Achieving Positive Rate With Undetectable Communication Over MIMO Rayleigh Channels

Seonwoo Lee
Georgia Institute of Technology
Atlanta, Georgia

Robert J. Baxley
Georgia Tech Research Institute
Atlanta, Georgia

Joseph B. McMahon
US Department of Defense
Washington, DC

R. Scott Frazier
US Department of Defense
Washington, DC

***Abstract*—In this paper we consider the problem of achieving a positive error-free communications rate while guaranteeing that the sum of the detector's probabilities of detection errors is arbitrarily close to one. Building on our previous work, we present approximations to the privacy rate over Multiple Input-Multiple Output (MIMO) Rayleigh fading channels when a detector employs a radiometer detector and has uncertainty about his noise variance. We conclude by presenting realizable privacy rates for several practical scenarios.**

I. Introduction

There are several applications of private communication which we discuss in [1], the most obvious of which is that by avoiding detection by a detector, one can avoid being targeted by active wireless attacks like jamming. Alternatively, private communications can also be viewed as an extreme version of underlay communications, where the private party is a secondary user seeking to avoid disrupting primary users.

We previously established in [1] that undetectable communication with positive rate is possible while using one antenna. By making practical assumptions that the detector, Dave, uses a radiometer and is uncertain about his noise power, we can overcome the square root law in [3]. This law states that when the transmitter, Alice, transmits with such low power that she forces Dave to have nonrobust detection, Alice's asymptotic rate of error-free communications over an additive Gaussian noise channel to a receiver, Bob, cannot exceed zero.

As defined in [1], a detector is said to have nonrobust detection when the sum of the probability of false alarm and the probability of missed detection is bounded arbitrarily close to one; i.e. $\xi = P_{FA} + P_{MD} \geq 1 - \epsilon$, $\epsilon \in (0, 1)$, which is a slight expansion of the Signal to Noise Ratio (SNR) wall nonrobust region defined in [4]. Nonrobust detection is equivalent to requiring that Dave's receiver operating characteristic curve is no better than the curve associated with random guessing. This constraint differs from that of secrecy capacity, which restricts Dave's ability to decode Alice's transmissions.

In this paper we consider the case when Alice and Bob use multiple antennas, while still using the two critical assumptions previously mentioned. We analyze the privacy rate under Rayleigh fading channels numerically and analytically, and provide numerical results on realizable rates.

II. MIMO Rayleigh Privacy Rate

A. Problem Statement

We assume MIMO Rayleigh fading channels with complex valued symbols (Fig. 1). We also assume that while Alice and Bob have multiple antennas, Dave only has one antenna.

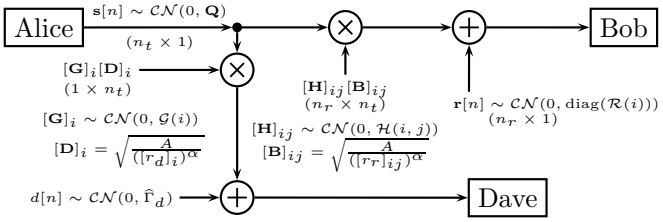

Fig. 1: The circle multiplication symbols denote matrix multiplication.

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 χ^2_N denote a chi squared random variable with N degrees of freedom, and let $Q_{\chi^2_N}(\cdot)$ be the tail probability of a χ^2_N distribution. Let $Q(\cdot)$ be the tail probability of a standard Gaussian distribution. Let n_t and n_r denote the number of transmit and receive antennas, respectively. Let the $[v]_i$ operator be the ith entry of a vector 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 $\mathrm{Var}([\mathbf{H}]_{ij}) = \mathcal{H}(i, j)$. 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 $[r_r]_{ij}$ away from Alice's ith antenna, and Dave's antenna is located $[r_d]_i$ away from Alice's ith antenna. Bob and Dave experience channel gains $\mathbf{H}$ and $\mathbf{G}$, respectively. We assume the received signal power $P = \frac{A}{r^\alpha}$, where A is some proportionality constant and α is the channel exponent. In the free-space path loss model, $\alpha = 2$. We denote the diagonal entries of $\mathbf{Q}$, the covariance matrix of $\mathbf{s}[n]$, as $\mathcal{S}(i)$. The uncertainty in Dave's measurement is given by $\widehat{\Gamma}_d \in [1/\rho\Gamma_d, \rho\Gamma_d], \rho > 1$. For simplicity, the channel gains $\mathbf{H}$ and $\mathbf{G}$ are assumed to be static over the signaling period.

