Guaranteeing Secrecy using Artificial Noise

Satashu Goel, *Student Member, IEEE,* and Rohit Negi, *Member, IEEE*

***Abstract*—The broadcast nature of the wireless medium makes the communication over this medium vulnerable to eavesdropping. This paper considers the problem of secret communication between two nodes, over a fading wireless medium, in the presence of a passive eavesdropper. The assumption used is that the transmitter and its helpers (amplifying relays) have more antennas than the eavesdropper. The transmitter ensures secrecy of communication by utilizing some of the available power to produce 'artificial noise', such that only the eavesdropper's channel is degraded. Two scenarios are considered, one where the transmitter has multiple transmit antennas, and the other where amplifying relays simulate the effect of multiple antennas. The channel state information (CSI) is assumed to be publicly known, and hence, the secrecy of communication is independent of the secrecy of CSI.**

***Index Terms*—Privacy, secrecy capacity, wireless.**

I. Introduction

WIRELESS networks have gained much popularity because of the broadcast nature of the wireless medium, which makes it easily accessible. However, this ease of accessibility also makes it easy to overhear communication over this medium, thus raising privacy concerns. Secrecy problems involve three nodes; transmitter, receiver and an eavesdropper. We consider the problem of secret communication from the transmitter to the receiver, over a wireless medium, where a passive eavesdropper may be present. The transmitter wants to transmit a secret message to the intended receiver, such that the eavesdropper is unable to decode it. The eavesdropper is assumed to be passive and hence, its location, and even its presence will be uncertain to the transmitter. Any scheme that guarantees secrecy in such a scenario, must do so regardless of the eavesdropper's position.

Claude Shannon laid the theoretical foundation for the study of secret communication [1]. He showed that perfect secrecy is achievable only if the secret key is at least as large as the secret message. However, this pessimistic result was based on the assumption that the eavesdropper has access to precisely the same information as the receiver, except the secret key. Later, [2] considered a scenario where the receiver and the eavesdropper have separate channels, and showed that secret communication is possible if the eavesdropper's channel has a smaller capacity than the receiver's channel. The paper generalized the scenario considered in [3] where the eavesdropper's channel was a degraded version of the receiver's channel. The paper also defined the notion of 'secrecy capacity', which essentially is the maximum rate at which the transmitter can reliably communicate a secret message to the intended receiver, without the eavesdropper being able to decode it. However, if the eavesdropper happens to have a better channel than the receiver (e.g., if the eavesdropper is closer to the transmitter, versus the receiver), then the secrecy capacity is zero, meaning that secrecy cannot be guaranteed. This paper presents a solution to this problem, where the transmitter can use some of the available power to transmit artificially generated noise. Since, this noise is generated by the transmitter, the transmitter can design it such that only the eavesdropper's channel is degraded. Thus, by selectively degrading the eavesdropper's channel, secret communication can be guaranteed, based on the result in [2].

Two schemes for generating artificial noise were presented in [5]. In the first scheme, the transmitter can use multiple transmit antennas to generate 'artificial noise'. This scenario was chosen because the artificial noise scheme can be presented in a simple manner, in this case. This scenario models a base station wanting to communicate a secret message to a mobile handset. In the second scheme, it was shown that even if the transmitter does not have multiple transmit antennas but 'amplifying relays' [20] (or 'helper nodes') are present, the effect of multiple antennas can be simulated and artificial noise can still be produced. This scenario models a mobile handset, with a single antenna, wanting to communicate a secret message to another mobile handset or the base station. The multiple antenna scheme was further analyzed in [6]. The paper explored the notion of 'MIMO secrecy capacity' and showed that it behaves differently from MIMO capacity, showing that the secrecy requirement changes the behavior of MIMO capacity. For example, the paper showed that secrecy capacity does not increase monotonically with the minimum of the number of transmit and receive antennas, unlike the celebrated result on usual MIMO capacity [7]. Thus, the paper highlighted the need to characterize MIMO secrecy capacity. The paper further showed that with the use of artificial noise, a certain minimum rate of secret transmission can be guaranteed, regardless of the eavesdropper's position. In this paper, we present results on the minimum secrecy capacity, that can be guaranteed regardless of the eavesdropper's position, called *minimum guaranteed secrecy capacity*, assuming a fading channel model. This requires a modification of the schemes analyzed in [5] and [6] to guarantee non-zero secrecy capacity.

Note that the result in [2], and consequently, this paper, considers information theoretic secrecy which is provably secure, as opposed to classical symmetric encryption schemes [4].

Manuscript received October 18, 2006; revised May 4, 2007, October 23, 2007, and April 20, 2008; accepted March 19, 2008. The associate editor coordinating the review of this paper and approving it for publication was A. Gulliver. This work was supported in part by Cylab, CMU under grant DAAD19-02-1-0389 from the Army Research Office. Part of the results in this paper have been presented in VTC Fall '05 and MILCOM '05.

S. Goel is pursuing his Ph.D. at the Department of Electrical and Computer Engineering, Carnegie Mellon University (e-mail: satashug@ece.cmu.edu).

R. Negi is an Associate Professor at the Department of Electrical and Computer Engineering, Carnegie Mellon University (e-mail: negi@ece.cmu.edu).

Digital Object Identifier 10.1109/TWC.2008.060848.

1536-1276/08$25.00 © 2008 IEEE

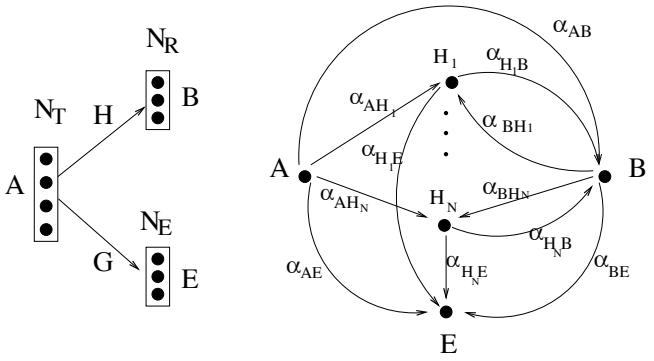
Information theoretic secrecy does not assume that a secure key exchange has occurred between the transmitter and the receiver, as is assumed in the classical symmetric encryption schemes. On the other hand, the secrecy rates guaranteed by the information theoretic results might be substantially smaller than those achievable through symmetric encryption schemes. Thus, information theoretic schemes can be used in conjunction with the classical schemes, by generating keys which can then be used to perform symmetric encryption. However, practical codes are not known which can achieve the rates guaranteed by information theoretic results on secrecy.

In related work, [8] presented a technique for introducing ambiguity in the eavesdropper's channel, using multiple transmit antennas. However, secrecy capacity obtained using this scheme was not analyzed. [9] described a technique for secret communication where the channel state information (CSI) was used as the secret key. In particular, the phase information was used as a secret key and the transmitter compensated for the phase before transmission. The phase of the eavesdropper's channel, being different from that of the receiver's channel, in general, prevented the eavesdropper from decoding the secret message. [10] generalized this technique for the multi-antenna scenario. [11] obtained an abstract characterization of secrecy capacity of the kind discussed in [9]. In contrast, this paper assumes that the CSI is publicly known, and thus, it cannot be used to obtain a secret key. The secrecy of the schemes discussed in this paper is independent of the secrecy of CSI. However, here we make the (admittedly strong) assumption that the number of eavesdropper antennas is strictly smaller than the number of transmitter (along with amplifying relays) antennas. This assumption may be valid in certain scenarios, such as a powerful base station deploying several antennas, serving as a transmitter. [12] presented an analytical solution for the multi-antenna scenario, assuming that the eavesdropper's channel is known to the transmitter. [13] analyzed secrecy capacity for slow fading wireless channels, but without the use of artificial noise. This paper shows that much lower outage probabilities can be guaranteed using artificial noise.

The paper is organized as follows. Section II formulates the secrecy problem considered in this paper. It introduces the two scenarios considered here, one with multiple antennas at the transmitter, and the other with amplifying relays. Section III introduces the scheme for artificial noise generation, using multiple transmit antennas. This section assumes that both the receiver and the eavesdropper have a single antenna each. Section IV presents the scheme for artificial noise generation, when all the nodes have a single antenna each. This section shows how the effect of multiple transmit antennas can be reproduced with the help of amplifying relays. Section V characterizes the behavior of MIMO secrecy capacity. It also presents analytic results in the regime of large number of antennas. Section VI presents simulation results and their discussion. Section VII concludes the paper.

II. Problem Scenario

We denote vectors and matrices with bold font, and the Hermitian operator by †. For convenience, we measure information in nats instead of bits (i.e., $\log_e(\cdot)$ is used to calculate entropy). We consider two scenarios, which demonstrate different methods of generating artificial noise. In the multiple amplifying relays scenario, we assume that transmissions of all nodes are synchronized (which is clearly an idealistic assumption). The key idea in this paper is that a transmitter, perhaps in cooperation with the amplifying relays, can generate noise artificially to conceal the secret message that it is transmitting. i.e., the transmitter can use some of the available power to transmit artificially generated noise, to selectively degrade eavesdropper's channel.



