection when it is heads [4]. Hence any algorithm the detector uses should be able to achieve $P_D \geq P_{FA}$.

III. AWGN Channel Privacy Rate with Measurement Uncertainty

A. Problem Statement and Strategy

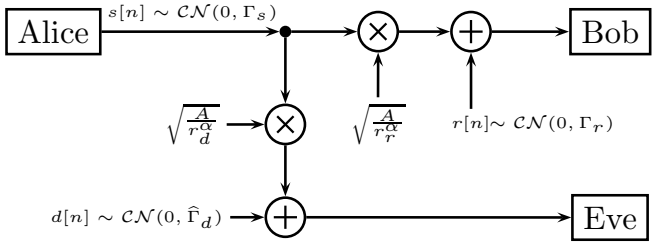

Fig. 1. System block diagram. $\widehat{\Gamma}_d \in [1/\rho\Gamma_d, \rho\Gamma_d]$

We assume AWGN channels with complex valued symbols as depicted in Fig. 1. When a random variable X has a circularly symmetric complex Gaussian distribution with mean μ and variance Γ it is denoted as $X \sim \mathcal{CN}(\mu, \Gamma)$. All of our signals are mutually independent. Alice sends signal $s[n]$. Bob and Eve are located distances r_r and r_d from Alice and experience noise $r[n]$ and $d[n]$, respectively. 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 $P \propto 1/r^2$ [7, p. 107], as well as multipath path loss models, where $P \propto 1/r^\alpha$ with α as low as 1.2 and as high as 6.2 [8]. We will let $P = A/r^\alpha$ for some proportionality constant A. The uncertainty in Eve's measurement is given by $\widehat{\Gamma}_d \in [(1/\rho)\Gamma_d, \rho\Gamma_d]$, $\rho > 1$ as done in [6].

Eve's goal is to detect Alice's signal. To do this, she will have to distinguish between the following two signal hypotheses,

$$H_0 : x[n] = d[n], \tag{2}$$

$$H_1 : x[n] = \sqrt{\tfrac{A}{r_d^\alpha}} s[n] + d[n], \tag{3}$$

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

Alice's objective is to find the maximum error-free rate at which she can communicate to Bob while guaranteeing $\xi > 1 - \epsilon$ for some small $\epsilon \in [0, 1]$.

With this objective and these constraints, we can define an associated quantity called the privacy capacity, C_{pr}, which is the maximum achievable error-free rate of communications such that $\xi > 1 - \epsilon$. We can bound ξ by bounding the total variation distance between $P_0(\mathbf{x})$ and $P_1(\mathbf{x})$. It is defined as

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

Because $\xi = 1 - \frac{1}{2}||P_1 - P_0||_1$ under the optimal detector [9, Ch. 13], forcing $||P_1 - P_0||_1 < 2\epsilon$ forces Eve's detector to have $\xi > 1 - \epsilon$.

To find C_{pr}, we would have to relax the constraint on Eve's detector and assume that she can employ an arbitrary detector. As noted in [3], the radiometer may not be the optimal detector for Eve when she has uncertainty about her noise power. Thus, it is probable that Alice's C_{pr} may be smaller than the R_{pr} under a radiometer detector. We leave finding the C_{pr} as an open problem and instead answer that highly practical question of determining R_{pr} under a radiometer detector.

Alice can achieve a rate of $\log_2(1 + \Gamma_s/\Gamma_r)$ bits per channel use when her power is constrained to Γ_s and Bob's noise power is Γ_r [11, Ch 9]. Using this we define the privacy rate as

$$R_{pr} = \max_{\Gamma_s:\ \lim_{N\to\infty} \xi(N, \Gamma_s) = 1} \log_2(1 + \tfrac{A}{r_r^\alpha} \tfrac{\Gamma_s}{\Gamma_r}), \tag{5}$$

where $\xi(N, \Gamma_s)$ is the sum of P_{FA} and P_D after N observations.

