# Asymptotic MIMO Artificial-Noise Secrecy Rates with Eigenmode Partitioning

Andrew D. Harper
School of Electrical and Computer Engineering
Georgia Institute of Technology, Atlanta, Georgia
Email: andrewharper@gatech.edu

Robert J. Baxley
Georgia Tech Research Institute
Atlanta, Georgia
Email: bob.baxley@gtri.gatech.edu

***Abstract*—In a multiple-input multiple-output (MIMO) wiretap channel system, it has been shown that artificial noise can be transmitted in the null space of the main channel to guarantee the secrecy at the intended receiver. Previous formulas for MIMO asymptotic capacity assume that all channel eigenmodes will be utilized. However, optimizing over possible antenna configurations requires partitioning the available eigenmodes. With only some eigenmodes used for signal transmission, finding an exact closed-form asymptotic solution is, in general, intractable. We present a large-scale MIMO approximation with eigenmode partitioning, accurate for realistic numbers of antennas, and with greatly reduced computational complexity.**

## I. Introduction

In a MIMO wiretap channel, secrecy capacity is defined as the amount of information that can be reliably communicated from transmitter (Tx) to intended receiver (Rx), with any eavesdropper (Ex) able to intercept the transmission gaining an arbitrarily small amount of information. Wyner first demonstrated for wired communications [1], and subsequently Csiszár and Körner for broadcast messages [2], that a relative advantage in signal to noise ratio (SNR) could guarantee secrecy from a third-party. In rich-scattering multipath channels, the average secrecy capacity is nonzero even when the SNR at the Ex exceeds that at the Rx [3], [4].

Goel and Negi demonstrated that a relative SNR advantage could be created for the Rx in a MIMO flat-fading channel through transmitting *artificial noise* (AN) in the null-space of the main channel [5], [6]. In this approach, the Tx divides transmission power between the message symbols to be communicated and the noise symbols to ensure secrecy. Leveraging spatial degrees of freedom in multipath MIMO systems, the advantage is established by effectively degrading all eigenmodes apart from that of the intended Rx. An eavesdropper's only choice is then to attempt to increase SNR by approaching the Tx. However, at high SNR the eavesdropper's gains saturate while those of the main channel continue increasing, thereby guaranteeing a positive secrecy capacity is attainable regardless of the eavesdropper's proximity to the Tx.

Calculating secrecy rate guaranteed with artificial noise involves expectation over random channel gains via Monte-Carlo simulation, followed by optimization over both antenna and power allocation variables. The complexity involved with this task makes it unfeasible for resource-constrained or adaptive systems. Comparing a chosen implementation to the maximum achievable requires either generation and storage of large lookup tables or simulation for each tested configuration. Our objective in this paper is to develop a method of approximating the AN secrecy rate[1] presented in [5] that: 1) is closed form, 2) is accurate and useful for realistic power levels and numbers of antennas, 3) generalizes the channel model to include arbitrary independent and identically distributed (i.i.d.) channels, and 4) does not weaken security by overestimating the rate at which secret communication is possible.

## II. Related Work

While AN inherently assumes multiple transmit (input) antennas, the many previous works in AN secrecy can be categorized based on the number of antennas at the Rx (output) and Ex (eavesdrop). Because no control is assumed over potential eavesdroppers, multiple antennas at the Ex is usually assumed. The standard possible antenna configurations have thus been termed multiple-input single-output multiple-eavesdrop (MISOME) and multiple-input multiple-output multiple-eavesdrop (MIMOME).

Khisti and Wornell [7] first explored the use of AN for the the deterministic MISOME wiretap channel, and showed that the AN method yields a rate asymptotically (in power) near secrecy capacity. Zhou and McKay further developed the theory of AN secrecy in [8] for the multiple-input single-output single-eavesdrop (MISOSE). This work allowed for multiple eavesdroppers in collusion, which can be considered equivalent to the MISOME case. Other works have also investigated the AN problem from a number of different perspectives: In [9], [10] optimal strategies for power allocation in AN secrecy systems are also investigated. Reference [11] considers the effectiveness of beamforming for maintaining security in a MIMO system, as well as optimal detection strategies at the eavesdropper. The effect of imperfect channel-state information (CSI) at the transmitter and noise leakage into the main channel is considered in [12], [13]; imperfect CSI at the receiver is considered in [14]. In [15], power

[1]While the original Goel and Negi text refers to this quantity as minimum-guaranteed secrecy *capacity*, [7] showed the AN solution to be sub-optimal in general. We hereafter refer to this as the minimum-guaranteed secrecy *rate*.