Dave's detection hypotheses are

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

$$H_1 : \; x[n] = \sum_{i=1}^{n_t} \sqrt{\frac{A}{([r_d]_i)^\alpha}} [\mathbf{G}]_i [\mathbf{s}[n]]_i + d[n]. \tag{2}$$

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

We distinguish privacy capacity, which assumes Dave uses the optimal detector under the noise power uncertainty assump-

978-1-4799-1481-4/14/$31.00 ©2014 IEEE

tion, from privacy rate, which assumes Dave uses a radiometer [1].

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

We assume Dave uses

$$T(x) = \tfrac{1}{N} x^H x = \tfrac{1}{N} \sum_{n=1}^{N} x[n]^* x[n] > \gamma', \tag{3}$$

where N is the number of samples, as his detection test (a radiometer detector). Let $L[n] = \sum_{i=1}^{n_t} \sqrt{\frac{A}{([r_d]_i)^\alpha}} [\mathbf{G}]_i [\mathbf{s}[n]]_i + d[n]$, and let $l = \sum_{i=1}^{n_t} \frac{A}{([r_d]_i)^\alpha} |[\mathbf{G}]_i|^2 \Gamma_{si} + \widehat{\Gamma}_d$. Therefore $L[n] \sim \mathcal{CN}(0, l)$. Then we can find Dave's detection probability

$$\begin{aligned} P_D &= Pr\left(\frac{1}{N} \sum_{n=1}^{N} (L[n]^* L[n]) > \gamma' \right) \\ &= Q_{\chi^2_{2N}} \left(\frac{2N\gamma'}{\sum_{i=1}^{n_t} \frac{A}{([r_d]_i)^\alpha} |[\mathbf{G}]_i|^2 \mathcal{S}(i) + \widehat{\Gamma}_d} \right). \end{aligned} \tag{4}$$

Dave's asymptotic P_D and P_{FA} are [1]

$$\lim_{N\to\infty} P_{FA} = \begin{cases} 0, & \gamma' > \widehat{\Gamma}_d \\ 1, & \gamma' < \widehat{\Gamma}_d \end{cases} \tag{5}$$

$$\lim_{N\to\infty} P_D = \begin{cases} 0, & \gamma' > \sum_{i=1}^{n_t} \frac{A}{([r_d]_i)^\alpha} |[\mathbf{G}]_i|^2 \mathcal{S}(i) + \widehat{\Gamma}_d \\ 1, & \gamma' < \sum_{i=1}^{n_t} \frac{A}{([r_d]_i)^\alpha} |[\mathbf{G}]_i|^2 \mathcal{S}(i) + \widehat{\Gamma}_d \end{cases} \tag{6}$$

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

$$Pr\left(\sum_{i=1}^{n_t} \frac{A}{([r_d]_i)^\alpha} |[\mathbf{G}]_i|^2 \mathcal{S}(i) < (\rho - \tfrac{1}{\rho}) \Gamma_d \right) \geq 1 - \epsilon. \tag{7}$$

Ideally we would use a generalized chi square distribution ($|[\mathbf{G}]_i|^2$ are χ^2_2 distributed) and calculate the set $\mathcal{S}$ that satisfies (7). However, we are unable to find an analytical solution. Instead, we use the Lyapunov Central Limit Theorem (LCLT) for an approximate analytical solution (see section II-B1), and also compute the constraint numerically (see section II-B2).

Once we have the set of valid power allocations,

$$R_{pr} = \max_{\substack{\mathbf{Q}: \ \mathcal{S} \text{ satisfies (7), } [\mathbf{Q}]_{ii} \leq S(i) \ \forall i, \\ \mathbf{Q} \text{ positive semidefinite}}} \log_2 |\mathbf{I} + \mathbf{HQH}^H|. \tag{8}$$