(a) Scenario 1 (b) Scenario 2

Fig. 1. Framework for secrecy capacity.

A. Multiple Antennas: Scenario 1

Scenario 1 in Fig. 1 shows transmitter A with N_T antennas, receiver B with N_R antennas and an eavesdropper E with N_E antennas. An eavesdropper with multiple antennas is an abstraction of the case where, a) either the eavesdropper has multiple receive antennas or b) several eavesdroppers (with perhaps one antenna each) collude. The latter case of collusion can be modeled as a single eavesdropper with multiple antennas, if we assume that their received signals can be processed by a central node. Clearly, this form of collusion represents the worst case scenario in terms of secrecy capacity, given a fixed number of colluding eavesdroppers. $\mathbf{H}_k$ and $\mathbf{G}_k$ denote the channels of the receiver and the eavesdropper respectively, at time k. The elements of $\mathbf{H}_k$ ($\mathbf{G}_k$), denoted by $h_{i,j}$ ($g_{i,j}$), is the channel gains from transmit antenna i to receive (eavesdropper) antenna j. A transmits $\mathbf{x}_k$ at time k. B and E receive, respectively,

$$\mathbf{z}_k = \mathbf{H}_k\mathbf{x}_k + \mathbf{n}_k, \quad (1)$$

$$\mathbf{y}_k = \mathbf{G}_k\mathbf{x}_k + \mathbf{e}_k, \quad (2)$$

where the components of $\mathbf{n}_k$ and $\mathbf{e}_k$ are i.i.d. Additive White Gaussian Noise (AWGN) samples with variance σ_n^2 and σ_e^2, respectively. Block fading is assumed, meaning that $\mathbf{H}_k$ and $\mathbf{G}_k$ are constant over a block of large number of symbols so that information theoretic results can be applied within each block and $\mathbf{H}_k$, $\mathbf{G}_k$ in different blocks are independent. Encoding and decoding is performed independently for each fading block. A more general fading channel could be used, but the resulting analysis will be much more complicated [21]. $h_{i,j}$ and $g_{i,j}$ are assumed to be complex numbers, i.i.d. and independent of each other. This would occur under 'rich

scattering' [14]. It is assumed that the receiver is able to estimate its channel $\mathbf{H}_k$ perfectly and feed it back to the transmitter noiselessly. We assume that $\mathbf{H}_k$ is communicated to the transmitter by an authenticated broadcast (which may be heard by the eavesdropper). Thus, it is assumed that the eavesdropper may know both the receiver's and its own channel. A passive eavesdropper is assumed, which means that it only listens but does not transmit. Hence, its channel $\mathbf{G}_k$ may not be known to the transmitter. Note that *the secrecy of this scheme is not dependent on the secrecy of channel gains.*

The transmitter is assumed to have a power constraint of P_0, i.e., $\mathbf{E}[\mathbf{x}_k^\dagger \mathbf{x}_k] \leq P_0$. Let the secret message $m^K \doteq (m_1, \ldots, m_K)$ be encoded into $\mathbf{x}^N$. $\mathbf{z}^N$ and $\mathbf{y}^N$ are then obtained following (1), (2). The rate of transmission between the transmitter and the receiver is $R = H(m^K)/N$. The secrecy condition is defined in terms of equivocation rate, defined as $R_e \doteq \frac{1}{K} H(m^K|\mathbf{y}^N)$. Perfect secrecy is achieved (as defined in [2]) if $R_e = R$. Note that this secrecy condition restricts the rate at which the eavesdropper can obtain the secret information. A stricter secrecy condition can be used which restricts the total amount of secret information obtained by the eavesdropper, using the techniques introduced in [19].

B. Multiple Amplifying Relays: Scenario 2

In the previous scenario, the transmitter could utilize its multiple transmit antennas for secret transmission. This scenario considers the case where the transmitter does not have multiple transmit antennas, but instead, has amplifying relays for cooperation. Henceforth, in this paper, we will refer to them as *relays*. Scenario 2 in Fig. 1 shows transmitter A, intended receiver B and an eavesdropper E with only a single antenna each. But several relays $(H_1, H_2, \ldots, H_N)$ exist to aid secret communication from A to B. The multiple relays must simulate the effect of having multiple transmit antennas. However, unlike Scenario 1, the transmitter cannot directly control the signal transmitted by the relays. The channel gain from X to Y is denoted α_{XY}, which models a fading channel. Note that the channels are not necessarily reciprocal, i.e., in general $\alpha_{XY} \neq \alpha_{YX}$. A frequency flat block fading channel model is assumed, similar to (1), (2). The transmission of secret information from the transmitter to the receiver occurs in two stages which will be discussed in detail in a later section. It is assumed that all the channel gains are known to all the nodes (possibly, even to the eavesdropper). Again, the secrecy of our communication scheme does not depend on the secrecy of channel gains. We assume that the total power transmitted by all the nodes for both the stages (including nodes A, B and the relays), is constrained to P_0.

III. Artificial Noise Using Transmit Antennas

In this section, we consider Scenario 1. This section assumes that both the receiver and the eavesdropper have a single antenna each, and that multiple eavesdroppers cannot collude (i.e., $N_R = N_E = 1$). An example of such a scenario is a wireless LAN, with the base station as the transmitter. The concept of artificial noise can be clearly illustrated in this scenario. The artificial noise is produced such that it lies in the null space of the receiver's channel, while the information signal is transmitted in the range space of the receiver's channel. This design relies on knowledge of the receiver's channel, but not of the eavesdropper's channel. The receiver's channel nulls out the artificial noise, and hence, the receiver is not affected by the noise. However, in general, the eavesdropper's channel will be degraded, since its range space will be different from that of the receiver's channel, and hence, some component of artificial noise will lie in its range space.

We now describe how the transmitter can generate artificial noise to degrade the eavesdropper's channel. The transmitter chooses $\mathbf{x}_k$ as the sum of information bearing signal $\mathbf{s}_k$ and the artificial noise signal $\mathbf{w}_k$,

$$\mathbf{x}_k = \mathbf{s}_k + \mathbf{w}_k. \tag{3}$$

Both $\mathbf{s}_k$ and $\mathbf{w}_k$ are assumed complex Gaussian vectors. $\mathbf{w}_k$ is chosen to lie in the null space of $\mathbf{H}_k$, such that $\mathbf{H}_k \mathbf{w}_k = \mathbf{0}$. If $\mathbf{Z}_k$ is an orthonormal basis for the null space of $\mathbf{H}_k$, then $\mathbf{w}_k = \mathbf{Z}_k \mathbf{v}_k$, and $\mathbf{Z}_k^\dagger \mathbf{Z}_k = I$. Then, the signals received by the receiver and the eavesdropper are given by, respectively,

$$z_k = \mathbf{H}_k \mathbf{s}_k + n_k, \tag{4}$$

$$y_k = \mathbf{G}_k \mathbf{s}_k + \mathbf{G}_k \mathbf{w}_k + e_k. \tag{5}$$

Note how the artificial noise $\mathbf{w}_k$ is nulled out by the receiver's channel but not necessarily by the eavesdropper's channel. Thus, the eavesdropper's channel is degraded with high probability, while that of the receiver remains unaffected. If $\mathbf{w}_k$ was chosen fixed, the artificial noise seen by the eavesdropper would be small if $\|\mathbf{G}_k \mathbf{w}_k\|$ is small. To avoid this possibility, the sequence of $\mathbf{w}_k$ is chosen to be complex Gaussian random vectors in the null space of $\mathbf{H}_k$. In particular, the transmitter chooses elements of $\mathbf{v}_k$ to be i.i.d. complex Gaussian *random* variables with variance σ_v^2, and independent in time as well. It follows that the elements of $\mathbf{w}_k$ are also Gaussian distributed.