978-1-4799-8882-2/14/$31.00 ©2014 IEEE

allocation is considered from an outage probability perspective for the MISO case.

In recent work [16], the authors generalize the artificial noise framework to allow transmission of AN power into the main channel for the special MISOSE case where the transmitter may have multiple antennas but the intended receiver and the eavesdropper are each equipped with only a single antenna. Their analysis determined that, contrary to intuition, the optimal beamforming matrix did not strictly limit the AN transmitted to the null-space of the main channel; rather, modest secrecy gains can be achieved in lower SNR regions where the zero-forcing solution yields zero secrecy capacity. The generalized approach quickly converges to that in [5] with increases in the number of transmit antennas, and more slowly with increases in SNR.

Recent literature has used random matrix theory to characterize the *per receive antenna* capacity of MIMO systems by looking at the asymptotic large-antenna limit. Central to this theory is the idea that, in a MIMO system with $t$ Tx antennas and $r$ Rx antennas, the eigenvalues of many classes of random matrices converge almost surely to a non-random limit as $t, r \to \infty$ with the ratio $t/r \to \beta$ [17]. In [18], the asymptotic capacity of MIMO systems in the presence of multiple-antenna interferers is derived. While a closed-form solution is not possible in general, the asymptotic capacity can be found as the solution to a set of polynomials.

The large-antenna asymptotic capacity of a MIMO channel with full CSIT is derived in closed form in [19]. With AN secrecy assuming CSIT, these asymptotic techniques can be used to arrive at an approximation for the main channel capacity. However, a key assumption in [19] is that SNR is sufficient such that *all available spatial eigenmodes* are utilized in the waterfilling power allocation. For the case of AN secrecy, optimization over the set of possible antenna configurations at times allocates only *a portion* of the spatial dimensions available for signal transmission may be allocated instead to artificial noise transmission.

The asymptotic solutions we present in this paper contribute to existing works in that they: 1) extend previous asymptotic formulas to the MIMOME case and effectively incorporate the eigenmode partitioning central to AN secrecy methods; 2) greatly reduce complexity and demonstrate bounded error; and 3) apply to a more general channel model and thus depend only on parameters controllable at the transmitter.

## III. System Model

We consider the standard MIMO wiretap channel, with $t$, $r$, and $e$ antennas at Alice (Tx), Bob (Rx) and Eve (Ex), respectively. $\mathbf{H} \in \mathbb{C}^{r\times t}$ is the MIMO main (Alice-Bob) channel matrix, and $\mathbf{G} \in \mathbb{C}^{e\times t}$ is the MIMO eavesdropper (Alice-Eve) channel matrix. We assume a rich scattering environment, and assume both channels to be slow flat-fading such that the channel is constant for the duration of the channel estimation and subsequent code word transmission. Thus the entries of $\mathbf{H}$ are i.i.d. complex Gaussian distributed. For comparison of antenna configurations, we normalize the channel entries to have unit variance such that the average received SNR is independent of number of transmit antennas.

Alice may attempt to give Bob a relative SNR advantage over Eve by broadcasting noise in the null space of Bob's channel [5]. Alice and Bob first estimate the channel, and use singular value decomposition (SVD) to arrive at $\mathbf{H} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^\dagger$, where $^\dagger$ denotes the Hermitian transpose. Assuming $t > r$, there are a maximum of $r$ dimensions on which Alice may transmit message symbols to Bob. However, Alice must have at least $e + 1$ degrees of freedom available to devote to the AN symbols so that Eve is not able to overcome the added noise through linear combining. Alice chooses AN dimensions $d_a \geq e$, signal dimensions $d_s = \min(r, t-e)$, with $d_s + d_a \leq t$, and forms combined message symbol and noise symbol vector $\mathbf{w} = [\mathbf{w}_s^\dagger \mathbf{w}_a^\dagger]^\dagger$. Note that, even when the main channel matrix is full rank, $d_s < r$ will require *partitioning* available eigenmodes between signal and AN.