Privacy rate analysis method: Capacity for a AWGN channel is maximized with a Gaussian input distribution, so we choose Gaussian signaling for Alice. We then assume that Eve uses a radiometery detector to distinguish between the two hypotheses (2) and (3). By analyzing P_D and P_{FA}, we show $\lim_{N\to\infty} \xi = 1$ when Alice transmits under the SNR wall of $\rho - \frac{1}{\rho}$. This same analysis is later applied to the Rayleigh case to find the fading SNR wall and consequently privacy rate for

a Rayleigh fading channel. By assuming SNR wall transmit power for Alice, we satisfy the constraints in (5). Finally, to maximize the rate, we employ the AWGN channel capacity expression, since we simply have an AWGN channel with a given power constraint.

B. Privacy Rate

We assume Alice uses

$$T(x) = \frac{1}{N}x^H x = \frac{1}{N}\sum_{n=1}^{N} x[n]^* x[n] > \gamma' \tag{6}$$

as her detection test, which is a classic radiometer detector. Let $Q_{\chi^2_{2N}}(\cdot)$ be the tail probability of a chi square random variable with $2N$ degrees of freedom. This gives rise to the following false alarm and detection probabilities,

$$\begin{aligned} P_{FA} &= Pr(T(x) > \gamma'; H_0) \\ &= Pr\left(\frac{1}{N}\sum_{n=1}^{N} d[n]^* d[n] > \gamma'\right) \\ &= Q_{\chi^2_{2N}}\left(\frac{2N\gamma'}{\widehat{\Gamma}_d}\right) \end{aligned} \tag{7}$$

$$\begin{aligned} P_D &= Pr(T(x) > \gamma'; H_1) \\ &= Q_{\chi^2_{2N}}\left(\frac{2N\gamma'}{\widehat{\Gamma}_d + \frac{A}{r_d^\alpha}\Gamma_s}\right) \end{aligned} \tag{8}$$

$$\lim_{N\to\infty} P_{FA} = \begin{cases} 0, & \text{if } \gamma' > \widehat{\Gamma}_d \\ 1, & \text{if } \gamma' < \widehat{\Gamma}_d \end{cases}, \tag{9}$$

$$\lim_{N\to\infty} P_D = \begin{cases} 0, & \text{if } \gamma' > \widehat{\Gamma}_d + \frac{A}{r_d^\alpha}\Gamma_s \\ 1, & \text{if } \gamma' < \widehat{\Gamma}_d + \frac{A}{r_d^\alpha}\Gamma_s, \end{cases} \tag{10}$$

for some choice of $\widehat{\Gamma}_d \in [1/\rho\Gamma_d, \rho\Gamma_d]$. We want to maximize our signal power while forcing $\xi \to 1$, so we can either force $P_D \to 0$ or $P_{FA} \to 1$. To do this we need to satisfy

$$\gamma' < \widehat{\Gamma}_d \tag{11}$$

or

$$\gamma' > \widehat{\Gamma}_d + \frac{A}{r_d^\alpha}\Gamma_s \tag{12}$$

for all γ' and some $\widehat{\Gamma}_d \in [1/\rho\Gamma_d, \rho\Gamma_d]$ while maximizing Γ_s. For $\gamma' < \rho\Gamma_d$, we can choose $\widehat{\Gamma}_d = \rho\Gamma_d$ to satisfy (11). For $\gamma' \geq \rho\Gamma_d$, we can't satisfy (11) but we can satisfy (12) by choosing $\widehat{\Gamma} = 1/\rho\Gamma_d$ and constraining

$$\frac{A}{r_d^\alpha}\Gamma_s < (\rho - 1/\rho)\Gamma_d. \tag{13}$$

Hence, the SNR wall to force $\xi \to 1$ is

$$\Gamma_s = \Gamma_d r_d^\alpha (\rho - \tfrac{1}{\rho})/A. \tag{14}$$

This argument is different from the one used in [5], which was based on showing that the number of samples required for detection is infinite as SNR approaches the SNR wall. By framing the problem as we have, we show that $\xi \to 1$ under the SNR wall. That is, for any (P_D, P_{FA}) pair that Eve chooses, she will always have all errors $(1 - P_D + P_{FA} \to 1)$. In contrast, [5] only claimed that $\xi \to 1$ for only one (P_D, P_{FA}) pair: $P_{FA} \to 1/2$ and $P_D \to 1/2$.

