FIXED SINR SOLUTIONS FOR THE MIMO WIRETAP CHANNEL

A. Lee Swindlehurst

Dept. of Electrical Engineering & Computer Science
University of California, Irvine
Irvine, CA 92697
e-mail: swindle@uci.edu

ABSTRACT

This paper studies the use of artificial interference in reducing the likelihood that a message transmitted between two multi-antenna nodes is intercepted by an undetected eavesdropper. Unlike previous work that assumes some prior knowledge of the eavesdropper's channel and focuses on the information theoretic concept of secrecy capacity, we also consider the case where no information regarding the eavesdropper is present, and we use the relative signal-to-interference-plus-noise-ratio (SINR) of a single transmitted data stream as our performance metric. A portion of the transmit power is used to broadcast the information signal with just enough power to guarantee a certain SINR at the desired receiver, and the remainder of the power is used to broadcast artificial noise in order to mask the desired signal from a potential eavesdropper. The interference is designed to be orthogonal to the information signal when it reaches the desired receiver, and we study the resulting relative SINR of the desired receiver and the eavesdropper assuming both employ optimal beamformers.

Index Terms— MIMO wiretap channel, secrecy capacity, secure communications, interference alignment

1. INTRODUCTION

By their very nature, wireless communications are inherently insecure. A passive eavesdropper in an unknown location within "earshot" of a wireless transmission obtains information about the transmitted signal without risk of detection. While encryption can be used to ensure confidentiality, its computational cost may be prohibitive and there are difficulties and vulnerabilities associated with key distribution and management. Even when encryption is available, it is often still desirable to augment the security of the link and prevent its detection or interception. Early work on this problem, referred to as the *wiretap* channel, focused on determining what information-theoretic conditions were necessary for reliable secure communications in the presence of an eavesdropper [1–3]. In particular, this work led to the development of the notion of *secrecy capacity*, which quantifies the rate at which a transmitter can reliably send a secret message to the receiver, without the eavesdropper being able to decode it. Ultimately, it was shown that a non-zero secrecy capacity can only be obtained if the eavesdropper's channel is of lower quality than that of the intended recipient. The work cited above assumed single antenna nodes; secrecy capacity for the MIMO wiretap channel, where all nodes may possess multiple antennas, has been studied in [4, 5].

Based on the above observations, there has recently been considerable interest in the use of physical layer mechanisms to increase the security of wireless communications links through the use of artificial interference. The idea behind this work is to increase the interference seen by the eavesdropper in such a way that her channel is degraded while the channel of the receiver is not. For example, assuming that the transmitter has more antennas than the intended recipient so that the corresponding channel has a non-trivial nullspace, one of the approaches taken in [6] is to broadcast artificial interference using transmit beamformers in this nullspace. Such interference will have no impact on the receiver, but will in general degrade the eavesdropper's channel since its nullspace (if any) will be different. The high-SNR performance of this type of technique was studied in [7]. While [6] studied the case where only the distribution of the eavesdropper's channel was known, [7, 8] focused on the situation where the eavesdropper's instantaneous channel is known to the transmitter, and developed an algorithm to optimally exploit such information for the case where the intended recipient has a single antenna. A different but related approach can be found in [9], where the channel nullspace is exploited to design time-varying transmit beamformers that result in a constant channel to the receiver, but a random time-varying channel for the eavesdropper.

In this paper, we study the MIMO wiretap problem in which three multiple-antenna nodes are present: a transmitter (Alice), a receiver (Bob), and an eavesdropper (Eve). We assume that both Alice and Bob possess channel state infor-

This work was supported by the U.S. Army Research Office under the Multi-University Research Initiative (MURI) grant W911NF-07-1-0318.

mation (CSI) for their link, and that Alice may or may not have CSI for Eve. Instead of attempting to maximize the secrecy rate, which is not possible without knowledge of Eve's channel, we focus on using only enough power to guarantee a certain Quality of Service (QoS) for Bob measured in terms of signal-to-interference-plus-noise-ratio (SINR), and then use the remaining power to generate artificial interference to jam Eve. We assume that both Bob and Eve use optimal linear receivers (beamformers) to capture the signal, and compare the resulting SINR for each.

In the next section, the assumed mathematical model is presented. Our algorithm for allocating transmit antennas and power is described in Section 3, and the resulting relative SINR performance is studied via simulation in Section 4.