Alice chooses the precoding matrix to be a subset of vectors from the right singular vector matrix, split by columns according to number of signal and noise dimensions as $\mathbf{V} = [\mathbf{V}_s\ \mathbf{V}_a]$. The transmitted vector is thus $\mathbf{x} = [\mathbf{V}_s\ \mathbf{V}_a]\mathbf{w}$. The received vectors at Rx and Ex, respectively, become

$$\mathbf{U}_{d_s}^\dagger \mathbf{y}_m = \mathbf{U}_{d_s}^\dagger \mathbf{H}\mathbf{x} + \mathbf{U}_{d_s}^\dagger \mathbf{n}_m \quad (1)$$

$$= \mathbf{\Sigma}_{d_s}\mathbf{w}_s + \tilde{\mathbf{n}}_m \quad (2)$$

$$\mathbf{y}_e = \mathbf{G}\mathbf{x} + \mathbf{n}_e \quad (3)$$

$$= \mathbf{G}\mathbf{V}_s\mathbf{w}_s + \mathbf{G}\mathbf{V}_a\mathbf{w}_a + \mathbf{n}_e, \quad (4)$$

where the subscript $d_s$ denotes the first $d_s$ columns, and $\{\mathbf{n}_m, \mathbf{n}_e, \tilde{\mathbf{n}}_m\} \sim \mathcal{CN}(\{\mathbf{0}, \mathbf{0}, \mathbf{0}\}, \{\sigma_{n_m}^2\mathbf{I}_r, \sigma_{n_e}^2\mathbf{I}_e, \sigma_{\tilde{n}_m}^2\mathbf{I}_m\})$ are AWGN vectors at Rx and Ex, with the elements of $\tilde{\mathbf{n}}_m$ distributed identically to those of $\mathbf{n}_m$ since $\mathbf{U}$ is unitary. By Tx precoding with $\mathbf{V}$ and Rx processing with $\mathbf{U}$, Alice and Bob effectively turn the main channel into a bank of $d_s$ parallel Gaussian channels, and, since the columns $\mathbf{V}$ are orthogonal, steer the noise into the null of the main channel. Eve, ignorant of $\mathbf{V}$ and $\mathbf{U}$, is unable to avoid the effects of the added noise so long as her channel matrix entries are not strongly correlated with Bob's; this condition is commonly assumed to be true in a rich-scattering environment when Eve's distance from Bob exceeds a half-wavelength.

Alice may optimize secrecy by allocating power selectively to message and AN symbols. Defining message signal power $P_s = \mathrm{E}[\mathbf{w}_s^\dagger \mathbf{w}_s]$, and AN signal power $P_a = \mathrm{E}[\mathbf{w}_a^\dagger \mathbf{w}_a]$, the total transmit power is constrained to $P_s + P_a \leq P$. For a given $P_s$, Alice chooses the signal covariance matrix $\mathbf{R}_s = \mathrm{E}[\mathbf{w}_s \mathbf{w}_s^\dagger]$ through standard waterfilling [20]. Since $\mathbf{G}$ is unknown to Alice, the noise covariance matrix $\mathbf{R}_a = \mathrm{E}[\mathbf{w}_a \mathbf{w}_a^\dagger]$ is chosen as the scaled identity matrix.

The instantaneous secrecy capacity of a three-party eavesdropper channel the non-negative maximum difference in mutual information between the main and eavesdropper channel [21],

$$C^{sec} = \max_{p(\mathbf{x})} [I(\mathbf{y}_m; \mathbf{x}|\mathbf{H}) - I(\mathbf{y}_e; \mathbf{x}|\mathbf{G})]^+, \quad (5)$$

where $p(\mathbf{x})$ is the input distribution of the message, $I(\mathbf{t};\mathbf{u})$ is the mutual information between vectors $\mathbf{t}$ and $\mathbf{u}$, and $[x]^+ = \max(0,x)$. With the AN approach, the eavesdropper channel is degraded by design, guaranteeing a strictly positive ergodic secrecy rate, given as

$$R^{sec} = \max_{\substack{(d_s,d_a)\in\mathcal{D}\\(P_s,P_a)\in\mathcal{P}}} \mathrm{E}_{\mathbf{G},\mathbf{H}}[I(\mathbf{y}_m;\mathbf{x}) - I(\mathbf{y}_e;\mathbf{x})], \tag{6}$$

with

$$\mathcal{D} = \{(d_s,d_a):\ d_a \geq e,\quad d_s \leq r,\quad d_s + d_a \leq t\} \tag{7}$$

$$\mathcal{P} = \{(P_s,P_a):\ P_s + P_a \leq P\}. \tag{8}$$

Since the proximity of a passive Ex to the Tx is in general unknown, the ergodic minimum guaranteed secrecy capacity is often characterized by assuming the worst case eavesdropper noise scenario where $\sigma^2_{n_e} \to 0$, given in [5] as:

$$R^{sec,mg} = \max_{\substack{(d_s,d_a)\in\mathcal{D}\\(P_s,P_a)\in\mathcal{P}}} \mathrm{E}_{\mathbf{G},\mathbf{H}}\left[\log_2\det\left(\mathbf{I}_r + \mathbf{H}\mathbf{R}_s\mathbf{H}^\dagger\right) - \log_2\frac{\det\left(\mathbf{G}\mathbf{V}_s\mathbf{R}_s\mathbf{V}_s^\dagger\mathbf{G}^\dagger + \mathbf{G}\mathbf{V}_a\mathbf{R}_a\mathbf{V}_a^\dagger\mathbf{G}^\dagger\right)}{\det(\mathbf{G}\mathbf{V}_a\mathbf{R}_a\mathbf{V}_a^\dagger\mathbf{G}^\dagger)}\right], \tag{9}$$

where $\sigma^2_{n_m} = 1$ and a mutual-information-maximizing Gaussian signaling alphabet have been assumed.

We note that, in contrast to [16], our work is similar to [5] in that we require all AN to be transmitted in the null-space of the main channel, and the equations we derive may thus be suboptimal with regards to the rates they generate. However, the advantage gained by this relaxation diminishes quickly with increases in Tx antennas; the effect is most noticed with two transmit antennas, and with only four antennas at Tx the secrecy rate is nearly identical to the zero-forcing approach. We hereforward assume sufficient Tx antennas to neglect optimizing the covariance structure beyond standard waterfilling. With such an assumption, the approximation we present is guaranteed to be in closed form.

## IV. Large-Scale MIMO Analysis

The number of acceptable dimension pairs $|\mathcal{D}|$ is predetermined by the MIMO antenna configuration, while the number of acceptable power-allocation pairs $|\mathcal{P}|$ will depend on the resolution chosen. It is easily seen that the size of the search space can quickly grow large as number of antennas increase or desired resolution decreases. Therefore an efficient method of calculating the Rx and Ex rates is of great interest in any system, particularly those that may be resource-constrained or adaptive in time.

We now present the main results of this paper by deriving accurate, low-complexity approximations to the minimum-guaranteed secrecy capacity for the MIMOME case. We proceed by analyzing the Ex and Rx terms in (9) independently. This produces values for the respective communication rates achieved by Bob and Eve,

$$R^B = I(\mathbf{y}_m,\mathbf{x}), \quad \text{and} \quad R^E = I(\mathbf{y}_e,\mathbf{x}). \tag{10}$$

We calculate the minimum-guaranteed secrecy rate approximation as follows: First, we reformulate the eavesdropper channel into a multiuser-interference framework to allow for partitioning of eigenmodes, and approximate using large-scale asymptotic analysis results from random matrix theory. Next, we provide a heuristic approach to modify existing main-channel capacity methods which is simple, intuitive, and accounts for the necessary eigenmode partitioning. With closed-form solutions for both Ex and Rx channels, the secrecy capacity is then easily and quickly approximated. The propositions that follow are given without proof due to space limitations; full proofs will be included in the journal version.

### A. Eavesdropper Channel: Large-Scale Approximation

We now approximate the first term in (6). Since AN symbols can be chosen to be independent of all message symbols, we can view the AN as though it were actually message symbols coming from an outside interfering user. Thus, the Ex will observe $d_s$ message symbols from the Tx, corrupted by additive white Gaussian noise (AWGN) and $d_a$ message symbols from a theoretical unknown user. We will use this multiuser-interference approach [18], [22] to approximate the per-eavesdrop antenna capacity $\mathcal{R}^{\mathrm{E}} = \frac{1}{e}R^{\mathrm{E}}$.

**Proposition 1.** *In a MIMO wireless channel with $t$ transmit and $e$ eavesdrop antennas, assume the transmitter chooses to transmit $d_s$ information symbols and $d_a \geq e$ AN symbols. Define the ratio of signal power to total power as $\alpha = \frac{P_s}{P_s+P_a}$. Let $t,e \to \infty$, with $t/e \to \beta$, $d_s/t \to \gamma_s$, and $d_a/t \to \gamma_a$. Then the worst-case (eavesdropper SNR $\to \infty$) per-antenna eavesdropper rate can be approximated in closed-form[2] as:*

$$\begin{aligned}\mathcal{R}^E \approx (\gamma_s+\gamma_a)\,\beta\Bigg[&\gamma_s\log_2\left(1+\alpha P\frac{\eta_1}{\gamma_s^2\beta}\right)\\ &+\gamma_a\log_2\left(1+(1-\alpha)P\frac{\eta_1}{\gamma_s\gamma_a\beta}\right)\Bigg]\\ &-\gamma_a\beta\left[\log_2\left(1+(1-\alpha)P\frac{\eta_2}{\gamma_s\gamma_a\beta}\right)\right]\\ &+\log_2\left(\frac{\eta_2}{\eta_1}\right)+(\eta_1-\eta_2)\log_2(e),\end{aligned} \tag{11}$$