Given this, for Alice to achieve privacy, she should emit less power than (14), resulting in

$$\begin{aligned} R_{pr} &= \lim_{N\to\infty} \log_2(1 + \tfrac{A}{r_r^\alpha}\tfrac{\Gamma_s}{\Gamma_r}) \\ &= \log_2\left(1 + \tfrac{\Gamma_d}{\Gamma_r}\left(\tfrac{r_d}{r_r}\right)^\alpha(\rho - \tfrac{1}{\rho})\right). \end{aligned} \tag{15}$$

C. Analysis

Alice can communicate with a positive rate given by (15) while forcing Eve's detector to have all errors so long as she talks below the SNR wall in (14). Unfortunately, Alice does not know what Eve'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. Eve's noise level depends on the temperature, so Alice can also lower bound ρ 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 Eve's receiver and some noise figure. The propagation parameter 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 $R < R_{pr} = \log_2(1 + \frac{\Gamma_d}{\Gamma_r}\left(\frac{r_d}{r_r}\right)^\alpha(\rho - \frac{1}{\rho}))$. Numerical results are discussed in Section V.

IV. Rayleigh Fading Channel Privacy Rate with Measurement Uncertainty

A. Problem Statement

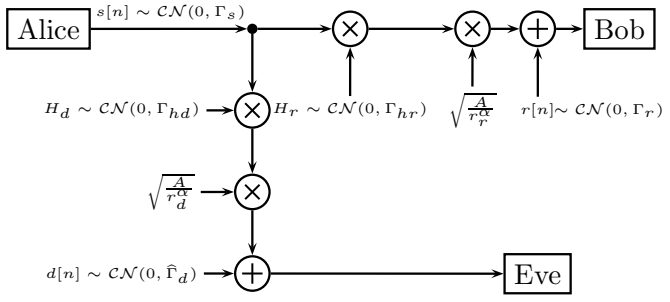

Fig. 2. System block diagram. $\widehat{\Gamma}_d \in [1/\rho\Gamma_d, \rho\Gamma_d]$

We assume Rayleigh fading channels with complex valued symbols as depicted in Fig. 2. All other aspects of the scenario are the same as described in Section III-A. For simplicity, the channel gains H_d and H_r are assumed to be static over the signaling period.

For detection the two hypotheses are:

$$H_0: \ x[n] = d[n] \tag{16}$$

$$H_1: \ x[n] = \sqrt{\frac{A}{r_d^\alpha}} H_d s[n] + d[n] \tag{17}$$

When Alice has channel state information (CSI) for the Alice-Eve channel, Eve 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, but the resulting privacy rate gives us an idea of the best case Alice can hope to achieve. When Alice only has channel distribution information (CDI) for the Alice-Eve channel, Eve'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 $\lim_{N\to\infty} E[\xi(\Gamma_s, N)] \geq 1 - \epsilon$, which is equivalent to requiring that $\lim_{N\to\infty} Pr(\xi(\Gamma_s, N) = 1) \geq 1 - \epsilon$.

B. Privacy Rate Under Alice-Eve 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. Eve uses the same detection test as the AWGN case and hence the same detection threshold. The probability of detection is now

$$\begin{aligned} P_D &= Pr(T(x) > \gamma'; H_1), \\ &= Q_{\chi^2_{2N}}\left(\frac{2N\gamma'}{\widehat{\Gamma}_d + \frac{A}{r_d^\alpha}|H_d|^2\Gamma_s}\right). \end{aligned} \tag{18}$$

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

$$\Gamma_s|H_d = \frac{\Gamma_d r_d^\alpha}{|H_d|^2 A}(\rho - 1/\rho). \tag{19}$$

Using the SNR from (19),

$$\begin{aligned} R_{pr}|H_d, H_r &= \lim_{N\to\infty} \log_2(1 + \tfrac{A}{r_r^\alpha}\tfrac{\Gamma_s}{\Gamma_r}) \\ &= \log_2(1 + \tfrac{\Gamma_d}{\Gamma_r}\left(\tfrac{r_d}{r_r}\right)^\alpha \tfrac{|H_r|^2}{|H_d|^2}(\rho - \tfrac{1}{\rho})). \end{aligned} \tag{20}$$