Since $\mathbf{H}_k$ is a vector channel, the transmitter chooses the information bearing signal as $\mathbf{s}_k = \mathbf{p}_k u_k$, where u_k is the information signal. We assume that Gaussian codes are used. $\mathbf{p}_k$ is chosen such that $\mathbf{H}_k \mathbf{p}_k \neq 0$ and $\|\mathbf{p}_k\| = 1$. Now, secrecy capacity is bounded below by the difference in mutual information between the transmitter and the receiver versus the transmitter and the eavesdropper [2], [15],

$$\text{Secrecy Capacity} \geq C_{sec}^a = I(Z;U) - I(Y;U) \tag{6}$$

$$= \log(1 + \frac{|\mathbf{H}_k \mathbf{p}_k|^2 \sigma_u^2}{\sigma_n^2}) - \log(1 + \frac{|\mathbf{G}_k \mathbf{p}_k|^2 \sigma_u^2}{\mathbf{E}|\mathbf{G}_k \mathbf{w}_k|^2 + \sigma_e^2}), \tag{7}$$

where $\mathbf{E}|\mathbf{G}_k \mathbf{w}_k|^2 = (\mathbf{G}_k \mathbf{Z}_k \mathbf{Z}_k^\dagger \mathbf{G}_k^\dagger)\sigma_v^2$. For a passive eavesdropper, $\mathbf{G}_k$ is not known to the transmitter, so using the concavity of $\log(\cdot)$ and the i.i.d. assumption of $\mathbf{H}_k$, the average secrecy capacity is maximized by choosing $\mathbf{p}_k = \mathbf{H}_k^\dagger / \|\mathbf{H}_k\|$. Thus, the information bearing signal $\mathbf{s}_k$ lies in the range space of $\mathbf{H}_k^\dagger$ whereas the artificial noise lies in the null space of $\mathbf{H}_k^\dagger$.

C_{sec}^a is a random variable because it is a function of random channel gains $\mathbf{H}_k$ and $\mathbf{G}_k$. Therefore, we study average secrecy capacity and outage probability (or outage capacity). We assume that the total transmit power, given by $f_1(\sigma_u^2, \sigma_v^2) = \mathbf{E}[\mathbf{x}_k^\dagger \mathbf{x}_k] \leq P_0 = \sigma_u^2 + (N_T - 1)\sigma_v^2$, is constrained to P_0. Now, σ_u^2, σ_v^2 can be chosen to maximize the lower bound on average secrecy capacity,

$$\overline{C_{sec}^a} \doteq \max_{f_1(\sigma_u^2, \sigma_v^2) \leq P_0} \mathop{\mathbf{E}}_{\mathbf{H}_k, \mathbf{G}_k} [C_{sec}^a]. \tag{8}$$

Note that the definition of $\overline{C^a_{sec}}$ involves both the expectation over $\mathbf{H}_k$, $\mathbf{G}_k$, and optimization over σ_u^2, σ_v^2. Similar notation will be used in the later sections to denote maximum average secrecy capacity. We now study the variation of $\overline{C^a_{sec}}$ with the eavesdropper's distance from the transmitter. For simplification, (5) is normalized by a factor of $\|\mathbf{G}_k\|$. Thus, the distance can be modeled as position dependent noise power σ_e^2, instead of position dependent channel gains. The worst case situation would occur if $\sigma_e^2 \rightarrow 0$ (e.g., when the eavesdropper is much closer to the transmitter, compared to the receiver). The minimum secrecy capacity that can be guaranteed, irrespective of the eavesdropper's position is given by,

$$\overline{C^a_{sec}} \geq \overline{C^a_{sec,mg}} \doteq \max_{f_1(\sigma_u^2,\sigma_v^2)\leq P_0} \mathop{\mathbf{E}}_{\mathbf{H}_k,\mathbf{G}_k} [\log(1+\frac{\|\mathbf{H}_k\|^2\sigma_u^2}{\sigma_n^2}) - \log(1+\frac{|\mathbf{G}_k\mathbf{p}_k|^2\sigma_u^2}{(\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger)\sigma_v^2})]. \quad (9)$$

Note that the average minimum guaranteed secrecy capacity can be positive, even as $\sigma_e^2 \rightarrow 0$, unlike the case where artificial noise is not used (i.e., if only the information bearing signal is transmitted). To see this, consider a specific choice for signal and artificial noise powers, $\sigma_u^2 = \theta P_0$ and $\sigma_v^2 = (1-\theta)P_0/(N_T-1)$, for some fixed θ. Now, the second term in (9) is a constant, while the first term tends to infinity, as $P_0 \rightarrow \infty$. Thus, $\overline{C^a_{sec,mg}} \rightarrow \infty$, as $P_0 \rightarrow \infty$ which shows that $\overline{C^a_{sec,mg}}$ is non-zero for large enough P_0. Further, as $\sigma_e^2 \rightarrow \infty$ (e.g., when the eavesdropper is much farther from the transmitter, than is the receiver), the second term in (8) goes to zero, for any choice of σ_u^2, σ_v^2. Now, $\overline{C^a_{sec}}$ can be maximized by choosing $\sigma_u^2 = P_0$, hence obtaining average capacity as the average minimum guaranteed secrecy capacity. Fig. 4 shows that $\overline{C^a_{sec}}$ achieves capacity when $\sigma_e^2 \rightarrow \infty$, while $\overline{C^a_{sec}}$ achieves a non-zero $\overline{C^a_{sec,mg}}$ when $\sigma_e^2 \rightarrow 0$.

IV. Artificial noise using relays

In Section III, we saw that multiple antennas at the transmitter can be used to produce artificial noise. We now consider the case when the transmitter has only a single antenna. The method used in the previous section can no longer be used here. However, we assume that several relays are present to aid the secret transmission of information. Coordination with the relays can, hopefully, simulate the effect of multiple antennas in producing artificial noise. However, as opposed to the case of multiple transmit antennas, the relays are not in direct control of the transmitter. How can they then coordinate in transmitting the artificial noise (which, by definition, is random and cannot be known to the relays)? We now describe a novel 2-stage protocol that achieves this coordination. In the first stage, the transmitter and the receiver both transmit independent artificial noise signals to the relays. The relays and the eavesdropper receive different linear combinations of these two signals. In the second stage, the relays simply replay a weighted version of the received signal, using a publicly available sequence of weights (i.e., weights that may also be known to the eavesdropper). At the same time, in this second stage, the transmitter transmits its secret message, along with a weighted version of its artificial noise, which was transmitted in the first stage. The weighted version is generated such that the artificial noise component due to the transmitter is canceled at the receiver. The artificial noise component due to the receiver is known to the receiver, and can be canceled off by the receiver. The two stages are now described in detail. In this section, the subscript for time, k will be suppressed for ease of presentation. Note that the information theoretic results used in this section hold, when a sequence of received samples is considered.

Stage 1: A and B transmit $\alpha_{AB}\ x$ and y respectively. H_i and E receive, respectively,

$$r_{H_i} = \alpha_{AH_i}\ \alpha_{AB}\ x + \alpha_{BH_i}\ y + n_i \quad (10)$$

$$r_{E,1} = \alpha_{AE}\ \alpha_{AB}\ x + \alpha_{BE}\ y + e_1 \quad (11)$$

Stage 2: A and H_i transmit $-\sum_i \beta_i\ \alpha_{AH_i}\ \alpha_{H_iB}\ x + z$ and $\beta_i\ r_{H_i}$ respectively. B and E receive,

$$r_B = \alpha_{AB}\ z + \sum_i \beta_i\ \alpha_{H_iB}(\alpha_{BH_i}\ \ y + n_i) + n_0 \quad (12)$$

$$r_{E,2} = \alpha_{AE}\ z + \sum_i \beta_i\ \alpha_{AH_i}[\alpha_{AB}\ \alpha_{H_iE} - \alpha_{AE}\alpha_{H_iB}]\ x + \sum_i \beta_i\alpha_{BH_i}\ \alpha_{H_iE}\ y + \sum_i \beta_i\ \alpha_{H_iE}\ n_i + e_2. \quad (13)$$

Here, $\{e_i\}_{i=1}^2$, $\{n_i\}_{i=0}^N$ are AWGN noise samples of variance σ_e^2 and σ_n^2 respectively. (11) and (13) are normalized so that $\mathbf{E}[|\alpha_{AE}|^2] = 1$. This allows us to model the transmitter-eavesdropper distance through σ_e^2. β_i are (publicly known) i.i.d. complex Gaussian random weights used by the relays. z is the Gaussian information bearing signal which must be communicated by A to B, while x and y are transmitted to conceal the transmission of z. Note that y is known to the receiver, and hence, the receiver can easily cancel it off. Thus, the equivalent channel from A to B is given by

$$\tilde{r}_B = \alpha_{AB} z + n_B, \quad (14)$$

where $n_B = \sum_{i=1}^{N_H} \beta_i\alpha_{H_iB}n_i + n_0$. Note how A's transmission of $-\sum_{i=1}^{N_H} \beta_i\alpha_{AH_i}\alpha_{H_iB}x$ cancels out the transmission of the relays precisely, only at the intended receiver, but not at the eavesdropper, thus causing artificial noise in the latter. Thus, the coordination with the relays enabled the transmitter to generate artificial noise, such that it degrades only the eavesdropper's channel. Varying the β_i performs the same function as varying $\mathbf{w}_k$ in Scenario 1, and thus, reduces the probability of the artificial noise being nulled at the eavesdropper. The channel from A to E can be written as,

$$\mathbf{r}_E = \mathbf{h}_z z + \mathbf{H}_{xy}\begin{pmatrix} x \\ y \end{pmatrix} + \mathbf{n}, \quad (15)$$