*where $\eta_1$ and $\eta_2$ are the solutions on interval $[0,1]$ to the following:*

$$\begin{aligned}\eta_1 + (\gamma_s+\gamma_a)\,\beta\Bigg[&\frac{\gamma_s\alpha P\eta_1}{\alpha P\eta_1+\gamma_s^2\beta}+\\ &\frac{\gamma_a(1-\alpha)P\eta_1}{(1-\alpha)P\eta_1+\gamma_s\gamma_a\beta}\Bigg] = 1\end{aligned} \tag{12}$$

[2]Writing the closed-form solution to the eavesdropper-channel efficiencies $\eta_1$ and $\eta_2$ is possible using the quadratic and cubic (Cardano) equations. However, doing so gives lengthy and cumbersome results that do not yield additional insight. Therefore in this paper we refer to the eavesdropper results as closed form while leaving them as solutions to 2nd and 3rd-order polynomials.

| Variable (units) | Definition |
|---|---|
| $d_s$ (dimensions) | eigenmodes devoted to signal transmission |
| $d_a$ (dimensions) | eigenmodes devoted to AN transmission |
| $\alpha$ (unitless) | proportion of total power devoted to signal |
| $\beta$ (unitless) | Tx antenna to Rx antenna ratio |
| $\gamma_s$ (dim/ant) | signal eigenmodes to total eigenmodes ratio |
| $\gamma_a$ (dim/ant) | AN eigenmodes to total eigenmodes ratio |
| $\zeta_s$ (dim/ant) | signal eigenmodes to Rx antenna ratio |

TABLE I: Variables and definitions.

$$\eta_2 + \gamma_a \beta \left[ \frac{(1-\alpha)P\eta_2}{(1-\alpha)P\eta_2 + \gamma_s\gamma_a\beta} \right] = 1 \tag{13}$$

Although we assume an i.i.d. Gaussian channel model here for comparison with previous literature, the derivation in Proposition 1 only requires i.i.d. channel entries. Note that the expectation over complex channel gains $\mathbf{H}$ and $\mathbf{G}$ has been replaced in the asymptotic analysis with the solution to a pair of polynomials in $\eta_1$ and $\eta_2$. These polynomials are also decoupled, which further reduces the complexity required to solve the system.

Thus for a given pair $(d_s, d_a) \in \mathcal{D}$, the worst-case reduction in secrecy capacity arising from an eavesdropper of unknown location can be estimated simply by solving for $\eta_1$ and $\eta_2$ and plugging the values into (11). This amounts to finding the zeros of a set of decoupled quadratic and cubic equations. Note that the secrecy capacity equation given in (9) is, in general, non-convex, and efficient optimization methods remain an open problem. The reduction in complexity afforded by the multiuser interference approximation method will be further scaled by the number of search points employed by the specific optimization method chosen, for which we introduce the following proposition.

**Proposition 2.** *The set of eigenmode allocation pairs $(d_s, d_a) \in \mathcal{D}$ over which to maximize secrecy rates can be reduced to a subset $\mathcal{D}' \subseteq \mathcal{D}$ by adding the constraint that*

$$d_a \geq \lceil \sqrt{et} - d_s \rceil, \tag{14}$$

*where $\lceil x \rceil$ is the smallest integer greater than or equal to $x$.*

If Alice is, perhaps sub-optimally, constricted to exhaust all available eigenmodes on either signal or AN such that $d_s + d_a = t$, then $\eta_1 = 0$ for $t \geq e$. Without $t \geq e$ the AN approach to secrecy is not possible, so in this restrictive case no new information is gained. However, in such a case the search space would already be greatly reduced. Note that we can similarly look at the asymptotic power limit of $\eta_2$ by rewriting (13) as

$$\eta_2 + \frac{1}{\frac{e}{d_a} + \frac{d_s}{(1-\alpha)tP\eta_2}} = 1, \tag{15}$$

the asymptotic limit becomes

$$\lim_{P\to\infty} \eta_2 = \left[ 1 - \frac{d_a}{e} \right]^+, \tag{16}$$

which yields the requirement that $d_a \geq e$. This condition was presented originally in [5] as a problem requirement, and is confirmed here from a multiuser interference approach. It is quite intuitive that Alice would not benefit from using only a small fraction of available eigenmodes. Figure 1 shows that the reduced search space achieved by imposing the additional eigenmode restriction from Proposition 2 has eliminated the eigenmode pairs smallest in numbers.