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

$$R_{pr} = \log_2(1 + \tfrac{\Gamma_d}{\Gamma_r}\left(\tfrac{r_d}{r_r}\right)^\alpha \psi \tfrac{\Gamma_{hr}}{\Gamma_{hd}}(\rho - 1/\rho)), \tag{21}$$

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

$$\begin{aligned} R_{pr,erg} &= \int_0^\infty \log_2\left(1 + \tfrac{\Gamma_d}{\Gamma_r}\left(\tfrac{r_d}{r_r}\right)^\alpha \tfrac{\Gamma_{hr}}{\Gamma_{hd}}(\rho - \tfrac{1}{\rho})x\right) f_x(x)dx \\ &= \int_0^\infty \log_2(1 + \tfrac{\Gamma_d}{\Gamma_r}\left(\tfrac{r_d}{r_r}\right)^\alpha \tfrac{\Gamma_{hr}}{\Gamma_{hd}}(\rho - 1/\rho)x)(1+x)^{-2}dx \\ &= \frac{\frac{\Gamma_{hr}}{\Gamma_{hd}}(\rho - \frac{1}{\rho})\frac{\Gamma_d}{\Gamma_r}\left(\frac{r_d}{r_r}\right)^\alpha}{\frac{\Gamma_{hr}}{\Gamma_{hd}}(\rho - \frac{1}{\rho})\frac{\Gamma_d}{\Gamma_r}\left(\frac{r_d}{r_r}\right)^\alpha - 1} \log_2(\tfrac{\Gamma_{hr}}{\Gamma_{hd}}(\rho - \tfrac{1}{\rho})\tfrac{\Gamma_d}{\Gamma_r}\left(\tfrac{r_d}{r_r}\right)^\alpha). \end{aligned} \tag{22}$$

We can also find the outage rate

$$Pr(R_{pr} < c) = Pr(F(2,2) \leq (2^c - 1)\tfrac{\Gamma_r}{\Gamma_d}(\tfrac{r_r}{r_d})^\alpha \tfrac{\Gamma_{hd}}{\Gamma_{hr}} \tfrac{1}{\rho - \frac{1}{\rho}})$$

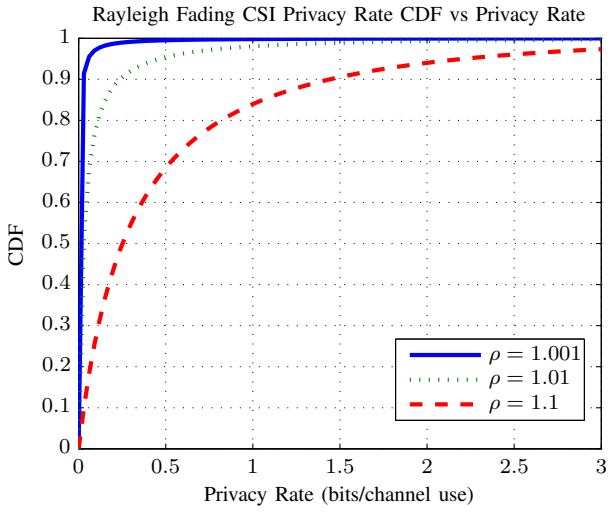

Fig. 3. Rayleigh Privacy Rate under CSI for various ρ's. All parameter ratios are 1.

$$= \frac{(2^c - 1)\tfrac{\Gamma_r}{\Gamma_d}(\tfrac{r_r}{r_d})^\alpha \tfrac{\Gamma_{hd}}{\Gamma_{hr}} \tfrac{1}{\rho - \frac{1}{\rho}}}{(2^c - 1)\tfrac{\Gamma_r}{\Gamma_d}(\tfrac{r_r}{r_d})^\alpha \tfrac{\Gamma_{hd}}{\Gamma_{hr}} \tfrac{1}{\rho - \frac{1}{\rho}} + 1}. \tag{23}$$

C. Analysis of Privacy Rate under CSI

Alice can communicate with a positive rate with zero probability of detection so long as she talks below the SNR wall in (19). If we compare the privacy rates of the Rayleigh fading and AWGN channels,

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

If the channel gains have similar distributions, then the probability that the Rayleigh fading channel under CSI has a greater privacy rate than the AWGN channel is actually one half. This occurs because the F-distributed random variable that appears in the privacy rate, the ratio of the channel gains between the Alice-Bob, and Alice-Eve channels, has an infinite support. 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 to 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 [12]. A plot of the outage rate can be found in Fig. 3. Some numerical results are discussed in Section V.