2. MATHEMATICAL MODEL AND ASSUMPTIONS

We assume a scenario with two cooperating nodes, Alice and Bob, and a passive eavesdropper, Eve. Each of the nodes may possess multiple antennas, the number of which we denote by N_a, N_b and N_e, respectively. Alice is attempting to communicate a message to Bob in the presence of Eve, who has access to Alice's transmissions. A fraction of Alice's power is devoted to the transmission of a noise-like waveform, in an attempt to degrade the ability of Eve to intercept the signal destined for Bob. Assuming a flat-fading scenario, the signals received by Bob and Eve can be represented as follows:

$$\mathbf{y}_b = \mathbf{H}_{ba}\mathbf{x}_a + \mathbf{n}_b \tag{1}$$
$$\mathbf{y}_e = \mathbf{H}_{ea}\mathbf{x}_a + \mathbf{n}_e \ , \tag{2}$$

where $\mathbf{x}_a$ is the signal vector transmitted by Alice, $\mathbf{n}_b, \mathbf{n}_e$ are the naturally occuring noise and interference received by Bob and Eve, respectively, and $\mathbf{H}_{ba}, \mathbf{H}_{ea}$ are the corresponding $N_b \times N_a, N_e \times N_a$ channel matrices. The background noise is assumed to be spatially white, with possibly different power levels:

$$\mathcal{E}\{\mathbf{n}_b\mathbf{n}_b^H\} = \sigma_b^2\mathbf{I}$$
$$\mathcal{E}\{\mathbf{n}_e\mathbf{n}_e^H\} = \sigma_e^2\mathbf{I} \ ,$$

where $\mathcal{E}\{\cdot\}$ denotes expectation, $(\cdot)^H$ the Hermitian transpose, and $\mathbf{I}$ is an identity matrix of appropriate dimension. The transmit power available for Alice is assumed to be bounded by P:

$$\mathcal{E}\{\mathbf{x}_a\mathbf{x}_a^H\} = \mathbf{Q}_a \qquad \mathrm{Tr}(\mathbf{Q}_a) \le P \ ,$$

where $\mathrm{Tr}(\cdot)$ denotes the trace operator. The channel matrices are assumed to be zero-mean, and without loss of generality we normalize $\mathbf{H}_{ba}$ so that its elements have unit-average variance (excess energy available from $\mathbf{H}_{ba}$ is lumped together with P):

$$\frac{\mathcal{E}\{\|\mathbf{H}_{ba}\|_F^2\}}{N_bN_a} = 1 \qquad \frac{\mathcal{E}\{\|\mathbf{H}_{ea}\|_F^2\}}{N_eN_a} = \gamma_{ea}^2$$

At this point, no other assumptions are made about the size or structure of the channel matrices.

As mentioned above, Alice's signal is split into two components, one that contains the secret message for Bob, a scalar data stream that we denote by z, and one that contains the jamming signal, which we denote by the $N_a \times 1$ vector $\mathbf{z}'$:

$$\mathbf{y}_b = \mathbf{H}_{ba}\mathbf{t}z + \mathbf{H}_{ba}\mathbf{z}' \ , \tag{3}$$

where $\mathbf{t}$ is the $N \times 1$ transmit beamformer used for the information signal. Similarly, Eve sees

$$\mathbf{y}_e = \mathbf{H}_{ea}\mathbf{t}z + \mathbf{H}_{ea}\mathbf{z}' \ . \tag{4}$$

Assume $\mathbf{t}^H\mathbf{t} = 1$ and let $\mathcal{E}\{|z|^2\} = \rho P$, where $0 < \rho \le 1$ is the fraction of the power devoted to the information signal, so that

$$\mathcal{E}\{\mathbf{z}'\mathbf{z}'^H\} = \mathbf{Q}'_z \qquad \mathrm{Tr}(\mathbf{Q}'_z) = (1-\rho)P \ .$$