1) Analytic Solution to Privacy Rate under Alice-Dave CDI: For this solution we assume $[r_d]_i = r_d, [\mathbf{G}]_i = \Gamma_g, \mathcal{R}(i) = \Gamma_r, [r_r]_{ij} = r_r, \mathcal{H}(i,j) = \Gamma_h \ \forall i,j$. These parameter uniformity assumptions allow us to use the Marchenko-Pastur (MP) law. 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 writing 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 (7),

$$\sum_{i=1}^{\tilde{n}} \frac{A}{r_d^\alpha} \Gamma_g \mathcal{S}(i) + Q^{-1}(\epsilon) \sqrt{\sum_{i=1}^{\tilde{n}} \left(\frac{A}{r_d^\alpha} \Gamma_g \mathcal{S}(i) \right)^2} \leq (\rho - \tfrac{1}{\rho}) \Gamma_d. \tag{9}$$

The combination of the LCLT's impractical $\tilde{n} \to \infty$ assumption with the following constraint results in a good approximation of privacy rate, as we will see in Section II-B2.

To simplify (9), we use the norm property that for $a_i \geq 0$,

$$\sqrt{\textstyle\sum_i a_i^2} \leq \textstyle\sum_i a_i, \tag{10}$$

giving us the new constraint function

$$\sum_{i=1}^{n_t} \mathcal{S}(i) \leq \frac{(\rho - 1/\rho)\Gamma_d}{(1 + Q^{-1}(\epsilon)) \frac{A}{r_d^\alpha} \Gamma_g}. \tag{11}$$

To see (10), observe that the unit ball described by setting the right hand side (RHS) of (10) to one is a strict subset of the unit ball described by setting the left hand side of (10) 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 $[\mathbf{J}]_{ij} \sim \mathcal{CN}(0,1)$. The parameter uniformity assumptions allow us to write our new channel matrix $\tilde{\mathbf{H}} = \sqrt{\Gamma_h} \mathbf{J} \mathbf{J}^H$. If the distribution of the eigenvalues for the general $\mathbf{H}$ were known, that 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

$$R_{pr,CLT} = \max_{\substack{\mathcal{S}: \ \mathcal{S}(i) \geq 0 \ \forall i, \\ \mathcal{S} \text{ satisfies (11)}}} \sum_{i=1}^{\tilde{n}} \log_2 \left(1 + \sigma_i^2 \frac{\Gamma_h A \mathcal{S}(i)}{r_r^\alpha \Gamma_r} \right) \tag{12}$$

where $\sigma_i^2 = \lambda_i$ are the eigenvalues of $\mathbf{JJ}^H$. Our numerical solution in II-B2 considers the off diagonal elements of $\mathbf{Q}$.

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

$$\mathcal{S}(i) = \left(\frac{\theta}{(1 + Q^{-1}(\epsilon)) \frac{A}{r_d^\alpha} \Gamma_g} - \frac{\Gamma_r r_r^\alpha}{A \Gamma_h \lambda_i} \right)^+ \quad \forall i \tag{13}$$

where θ is a water filling parameter. The familiar water filling solution follows from the fact that applying the LCLT and (10) changes our constraint function (11) 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 (15), (19), (20), and (21) in [2] with

$$P_0 = \frac{\rho - 1/\rho}{1 + Q^{-1}(\epsilon)} \frac{\Gamma_d}{\Gamma_r} \frac{\Gamma_h}{\Gamma_g} \left(\frac{r_d}{r_r} \right)^\alpha \tag{14}$$

we get an analytical approximation of the privacy rate.

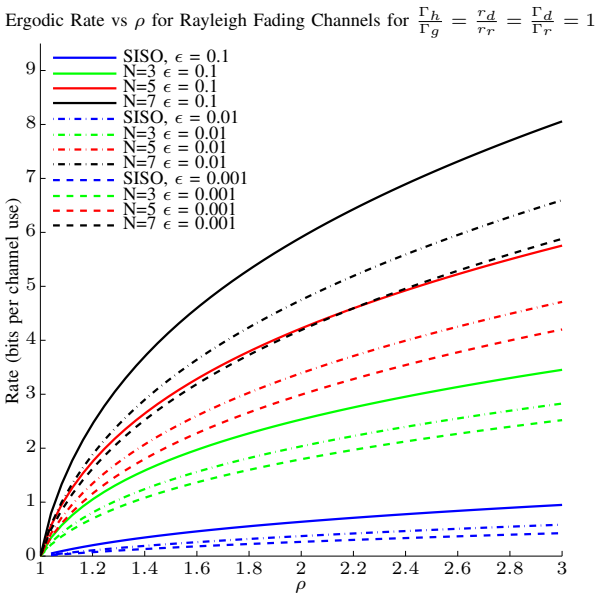

Fig. 2: Privacy rates vs ρ under the LCLT model.