D. Privacy Rate under Alice-Eve CDI

Next we study the privacy rate when only channel distribution information is known about the Alice-Eve channel. We still assume CSI for the Alice-Bob channel. We assume that $H_d \perp\!\!\!\perp S$, where $\perp\!\!\!\perp$ denotes independence. Otherwise the system setup is the same as the CSI case. However, Alice can no longer guarantee that $\xi \to 1$ 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

$$\tilde{R}_{pr,\epsilon} = \max_{\lim_{N\to\infty} E[\xi(\Gamma_s,N)]\geq 1-\epsilon} \log_2(1+\tfrac{A}{r_r^\alpha}\tfrac{\Gamma_s}{\Gamma_r}). \quad (24)$$

While P_{FA} remains the same, P_D now changes to

$$P_D = \begin{cases} 0, & \text{with probability } 1 - Q_{\chi_2^2}\left(\dfrac{\gamma' - \widehat{\Gamma}_d}{\frac{A}{r_d^\alpha}\Gamma_s\Gamma_{hd}/2}\right) \\ 1, & \text{with probability } Q_{\chi_2^2}\left(\dfrac{\gamma' - \widehat{\Gamma}_d}{\frac{A}{r_d^\alpha}\Gamma_s\Gamma_{hd}/2}\right). \end{cases} \quad (25)$$

When we analyze ξ we can see that the worst case scenario for Alice is when Eve picks $\gamma' = \rho\Gamma_d$, which maximizes P_D. For any $\gamma' < \rho\Gamma_d$, we choose $\rho\Gamma_d$ for the value of $\widehat{\Gamma}_d$. Hence to have $\lim_{N\to\infty} \mathrm{E}[\xi(N)] \geq 1-\epsilon$ or $\lim_{N\to\infty} Pr(\xi(N) = 1) \geq 1-\epsilon$, we need

$$\begin{aligned} P_{FA} + P_{MD} &\geq 1-\epsilon \\ 1 - Q_{\chi_2^2}\left(\frac{(\rho - \frac{1}{\rho})\Gamma_d}{\frac{A}{r_d^\alpha}\Gamma_s\Gamma_{hd}/2}\right) &\geq 1-\epsilon. \end{aligned} \quad (26)$$

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

$$\Gamma_s = \frac{(\rho - \frac{1}{\rho})\Gamma_d}{\frac{A}{r_d^\alpha}Q^{-1}_{\chi_2^2}(\epsilon)\Gamma_{hd}/2}.$$

Assuming CSI on the Alice-Bob channel, we have

$$\tilde{R}_{pr,\epsilon}|H_r = \log_2\left(1 + \frac{|H_r|^2}{\Gamma_{hd}/2}\frac{\Gamma_d}{\Gamma_r}\left(\frac{r_d}{r_r}\right)^\alpha \frac{\rho - \frac{1}{\rho}}{Q^{-1}_{\chi_2^2}(\epsilon)}\right). \quad (27)$$

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

$$\begin{aligned} \tilde{R}_{pr,\epsilon,erg} &= \int_0^\infty \log_2(1+Bx)\frac{e^{-x/2}}{2}dx \\ &= \frac{1}{\ln(2)}\exp\left(\frac{1}{2B}\right)\mathrm{E}_1\left(\frac{1}{2B}\right) \end{aligned} \quad (28)$$

where $E_1(x) = \int_x^\infty \frac{e^{-t}}{t}dt$ and $B = \left(\frac{r_d}{r_r}\right)^\alpha \frac{\Gamma_d}{\Gamma_r}\frac{\Gamma_{hr}}{\Gamma_{hd}}\frac{\rho - \frac{1}{\rho}}{Q^{-1}_{\chi_2^2}(\epsilon)}$.