We assume that both Bob and Eve use beamformers in an attempt to recover z. In particular, let $\mathbf{w}_b, \mathbf{w}_e$ respectively denote these $N_b \times 1, N_e \times 1$ beamformers, so that

$$\hat{z}_b = \mathbf{w}_b^H\mathbf{y}_b = \mathbf{w}_b^H\left(\mathbf{H}_{ba}\mathbf{t}z + \mathbf{H}_{ba}\mathbf{z}' + \mathbf{n}_b\right) \tag{5}$$
$$\hat{z}_e = \mathbf{w}_e^H\mathbf{y}_e = \mathbf{w}_e^H\left(\mathbf{H}_{ea}\mathbf{t}z + \mathbf{H}_{ea}\mathbf{z}' + \mathbf{n}_e\right) \ . \tag{6}$$

The resulting SINR available for Bob and Eve to decode z will be given by

$$\mathrm{SINR}_b = \frac{\rho P|\mathbf{w}_b^H\mathbf{H}_{ba}\mathbf{t}|^2}{\mathbf{w}_b^H\left(\mathbf{H}_{ba}\mathbf{Q}'_z\mathbf{H}_{ba}^H + \sigma_b^2\mathbf{I}\right)\mathbf{w}_b} \tag{7}$$

$$\mathrm{SINR}_e = \frac{\rho P|\mathbf{w}_e^H\mathbf{H}_{ea}\mathbf{t}|^2}{\mathbf{w}_e^H\left(\mathbf{H}_{ea}\mathbf{Q}'_z\mathbf{H}_{ea}^H + \sigma_e^2\mathbf{I}\right)\mathbf{w}_e} \ , \tag{8}$$

and the relative SINR is defined to be

$$\mathrm{RSINR} = \frac{\mathrm{SINR}_b}{\mathrm{SINR}_e} \ . \tag{9}$$

Roughly speaking, as long as RSINR > 1, there will exist modulation/coding schemes that allow Bob but not Eve to reliably decode z. In the next section, we discuss various algorithms for choosing N, ρ and $\mathbf{Q}'_z$ and the appropriate columns of $\mathbf{H}_{ba}$ to try and maximize RSINR.

3. FIXED SINR BEAMFORMING WITH INTERFERENCE ALIGNMENT

In many applications, it may be impractical to assume that any information about the eavesdropper's CSI is available, or even that an eavesdropper is present at all. If secure communications were desired in such cases, a reasonable approach would be to allocate only those resources necessary to obtain a certain guaranteed level of link quality for the intended receiver, and devote all other resources to making the unintended reception of the signal more difficult. Obviously, the

performance of such a scheme cannot be guaranteed; a well endowed eavesdropper in the right location could end up with a better quality signal. Here we rely on the goal of making the probability of such an event as low as possible.

The proposed approach can be generally outlined as follows:

1. Specify a target SINR for Bob.
2. Allocate a fraction ρ of the available transmit power to achieve the desired SINR (if possible) assuming Bob experiences no interference other than the background noise of power σ_b^2.
3. Distribute Alice's remaining power to yield as much interference as possible, while guaranteeing that when the interference is received by Bob, it lies in a subspace orthogonal to the desired signal.

This approach may not in general yield the best possible RSINR, since it may be possible to increase the RSINR by allowing some small amount of interference to leak into Bob's signal. However, the above approach is considerably simpler to implement. Obviously, a given $\mathbf{H}_{ba}$ may not support the desired SINR with a total transmit power P; in such cases, the link is assumed to be in outage. When the desired SINR is feasible, there will in general be many power allocation strategies that achieve it. As explained below, our approach will be to maximize the interference effect using the smallest possible power necessary to meet the SINR objective.

Let S denote the target SINR for Bob. To minimize the fraction of the transmit power required to achieve S, Alice should choose $\mathbf{t}$ to be the right singular vector of $\mathbf{H}_{ba}$ with largest singular value, and Bob should choose $\mathbf{w}_b = \mathbf{H}_{ba}\mathbf{t}$ as his receive beamformer. Using this approach, we have

$$\rho = \frac{\sigma_b^2 S}{\mathbf{t}^H \mathbf{H}_{ba}^H \mathbf{H}_{ba} \mathbf{t} P} = \frac{\sigma_b^2 S}{\sigma_1^2 P} , \tag{10}$$

where σ_1 is the largest singular value of $\mathbf{H}_{ba}$. As long as $\rho < 1$, we have power available for generating the artificial interference. We consider the cases of unknown and known $\mathbf{H}_{ea}$ in the sections below.