$$\mathbf{h}_z = \begin{pmatrix} 0 \\ \alpha_{AE} \end{pmatrix}, \mathbf{n} = \begin{pmatrix} e_1 \\ \sum_{i=1}^{N_H} \beta_i\ \alpha_{H_iE}\ n_i + e_2 \end{pmatrix}, \quad (16)$$

$$\mathbf{H}_{xy} = \begin{pmatrix} \alpha_{AB}\ \alpha_{AE} & \alpha_{BE} \\ \gamma & \sum_{i=1}^{N_H} \beta_i\alpha_{BH_i}\ \alpha_{H_iE} \end{pmatrix}, \quad (17)$$

where $\gamma = \alpha_{AB} \sum_{i=1}^{N_H} \beta_i\ \alpha_{AH_i}\ \alpha_{H_iE} - \alpha_{AE} \sum_{i=1}^{N_H} \beta_i\alpha_{AH_i}\alpha_{H_iB}$. Note that (14), (15) are similar to the ones obtained for the multiple antenna scenario (4), (5). Eq. (15) represents a Single Input Multiple Output (SIMO) channel which is degraded by both AWGN and interference,

and its capacity is given by [16],

$$C = \log|\mathbf{h}_z\mathbf{h}_z^\dagger\sigma_z^2 + \mathbf{K}| - \log|\mathbf{K}|, \quad (18)$$

$$\mathbf{K} = \begin{pmatrix} |h_{11}|^2\sigma_x^2 + |h_{12}|^2\sigma_y^2 + \sigma_e^2 & 0 \\ 0 & \eta \end{pmatrix}, \quad (19)$$

where h_{11}, h_{12}, h_{21}, h_{22} are the elements of $\mathbf{H}_{xy}$, and $\eta = |h_{21}|^2\sigma_x^2 + |h_{22}|^2\sigma_y^2 + \sum_{i=1}^{N_H}(|\alpha_{H_iE}|^2\sigma_{\beta_i}^2)\sigma_n^2 + \sigma_e^2$. Note that the off-diagonal elements of $\mathbf{K}$ are zero, because β_i's are assumed complex Gaussian. Thus, the lower bound on secrecy capacity is given by,

$$C_{sec}^h = I(Z;\tilde{R}_B) - I(Z;R_{E,1},R_{E,2}) \quad (20)$$

$$= \log(1 + |\alpha_{AB}|^2\sigma_z^2/\sigma_{n_B}^2) - \log|\mathbf{h}_z\mathbf{h}_z^\dagger\sigma_z^2 + \mathbf{K}|/|\mathbf{K}|, \quad (21)$$

where $\sigma_{n_B}^2 = \sum_{i=1}^{N_H}(|\alpha_{H_iB}|^2\sigma_{\beta_i}^2)\sigma_n^2 + \sigma_e^2$. Note the similarity in expressions in (7) and (20).

C_{sec}^h is a random variable because it is a function of random channel gains. The (average) total power, transmitted by all nodes, in the two stages, is given by $f_2(\sigma_x^2,\sigma_y^2,\sigma_z^2,\xi) = (2N_H\xi + 1)\sigma_x^2 + (N_H\xi + 1)\sigma_y^2 + \sigma_z^2 + N_H\xi\sigma_n^2$, where we choose $\sigma_{\beta_i}^2 = \xi \quad \forall i$ for simplicity. Further, it is assumed that $\mathbf{E}[|\alpha_{XY}|^2] = 1$. The combination of powers $(\sigma_x^2,\sigma_y^2,\sigma_z^2,\xi)$ is chosen to maximize the average C_{sec}^h and hence,

$$\overline{C_{sec}^h} \doteq \max_{f_2(\sigma_x^2,\sigma_y^2,\sigma_z^2,\xi)\le P_0} \mathbf{E}[\log(1 + |\alpha_{AB}|^2\sigma_z^2/\sigma_{n_B}^2) - \log|\mathbf{h}_z\mathbf{h}_z^\dagger\sigma_z^2 + \mathbf{K}|/|\mathbf{K}|], \quad (22)$$

where the expectation is over all the channel gains. Note that the *total* transmit power (including transmit power of relays) is constrained to P_0.

Again, secrecy capacity depends on the AWGN power seen by the eavesdropper σ_e^2. The average minimum guaranteed secrecy capacity, $\overline{C_{sec,mg}^h}$ can be obtained by putting $\sigma_e^2 = 0$. It is clear that by choosing the specific values, $\sigma_z^2 = \theta_0 P_0$, $\sigma_x^2 = \theta_1 P_0$, $\sigma_y^2 = \theta_2 P_0$ (where θ_0, θ_1, $\theta_2 > 0$ and satisfy the power constraint), putting $\sigma_e^2 = 0$, and letting $P_0 \to \infty$, the second term in (22) is a constant, while the first term goes to infinity. Therefore, $\overline{C_{sec,mg}^h} \to \infty$, as $P_0 \to \infty$. Further, as $\sigma_e^2 \to \infty$, the second term in (22) goes to zero. In that case, the first term can be maximized by choosing $\sigma_{\beta_i}^2 = 0$ and setting $\sigma_z^2 = P_0$, thus achieving average capacity of the transmitter-receiver link as the average minimum guaranteed secrecy capacity. Fig. 5 shows that $\overline{C_{sec}^h}$ achieves the usual Shannon capacity when $\sigma_e^2 \to \infty$, while $\overline{C_{sec}^h}$ achieves a non-zero $\overline{C_{sec,mg}^h}$ when $\sigma_e^2 \to 0$.

V. Artificial Noise in MIMO Scenario

In the previous two sections, we presented methods for artificial noise generation, both using multiple transmit antennas and relays, assuming a single-antenna eavesdropper. It was shown that in both the scenarios, some minimum secrecy capacity can be guaranteed, using artificial noise, so long as the transmitter, along with relays, has more than one antenna. We now consider an extension of the multiple antenna scenario where all the nodes, including the eavesdropper, can have multiple antennas. In recent years, several results have characterized the capacity of such Multiple Input Multiple Output (MIMO) communication systems, showing a linear increase in capacity with the minimum of the number of transmit and receive antennas [7]. In this section, we characterize the *minimum guaranteed* 'MIMO secrecy capacity', and show that it does not necessarily grow linearly with the minimum of the number of transmit and receive antennas, and thus behaves differently from the usual MIMO capacity.

Consider the case where $N_R = N_E$, i.e., both the receiver and the eavesdropper have similar capabilities. An increase in the number of receive antennas affects two aspects of secrecy capacity; the ability to utilize 'parallel channels' and the ability to produce artificial noise. Intuitively, the more the number of receive antennas, more the number of parallel channels that can be created between the transmitter and the receiver, leading to capacity gain. On the other hand, more receive antennas (and thus, more eavesdropper antennas) requires artificial noise to be produced in more dimensions, thus limiting the number of dimensions available for information transmission. These two opposing effects suggest that the effect of increasing $N_R(= N_E)$ on MIMO secrecy capacity is not obvious. [6] investigated the notion of MIMO secrecy capacity and showed that its behavior differs from that of capacity. However, [6] considered the case when the eavesdropper's channel is degraded with AWGN. We now consider the worst case scenario, where the eavesdropper's channel has no AWGN, and hence characterize the minimum guaranteed secrecy capacity. The transmission strategy needs to be modified compared to [6], in order to obtain non-zero secrecy capacity.

A. Artificial Noise Generation in MIMO Scenario

Equations (1), (2) hold in this case, except that we have matrix channels $\mathbf{H}_k$ and $\mathbf{G}_k$. The elements of noise vectors, $\mathbf{n}_k$ and $\mathbf{e}_k$ are i.i.d. AWGN samples. The transmitter transmits $\mathbf{x}_k$ as in (3), where $\mathbf{H}_k\mathbf{w}_k = \mathbf{0}$, so that $\mathbf{w}_k = \mathbf{Z}_k\mathbf{v}_k$. However, in this case we choose $\mathbf{Z}_k$ to be a *subset* of an orthonormal basis of the null space of $\mathbf{H}_k$. The receiver and the eavesdropper receive vector signals $\mathbf{z}_k$ and $\mathbf{y}_k$, respectively. Based on (5), the eavesdropper E observes colored Gaussian noise with covariance $\mathbf{K} = (\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger)\sigma_v^2 + \mathbf{I}\sigma_e^2$. Now, the lower bound on secrecy capacity is given by [2], [15],

$$C_{sec}^a = I(\mathbf{Z};\mathbf{S}) - I(\mathbf{Y};\mathbf{S}) \quad (23)$$

$$= \log|\mathbf{I}\sigma_n^2 + \mathbf{H}_k\mathbf{Q}_\mathbf{s}\mathbf{H}_k^\dagger| - \log\Big(|\mathbf{K} + \mathbf{G}_k\mathbf{Q}_\mathbf{s}\mathbf{G}_k^\dagger|/|\mathbf{K}|\Big), \quad (24)$$