We can also find the outage rate

$$\begin{aligned} Pr(\tilde{R}_{pr,\epsilon} \leq c) &= Pr\left(\chi_2^2 \leq (2^c - 1)\frac{1}{B}\right) \\ &= 1 - Q_{\chi_2^2}\left((2^c-1)\frac{1}{B}\right). \end{aligned} \quad (29)$$

E. Comparison of Privacy Rates Under Different Channels

A plot of the privacy rates can be found in Fig. 4 with all parameter ratios set to one (that is, $\frac{\Gamma_{hr}}{\Gamma_{hd}} = \frac{\Gamma_r}{\Gamma_d} = \frac{r_r}{r_d} = 1$). 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.

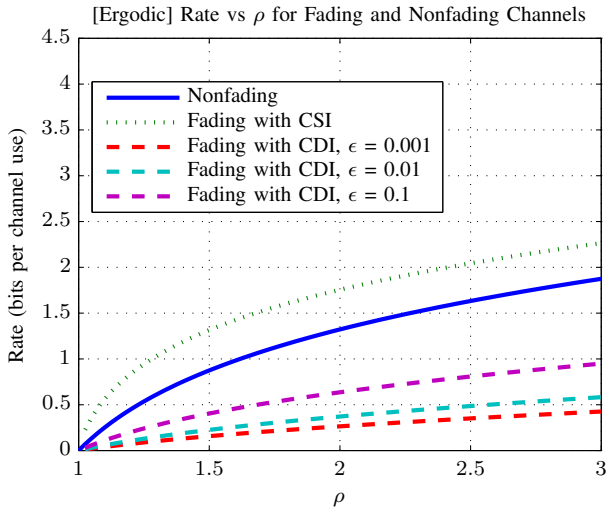

Fig. 4. Comparison of Rate or Ergodic Rate vs ρ. All parameter ratios are 1. The ergodic rate under CDI increases with ϵ.

V. Practical Rates

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 on AWGN channels we can assume some reasonable lower bounds.

For the non-fading case let us assume Eve 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 Eve's temperature uncertainty. Thermal noise power can be written as

$$\Gamma_d = k_B\widehat{T}B, \quad (30)$$

where k_B is Boltzman's constant, $\widehat{T}$ is an uncertain temperature in Kelvin in the range $[1/\rho_T T, \rho_T T]$, B is bandwidth, and ρ_T is temperature uncertainty. Because of the multiplicative nature of the temperature uncertainty, the overall noise power measurement uncertainty can be lower bounded by ρ_T. An example accurate thermometer provides readings within 0.015 K at 298 K [13]. The thermometer accuracy is arithmetically symmetric, which does not fit our model exactly. However, at such small uncertainties, the geometric symmetry in our model fits closely enough: after rounding, using $\rho_T = 1.0000503$ gives a temperature range of [297.985K, 298.015K]. For propagation loss, we will adopt a free space propagation model. 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-Eve channel and the Alice-Bob channel are the same. We will also assume that Alice knows Bob is 20 meters away. 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 I.

We analyze common bandwidths of 1, 10, and 20 MHz. While these bitrates found in Table II are low, if Alice can obtain better estimates of the noise uncertainty by taking

TABLE I. ASSUMED VALUES

True Temperature (T)	298 K
Temperature Uncertainty (ρ_T)	1.0000503
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-Eve Noise Power	Alice-Bob Noise power
Wavelength	333 mm

TABLE II. PRIVACY RATES

Bandwidth	SNR Wall	Privacy Rate
1 Mhz	14.7 fW	9.07 bits/s
10 Mhz	14.7 fW	90.7 bits/s
20 Mhz	29.4 fW	181.4 bits/s

into account interference sources or other factors, this privacy rate can increase. Fig. 5 shows the privacy rate versus ρ. Additionally, if Bob gets closer, the bitrates can increase significantly, as seen in Fig. 6.

VI. CONCLUSION

Bash, Goeckel, and Towsley recently discovered the limits of communication under low probability of detection: $O(\sqrt{N})$ bits can be implemented in N channel uses under an optimal detector. Unfortunately this is not a positive rate. However, by introducing noise power measurement uncertainty and the assumption of a sub-optimal radiometer detector, two significant possibilities open up—communication can occur with Eve's sum of probabilities of detection errors approaching one, and such undetectable communication can occur at a positive rate. By assuming some reasonable lower bounds Alice can achieve undetectable communication.