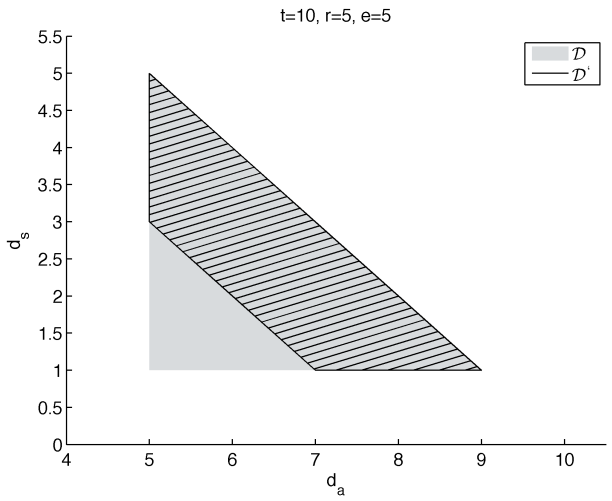


Fig. 1: Example reduction in search space from $\mathcal{D}$ (gray) to $\mathcal{D}$ (lines) as a result of adding the restriction in Proposition 2.

### *B. Main Channel: Large-Scale Approximation (LSA)*

**Proposition 3.** *In a MIMO system with $t$ transmit and $r$ receive antennas, with $t > r$, define the number of eigenmodes allocated to signal transmission $d_s \leq r$. Let $t, r \to \infty$, $t/r \to \beta$, $d_s/t \to \gamma_s$, and $r/d_s \to \zeta_s$. Define $\alpha = P_s/P$ as the ratio of signal to total power transmitted. Then the per-antenna main-channel rate can be approximated by:*

$$\mathcal{R}^B \approx \frac{1}{\zeta_s} \left[ \log_2 \left( \frac{\alpha P}{\gamma_s} + \frac{1}{1-\gamma_s} \right) + \frac{1-\gamma_s}{\gamma_s} \log_2 \left( \frac{1}{1-\gamma_s} \right) - \log_2 \mathrm{e} \right]. \tag{17}$$

Intuitively, this approximation can be thought of as a scaling of the asymptotic antenna ratio $\beta$ by $r/d_s$ to reflect the reduction in signal dimensions, and subsequent scaling of the asymptotic capacity by $d_s/r$ to transform the units of the result from bps/Hz per signal dimension to bps/Hz per receive antenna. Though this analysis is heuristic, we will see that the performance is nonetheless good for the cases tested.

**Proposition 4.** *Define the approximation error incurred by using the large-scale asymptotic approximation in (17) as*

$$\epsilon = \frac{1}{r} \mathrm{E}_{\mathbf{H}} \left[ \log_2 \det \left( \mathbf{I}_r + \mathbf{H}\mathbf{V}_s\mathbf{R}_s\mathbf{V}_s^\dagger\mathbf{H}^\dagger \right) \right] - \mathcal{R}^B. \tag{18}$$

*The magnitude of this approximation error is upper-bounded by*

$$|\epsilon| \leq \frac{\log_2(\mathrm{e})}{\zeta_s}. \tag{19}$$

As evidenced by Propositions 3 and 4, we witness an interesting interplay between the error upper bound and the actual error observed. On the one hand, using fewer available eigenmodes increases the value of $\zeta_s$, which in turn decreases the maximum possible error magnitude. On the other hand, using more available eigenmodes brings $d_s$ closer in value to $r$, which decreases the modeling error. Note that, when all available signal dimensions are utilized by setting $d_s = r$, the original closed-form asymptotic capacity solution is regained. Therefore we expect the largest error for largest $|r - d_s|$, and smallest error both as $d_s \to r$ and $d_s \to 0$.