3.1. Unknown Eavesdropper CSI

In this case, the best option available to Alice is to uniformly spread the remaining transmit power along spatial dimensions that will produce no interference for Bob. We require that

$$\mathbf{H}_{ba}\mathbf{t} \perp \mathbf{H}_{ba}\mathbf{z}' \tag{11}$$

for all $\mathbf{z}'$. With $\mathbf{t}$ chosen as above, it is easy to see that $\mathbf{z}'$ must be chosen as a linear combination of the $N_a - 1$ right singular vectors of $\mathbf{H}_{ba}$ with smallest singular values, which we denote by $\mathbf{T}'$. Uniformly distributing the remaining transmit power over these vectors yields the following transmit covariance for the artificial interference:

$$\mathbf{Q}_z' = \frac{(1-\rho)P}{N_a - 1}\mathbf{T}'\mathbf{T}'^H . \tag{12}$$

3.2. Known Eavesdropper CSI

Obviously, the drawback of having no eavesdropper CSI is that some of the artificial noise will end up orthogonal to the desired signal at Eve, and thus will provide no interference effect. When $\mathbf{H}_{ea}$ is known, however, we can focus all of the available noise power so that it aligns as closely as possible to the spatial signature of the desired signal when received by Eve. Since this interference must still be orthogonal to Bob's signal, we require as above that $\mathbf{z}'$ be formed from the columns of $\mathbf{T}'$, or $\mathbf{z}' = \mathbf{T}'\mathbf{g}r$ for some $N_a - 1 \times 1$ vector $\mathbf{g}$ and some unit variance random variable r. To align the interference with the desired signal at Eve, we solve for $\mathbf{g}$ as follows:

$$\min_{\alpha,\mathbf{g}} \|\alpha \mathbf{H}_{ea}\mathbf{t} - \mathbf{H}_{ea}\mathbf{T}'\mathbf{g}\|^2 , \tag{13}$$

such that

$$\mathbf{g}^H \mathbf{T}'^H \mathbf{T}'\mathbf{g} = \mathbf{g}^H\mathbf{g} = (1-\rho)P , \tag{14}$$

and α is a scalar used to enforce the power constraint. The solution is given by

$$\mathbf{g} = \alpha(\mathbf{H}_{ea}\mathbf{T}')^\dagger \mathbf{H}_{ea}\mathbf{t} , \tag{15}$$

where $(\cdot)^\dagger$ is either the right pseudo-inverse (used when $N_a - 1 \geq \mathbf{N}_e$) or the left pseudo-inverse operator (used when $N_a - 1 < \mathbf{N}_e$), and α is chosen to guarantee the power constraint of (14). In this case, the covariance of the interference is a rank-one matrix:

$$\mathbf{Q}_z' = \mathbf{T}'\mathbf{g}\mathbf{g}^H\mathbf{T}'^H . \tag{16}$$

3.3. Maximum SINR Receive Beamforming

As indicated above, the optimal (in the maximum SINR sense) receive beamformer for Bob is simply the maximal ratio combiner, $\mathbf{w}_b = \mathbf{H}_{ba}\mathbf{t}$, since Bob experiences only white noise. For Eve, the maximum SINR beamformer is given by

$$\mathbf{w}_e = \left(\mathbf{H}_{ea}\mathbf{Q}_z'\mathbf{H}_{ea}^H + \sigma_e^2\mathbf{I}\right)^{-1}\mathbf{H}_{ea}\mathbf{t} , \tag{17}$$

where $\mathbf{Q}_z'$ is given by either (12) or (16), depending on whether Alice has CSI for Eve or not. The use of an optimal beamformer here presumes that Eve is somehow aware of $\mathbf{H}_{ea}\mathbf{t}$. With this choice for $\mathbf{w}_e$, the SINR experienced by Eve can be expressed as

$$\text{SINR}_e = \rho P \mathbf{t}^H \mathbf{H}_{ea}^H \left(\mathbf{H}_{ea}\mathbf{Q}_z'\mathbf{H}_{ea}^H + \sigma_e^2\mathbf{I}\right)^{-1}\mathbf{H}_{ea}\mathbf{t} . \tag{18}$$

4. SIMULATION RESULTS

We present some examples that show the eavesdropper's SINR for various array sizes and target performance levels. In all simulations, the channel matrices were assumed to be composed of independent, zero-mean Gaussian random variables with unit variance ($\gamma_{ea}^2 = 1$). All displayed results are calculated based on an average of 1000 independent trials. The background noise power was assumed to be the same for both Bob and Eve: $\sigma_b^2 = \sigma_e^2 = 1$, and in all cases the available transmit power was assumed to be $P = 100$, or 20dB. In situations where the desired SINR for Bob cannot be achieved with the given P, rather than indicate an outage, we simply assign all power to Bob and zero to artificial interference and average the resulting SINR with the others.