where $\mathbf{Q}_\mathbf{s} = \mathbf{E}[\mathbf{s}_k\mathbf{s}_k^\dagger]$ and $\mathbf{s}_k$ is complex Gaussian distributed. The minimum guaranteed secrecy capacity can be obtained by substituting $\mathbf{K}$ with $\mathbf{K}'$ in (23), where $\mathbf{K}' = (\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger)\sigma_v^2$. We immediately note that in order to avoid the case $|\mathbf{K}'| = 0$, the rank of $\mathbf{Z}_k$ (which lies in the null-space of $\mathbf{H}_k$), must be at least N_E. Thus, the transmitter must use at least N_E dimensions for artificial noise. The remaining dimensions can be used for transmitting the information signal. Let N_{ND} and N_S denote the number of dimensions used for artificial noise and the information signal, respectively. The transmitter first chooses N_{ND}, where $N_E \le N_{ND} \le N_T - 1$. It then determines $N_S = \min(N_R, N_T - N_{ND})$. Then, it designs $\mathbf{Q}_s$ and $\mathbf{Z}_k$, based on $\mathbf{H}_k$. Let the Singular Value Decomposition (SVD) of $\mathbf{H}_k$ be given by $\mathbf{H}_k = \mathbf{U}_k\mathbf{\Lambda}_k\mathbf{V}_k^\dagger$. The transmitter chooses $\mathbf{s}_k = \mathbf{V}_k\mathbf{r}_k$, where $\mathbf{r}_k$ is the information

signal. The receiver processes the received signal ($\mathbf{z}_k$) by multiplying it by $\mathbf{U}_k^\dagger$. Then, the equivalent channel to the receiver becomes $\tilde{\mathbf{z}}_k = \mathbf{\Lambda}_k \mathbf{r}_k + \tilde{\mathbf{n}}_k$, where the components of $\tilde{\mathbf{n}}_k$ are i.i.d. complex Gaussian with mean 0 and variance σ_n^2. To maximize the mutual information between the transmitter and the receiver, the transmitter chooses $\mathbf{Q_r} = \mathbf{E}[\mathbf{r}_k \mathbf{r}_k^\dagger] = diag(\sigma_{r,1}^2, \ldots, \sigma_{r,N_T}^2)$, with $\{\sigma_{r,i}^2\}$ chosen according to the waterfilling solution, corresponding to the N_S largest singular values of $\mathbf{H}_k$, with power constraint of $P_{info} (\leq P_0)$. $\mathbf{Z}_k$ consists of N_{ND} columns of $\mathbf{V}_k$, which do not contribute to the signal space. Then, the minimum guaranteed secrecy capacity is given by,

$$C_{sec,mg}^a = \log|\mathbf{I}\sigma_n^2 + \mathbf{\Lambda}_k \mathbf{Q_r} \mathbf{\Lambda}_k^\dagger| - \log\Big(|\mathbf{K}''|/|\mathbf{K}'|\Big), \quad (25)$$

where $\mathbf{K}'' = \mathbf{K}' + \mathbf{G}_k \mathbf{V}_k \mathbf{Q_r} \mathbf{V}_k^\dagger \mathbf{G}_k^\dagger$. $C_{sec,mg}^a$ is a random variable because it is a function of random channel gains $\mathbf{H}_k$ and $\mathbf{G}_k$. We assume that the total transmit power, given by trace$(\mathbf{E}[\mathbf{x}_k \mathbf{x}_k^\dagger])$ = trace$(\mathbf{V}_k \mathbf{Q_r} \mathbf{V}_k^\dagger) + N_{ND}\ \sigma_v^2$, is constrained to P_0. Now, P_{info} = trace$(\mathbf{V}_k \mathbf{Q_r} \mathbf{V}_k^\dagger)$, N_{ND} and σ_v^2 are chosen to maximize the average $C_{sec,mg}^a$,

$$\overline{C_{sec,mg}^a} \doteq \max_{tr(\mathbf{V}_k \mathbf{Q_r} \mathbf{V}_k^\dagger) + N_{ND}\sigma_v^2 \leq P_0} \mathbf{E}[C_{sec,mg}^a], \quad (26)$$

where the expectation is over the random gains $\mathbf{H}_k$, $\mathbf{G}_k$.

B. Asymptotic Results

Analytical results on (usual) MIMO capacity are available for the asymptotic case of large number of antennas. We derive similar analytical results for MIMO secrecy capacity $\overline{C_{sec,mg}^a}$, for large number of antennas. (We also compare the two through numerical results, later in this section.) The presence of artificial noise significantly complicates the asymptotic analysis. Recall that the SVD of $\mathbf{H}_k = \mathbf{U}_k \mathbf{\Lambda}_k \mathbf{V}_k^\dagger$. The transmitter chooses N_{ND}, and then designs the covariance matrices for artificial noise ($\mathbf{Q_n}$), and ($\mathbf{Q_s}$),

$$\mathbf{Q}_n = \mathbf{V}_k \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{N_{ND}} \sigma_v^2 \end{bmatrix} \mathbf{V}_k^\dagger,\ \mathbf{Q_s} = \mathbf{V}_k \begin{bmatrix} \mathbf{\Sigma_s} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \mathbf{V}_k^\dagger, \quad (27)$$

where $\mathbf{\Sigma_s}$ is a $N_S \times N_S$ diagonal matrix, obtained as the waterfilling solution over the N_S largest singular values of $\mathbf{H}_k$. Let $\mathbf{V}_1$ denote the matrix with the first N_S columns of $\mathbf{V}_k$, and $\mathbf{V}_2$ denote the matrix with last N_{ND} columns of $\mathbf{V}_k$. Then, $\mathbf{Q_s} = \mathbf{V}_1 \mathbf{\Sigma_s} \mathbf{V}_1^\dagger$, and $\mathbf{Z}_k = \mathbf{V}_2$. We define $\tilde{\mathbf{G}}_1 \doteq \mathbf{G}\ \mathbf{V}_1$ and $\tilde{\mathbf{G}}_2 \doteq \mathbf{G}\ \mathbf{V}_2$, which represent the equivalent channels from the information signal $\mathbf{r}_k$ and artificial noise signal $\mathbf{v}_k$ respectively, to the eavesdropper. Note that due to the orthonormality of $[\mathbf{V}_1\ \mathbf{V}_2]$, $\tilde{\mathbf{G}}_1$ and $\tilde{\mathbf{G}}_2$ both have circularly symmetric i.i.d. complex Gaussian distributed elements. Eq. (26) can now be written as,

$$\begin{aligned} \overline{C_{sec,mg}^a} \ = \max_{tr(\mathbf{V}_k \mathbf{Q_r} \mathbf{V}_k^\dagger) + N_{ND}\sigma_v^2 \leq P_0} & \mathbf{E}[\log|\mathbf{I}\sigma_n^2 + \mathbf{\Lambda}_k \mathbf{Q_r} \mathbf{\Lambda}_k^\dagger| \\ & - \log|\tilde{\mathbf{G}}_1 \mathbf{\Sigma_s} \tilde{\mathbf{G}}_1^\dagger + \tilde{\mathbf{G}}_2 \tilde{\mathbf{G}}_2^\dagger \sigma_v^2| + \log|\tilde{\mathbf{G}}_2 \tilde{\mathbf{G}}_2^\dagger \sigma_v^2|]. \quad (28) \end{aligned}$$

Now, the second term can be written as a function of $\mathbf{\Sigma_s}$ as, $S(\mathbf{\Sigma_s}) = \mathbf{E}[\log|\tilde{\mathbf{G}}_1 \mathbf{\Sigma_s} \tilde{\mathbf{G}}_1^\dagger + \tilde{\mathbf{G}}_2 \tilde{\mathbf{G}}_2^\dagger \sigma_v^2|]$. Then,

$$\begin{aligned} S(\mathbf{P}\mathbf{\Sigma_s}\mathbf{P}^\dagger) &= \mathbf{E}[\log|\tilde{\mathbf{G}}_1 \mathbf{P}\mathbf{\Sigma_s}\mathbf{P}^\dagger \tilde{\mathbf{G}}_1^\dagger + \tilde{\mathbf{G}}_2 \tilde{\mathbf{G}}_2^\dagger \sigma_v^2|] \\ &\overset{a}{=} S(\mathbf{\Sigma_s}), \end{aligned} \quad (29)$$

where $\mathbf{P}$ is a permutation matrix, and (a) holds because the elements of $\tilde{\mathbf{G}}_1$ are circularly symmetric i.i.d. complex Gaussian random variables. Let N be the number of such permutation matrices. Then,