### C. Computing the MIMOME Secrecy Rate

To compute the AN generated secrecy capacity for the general MIMOME case, we combine the results of Propositions 1-3. With the approximations for each channel and new set $\mathcal{D}'$ of antenna pairs, the secrecy rate $\hat{C}^{sec}$ of the MIMOME system can be approximated via

$$\hat{R}^{sec} = \max_{\substack{(d_s,d_a):d_s+d_a\leq t,\ d_s\leq r,\ d_a\geq\lceil\sqrt{et}-d_s\rceil \\ (P_s,P_a):P_s+P_a\leq P}} [r\mathcal{R}^B - e\mathcal{R}^E], \tag{20}$$

The simplicity of this approximation is evident upon comparing with (6). Expectation over random channel gains has been eliminated and replaced with closed-form expressions, and the optimization method of choice can be implemented over a smaller search space. Even if the result is non-convex, the results can be used to intelligently select initial conditions to efficiently search the space with gradient descent methods. However, because of the great reduction in computation, exhaustive search becomes a quite reasonable approach.

While most capacity calculations are done offline during the system design phase, it is still advantageous to have easy-to-compute expressions for a maximum rate for several reasons. First, with the proposed expressions, an eavesdropper will be able to quickly bound the secrecy rate of the main channel. If the channel is evolving in time, using our proposed expression will greatly reduce the complexity required to make the approximations. But a more compelling case is that these expressions simply make it easier for secrecy researcher to compare the rates achievable with a suggested implementation to the best case rates.

## V. Results

To test the accuracy of the approximated secrecy rate, we compared our results with $10^4$ Monte Carlo trials. Figure 2 shows an example of the overall asymptotic secrecy rate approximation given in (20) for various antenna configurations plotted against the actual ergodic secrecy rate. Although the approximation combines two asymptotic approaches, it nonetheless performs accurately for realistic numbers of antennas. For $t = 8$, we tested cases of equal numbers of antennas at Ex and Rx, along with cases where $r > e$ and $e > r$. Performance is good for all configurations, with the exception of the case of $e = 3$ and $r = 5$ for SNR $< 5$ dB, where the secrecy rate is overestimated; however, for such low power

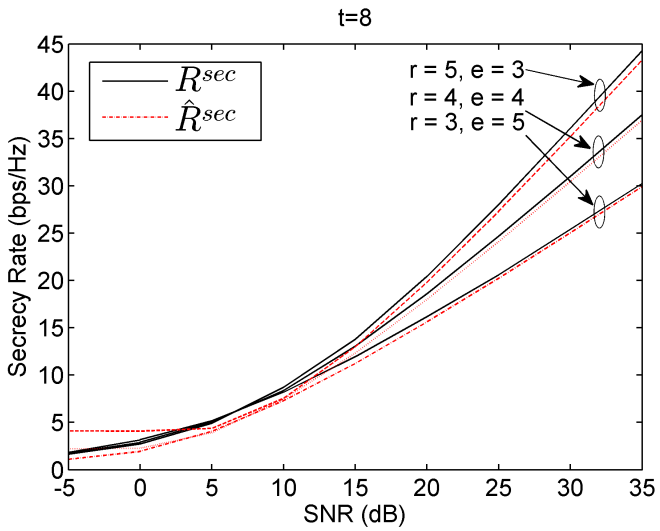


Fig. 2: Performance comparison of the large-scale AN secrecy rate approximation $\hat{R}^{sec}$ to ergodic secrecy rate $R^{sec}$.

and rates, AN is unlikely to be an efficient choice of secrecy methods. Note that, for SNRs of interest, the relative error for the case where $e > r$ is smaller than the $r > e$ case; this is due to the decrease in approximation error with decrease in allocated signal dimensions.

## VI. Conclusion

While an exact closed-form solution to the AN-generated secrecy rate is an intractable problem for the MIMOME channel with allowance for eigenmode partitioning, we have demonstrated that asymptotic approximations can be used effectively in place of ergodic Monte-Carlo simulation to accurately estimate the secrecy rate in an AN system with Tx-Rx antenna ratio over a wide range of SNR. In doing so, the computational complexity involved can be enormously reduced, potentially by many orders of magnitudes. This complexity reduction would allow for comparison of the specific implementation with secrecy capacity in complexity constrained or adaptive systems with some expected channel evolution.

## References

[1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *Information Theory, IEEE Transactions on*, vol. 24, no. 3, pp. 339 – 348, may 1978.

[3] J. Barros and M. Rodrigues, "Secrecy Capacity of Wireless Channels," in *Information Theory, 2006 IEEE International Symposium on*, july 2006, pp. 356 –360.