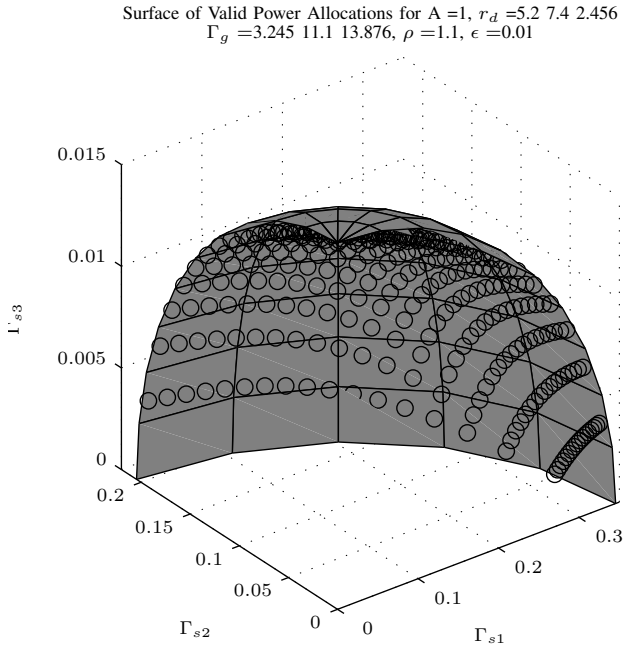

Fig. 3: Boundary surface of valid power allocations for arbitrary A, ϵ, ρ, Γ_g, r_d. All points below the surface in the first octant are also valid. The discrete points are the true boundary, whereas the background surface is an ellipsoid.

If $n_t \neq n_r$, the rate bound can be found numerically by evaluating (15) in [2]. The privacy rates are plotted in Fig. 2.

It is important to note that there is no SNR term in the privacy rate. By solving for the maximum allowable power given the detector noise uncertainty and the ratios of parameters, we eliminate SNR.

This privacy rate differs to that in [6]. 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, his low probability of detection (LPD) constraint differs from ours—he constrains the Chernoff exponent, which limits how quickly Dave's detection errors decay exponentially to zero. This 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.

2) Numerical Solution to Privacy Rate under Alice-Dave CDI: Again, we are interested in maximizing Alice-Bob rate under the constraint given by (7). By using the generalized χ_2^2 distribution [7], we plot valid power allocations for arbitrary values of $A, \mathcal{G}, \Gamma_d$ and r_d and $\tilde{n} = 3$. Because the rate monotonically increases in power, we are only interested in power allocations at the boundary of our constraint function. The discrete points in Fig. 3 come from (7), whereas the surface plot is that of an ellipsoid, $(\frac{x}{\mathcal{S}(1)})^2 + (\frac{y}{\mathcal{S}(2)})^2 + (\frac{z}{\mathcal{S}(3)})^2 = 1$, where $\mathcal{S}$ can be found by solving $\mathcal{S}(i) = \frac{(\rho-1/\rho)\Gamma_d}{\frac{A}{(|r_d|_i)^\alpha} Q_{\chi_2^2}^{-1}(\epsilon)\mathcal{G}(i)/2}$, the maximum power allowed for that antenna if only that antenna were used [1]. 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 noise from temperature, we have a low resultant transmit power, as we will see in section III. 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 LPD MIMO 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 [8]. Finding the LPD rate can be reformulated as finding the maximum of the capacities with per-antenna power constraints for each valid power allocation in Fig. 3. 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 $\mathbf{H}\mathbf{H}^H$,

$$R_{pr,\text{beamforming}} = \log_2(1 + \tfrac{\sigma_x^2\lambda_1}{\Gamma_r}). \tag{15}$$