Figure 1 shows the resulting SINRs for Bob and Eve as a function of S, the desired SINR for Bob, for cases where everyone has the same number of antennas: $N_a = N_b = N_e = N = 3, 5, 10$. In this case, where the number of antennas is equal, knowledge of Eve's CSI is of relatively little value. For moderate values of S, Eve's SINR is significantly below that of Bob, from about 7dB when $N = 3$ to 14dB when $N = 10$. Bob's curve begins to flatten out for high desired SINR values when $N = 3$, since the specified SINR is not always feasible. Note that Bob will still continue to enjoy an SINR advantage over Eve when Eve and Bob share similar capabilities (number of antennas, background noise power, channel gains) even when no power is allocated to interference, since the transmit beamformer $\mathbf{t}$ is optimized for Bob and not for Eve.

Figure 2 illustrates the performance of the algorithm when $S = 20$dB and $N_e \in [1, 20]$. The number of antennas for Alice and Bob are assumed to be equal, and results are shown for $N_a = N_b = 3, 5, 10$. We see that knowledge of Eve's channel only provides a significant benefit when $N_e < \{N_a, N_b\}$. We also see that Eve can achieve a higher SINR than Bob when N_e is sufficiently large, although the assumed model of independent Rayleigh fading may be more difficult to justify in such situations.

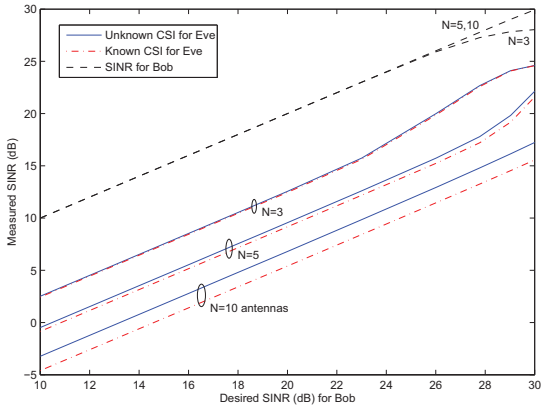

Fig. 1. SINR vs. desired rate for Bob.

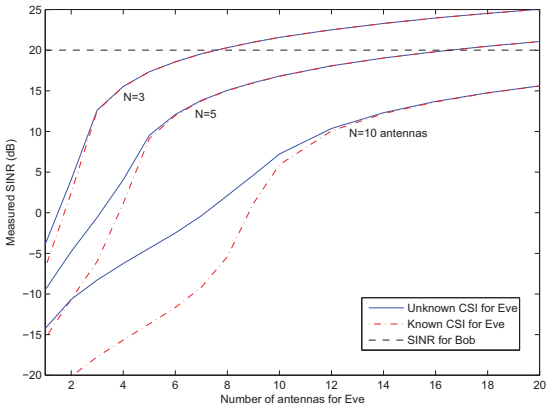

Fig. 2. SINR vs. number of antennas for Eve.

5. REFERENCES

[1] A. D. Wyner, "The Wiretap Channel," *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[2] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Info. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Info. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[4] A. Hero, "Secure space-time communication," *IEEE Trans. Info. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[5] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *IEEE Int'l Symp. on Info. Theory*, July 2008, pp. 524–528.

[6] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Info. Theory*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[7] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the gaussian MIMO wiretap channel," in *IEEE Int'l Symp. on Info. Theory*, June 2007, pp. 2471–2475.

[8] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *41st Conf. on Info. Sci. and Sys.*, Mar. 2007, pp. 905–910.

[9] X. Li, M. Chen, and E. P. Ratazzi, "Space-time transmissions for wireless secret-key agreement with information-theoretic secrecy," in *6th IEEE Worskhop on Sig. Proc. Adv. in Wireless Commun.*, June 2005, pp. 811–815.