An avenue of future research is extending this privacy rate to a privacy capacity. Additionally, being able to lower bound other sources of noise would increase the SNR wall and allow for higher data rates of communication.

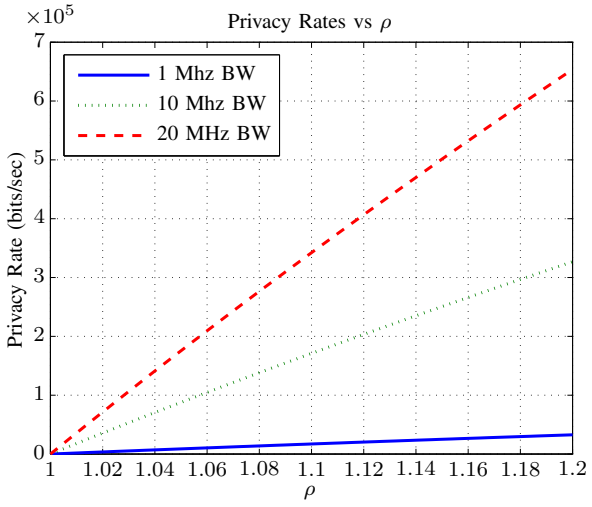

Fig. 5. Privacy rates vs ρ.

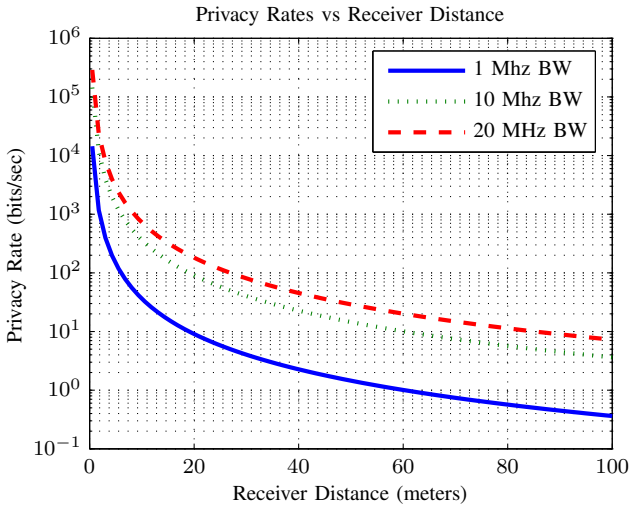

Fig. 6. Privacy rates vs r_r.

REFERENCES

[1] A. Goldsmith, S. A. Jafar, I. Mari, and S. Srinivasa, "Breaking Spectrum Gridlock with Cognitive Radios: An Information Theoretic Perspective," *Proceedings of the IEEE*, vol. 97, no. 5, 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] S. Kay, "Random Signals" in *Fundamentals of Statistical Signal Processing Detection Theory*, Upper City River, New Jersey: Prentice Hall, Inc., 1998, ch. 13, sec. 3.3, pp. 479-480.

[5] Bash, B.A.; Goeckel, D.; Towsley, D., "Square root law for communication with low probability of detection on AWGN channels," in *nformation Theory Proceedings (ISIT), Proc. 2012 IEEE International Symposium on*, pp.448,452, 1-6 July 2012

[6] Tandra, R.; Sahai, A., "SNR Walls for Signal Detection," *Selected Topics in Signal Processing, IEEE Journal of*, vol. 2, no.1, pp.4–17, Feb. 2008

[7] T.S. Rappaport, *Wireless Communications*, 2nd edition, Upper Saddle River, NJ: Prentice Hall, 2002.

[8] Alexander, S.E., "Characterising buildings for propagation at 900 MHz," *Electronics Letters*, vol.19, no.20, pp.860,, September 29 1983

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

[10] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. 2nd ed, Cambridge, Massachussets: MIT Press, 2001.

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

[12] Bloch, M.; Barros, J.; Rodrigues, M. R D; McLaughlin, S.W., "Wireless Information-Theoretic Security," Information Theory, IEEE Transactions on , vol.54, no.6, pp.2515,2534, June 2008

[13] ICL Calibration Laboratories, "Dostmann D795-PT", D795-PT datasheet