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

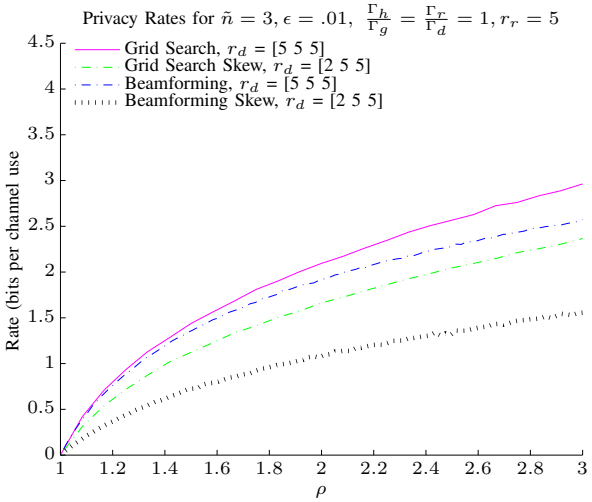

Fig. 4: Privacy rates vs ρ. in skewed vs not skewed

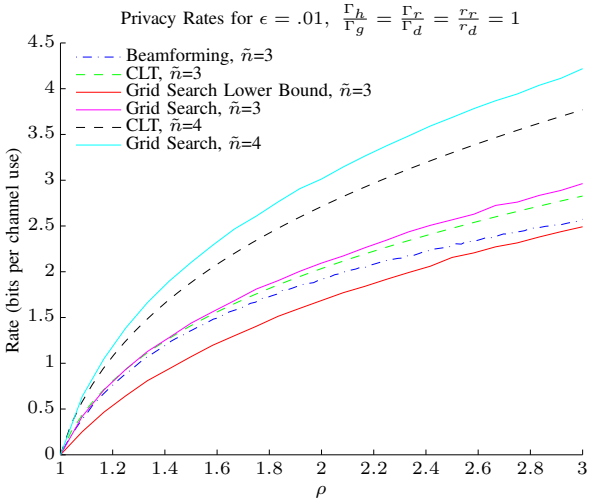

Fig. 5: Comparison of privacy rates vs ρ under different models

(PAPC) capacity at each allocation [8], and then pick the maximum across all power allocations. Because calculating the PAPC capacity is computationally expensive at low power allocations [8], 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. 5. We see that at 3 antennas the computationally fast LCLT method provides a 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 (10). All these 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.

The beamforming solution performs well with parameter uniformity, but as the privacy constraint region becomes skewed, the approximation error grows (Fig. 4). 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.

III. Practical Rates

To give some practical rates we can assume some reasonable lower bounds, which can be found in Table I. We adopt a free space propagation model with isotropic antennas. The measurement uncertainty can be lower bounded by Dave's temperature uncertainty ρ_T [1]. An example accurate thermometer provides readings within 0.015 K at 298 K [5]. While the bitrates in Table II are low, if Alice can obtain better estimates of the noise uncertainty by taking into account other factors, the privacy rate increases.

These privacy rates are 2.7 times greater than having four separate SISO channels under the LCLT approximation.

TABLE I: Assumed Values

True T	298 K
ρ_T	1.0000503
T interval	[297.985, 298.015] K
r_d	5 meters
r_r	20 meters
α	2
Γ_h	2
Γ_g	3
Γ_d	Γ_r
Wavelength	333 mm
$\tilde{n}$	4

TABLE II: 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

IV. Conclusion

We have quantified the increase in privacy rates that multiple antennas affords while assuming Dave is uncertain about his noise power. Possible future research directions are finding the privacy capacity and also devising a coding scheme to achieve positive privacy rate communication.

References

[1] S. Lee and R.J. Baxley, "Achieving Positive Rate With Undetectable Communication Over AWGN and Rayleigh Channels," in Proc. IEEE International Conference on Communications, Sydney, Australia, June, 2014.

[2] Bliss, D.W.; Forsythe, K.W.; Yegulalp, A.F., "MIMO communication capacity using infinite dimension random matrix eigenvalue distributions," Signals, Systems and Computers, 2001. Conference Record of the Thirty-Fifth Asilomar Conference on , vol.2, no., pp.969,974 vol.2, 4-7 Nov. 2001

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

[4] 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

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

[6] Hero, A.O., "Secure space-time communication," Information Theory, IEEE Transactions on , vol.49, no.12, pp.3235,3249, Dec. 2003

[7] Hammarwall, D.; Bengtsson, M.; Ottersten, B., "Acquiring Partial CSI for Spatially Selective Transmission by Instantaneous Channel Norm Feedback," Signal Processing, IEEE Transactions on , vol.56, no.3, pp.1188,1204, March 2008

[8] Vu, Mai, "MIMO Capacity with Per-Antenna Power Constraint," Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE , vol., no., pp.1,5, 5-9 Dec. 2011