$$\begin{aligned} S(\mathbf{\Sigma_s}) &= \frac{1}{N} \sum_{\mathbf{P}} \mathbf{E}[\log|\tilde{\mathbf{G}}_1 \mathbf{P}\mathbf{\Sigma_s}\mathbf{P}^\dagger \tilde{\mathbf{G}}_1^\dagger + \tilde{\mathbf{G}}_2 \tilde{\mathbf{G}}_2^\dagger \sigma_v^2|] \\ &\overset{b}{\leq} \mathbf{E}[\log|\tilde{\mathbf{G}}_1 \frac{1}{N} \sum_{\mathbf{P}} (\mathbf{P}\mathbf{\Sigma_s}\mathbf{P}^\dagger) \tilde{\mathbf{G}}_1^\dagger + \tilde{\mathbf{G}}_2 \tilde{\mathbf{G}}_2^\dagger \sigma_v^2|] \\ &= \mathbf{E}[\log|\tilde{\mathbf{G}}_1 \tilde{\mathbf{G}}_1^\dagger \sigma_p^2 + \tilde{\mathbf{G}}_2 \tilde{\mathbf{G}}_2^\dagger \sigma_v^2|] \\ &\overset{c}{\leq} \underset{\tilde{\mathbf{G}}_2}{\mathbf{E}}[\log|\underset{\tilde{\mathbf{G}}_1}{\mathbf{E}}[\tilde{\mathbf{G}}_1 \tilde{\mathbf{G}}_1^\dagger] \sigma_p^2 + \tilde{\mathbf{G}}_2 \tilde{\mathbf{G}}_2^\dagger \sigma_v^2|] \\ &= \mathbf{E}[\sum_i \log\Big(P_{info} + \lambda_i \sigma_v^2\Big)], \end{aligned} \quad (30)$$

where σ_p^2 is the arithmetic mean of the diagonal elements of $\mathbf{\Sigma_s}$. (b) and (c) hold due to the concavity of log-determinant function. The expectation in the final equation is over $\{\lambda_i\}$, which are the eigenvalues of the Wishart matrix $\tilde{\mathbf{G}}_2 \tilde{\mathbf{G}}_2^\dagger$, which have the following distribution [17], [18].

$$p(\lambda) = \begin{cases} \frac{1}{\pi} \sqrt{\frac{\beta}{\lambda} - \frac{1}{4}\Big(1 + \frac{\beta - 1}{\lambda}\Big)^2}, & \text{if } (\sqrt{\beta}-1)^2 \leq \lambda \leq (\sqrt{\beta}+1)^2 \\ 0, & \text{otherwise,} \end{cases} \quad (31)$$

where $\beta = \max(N_E/(N_T - N_R), (N_T - N_R)/N_E)$. The use of permutation matrix $\mathbf{P}$ and expectation over $\tilde{\mathbf{G}}_1$ resulted in an upper bound on $S(\mathbf{\Sigma_s})$ in terms of only the eigenvalues of $\tilde{\mathbf{G}}_2 \tilde{\mathbf{G}}_2^\dagger$. Therefore,

$$\begin{aligned} \overline{C_{sec,mg}^a} \ \geq \ \overline{C_{sec,mg}^a}(LB) = & \max_{tr(\mathbf{V}_k \mathbf{Q_r} \mathbf{V}_k^\dagger) + N_{ND}\sigma_v^2 \leq P_0} \\ & \mathbf{E}[\log|\mathbf{I}\sigma_n^2 + \mathbf{\Lambda}_k \mathbf{Q_r} \mathbf{\Lambda}_k^\dagger| - \sum_i \log\Big(\frac{P_{info} + \lambda_i \sigma_v^2}{\lambda_i \sigma_v^2}\Big)]. \quad (32) \end{aligned}$$

Now, given the distribution of eigenvalues of a Wishart matrix (31), the lower bound obtained in (32), can be computed numerically. Note that for the first term in (32), we consider the N_S largest eigenvalues, and hence, the distribution given in (31) has to be modified appropriately, as follows. In the limit of large number of antennas, the distribution of eigenvalues can be used as a histogram. Let λ_{th} be such that, $\int_{\lambda_{th}}^{\infty} p(\lambda) d\lambda = N_S/N_R$. Then, the distribution of one of the largest N_S eigenvalues is given by,

$$p_{N_S}(\lambda) = \begin{cases} p(\lambda) \cdot N_R/N_S, & \lambda > \lambda_{th} \\ 0, & \text{otherwise.} \end{cases} \quad (33)$$

Fig. 2 shows the variation of $\overline{C_{sec,mg}^a}(LB)$ (normalized w.r.t. N_R) calculated using (32), as a function of N_R, with $N_T/N_R = 5$ and $N_R/N_E = 1$. Note that the variation of $\overline{C_{sec,mg}^a}(LB)$ with N_R is similar to that of average capacity, in this case. Intuitively, a fixed proportion of the dimensions are used to produce artificial noise, and the number of dimensions used to transmit the signal also increases proportionally. Thus, $\overline{C_{sec,mg}^a}(LB)$ increases with the number of receive antennas.

Fig. 3 shows the variation of $\overline{C_{sec,mg}^a}(LB)$ with N_R, with $N_T = 1000$ and $N_R/N_E = 2$. In this case, the (normalized) average capacity remains fairly constant, whereas the (normalized) $\overline{C_{sec,mg}^a}(LB)$ reduces with increasing N_R, especially when N_R ($= 2N_E$) is large. Recall that at least

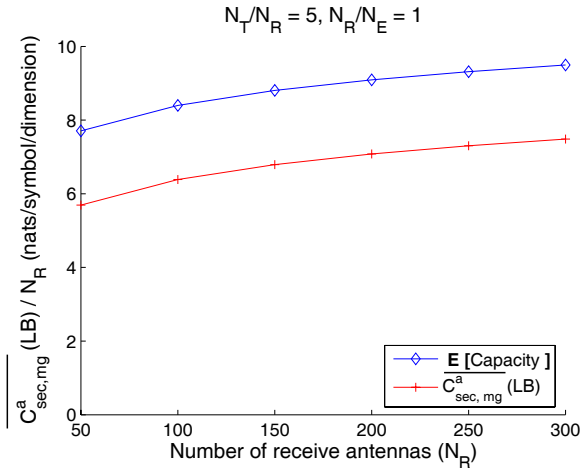


Fig. 2. $\overline{C^a_{sec,mg}}$: variation with N_R (N_T/N_R fixed).

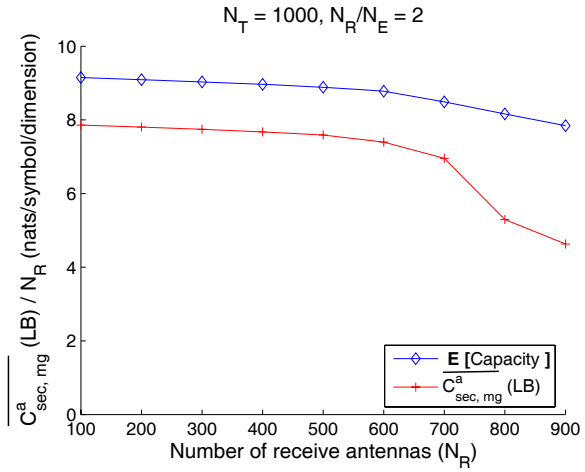


Fig. 3. $\overline{C^a_{sec,mg}}$: variation with N_R (N_T fixed).

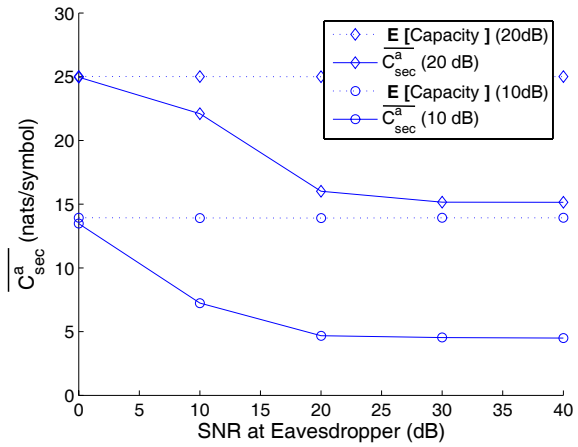


Fig. 4. $\overline{C^a_{sec,mg}}$: variation with distance.

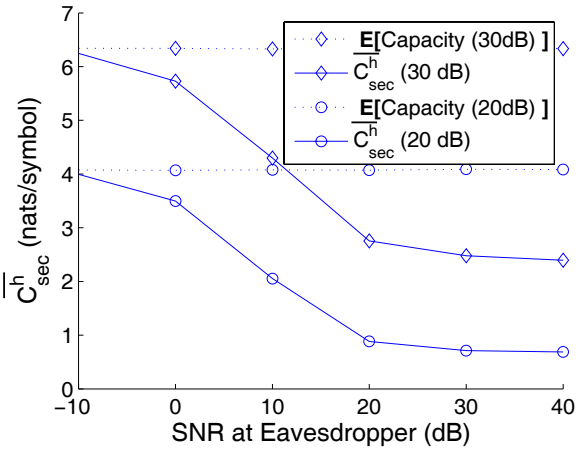


Fig. 5. $\overline{C^h_{sec,mg}}$: variation with distance.