[4] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless Information-Theoretic Security," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2515 –2534, june 2008.

[5] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *Military Communications Conference, 2005. MILCOM 2005. IEEE*, oct. 2005, pp. 1501 –1506 Vol. 3.

[6] ——, "Guaranteeing Secrecy using Artificial Noise," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 6, pp. 2180 –2189, june 2008.

[7] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas i: The misome wiretap channel," *Information Theory, IEEE Transactions on*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[8] X. Zhou and M. McKay, "Secure Transmission With Artificial Noise Over Fading Channels: Achievable Rate and Optimal Power Allocation," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 8, pp. 3831 –3842, oct. 2010.

[9] H. Qin, X. Chen, Y. Sun, M. Zhao, and J. Wang, "Optimal Power Allocation for Joint Beamforming and Artificial Noise Design in Secure Wireless Communications," in *Communications Workshops (ICC), 2011 IEEE International Conference on*, 2011, pp. 1–5.

[10] X. Zhang, X. Zhou, and M. McKay, "On the Design of Artificial-Noise-Aided Secure Multi-Antenna Transmission in Slow Fading Channels," *Vehicular Technology, IEEE Transactions on*, vol. 62, no. 5, pp. 2170–2181, 2013.

[11] A. Mukherjee and A. Swindlehurst, "Utility of beamforming strategies for secrecy in multiuser MIMO wiretap channels," in *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*, 2009, pp. 1134–1141.

[12] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y. Hong, and C.-Y. Chi, "On the Impact of Quantized Channel Feedback in Guaranteeing Secrecy with Artificial Noise: The Noise Leakage Problem," *Wireless Communications, IEEE Transactions on*, vol. 10, no. 3, pp. 901–915, 2011.

[13] Y.-L. Liang, Y.-S. Wang, T.-H. Chang, Y.-W. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise," in *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, 2009, pp. 2351–2355.

[14] X. Yang and A. Swindlehurst, "On the use of artificial interference for secrecy with imperfect CSI," in *Signal Processing Advances in Wireless Communications (SPAWC), 2011 IEEE 12th International Workshop on*, 2011, pp. 476–480.

[15] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage Probability Based Power Distribution Between Data and Artificial Noise for Physical Layer Security," *Signal Processing Letters, IEEE*, vol. 19, no. 2, pp. 71–74, 2012.

[16] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On Secrecy Rate of the Generalized Artificial-Noise Assisted Secure Beamforming for Wiretap Channels," *Selected Areas in Communications, IEEE Journal on*, vol. 31, no. 9, pp. 1728–1740, 2013.

[17] A. Tulino and S. Verdu, *Random Matrix Theory and Wireless Communications*. now Publishers Inc., 2004.

[18] A. Lozano and A. Tulino, "Capacity of multiple-transmit multiple-receive antenna architectures," *Information Theory, IEEE Transactions on*, vol. 48, no. 12, pp. 3117–3128, 2002.

[19] A. Tulino, A. Lozano, and S. Verdu, "MIMO capacity with channel state information at the transmitter," in *Spread Spectrum Techniques and Applications, 2004 IEEE Eighth International Symposium on*, 2004, pp. 22–26.

[20] A. Goldsmith, S. Jafar, N. Jindal, and S. Vishwanath, "Capacity limits of MIMO channels," *Selected Areas in Communications, IEEE Journal on*, vol. 21, no. 5, pp. 684 – 702, june 2003.

[21] M. Bloch and J. ao Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[22] S. Shamai and S. Verdu, "The impact of frequency-flat fading on the spectral efficiency of CDMA," *Information Theory, IEEE Transactions on*, vol. 47, no. 4, pp. 1302–1327, 2001.

[23] D. Tse and S. Hanly, "Linear multiuser receivers: effective interference, effective bandwidth and user capacity," *Information Theory, IEEE Transactions on*, vol. 45, no. 2, pp. 641–657, 1999.

[24] S. Verdu, *Multiuser Detection*. Cambridge University Press, 1998.

[25] P. Rapajic and D. Popescu, "Information capacity of a random signature multiple-input multiple-output channel," *Communications, IEEE Transactions on*, vol. 48, no. 8, pp. 1245–1248, 2000.

[26] C. Moler. (2000) MATLAB Incorporates LAPACK@ONLINE. [Online]. Available: http://www.mathworks.com/company/newsletters/articles/matlab-incorporates-lapack.html