N_E dimensions must be used for artificial noise, to guarantee non zero secrecy capacity. As N_E increases, the number of dimensions available for transmitting the signal reduces, reducing secrecy capacity. Similar trends are observed in the simulation results, obtained for a small number of antennas, presented next.

VI. Simulation Results

We use $C_{sec,mg}$ to refer to both $C^a_{sec,mg}$ and $C^h_{sec,mg}$, and C_{sec} to refer to both C^a_{sec} and C^h_{sec}, when the context is clear. We use similar notation for the average capacities. We compute the average minimum guaranteed secrecy capacity $\overline{C_{sec,mg}}$, which is compared with the average capacity of the transmitter-receiver link (without secrecy requirements), both computed under a power constraint of P_0. Further, given an outage capacity C_{outage}, we compute the outage probability $Pr\{C_{sec,mg} < C_{outage}\}$. $\overline{C_{sec,mg}}$ and outage probability are computed using Monte Carlo simulations, using 10^5 and 10^6 iterations, respectively. In the multiple antenna scenario, it is assumed that the elements of $\mathbf{H}_k$ and $\mathbf{G}_k$ are statistically independent complex Gaussian random variables with $\mathbf{E}[|h_{i,j}|^2] = \mathbf{E}[|g_{i,j}|^2] = 1$. In the multiple relays scenario, the channel gains are assumed to be i.i.d. complex Gaussian with $\mathbf{E}[|\alpha_{XY}|^2] = 1$. When computing outage probabilities, the combination of powers optimum for $\overline{C_{sec,mg}}$ is used.

A. Variation of secrecy capacity (lower bound) with distance

Figures 4 and 5 show the variation of $\overline{C_{sec}}$ with the distance between the transmitter and eavesdropper, for the multiple antenna and multiple relays scenario respectively. The variation in eavesdropper's distance was modeled by varying the per-antenna SNR at the eavesdropper. The distance between the transmitter and receiver is assumed to remain constant. Figures 4 and 5 show that in both the scenarios, when the eavesdropper's distance from the transmitter is much larger than that of the receiver (i.e., when the eavesdropper's SNR is low), $\overline{C_{sec}}$ is close to the average capacity, as expected. As the eavesdropper comes closer to the transmitter, $\overline{C_{sec}}$ reduces. However, instead of becoming arbitrarily small, it ultimately approaches a floor. This is an important result, since, this guarantees a minimum average secrecy capacity, regardless of the eavesdropper's position. This effect is produced by the fact that artificial noise power can be made proportional to the signal power, which is not the case for AWGN.

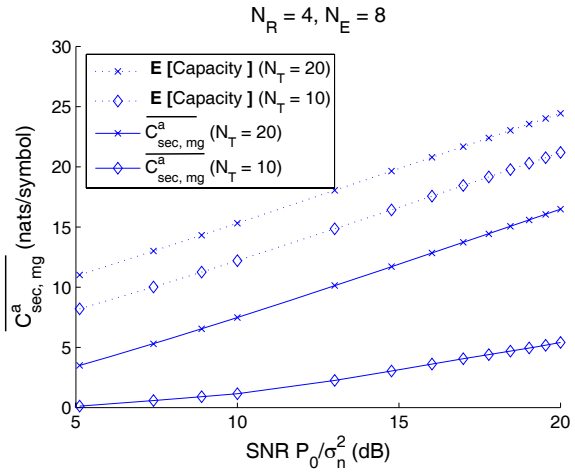


Fig. 6. $\overline{C^a_{sec,mg}}$: variation with P_0.

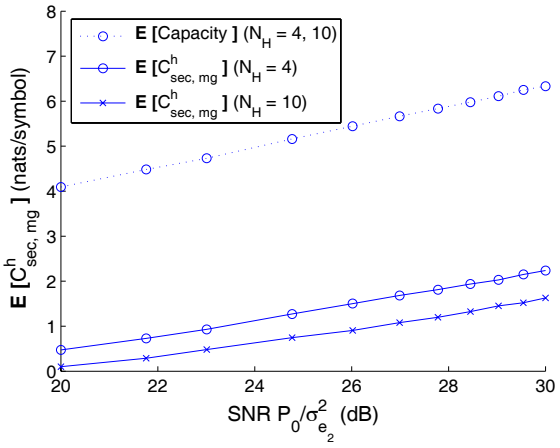


Fig. 7. $\overline{C^h_{sec,mg}}$: variation with P_0.

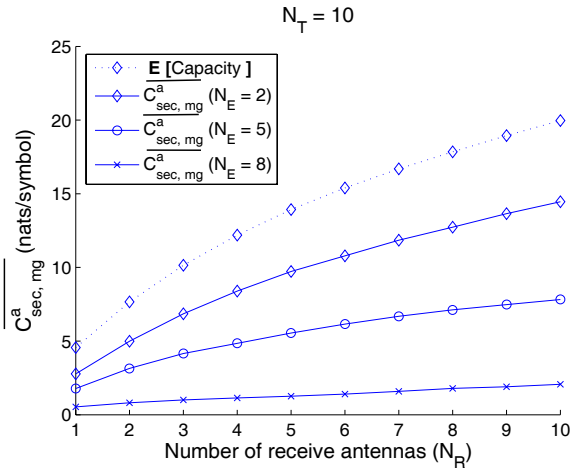


Fig. 8. $\overline{C^a_{sec,mg}}$: variation with N_E and N_R.

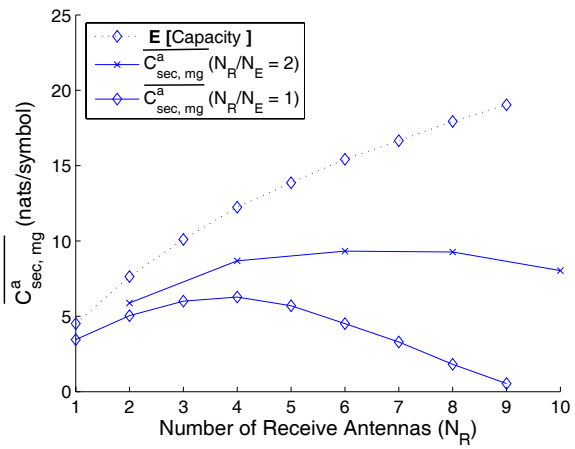


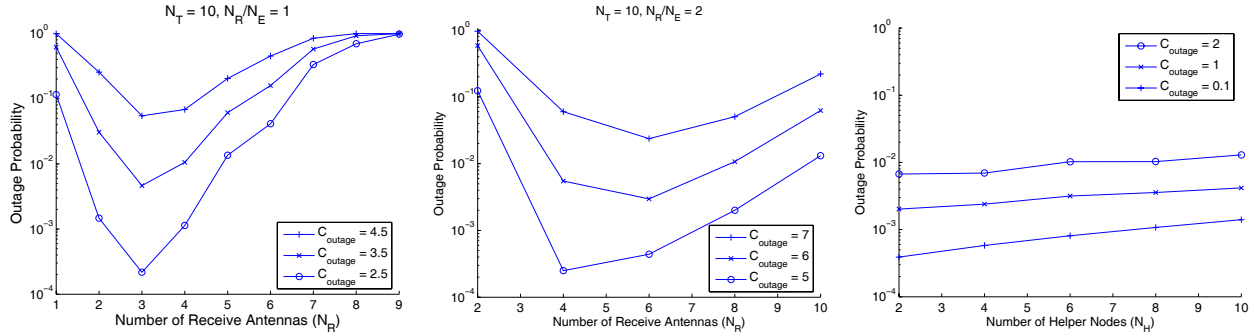
Fig. 9. $\overline{C^a_{sec,mg}}$: fixed ratio of N_E and N_R.

B. Average Minimum Guaranteed Secrecy Capacity

Figures 6 and 7 show the variation of $\overline{C_{sec,mg}}$ with the total available transmit power P_0. In both the scenarios, $\overline{C_{sec,mg}}$ and average capacity have similar behavior. Further, in the case of multiple antenna scenario, $\overline{C_{sec,mg}}$ increases with N_T, just like average capacity. In the multiple relays scenario, on the other hand, $\overline{C_{sec,mg}}$ reduces as N_H increases. In this scenario, the helper nodes only transmit artificial noise. Thus, under a fixed total power constraint, increasing N_H reduces the power used for transmitting the information signal, in contrast to the multiple antenna scenario. Note that if there is more than one colluding eavesdropper, we will need to use more than one relay node to ensure secrecy.

All simulation results related to characterizing the behavior of $\overline{C_{sec,mg}}$ show that, as expected, average capacity is an upper bound on $\overline{C_{sec,mg}}$. The difference between the two represents the loss in capacity because of the secrecy requirement. This loss occurs because of two reasons. Firstly, only part of the power P_{info} is used for the information signal while the rest of the power $(P_0 - P_{info})$ is used for artificial noise. This reduces the mutual information $I(\mathbf{Z};\mathbf{S})$ (or $I(Z;\tilde{R}_B)$) between the information signal and the signal received by the receiver. Secondly, the information that the eavesdropper gains about the information signal $I(\mathbf{Y};\mathbf{S})$ (or $I(Z;\tilde{R}_{E,1},\tilde{R}_{E,2})$) reduces secrecy capacity (lower bound), based on (6), (20) or (23).

Fig. 8 shows that $\overline{C_{sec,mg}}$ increases with N_R, similar to average capacity, when N_T (=10) and N_E are fixed. An increase in N_R increases the average capacity, and also increases $I(\mathbf{Z};\mathbf{S})$, as the number of dimensions available for transmitting the information signal increase. Further, for a fixed N_R, $\overline{C_{sec,mg}}$ reduces with an increase in N_E, as expected. In Fig. 9, the ratio between N_R and N_E was kept constant, and N_T was kept fixed at 10. Two cases are considered, one with $N_R = N_E$ and the other with $N_R = 2N_E$. Specifically, the case $N_R = N_E$ suggests fairness, as both the eavesdropper and the receiver nodes are assumed to have similar capabilities. An interesting phenomenon is observed in both the cases; secrecy capacity (lower bound) attains a maximum at a value of N_R smaller than N_T, rather than at $N_R = N_T$, as would be the case with usual MIMO capacity. Intuitively, as N_E increases, the number of dimensions available for transmission of information signal becomes limited. Further, more power is required to produce artificial noise with the same noise power per dimension. It can be observed that the maximum occurs roughly when $N_R + N_E \approx N_T$, although we were unable to prove this conjecture analytically. These trends



(a) Multiple antenna scenario ($N_R = N_E$) (b) Multiple antenna scenario ($N_R = 2N_E$) (c) Multiple relays scenario

Fig. 10. Outage Probability

show that secrecy capacity does not behave like the usual MIMO capacity (without secrecy requirements). Formally, $\overline{C_{sec,mg}} = 0$ when $N_E = N_R = 0$, or when $N_E = N_R = N_T$, whereas $\overline{C_{sec,mg}}$ is positive for $0 < N_E = N_R < N_T$. Thus, $\overline{C_{sec,mg}}$ cannot be a monotonically increasing function of $\min\{N_R, N_T\}$.

C. Outage Probability

Figures 10(a) and 10(b) show the variation of outage probability with N_R, with the ratio between N_R and N_E kept constant, for a fixed outage capacity. For all of these simulations, the SNR per antenna P_0/σ_n^2 was fixed at 10 dB. Figures 10(a) and 10(b) show the same interesting phenomenon as described earlier for $\overline{C_{sec,mg}}$; the outage probability is minimized at a value of N_R less than N_T. When N_R is small, the outage probability is limited mainly by the diversity available on the transmitter-receiver link, rather than by the secrecy requirement, since almost all the parallel channels of the eavesdropper are interference limited, with a high probability. As N_R increases, the number of parallel channels of the receiver increase resulting in high diversity, and hence, the outage probability reduces. However, for large N_R (and hence, large N_E), at most $N_T - N_E$ dimensions are available for transmission of information signal, again reducing the available diversity, and hence, increasing the outage probability. Fig. 10(c) shows the variation of outage probability with N_H, for the multiple relays scenario. As opposed to the multiple antenna scenario, the outage probabilities (for a fixed outage capacity) are fairly constant, as N_H is varied. The results suggest that as N_H increases, the limitation on the power available for information signal, is balanced out by the increase in the number of dimensions available for artificial noise.

VII. Conclusion

This paper considered the problem of secret communication in a fading environment, in presence of passive eavesdroppers. The eavesdroppers were assumed to know the channel gains of all the channels (thus, secrecy was not dependent on the secrecy of channel gains) and they were allowed to collude. The paper showed how secrecy can be achieved, by adding artificially generated noise to the information signal. It was shown that multiple antennas can be used to generate artificial noise, such that only the eavesdropper's channel is degraded. Further, even if the transmitter has only a single antenna, artificial noise can still be produced, with the help of relays. A necessary condition for using the method of artificial noise is that the total number of transmit antennas (including relays) must exceed the number of eavesdropper antennas. It was shown that MIMO secrecy capacity behaves differently from non-secret MIMO capacity, so that MIMO design is different under the secrecy requirement. It was shown that a non-zero rate for secret communication can be guaranteed, regardless of eavesdropper's position, i.e., even if the eavesdropper is much closer to the transmitter, compared to receiver. Further, it was shown that low outage probabilities of secrecy capacity can be achieved. Analytical results were presented for the multiple antenna scenario, in the regime of large number of antennas.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656-715, 1949.
[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, pp. 339-348, May 1978.
[3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, 1975.
[4] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 733-742, May 1993.
[5] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. VTC Fall 2005*, vol. 3, pp. 1906-1910, Sept. 2005.
[6] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *Proc. MILCOM*, vol. 3, pp. 1501-1506, Nov. 2005.
[7] G. J. Foschini and M. J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," *Wireless Personal Commun.: Kluwer Academic Press*, no. 6, pp. 311-335, 1998.
[8] X. Li, M. Chen, and E. P. Ratazzi "Space-time transmissions for wireless secret-key agreement with information-theoretic secrecy," in *Proc. IEEE SPAWC 2005*, pp. 811-815, June 2005.
[9] H. Koorapaty, A. A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Trans. Wireless Commun.*, pp. 52-55, July 2003.
[10] A. E. Hero, "Secure space-time communication," *IEEE Trans. Inform. Theory*, pp. 3235-3249, Dec. 2003.
[11] U. M. Maurer and S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information," *IEEE Trans. Inform. Theory*, vol. 45, no. 2, pp. 499-514, Mar. 1999.
[12] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. CISS '07*, pp. 905-910, Mar. 2007, Baltimore, MD.
[13] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," to appear in *Proc. ISIT 2006*, July 2006.
[14] D. Chizhik, J. Ling, P. W. Wolniansky, R. A. Valenzuela, N. E. Costa, and K. Huber, "Multiple-input-multiple-output measurements and modeling in manhattan," *IEEE J. Select. Areas Commun.*, vol. 21, no. 3, pp. 321-331, Apr. 2003.

[15] E. Telatar, "Capacity of multi-antenna Gaussian channels," *Eur. Trans. Telecomm. ETT*, vol. 10, no. 6, pp. 585-596, Nov. 1999.
[16] G. J. Foschini, D. Chizhik, M. J. Gans, C. Papadias, and R. A. Valenzuela, "Analysis and performance of some basic spacetime architectures," *IEEE J. Select. Areas Commun.*, special issue on MIMO systems, part I, vol. 21, pp. 303-320, Apr. 2003.
[17] B. M. Hochwald, T. L. Marzetta, and V. Tarokh, "Multiple-antenna channel hardening and its implications for rate feedback and scheduling," *IEEE Trans. Inform. Theory*, vol. 50, no. 9, pp. 1893-1909, Sept. 2004.
[18] J. W. Silverstein and Z. D. Bai, "On the empirical distribution of eigenvalues of a class of large dimensional random matrices," *J. Mult. Anal.*, vol. 54, pp. 175-192, 1995.
[19] U. Maurer and S. Wolf, "Information-theoretic key agreement: from weak to strong secrecy for free," *Lecture Notes in Computer Science*, vol. 1807, pp. 352–368, Springer-Verlag, 2000.
[20] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: efficient protocols and outage behavior," *IEEE Trans. Inform. Theory*, vol. 50, no. 12, pp. 3062-3080, Dec. 2004.
[21] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," submitted to *IEEE Trans. Inform. Theory*, Nov. 2006.

Satashu Goel received the B.Tech. degree in Electrical Engineering from the Indian Institute of Technology, Delhi, in 2003. Currently, he is a Ph.D. student in the Electrical and Computer Engineering Department at Carnegie Mellon University, Pittsburgh. His research interests include cross-layer optimization, information theory, coding for communications systems, and physical layer security.

Rohit Negi received the B.Tech. degree in electrical engineering from the Indian Institute of Technology, Bombay, in 1995. He received the M.S. and Ph.D. degrees from Stanford University, CA, in 1996 and 2000, respectively, both in electrical engineering. Since 2000, he has been with the Electrical and Computer Engineering Department, Carnegie Mellon University, Pittsburgh, PA, where he is an Associate Professor. His research interests include signal processing, coding for communications systems, information theory, networking, cross-layer optimization, and sensor networks. Dr. Negi received the President of India Gold Medal in 1995.